Algebraic Number Theor

René Schoof

Dipartimento di Matematica
Università degli Studi di Trento
I-38050 Povo (Trento) ITALY
Email: schoof@itnvax.cineca.it

Abstract. Note provvisorie per il corso *Teoria algebrica dei numeri* , Trento 1991.

1. Introduzione.

Un aspetto importante della teoria dei numeri è lo studio delle equazioni “Diofantee”. Sono equazioni, spesso polinomiali, a coefficienti interi di cui si cercano soluzioni intere o razionali. Anche se i problemi originali riguardano solo numeri in $\mathbf{Z}$ o $\mathbf{Q}$, vedremo che spesso si affrontano introducendo una classe più generale di numeri, quella dei numeri algebrici su $\mathbf{Q}$. Lo studio degli anelli e dei corpi che contengono numeri algebrici su $\mathbf{Q}$ fa parte della *teoria algebrica dei numeri.* Se ciò è per vari aspetti comodo e naturale, d'altra parte comporta anche nuove difficoltà. In questa introduzione ne diamo alcuni esempi seguendo la storia del soggetto.

Diofanto di Alessandria visse in Egitto nel terzo secolo d.c. e si interessò a vari problemi riguardanti i numeri razionali. Dei 13 “libri” che scrisse su questi argomenti, oggi se ne conoscono solo 6. I suoi libri erano tradotti e conosciuti in Europa sin dal medioevo [21]. L'equazione pitagorea $X^2+Y^2=Z^2$, ben conosciuta anche assai prima di Diofanto, rappresenta un esempio significativo del tipo di problemi trattati nei suoi libri. Tutti sanno che soluzioni $X, Y, Z \in \mathbf{Z}$ di tale equazione sono ad esempio $3, 4, 5$ oppure $5, 12, 13$. Una caratterizzazione completa delle soluzioni è data dal teorema seguente.

Teorema (1.1). *Tutte le soluzioni* $X, Y, Z \in \mathbf{Z}_{>0}$ *con* $\operatorname{mcd}(X, Y, Z) = 1$ *della equazione*

$$X^2+Y^2=Z^2$$

sono date da

$$\begin{aligned} X &= a^2-b^2, \\ Y &= 2ab, \\ Z &= a^2+b^2. \end{aligned}$$

(o con X *e* Y *scambiati) dove* $a, b \in \mathbf{Z}$ *soddisfano* $a > b > 0$ e $\operatorname{mcd}(a, b) = 1$.

Dimostrazione. Si verifica facilmente che $X = a^2-b^2$, $Y = 2ab$ e $Z = a^2+b^2$ sono effettivamente soluzioni dell'equazione $X^2+Y^2=Z^2$. Dobbiamo dimostrare ora che ogni soluzione è di questo tipo. Siano dunque $X, Y, Z \in \mathbf{Z}_{>0}$ con $\operatorname{mcd}(X, Y, Z) = 1$ e $X^2+Y^2=Z^2$. Siccome $\operatorname{mcd}(X, Y, Z) = 1$ almeno uno di X e Y è dispari. Se tutti e due fossero dispari, avremmo

$$Z^2 = X^2+Y^2 \equiv 1+1 = 2 \pmod 4,$$

mentre il quadrato Z^2 può solo essere congruente a 1 o 0 modulo 4. Dunque, precisamente uno fra X e Y è dispari e, a meno di scambiare X e Y, possiamo assumere X dispari.

Scriviamo

$$Y^2 = Z^2 - X^2,$$

$$\left(\frac{Y}{2}\right)^2 = \frac{Z-X}{2}\frac{Z+X}{2}.$$

Osserviamo innanzitutto che $(Z-X)/2$ e $(Z+X)/2$ sono interi perché Z e X sono entrambi dispari. Un divisore comune di $(Z-X)/2$ e $(Z+X)/2$ dividerebbe la loro somma uguale a Z, la loro differenza uguale a X ed anche Y, dato da $Z^2 - X^2 = Y^2$. Dal fatto che $\mathrm{mcd}(X, Y, Z) = 1$ segue dunque che

$$\mathrm{mcd}\left(\frac{Z-X}{2}, \frac{Z+X}{2}\right) = 1.$$

Adesso utilizziamo il seguente principio:

Se il prodotto di due interi coprimi è una potenza n-sima, allora gli interi stessi sono, a meno del segno, potenze n-esime. (P)

Questo fatto si verifica facilmente scrivendo gli interi come prodotto di numeri primi e sfruttando l'unicità di tale decomposizione

Poiché $(Z+X)$ e $(Z-X)$ sono positivi, esistono due interi a e b tali che

$$\frac{Z+X}{2} = a^2,$$
$$\frac{Z-X}{2} = b^2.$$

Chiaramente si possono prendere $a, b > 0$ e siccome $\mathrm{mcd}(X, Y, Z) = 1$ vale anche $\mathrm{mcd}(a, b) = 1$. Sommando e sottraendo le equazioni otteniamo rispettivamente $Z = a^2 + b^2$ e $X = a^2 - b^2$ (dunque $a > b$) e successivamente $Y = 2ab$. Questo conclude la dimostrazione.

Pierre de Fermat (1601-1665) fu magistrato a Tolosa in Francia e matematico famoso che contribuì al calcolo differenziale, alla teoria della probabilità e alla teoria dei numeri [25]. Fermat fece un passo in più rispetto a Diofanto. I problemi che considerava erano, in un senso che potrebbe essere precisato (vedi Weil [83, Ch.II]), effettivamente più difficili di quelli considerati da Diofanto. Spesso non pubblicava le sue dimostrazioni, ma si sa che ebbe, ad esempio, metodi per risolvere l'equazione $X^2 - dY^2 = 1$ per $d \in \mathbf{Z}_{>0}$. Il suo "metodo" piu famoso è il metodo della discesa infinita. Con questo metodo, per dimostrare ad esempio che una certa equazione non ha soluzioni intere, si dimostra che, a partire da una ipotetica soluzione, se ne può sempre costruire una piu "piccola". Siccome non esistono interi positivi arbitrariamente piccoli questo fatto implica che non esistono soluzioni. Questa idea è anche oggigiorno, pur in un linguaggio diverso, uno dei metodi piu efficaci per risolvere le equazioni Diofantee [53 §9, 54 p.148]. Il prossimo teorema è un esempio di utilizzazione del metodo della discesa infinita.

Teorema (1.2). *(P. de Fermat) Le uniche soluzioni intere della equazione*

$$X^4 + Y^4 = Z^2$$

sono quelle banali, ossia quelle con $XYZ = 0$.

Dimostrazione. Supponiamo che esista una soluzione non banale. Sia X, Y, Z una tale soluzione con $|Z| > 0$ *minimale.* Allora $\mathrm{mcd}(X, Y, Z) = 1$ e possiamo anche assumere $X, Y, Z > 0$. Mediante la riduzione modulo 4, si può vedere che precisamente uno fra X e Y deve essere dispari. Diciamo che X è dispari. Per il Teorema 1.1 esistono interi $a > b > 0$ con $\mathrm{mcd}(a, b) = 1$ tali che

$$\begin{aligned} X^2 &= a^2 - b^2, \\ Y^2 &= 2ab, \\ Z &= a^2 + b^2. \end{aligned}$$

Studiamo la prima equazione $X^2 + b^2 = a^2$. Siccome $\mathrm{mcd}(a, b, X) = 1$, possiamo applicare un' altra volta il Teorema 1.1, ottenendo

$$\begin{aligned} X &= c^2 - d^2, \\ b &= 2cd, \\ a &= c^2 + d^2, \end{aligned}$$

per certi interi $c > d > 0$. Sostituiamo queste espressioni di a e b nella equazione $Y^2 = 2ab$ sopra:

$$\begin{aligned} Y^2 &= 2ab = 2(2cd)(c^2 + d^2), \\ \left(\frac{Y}{2}\right)^2 &= c \cdot d \cdot (c^2 + d^2). \end{aligned}$$

Troviamo un prodotto di tre fattori coprimi che è un quadrato. Per il principio (P) esistono interi U, V, W tali che

$$\begin{aligned} c &= U^2, \\ d &= V^2, \\ c^2 + d^2 &= W^2. \end{aligned}$$

È facile verificare che $\mathrm{mcd}(U, V, W) = 1$ e che

$$U^4 + V^4 = W^2.$$

Abbiamo così trovato una nuova soluzione della nostra equazione! Possiamo vedere infine che $W \neq 0$ e verificare che $|W| < W^2 = c^2 + d^2 = a \leq a^2 \leq |Z|$, contro l'ipotesi di minimalità di Z. Dunque non ci sono soluzioni non-banali e la dimostrazione è completa.

Fermat fece tante affermazioni senza darne dimostrazione. Spesso possiamo immaginare che ne avesse davvero una dimostrazione, ma qualche volta non è così chiaro. Affermò, per esempio, che è possibile scrivere un numero primo $p \neq 2$ come somma di due quadrati se e soltanto se $p \equiv 1 \pmod 4$. Tale fatto fu dimostrato quasi 100 anni dopo, nel 1754, da Eulero. Fermat affermò anche che ogni intero positivo è somma di 4 quadrati. Questo "non inelegans theorema" (secondo Eulero) fu dimostrato da Lagrange solo nel 1770. Però Fermat pensò anche che tutti i numeri

$$F_k = 2^{2^k} + 1$$

fossero numeri primi. È vero che $F_0, \ldots, F_4$ sono primi, ma Eulero trovò nel 1732 che il numero primo 641 divide $F_5 = 4\,294\,967\,297$. Oggigiorno si sa che almeno per $5 \leq k \leq 21$ i numeri F_i non sono primi [50]. Non si sa se F_{22}, un numero con più di 1 millione di ciffre decimali, sia primo o meno. Dunque, Fermat non ebbe sempre ragione ...

La più famosa affermazione di Fermat è che per tutti gli interi $n \geq 3$ l'equazione

$$X^n + Y^n = Z^n$$

ha solo soluzioni intere banali i.e. soluzioni X, Y, Z con $XYZ = 0$. Sulla sua copia del libro di Diofanto, ove spesso annotò osservazioni e generalizzazioni, scrisse di aver trovato una dimostrazione mirabile di questo fatto, ma che, purtoppo, il margine era troppo stretto per contenerla:

> *Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos*
> *et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem*
> *nomines fas est dividere cuius rei demonstrationem mirabilem sane detexi.*
> *Hanc marginis exiguitas non caperet.*

Prima o poi tutti i quesiti di Fermat sono stati risolti, eccetto questo, l'ultimo. Neppure oggi si sa dimostrare completamente questa affermazione.

È una semplice conseguenza del Teorema 1.2 che l'equazione $X^4+Y^4 = Z^4$ ha soltanto soluzioni banali. Dunque l'ultimo teorema di Fermat è vero per $n = 4$. Per $n = 3$ venne dimostrato da Eulero nel 1743, mentre Lagrange, a 75 anni, lo dimostrò per $n = 5$ nel 1789. Il teorema è vero anche per $n = 6$. Segue dal fatto che $6 = 3 \cdot 2$ e che il teorema vale per $n = 3$. In generale vale il seguente fatto.

Proposizione (1.3). *L'ultimo teorema di Fermat è vero se e soltanto se per ogni primo $p \neq 2$ l'equazione*

$$X^p + Y^p = Z^p$$

ha soltanto soluzioni intere banali i.e. soluzioni X, Y, Z con $XYZ = 0$.

Dimostrazione. Poiché la condizione è chiaramente necessaria, basta dimostrarne la sufficienza. Sia n un intero maggiore di 2. Dimostreremo che non ci sono soluzioni non banali della equazione $X^n + Y^n = Z^n$. Distinguiamo due casi. Supponiamo prima che n sia divisibile per un primo $p > 2$. Se x, y, z è una soluzione, possiamo scrivere

$$(x^{n/p})^p + (y^{n/p})^p = (z^{n/p})^p,$$

da cui risulta che $x^{n/p}, y^{n/p}, z^{n/p}$ è una soluzione di $X^p + Y^p = Z^p$. Ma allora deve essere banale i.e. $(xyz)^{n/p} = 0$, da cui $xyz = 0$. Supponiamo ora che n non sia divisibile per un primo $p > 2$. Allora n è una poten m b oa po b c b b S M b b cu b uzi o b M b e v o ssiamo S b re

$z P^n_i \geq_i {}^n {}^n \geq\geq_i {}^n \geq_i {}^n_i {}^n_i {}^n \geq N$

Proposizione (1.4). *L'anello* $\mathbf{Z}[i]$ *degli interi di Gauß è un dominio a fattorizzazione unica. Il gruppo delle unità* $\mathbf{Z}[i]^*$ *è formato dagli elementi* $\{1, -1, i, -i\}$.

Dimostrazione. Per l'Eserc.1.B l'anello $\mathbf{Z}[i]$ è un annello Euclideo rispetto alla norma $\mathrm{N} : \mathbf{Z}[i] \longrightarrow \mathbf{Z}$, data da $\mathrm{N}(a + bi) = a^2 + b^2$. In particolare, è un dominio principale. Siccome ogni dominio principale è un dominio a fattorizzazione unica, la prima parte della proposizione è dimostrata.

La seconda affermazione segue dall' Eserc.1.A(iv).

Teorema (1.5). *L' unica soluzione* $X, Y \in \mathbf{Z}$ *della equazione*

$$X^3 = Y^2 + 1$$

è data da $X = 1$ *e* $Y = 0$.

Dimostrazione. Sia X, Y una soluzione. Se X fosse pari, avremmo $Y^2 = X^3 - 1 \equiv -1 \pmod 4$ il che è impossibile. Allora X è dispari. Nell'anello $\mathbf{Z}[i]$, scriviamo

$$X^3 = (Y + i)(Y - i).$$

Un divisore comune di $(Y + i)$ e $(Y - i)$ in $\mathbf{Z}[i]$ dividerebbe la loro differenza uguale a $2i$ e dunque 2. Tale divisore dividerebbe anche X^3, che è della forma $2k + 1$ per un intero k. Di consequenza, dividerebbe anche 1. Cosı̀ il massimo comun divisore di $(Y + i)$ e $(Y - i)$ è 1. Per la Prop.1.4, l'anello $\mathbf{Z}[i]$ è un dominio a fattorizzazione unica e possiamo dunque applicare il "principio" (P): poiché sono coprimi e il loro prodotto è un cubo, $(Y + i)$ e $(Y - i)$ sono il prodotto di un'unità per un cubo. Per la Prop.1.4 il gruppo delle unità di $\mathbf{Z}[i]$ è uguale a $\{\pm 1, \pm i\}$. Dunque il suo ordine è 4 e ogni unità risulta quindi un cubo.

Concludiamo allora che esiste $a + bi \in \mathbf{Z}[i]$ tale che

$$Y + i = (a + bi)^3.$$

Non abbiamo bisogno di una formula analoga per $(Y - i)$. Per la parte reale e la parte immaginaria di $(Y + i)$ troviamo rispettivamente:

$$Y = a^3 - 3ab^2,$$
$$1 = 3a^2b - b^3.$$

La seconda relazione ci dà $b(3a^2 - b^2) = 1$. Dunque $b = 1$ e $3a^2 - 1 = 1$ oppure $b = -1$ e $3a^2 - 1 = -1$. Solo la seconda possibilità, $b = -1$ e $a = 0$, ci fornisce una soluzione dell'equazione $X^3 = Y^2 + 1$ ed essa è $Y = 0$, $X = 1$ come richiesto.

Cerchiamo adesso di risolvere un'equazione del tutto simile:

$$X^3 = Y^2 + 61.$$

Se X fosse pari avremmo $Y^2 = X^3 - 61 \equiv -1 \pmod 4$ il che è impossibile. Se X fosse divisibile per il primo 61, allora lo sarebbe anche Y. Ma questo è impossibile perché X^3 sarebbe divisibile per 61^3 mentre $Y^2 + 61$ soltanto per 61. Dunque X non risulta divisibile nè per 2 nè per 61.

Nell' anello $\mathbf{Z}[\sqrt{-61}]$ scriviamo

$$X^3 = (Y + \sqrt{-61})(Y - \sqrt{-61}).$$

Un divisore comune $\delta \in \mathbf{Z}[\sqrt{-61}]$ di $(Y + \sqrt{-61})$ e $(Y - \sqrt{-61})$ dividerebbe $2\sqrt{-61}$ e dunque anche $2 \cdot 61$. Il divisore δ dividerebbe poi X^3 perché $Y^2 + 61 = X^3$. Siccome 2 e 61 non dividono X, si ha che $\mathrm{mcd}(X^3, 2\cdot 61) = 1$. Esistono dunque $a, b \in \mathbf{Z}$ tali che $X^3a + 2\cdot 61b = 1$. Il divisore δ dividerebbe allora 1. Segue allora che $\mathrm{mcd}(Y + \sqrt{-61}, Y - \sqrt{-61}) = 1$.

Adesso applichiamo il "principio" (P) e troviamo che $Y + \sqrt{-61}$ è un unità per un cubo. Le unità di $\mathbf{Z}[\sqrt{-61}]$ sono 1 e -1 (Eserc.1.C). In particolare, sono esse stesse dei cubi. Esiste allora $a + b\sqrt{-61} \in \mathbf{Z}[\sqrt{-61}]$ tale che

$$Y + \sqrt{-61} = (a + b\sqrt{-61})^3.$$

Segue che

$$\begin{aligned} Y &= a^3 - 3\cdot 61ab^2, \\ 1 &= 3a^2b - 61b^3. \end{aligned}$$

È facile vedere che la seconda equazione $b(3a^2 - 61b^2) = 1$ non ha soluzioni $a, b \in \mathbf{Z}$. Lo stesso si vorrebbe concludere per l'equazione $X^3 = Y^2 + 61$. Invece non è così, come dimostra l'ugualianza

$$5^3 = 8^2 + 61$$

Che cosa è successo? Il problema è che in questo caso il principio (P) non può essere utilizzato perché l'anello $\mathbf{Z}[\sqrt{-61}]$ non è a fattorizzazione unica. Eccone un esempio esplicito:

$$\begin{aligned} 62 &= 2\cdot 31 \\ &= (1 + \sqrt{-61})(1 - \sqrt{-61}) \end{aligned}$$

sono due fattorizzazioni di 62 nell' anello $\mathbf{Z}[\sqrt{-61}]$. Verifichiamo che i vari fattori sono elementi irriducibili in $\mathbf{Z}[\sqrt{-61}]$. Utilizzando le proprietà della norma $N : \mathbf{Z}[\sqrt{-61}] \longrightarrow \mathbf{Z}$ dell' Eserc.1.C si vede che $N(2) = 2^2$, $N(31) = 31^2$ e $N(1 \pm \sqrt{-61}) = 2\cdot 31$. Se gli elementi $2, 31$ e $1 \pm \sqrt{-61}$ non fossero irriducibili, conterrebbero fattori non banali $a + b\sqrt{-61}$ con norma uguale a 2 o 31. Significherebbe che le equazioni Diofantee $a^2 + 61b^2 = 2$ oppure $a^2 + 61b^2 = 31$ avrebbero soluzioni $a, b \in \mathbf{Z}$. Si verifica facilmente invece che tali soluzioni non esistono.

Kummer trovò che per $p = 23$ la proprietà della fattorizzazione unica non vale per l'anello $\mathbf{Z}[\zeta_p]$. Oggigiorno si sa dimostrare [80,Chpt.11] che tale proprietà vale in $\mathbf{Z}[\zeta_p]$ solo per i primi $p \leq 19$. Per risolvere questo tipo di problemi, nei suoi studi sull' ultimo teorema di Fermat, Kummer introdusse nel 1847 certi elementi irriducibili "virtuali". Li chiamò "*elementi ideali*" inventando più o meno la nozione di ideale. Come vedremo, nella terminologia moderna, i suoi elementi irriducibili "virtuali" sono ideali primi che non sono principali. Mancano cioè degli elementi irriducibili che li generano.

Utilizzando la sua teoria degli ideali, Kummer riuscì a dimostrare l'ultimo teorema di Fermat per una classe di numeri primi assai grande. Esiste una congettura che afferma che tale classe contiene il 61% dei numeri primi [80, Ch.I]. Il risultato principale di Kummer è stato il seguente teorema.

Teorema (1.6). *(E.E. Kummer 1847) Sia $p \neq 2$ un primo. Se p non divide i numeri di Bernoulli $B_2, B_4, \ldots, B_{p-3}$, l'equazione*

$$X^p + Y^p = Z^p$$

ha soltanto soluzioni intere con $XYZ = 0$.

I numeri di Bernoulli B_k sono definiti dalla serie

$$\frac{X}{e^X - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} X^k.$$

Intervengono anche come valori della funzione ζ di Riemann sui numeri pari $k \geq 2$:

$$\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k} = -\frac{(2\pi i)^k}{2 \cdot k!} B_k.$$

I numeri di Bernoulli sono numeri razionali e siccome $h(X) = X/(e^X - 1) + X/2 = \frac{X}{2}\coth(\frac{X}{2})$ è una funzione pari, tutti i B_k con $k \geq 3$ dispari, sono uguali a zero. Eccone alcuni

$$B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30},$$
$$B_{10} = \frac{5}{66}, \quad B_{12} = -\frac{691}{2730}, \quad B_{14} = \frac{7}{6}, \quad B_{16} = -\frac{3617}{510}, \ldots$$

Vedi [1,80] per numeri di Bernoulli successivi. I numeri primi che dividono il denominatore di B_k sono minori o uguali a $k+1$. Si dice allora che un numero primo p divide un numero di Bernoulli B_k, con $k > p-1$ se divide il suo numeratore. Si vede che il teorema di Kummer non vale per i primi dati da 691 e 3617. I soli numeri primi minori di 100, per i quali non vale, sono 37, 59 e 67. Daremo in sezione 13 una dimostrazione completa del Teorema 1.6.

A tutt'oggi nel 1991, utilizzando il Teorema 1.6 di Kummer e certe sue varianti [79], l'ultimo teorema di Fermat è stato dimostrato per tutti i primi $p < 150\,000$ (Vede [73,79]). Nel 1983 il matematico tedesco G. Faltings ha dimostrato un teorema assai profondo e generale di geometria algebrica aritmetica [24,6,7]. Tale risultato implica fra l'altro che per ogni p l'equazione $(X/Z)^p + (Y/Z)^p = 1$ ha soltanto un numero finito di soluzioni razionali X/Z e Y/Z. Sfortunatamente però la sua dimostrazione non è "effettiva": non dà una stima nè della quantità nè della grandezza delle possibili soluzioni. Nel 1988 l'americano K. Ribet [61] ha dimostrato che l'ultimo teorema di Fermat è conseguenza di certe congetture sull' aritmetica delle curve ellittiche su $\mathbf{Q}$: con una soluzione non-banale di $X^p + Y^p = Z^p$ si può costruire una curva ellittica con proprietà molto strane. Secondo le cosidette congetture "standard", che a buona ragione sono ritenute vere dai matematici, questa curva non può esistere.

L'ultimo teorema di Fermat, in sè forse un problema naïve, è stato molto importante per lo sviluppo della teoria dei numeri e dell' algebra moderna. Matematici come R. Dedekind (1831–1916), D. Hilbert (1862–1943) e E. Noether (1882–1955), generalizzando le idee e i risultati di Kummer nella teoria dei numeri, hanno creato un'intera parte dell'algebra [10,18,24].

Questo corso consiste di due parti. Nella prima parte trattiamo la teoria fondamentale: introduciamo i corpi di numeri ed i loro anelli degli interi. Gli anelli che abbiamo visto sopra ne sono degli esempi. Anche se gli anelli $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{-61}]$ e gli anelli $\mathbf{Z}[\zeta_p]$ sembrano essere molto diversi fra loro, sono tutti esempi di una classe importante di anelli , i cosidetti *anelli di Dedekind.* Diamo una trattazione unificata di questi anelli ed introduciamo i due importanti invarianti ad essi associati: il gruppo delle unità e il gruppo di classi. In section 7 we prove the finiteness of the class group of the ring of integers of a number field and Dirichlet's Unit Theorem. Testi consigliati per questi argomenti sono anche il libro di Stewart [72], quello di Ono [58] e quello di Samuel [65]. In section 8 we give three examples, illustrating the theory. Finally we calculate the residue of the Dedekind ζ-function $\zeta(s)$ at $s = 1$. The answer will involve all the arithmetical invariants that have been discussed in the previous sections.

In the second part we will assume that the reader knows the basic results of Galois Theory. In section 10 we discuss decomposition groups and inertia groups associated to prime ideals. In the next sections we introduce Dirichlet L-series. We use them to prove Dirichlet's famous theorem on primes in arithmetic progressions. In section 12 we focus our attention on the field of the p-th roots of unity, where p is an odd prime. Our results will be used in the final section, where we give a proof of Theorem 1.6, che implica l'ultimo teorema di Fermat in molti casi. Per questi argomenti si vedano, ad esempio, il libro di L.C. Washington [80] e l'approcio storico di H.M. Edwards [23].

During the preparation of these notes, Lenstra's Amsterdam syllabus [49] was very useful. Some of the exercises are his. The second part owes much to the book of Borevič and Shafarevič [8]. For the algebra that we will use see Lang's book [L41], or the Bourbaki volumes [9]. Sometimes we will use well known facts from elementary number theory. These can be found in the book by Hardy and Wright [29]. Per la storia della teoria dei numeri si veda l'articolo di H.W. Lenstra [34] o il libro di André Weil [83], nel quale si discute la storia fino al 1800. Per la storia della matematica si consiglia *"Elements d'histoire des Mathématiques"* di N. Bourbaki [10].

Nel corso di queste note adotteremo le seguenti convenzioni: ogni anello possiede un'identità 1; gli omomorfismi f di anelli soddisfanno sempre $f(1) = 1$; se R è un anello ed $\alpha \in R$ allora (α) oppure αR indica l'ideale principale genarato da α; il gruppo delle unità di R è indicato da R^*; i corpi sono sempre corpi commutativi. Gli esercizi con l'asterisco sono più difficili o richiedono maggiori conoscienze.

(1.A) Sia $\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$ l'anello degli interi di Gauss. Sia $\mathrm{N} : \mathbf{Z}[i] \longrightarrow \mathbf{Z}$ la norma definita da $\mathrm{N}(a + bi) = a^2 + b^2$. Dimostrare che
(i) $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ per $\alpha, \beta \in \mathbf{Z}[i]$.
(ii) se α divide β allora $\mathrm{N}(\alpha)$ divide $\mathrm{N}(\beta)$.
(iii) α è una unità in $\mathbf{Z}[i]$ se e soltanto se $\mathrm{N}(\alpha) = 1$.
(iv) il gruppo delle unità di $\mathbf{Z}[i]$ è uguale a $\{\pm 1, \pm i\}$.

(1.B) Dimostrare che l'anello $\mathbf{Z}[i]$ è Euclideo rispetto alla norma $\mathrm{N}(a + bi) = a^2 + b^2$.

(1.C) Sia $\mathbf{Z}[\sqrt{-61}] = \mathbf{Z}[X]/(X^2+61)$. Sia $\mathrm{N} : \mathbf{Z}[\sqrt{-61}] \longrightarrow \mathbf{Z}$ la norma definita da $\mathrm{N}(a+b\sqrt{-61}) = a^2+61b^2$. Dimostrare che:
(i) $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)N(\beta)$ per $\alpha, \beta \in \mathbf{Z}[\sqrt{-61}]$.
(ii) se α divide β allora $\mathrm{N}(\alpha)$ divide $\mathrm{N}(\beta)$.
(iii) α è una unitá in $\mathbf{Z}[\sqrt{-61}]$ se e soltanto se $\mathrm{N}(\alpha) = 1$.
(iv) il gruppo delle unità di $\mathbf{Z}[\sqrt{-61}]$ è uguale a $\{\pm 1\}$.

(1.D) Dimostrare che l'anello $\mathbf{Z}[\sqrt{-2}] = \mathbf{Z}[X]/(X^2 + 2)$ è Euclideo.

(1.E) Dimostrare che tutte le soluzioni $X, Y \in \mathbf{Z}$ di $X^2 + 2 = Y^3$ sono $X = \pm 5$, $Y = 3$. (utilizzare 1.C)

(1.F) Dimostrare che tutte le soluzioni di $Y^2+4 = X^3$ sono $X = 5$, $Y = \pm 11$ e $X = 2$, $Y = \pm 2$. (Distinguere due casi: Y dispari o pari. Nel secondo caso dividere per $2 + 2i$, il massimo comun divisore di $Y + 2i$ e $Y - 2i$)

(1.G) Dimostrare che $6 = 2 \cdot 3$ e $6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ sono due fattorizzazioni in fattori irriducibili nell'anello $\mathbf{Z}[\sqrt{-5}]$. Concludere che $\mathbf{Z}[\sqrt{-5}]$ non ammette fattorizzazione unica.

(1.H)*Dimostrare che l'anello $\mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$ non è Euclideo. (Nell' Eserc.7.D dimostriamo communque che è un anello principale).

(1.I)*Lo scopo di questo esercizio è dimostrare che per i numeri primi $p \neq 2$ vale: $p \equiv 1 \pmod 4$ se e soltanto se $p = a^2 + b^2$ per certi $a, b \in \mathbf{Z}$. Sia $p \neq 2$ un primo.
(i) Dimostrare che se $p = a^2 + b^2$ per $a, b \in \mathbf{Z}$ allora $p \equiv 1 \pmod 4$.
Sia ora $p \equiv 1 \pmod 4$. Dimostrare che:
(ii) esiste $z \in \mathbf{Z}$ con $|z| < p/2$ e $z^2 + 1 \equiv 0 \pmod p$.
(iii) l'ideale $(z - i, p) \subset \mathbf{Z}[i]$ è generato da un solo elemento π.
(iv) $\mathrm{N}(\pi) = p$. Concludere che esistono $a, b \in \mathbf{Z}$ tali che $p = a^2 + b^2$. (utilizzare 1.A)

(1.J)*Dimostrare che per numeri primi $p \neq 3$ vale: $p \equiv 1 \pmod 3$ se e soltanto se $p = a^2 + ab + b^2$ per certi $a, b \in \mathbf{Z}$. (utilizzare l'anello $\mathbf{Z}[\zeta_3]$ dove ζ_3 è una radice cubica dell'unità, e copiare Eserc.1.I).

(1.K) Sia $\mathbf{H} = \mathbf{R} + i\mathbf{R} + j\mathbf{R} + k\mathbf{R}$ l'algebra dei quaternioni di Hamilton. Per $x = a + bi + cj + dk \in \mathbf{H}$ definiamo $\bar{x} = a - bi - cj - dk$.
(i) Dimostrare che $\mathrm{Tr}(x) = x + \bar{x} = 2a$ e $\mathrm{N}(x) = x\bar{x} = a^2 + b^2 + c^2 + d^2$. Dimostrare che $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$ e $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$.

(ii) Dimostrare che l'insieme $\{a+bi+cj+dk \in \mathbf{H} : a,b,c,d \in \mathbf{Z}$ oppure $a,b,c,d \in \frac{1}{2}+\mathbf{Z}\}$ è un sottoanello di $\mathbf{H}$. È l'anello degli interi di Hurwitz. Provare che per ogni intero x si ha $Tr(x), N(x) \in \mathbf{Z}$.

(1.L)*Lo scopo di questo esercizio è di dimostrare che ogni intero è somma di 4 quadrati. Dimostrare che

(i) per ogni $y \in \mathbf{H}$ esiste x nell'anello degli interi di Hurwitz tale che $N(x-y) < 1$. Concludere che gli interi di Hurwitz formano un anello Euclideo non commutativo, ossia che per tutti gli interi x e $y \neq 0$ esistono interi q, r tali che $x = qy + r$ con $N(r) < N(y)$.

(ii) per ogni primo dispari p esistono $x, y \in \mathbf{Z}$ con $|x|, |y| < p/2$ e $x^2 + y^2 \equiv -1 \pmod{p}$ (Contare i sottoinsiemi $\{-x^2 : x \in \mathbf{Z}/p\mathbf{Z}\}$ e $\{y^2+1 : y \in \mathbf{Z}/p\mathbf{Z}\}$ di $\mathbf{Z}/p\mathbf{Z}$).

(ii) l'ideale sinistro $(p, 1+xi+yj)$ nell'anello degli interi di Hurwitz è generato da un'elemento solo: π.

(iv) Concludere che $N(\pi) = p$ e che p è somma di 4 quadrati. Concludere che ogni intero positivo è somma di 4 quadrati.

(1.M)*(Stewart [S,p.23]) Lo scopo di questo esercizio è dimostrare che l'equazione di Ramanujan $X^2+7=2^n$ ha solo soluzioni $X, n \in \mathbf{Z}_{\geq 0}$ per $n = 3,4,5,7,15$ (e $X = 1,3,5,11,181$) (Nagell). Dimostrare che

(i) l'unico valore di n pari per il quale esistono soluzioni è $n=4$. Sia $X^2+7=2^n$ con $n \geq 5$ *dispari.* Sia $m = n-2$ e $\pi = \frac{1+\sqrt{-7}}{2}$. Dimostrare che

(ii) l'anello $\mathbf{Z}[\pi]$ è Euclideo e, utilizzando il principio (P), che $\pi^m = \pm\frac{X\pm\sqrt{-7}}{2}$.

(iii) $-\sqrt{-7} = \pi^m - \bar{\pi}^m$ (Per determinare il segno di $\pm\sqrt{-7}$ calcolare modulo π^2).

(iv) $-2^{m-1} \equiv m \pmod{7}$ e dunque $m \equiv 3,5,13 \pmod{42}$ (Prendere la parte immaginaria di (iii)).

(v) Sia $m_1 \equiv m_2 \pmod{42}$. Dimostrare che se $m_1 \equiv m_2 \pmod{7^l}$ per $l \geq 1$, allora $\pi^{m_1} - \pi^{m_2} \equiv \pi^{m_1}(m_1-m_2)\sqrt{-7} \pmod{7^{l+1}}$. Concludere che $m_1 \equiv m_2 \pmod{7^l}$ implica che $m_1 \equiv m_2 \pmod{7^{l+1}}$ e finire la dimostrazione.

2. Number fields.

In this section we will discuss number fields. We will introduce discriminants and the real vector space $F \otimes \mathbf{R}$ associated to a number field F. No knowledge of Galois Theory is assumed. We will prove the Theorem of the Primitive Element and this will, instead of Galois Theory, suffice for our purposes.

Definition. *A number field F is a finite field extension of $\mathbf{Q}$. The dimension of F as a $\mathbf{Q}$-vector space is called the degree of F. It is denoted by $[F:\mathbf{Q}]$.*

Examples of number fields are $\mathbf{Q}$, $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt[4]{2})$, $\mathbf{Q}(\sqrt[3]{3}, \sqrt{7})$ of degrees 1,2,4 and 6 respectively. Another example is the field $\mathbf{Q}(\zeta_n)$ where ζ_n denotes a primitive n-th root of unity. Its degree is $\phi(n)$, where $\phi(n) = \#((\mathbf{Z}/n\mathbf{Z})^*)$ is the ϕ-function of Euler. This will be proved in section 10. The following theorem says that every number field can be generated by one element only.

Theorem (2.1). *(Theorem of the primitive element.) Let F be a finite extension of $\mathbf{Q}$. Then there exists $\alpha \in F$ such that $F = \mathbf{Q}(\alpha)$.*

Proof. It suffices to consider the case where $F = \mathbf{Q}(\alpha, \beta)$. The general case follows by induction. We must show that there is $\theta \in F$ such that $\mathbf{Q}(\alpha,\beta) = \mathbf{Q}(\theta)$.

We will take for θ a suitable linear combination of α and β: let $f(T) = f^{\alpha}_{\rm min}(T)$ the minimum polynomial of α over K. Let $n = \deg(f)$ and let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the zeroes of f in $\mathbf{C}$. The α_i are all distinct. Similarly we let $g(T) = f^{\beta}_{\rm min}(T)$ the minimum polynomial of β over K. Let $m = \deg(g)$ and let $\beta = \beta_1, \beta_2, \ldots, \beta_m$ be the zeroes of g in $\mathbf{C}$. Since $\mathbf{Q}$ is an infinite field, we can find $\lambda \in \mathbf{Q}^*$ such that

$$\lambda \neq \frac{\alpha_i - \alpha}{\beta - \beta_j} \qquad \text{for } 1 \leq i \leq n \text{ and for } 2 \leq j \leq m,$$

or equivalently,

$$\alpha + \lambda\beta \neq \alpha_i + \lambda\beta_j \qquad \text{for } 1 \le i \le n \text{ and for } 2 \le j \le m.$$

Put

$$\theta = \alpha + \lambda\beta.$$

The polynomials $h(T) = f(\theta - \lambda T)$ and $g(T)$ are both in $\mathbf{Q}(\theta)[T]$ and they both have β as a zero. The remaining zeroes of $g(T)$ are $\beta_2, \ldots, \beta_m$ and those of $h(T)$ are $(\theta - \alpha_i)/\lambda$ for $2 \le i \le n$. By our choice of λ, we have that $\beta_j \neq (\theta - \alpha_i)/\lambda$ for all $1 \le i \le n$ and $2 \le j \le m$. Therefore the gcd of $h(T)$ and $g(T)$ is $T - \beta$. Since $g(T), h(T) \in \mathbf{Q}(\theta)[T]$ we have that $T - \beta \in \mathbf{Q}(\theta)[T]$. This implies that $\beta \in \mathbf{Q}(\theta)$ and hence that $\alpha \in \mathbf{Q}(\theta)$. It follows that $\mathbf{Q}(\alpha, \beta) = \mathbf{Q}(\theta)$ as required.

Corollary (2.2). *Let F be a finite extension of degree n of $\mathbf{Q}$. There are exactly n distinct field homomorphisms $\phi : F \longrightarrow \mathbf{C}$.*

Proof. By Theorem 2.1 we can write $f = \mathbf{Q}(\alpha)$ for some α. Let F be the minimum polynomial of α over $\mathbf{Q}$. A homomorphism ϕ from F to $\mathbf{C}$ is determined by the image $\phi(\alpha)$ of α. We have that $0 = \phi(f(\alpha)) = f(\phi(\alpha))$. In other words, $\phi(\alpha)$ is a zero of $f(T)$. Conversely, every zero $\beta \in \mathbf{C}$ of $f(T)$ gives rise to a homomorphism $\phi : F \longrightarrow \mathbf{C}$ given by $\phi(\alpha) = \beta$. This shows that there are exactly as many distinct homomorphism $F \longrightarrow \mathbf{C}$ as the degree n of f, as required.

Proposition (2.3). *Let F be a number field of degree n over $\mathbf{Q}$. Let $\omega_1, \ldots, \omega_n \in F$. Then $\omega_1, \ldots, \omega_n$ form a basis for F as a $\mathbf{Q}$-vector space if and only if* $\det(\phi(\omega_i))_{\phi,i} \neq 0$. *Here i runs from 1 to n and ϕ runs over all homomorphisms $\phi : F \longrightarrow C$.*

Proof. First of all, note that by Cor.2.2, the matrix $(\phi(\omega_i))_{\phi,i}$ is a square matrix! Suppose that there exists a relation $\sum_i \lambda_i\omega_i = 0$ with $\lambda_i \in \mathbf{Q}$ not all zero. Since $\phi(\lambda) = \lambda$ for every $\lambda \in \mathbf{Q}$ (see Exer.2.A), We see that $\sum_i \lambda_i\phi(\omega_i) = 0$ for every $\phi : F \longrightarrow \mathbf{C}$. This implies that $\det(\phi(\omega_i))_{\phi,i} = 0$.

To prove the converse, we write $F = \mathbf{Q}(\alpha)$ for some α. Consider the $\mathbf{Q}$-basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. For this basis the the matrix $(\phi(\omega_i))_{\phi,i}$ is a Vandermonde matrix with determinant equal to a product of terms of the form $(\phi_1(\alpha) - \phi_2(\alpha))$ with $\phi_1 \neq \phi_2$. Since the zeroes $\phi(\alpha) \in \mathbf{C}$ of the minimum polynomial of α are all distinct, this determinant is not zero.

So, for the basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ the theorem is valid. For an arbitrary $\mathbf{Q}$-basis $\omega_1, \ldots, \omega_n$ there exists a matrix $M \in \mathrm{GL}_n(\mathbf{Q})$ such that

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = M \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix}.$$

applying the homomorphisms $\phi : F \longrightarrow \mathbf{C}$ one obtains

$$(\phi(\omega_i))_{\phi,i} = M(\phi(\alpha^i))_{\phi,i}$$

and therefore

$$\det((\phi(\omega_i))_{\phi,i}) = \det(M) \cdot \det((\phi(\alpha^i))_{\phi,i}) \neq 0,$$

as required. This proves the proposition.

The number field $\mathbf{Q}$ admits a unique embedding into the field of complex numbers $\mathbf{C}$. The image of this embedding is contained in $\mathbf{R}$. In general, a number field F admits several embeddings in $\mathbf{C}$, and the images of these embeddings are not necessarily contained in $\mathbf{R}$. We generalize the embedding $\Phi : \mathbf{Q} \hookrightarrow \mathbf{R}$ as follows.

Let F be a number field and let $\alpha \in F$ be such that $F = \mathbf{Q}(\alpha)$. In other words $F = \mathbf{Q}[T]/(f(T))$ where $f(T)$ denotes the minimum polynomial of α. We put

$$F \otimes \mathbf{R} = \mathbf{R}[T]/(f(T)).$$

In these notes, $F \otimes \mathbf{R}$ is just our notation for the $\mathbf{R}$-algebra $\mathbf{R}[T]/(f(T))$. This algebra is actually the tensor product of F over $\mathbf{Q}$ with $\mathbf{R}$, but we will not use this interpretation. There is a natural map

$$\Phi : F \longrightarrow F \otimes \mathbf{R}.$$

Since $\mathbf{C}$ is an algebraically closed field, the polynomial $f(T) \in \mathbf{Q}[T]$ factors completely over $\mathbf{C}$. Let's say it has precisely r_1 real zeroes $\beta_1, \ldots, \beta_{r_1}$ and r_2 pairs of complex conjugate zeroes $\gamma_1, \bar{\gamma}_1, \ldots, \gamma_{r_2}, \bar{\gamma}_{r_2}$. We have the canonical isomorphism

$$F \otimes \mathbf{R} \xrightarrow{\cong} \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$$

given by $\mapsto T(\beta_1, \ldots, \beta_{r_1}, \gamma_1, \ldots, \gamma_{r_2})$. Identifying these spaces, we obtain an explicit description of the map Φ:

Definition (2.4). *Let F be a number field. With the notation above, the map Φ*

$$\Phi : F \longrightarrow \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$$

is defined by

$$\Phi(x) = (\phi_1(x), \ldots, \phi_{r_1}(x), \phi_{r_1+1}(x), \ldots, \phi_{r_2+r_1}(x))$$

where the $\phi_i : F \longrightarrow \mathbf{C}$ are determined by $\phi_i(\alpha) = \beta_i$ for $1 \leq i \leq r_1$ and $\phi_{r_1+i}(\alpha) = \gamma_i$ for $1 \leq i \leq r_2$.

For completeness we let $\phi_{r_1+r_2+i}(\alpha) = \bar{\gamma}_i$ for $1 \leq i \leq r_2$. Notice that the map Φ is obviously injective.

Example. Let $\alpha = \sqrt[4]{}\quad 2$ be a zero of $T^4 - 2 \in \mathbf{Q}[T]$ and let $F = \mathbf{Q}(\alpha)$. The minimum polynomial of α is $T^4 - 2$. It has two real roots $\pm\sqrt[4]{2}$ and two complex conjugate roots $\pm i\sqrt[4]{2}$. We conclude that $r_1 = 2$ and $r_2 = 1$. The homomorphisms $\phi_i : F \longrightarrow \mathbf{C}$ are determined by

$$\begin{aligned}
\phi_1(\alpha) &= \sqrt[4]{2}, \\
\phi_2(\alpha) &= -\sqrt[4]{2}, \\
\phi_3(\alpha) &= i\sqrt[4]{2}, \\
\phi_4(\alpha) &= -i\sqrt[4]{2}.
\end{aligned}$$

The map

$$\Phi : F \longrightarrow F \otimes \mathbf{R} = \mathbf{R} \times \mathbf{R} \times \mathbf{C}$$

is, given by

$$\Phi(x) = (\phi_1(x), \phi_2(x), \phi_3(x)).$$

Lemma (2.5). *Let F be a number field of degree n. The map $\Phi : F \longrightarrow F \otimes \mathbf{R}$ maps a $\mathbf{Q}$-basis of F to an $\mathbf{R}$-basis of $F \otimes \mathbf{R}$. The image of F is, in the usual topology of $F \otimes \mathbf{R} = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$, a dense subset.*

Proof. We identify the real vectorspace $\mathbf{C}$ with $\mathbf{R}^2$ by means of the usual correspondence $z \leftrightarrow (\mathrm{Re}(z), \mathrm{Im}(z))$. Let $\omega_1, \ldots, \omega_n$ be a $\mathbf{Q}$-basis of F. Then

$$\Phi(\omega_i) = (\ldots, \phi_k(\omega_i), \ldots, \mathrm{Re}(\phi_l(\omega_i)), \mathrm{Im}(\phi_l(\omega_i)), \ldots),$$

where k denotes a "real" index whenever $1 \le k \le r_1$ and l denotes a "complex" index whenever $r_1 + 1 \le l \le r_1 + r_2$. We put the vectors $\Phi(\omega_i)$ in an $n \times n$-matrix:

$$\Phi \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = \begin{pmatrix} \ldots & \phi_k(\omega_1) & \ldots & \mathrm{Re}\phi_l(\omega_1) & \mathrm{Im}\phi_l(\omega_1) & \ldots \\ \ldots & \phi_k(\omega_2) & \ldots & \mathrm{Re}\phi_l(\omega_2) & \mathrm{Im}\phi_l(\omega_2) & \ldots \\ & \vdots & & \vdots & \vdots & \\ \ldots & \phi_k(\omega_n) & \ldots & \mathrm{Re}\phi_l(\omega_n) & \mathrm{Im}\phi_l(\omega_n) & \ldots \end{pmatrix}.$$

The first r_1 columns correspond to the homomorphisms $\phi_k : F \hookrightarrow \mathbf{R}$ and the remaining $2r_2$ to the real and imaginary parts of the remaining non-conjugate homomorphisms $\phi_l : F \hookrightarrow \mathbf{C}$. Using the formula $\mathrm{Re}(z) = (z + \bar{z})/2$ and $\mathrm{Im}(z) = (z - \bar{z})/2i$ one sees that the determinant of this matrix is equal to

$$(2i)^{-r_2} \det(\phi_k(\omega_j))_{k,j}.$$

By Prop.2.3 its value is different from zero. Since the image of Φ is a $\mathbf{Q}$-vector space and contains an $\mathbf{R}$-basis, it is obviously dense. This proves the lemma.

Let F be a number field of degree n and let $x \in F$. Multiplication by x is a $\mathbf{Q}$-linear map $M_x : F \longrightarrow F$. With respect to a $\mathbf{Q}$-basis of F, one can view M_x as an $n \times n$-matrix with rational coefficients.

Definition (2.6). *Let F be a number field of degree n and let $x \in F$. The characteristic polynomial* $f^x_{\mathrm{char}}(T) \in \mathbf{Q}[T]$ of x is

$$f^x_{\mathrm{char}}(T) = \det(T \cdot \mathrm{Id} - M_x).$$

Writing $f^x_{\mathrm{char}}(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0$, we define the *norm* $\mathrm{N}(x)$ and the *trace* $\mathrm{Tr}(x)$ of x by

$$\mathrm{N}(x) = \mathrm{N}(M_x) = (-1)^n a_0,$$
$$\mathrm{Tr}(x) = \mathrm{Tr}(M_x) = -a_{n-1}.$$

It is immediate from the definitions that $\mathrm{Tr}(x)$ and $\mathrm{N}(x)$ are rational numbers. They are well defined, because the characteristic polynomial, the norm and the trace of x do not depend on the basis with respect to which the matrix M_x has been defined. One should realize that the characteristic polynomial $f^x_{\mathrm{char}}(T)$, and therefore the norm $\mathrm{N}(x)$ and the trace $\mathrm{Tr}(x)$ depend on the field F in which we consider x to be! We don't write $\mathrm{Tr}_F(x)$ or $\mathrm{N}_F(x)$ in order not to make the notation to heavy. The norm and the trace have the following, usual properties: $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$ and $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$ for every $x, y \in F$.

Example. Let $F = \mathbf{Q}(\sqrt[4]{2})$ and let $x = \sqrt{2} = (\sqrt[4]{2})^2 \in F$. We take $\{1, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3\}$ as a $\mathbf{Q}$-basis of F. With respect to this basis, the multiplication by x is given by the matrix M_x

$$\begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

It is easily verified that the characteristic polynomial of x is $f^x_{\mathrm{char}}(T) = T^4 - 4T^2 + 4$, its norm is $\mathrm{N}(x) = 4$ and its trace is $\mathrm{Tr}(x) = 0$. If we consider, on the other hand, $x = \sqrt{2}$ in $F = \mathbf{Q}(\sqrt{2})$, then the characteristic polynomial of $x = \sqrt{2}$ is $f^x_{\text{char}}(T) = T^2 - 2$, its norm $\mathrm{N}(x) = 2$ and its trace $\mathrm{Tr}(x) = 0$.

Proposition (2.7). *Let F be a number field of degree n and let $x \in F$. Then*
(i)

$$f^x_{\text{char}}(T) = \prod_{\phi : F \hookrightarrow \mathbf{C}} (T - \phi(x)).$$

(ii)

$$f^x_{\text{char}}(T) = f^x_{\min}(T)^{[F:\mathbf{Q}(x)]}$$

(iii) $\mathrm{N}(x) = \prod_\phi \phi(x)$ *e* $\mathrm{Tr}(x) = \sum_\phi \phi(x)$*, where the product and the sum run over all embeddings* $\phi : F \hookrightarrow \mathbf{C}$.

Proof. (i) We have the following commutative diagram:

$$\begin{tikzcd} F \arrow[r, "\Phi"] \arrow[d, "x"] & F \otimes \mathbf{R} \arrow[d, "(\phi_1(x),\ldots,\phi_{r_1+r_2}(x))"] \\ F \arrow[r, "\Phi"] & F \otimes \mathbf{R} \end{tikzcd}$$

where the righthand arrow is the multiplication by $\phi_i(x)$ on the i-th coordinate of $F \otimes \mathbf{R} = \mathbf{R}^{r_1} \otimes \mathbf{C}^{r-2}$. If the i-th coordinate is "complex", we identify $\mathbf{C}$ with $\mathbf{R}^2$ via $z \leftrightarrow (\mathrm{Re}(z), \mathrm{Im}(z))$. In this way, the multiplication by $\phi_i(x)$ can be represented by a 2 × 2-matrix

$$\begin{pmatrix} \mathrm{Re}\sigma_i(x) & \mathrm{Im}\sigma_i(x) \\ -\mathrm{Im}\sigma_i(x) & \mathrm{Re}\sigma_i(x) \end{pmatrix}$$

with eigenvalues $\phi_i(x)$ and $\phi_{r_2+i}(x) = \overline{\phi_i(x)}$. Altogether we find an $n \times n$-matrix which is almost diagonal with eigenvalues the $\phi_i(x)$ for $1 \leq i \leq n$. Since the characteristic polinomial of M_x does not depend on the basis, the result follows.
(ii) Let $g(T) \in \mathbf{Q}[T]$ be an irreducible divisor of $f^x_{\text{char}}(T)$. We conclude from *(i)* that $g(T)$ has one of the $\phi_i(x)$ as a zero. Since g has rational coefficients, we have that

$$\phi_i(g(x)) = g(\phi_i(x)) = 0$$

and hence, since ϕ_i is an injective field homomorphism, that $g(x) = 0$. Therefore $f^x_{\min}$ divides g and by the irreducibility we have that $g = f^x_{\min}$. Since g was an arbitrary irreducible divisor of the characteristic polynomial, it follows that $f^x_{\text{char}}(T)$ is a power of $f^x_{\min}$. Finally, the degree of f^x_{char} is $n = [F : \mathbf{Q}]$ and the degree of $f^x_{\min}$ is $[\mathbf{Q}(x) : \mathbf{Q}]$. This easily implies *(ii)*.
(iii) This is immediate from *(i)*. The proof of the proposition is now complete.

Next we introduce *discriminants.*

Definition (2.8). *Let F be a number field of degree n and let $\omega_1, \omega_2, \ldots, \omega_n \in F$. We define the discriminant* $\Delta(\omega_1, \omega_2, \ldots, \omega_n) \in \mathbf{Q}$ by

$$\Delta(\omega_1, \omega_2, \ldots, \omega_n) = \det(\mathrm{Tr}(\omega_i \omega_j)_{1 \leq i,j \leq n}).$$

The basic properties of discriminants are contained in the following proposition.

Proposition (2.9). *Let F be a number field of degree n and let $\omega_1, \omega_2, \ldots, \omega_n \in F$. then*
(i)

$$\Delta(\omega_1, \omega_2, \ldots, \omega_n) = \det(\phi(\omega_i))^2_{i,\phi} \in \mathbf{Q}.$$

(ii) $\Delta(\omega_1, \omega_2, \ldots, \omega_n) \neq 0$ *if and only if* $\omega_1, \omega_2, \ldots, \omega_n$ *is a basis for F as a vector space over* $\mathbf{Q}$.
(iii) If $\omega'_i = \sum_{j=1}^{n} \lambda_{ij}\omega_j$ *with* $\lambda_{ij} \in \mathbf{Q}$ *for* $1 \le i, j \le n$, *then one has that*

$$\Delta(\omega'_1, \omega'_2, \ldots, \omega'_n) = \det(\lambda_{ij})^2 \Delta(\omega_1, \omega_2, \ldots, \omega_n).$$

Proof. *(i)* The determinant is rational, because its entries are traces of elements in F and therefore rational numbers. From Prop.2.7*(iii)* one deduces the following equality of matrices

$$(\sigma_i(\omega_j))_{i,j}(\sigma_i(\omega_j))_{j,k} = (\mathrm{Tr}(\omega_i\omega_k))_{i,k}$$

and *(i)* easily follows.
(ii) Immediate from Prop 2.3.
(iii) We have the following matrix product

$$(\lambda_{i,j})(\sigma_j(\omega'_k))_{j,k} = (\sigma_i(\omega_k))_{i,k}$$

and *(iii)* follows from *(i)*.

This finishes the proof of prop.2.9.

In the sequel we will calculate several discriminants. Therefore we briefly recall the relation of our discriminants to the discriminants and resultants of polynomials.

Let K be a field, let $b, c \in K^*$ and let $\beta_1, \beta_2, \ldots, \beta_r \in K$ and $\gamma_1, \gamma_2, \ldots, \gamma_s \in K$. Put $g(T) = b\prod_{i=1}^{r}(T - \beta_i)$ and $h(T) = c\prod_{i=1}^{s}(T - \gamma_i)$. The *Resultant* $\mathrm{Res}(g, h)$ of g and h is defined by

$$\mathrm{Res}(g, h) = b^s c^r \prod_{i=1}^{r}\prod_{j=1}^{s}(\beta_i - \gamma_j).$$

Resultants can be calculated efficiently by means of an algorithm, which is very similar to the Euclidean algorithm in the polynomial ring $K[T]$. See Exer.2.O for the details. Discriminants of polynomials are closely related to resultants. Let $\alpha_1, \ldots, \alpha_n \in K$. Let $f(T) = \prod_{i=1}^{n}(T - \alpha_i) \in K[T]$. The *discriminant* $\mathrm{Disc}(f)$ of f is defined by

$$\mathrm{Disc}(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

By differentiating the relation $f(T) = \prod_{i=1}^{n}(T - \alpha_i)$ one finds that $f'(\alpha_i) = \prod_{j \neq i}^{n}(\alpha_i - \alpha_j)$ and one deduces easily that

$$\mathrm{Disc}(f) = (-1)^{\frac{n(n-1)}{2}}\mathrm{Res}(f, f').$$

Proposition (2.10). *Let F be a number field of degree n. Let $\alpha \in F$ and let $f = f^{\alpha}_{\text{char}}$ denote its characteristic polynomial. Then*

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \mathrm{Disc}(f) = (-1)^{\frac{n(n-1)}{2}}\mathrm{N}(f'(\alpha)) = (-1)^{\frac{n(n-1)}{2}}\mathrm{Res}(f, f').$$

Proof. The first equality follows from Prop.2.7*(i)* and the Vandermonde determinant in Prop.2.9*(i)*. The second follows by differentiating both sides of the equation $f(T) = \prod_{j=1}^{n}(T - \phi_j(\alpha))$, substituting $\phi_i(\alpha)$ for T and applying Prop.2.7*(iii)*. The third equality has been explained above.

Example (2.11). (*Cyclotomic Polynomials*) For any $m \in \mathbf{Z}_{\geq 1}$ we define inductively the *Cyclotomic polynomial* $\Phi_m(T)$ by

$$X^m - 1 = \prod_{d|m} \Phi_d(T).$$

The first few are given by

$$\begin{aligned}
\Phi_1(T) &= T - 1,\\
\Phi_2(T) &= T + 1,\\
\Phi_3(T) &= T^2 + T + 1,\\
\Phi_4(T) &= T^2 + 1,\\
\Phi_5(T) &= T^4 + T^3 + T^2 + T + 1,\\
\Phi_6(T) &= \ldots
\end{aligned}$$

The degrees of the cyclotomic polynomials satisfy $\sum_{d|m} \deg(\Phi_d) = \deg(T^m - 1) = m$ and therefore one has that $\deg(\Phi_m) = \phi(m)$ where $\phi(m) = \#((\mathbf{Z}/m\mathbf{Z})^*)$ denotes the ϕ-function of Euler.

One establishes inductively that for a prime power l^k one has that

$$\Phi_{l^k}(T) = T^{l^{k-1}(l-1)} + T^{l^{k-1}(l-2)} + \ldots + T^{l^{k-1}} + 1.$$

Since $\Phi_{l^k}(T+1)$ is an Eisenstein polynomial, we see that Φ_{l^k} is irreducible and that the degree of the field $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$ is $l^{k-1}(l-1)$. Here ζ denotes a zero of Φ_{l^k}; it is a primitive l^k-th root of unity. To calculate the discriminant of $\Phi_{l^k}(T)$, we differentiate the relation

$$\prod_{i=0}^{k} \Phi_{l^i}(T) = T^{l^k} - 1$$

and substitute ζ. This gives

$$\Phi'_{l^k}(\zeta)(\zeta^{l^{k-1}} - 1) = l^k \zeta^{l^k - 1}$$

Next we take norms in the field $\mathbf{Q}(\zeta_{l^k})$. The norm of ζ is 1. To calculate the norm of $\xi = \zeta^{l^{k-1}} - 1$, we observe that $\zeta^{l^{k-1}}$ is a primitive l-th root of unity. Therefore the mininimum polynomial of ξ is $\Phi_l(T+1)$. By Prop.2.7*(ii)* we see that $\mathrm{N}(\xi) = \Phi(1)^{l^{k-1}} = l^{l^{k-1}}$. We conclude from Prop 2.10 that

$$\mathrm{Disc}(\Phi_{l^k}) = \pm l^{-l^{k-1}} l^{kl^{k-1}(l-1)} = \pm l^{l^{k-1}(kl-k-1)}.$$

Here the sign is given by $(-1)^{l(l-1)/2}$, except when $l^n = 4$. In this case the sign is -1. See Exer.3.L for the discrimiant of $\Phi_m(T)$, for arbitrary m.

(2.A) Let $\phi : \mathbf{Q} \to \mathbf{C}$ be a field homomorphism. Show that $\phi(q) = q$ for every $q \in \mathbf{Q}$.

(2.B) Find an element $\alpha \in F = \mathbf{Q}(\sqrt{3}, \sqrt{-5})$ such that $F = \mathbf{Q}(\alpha)$.

(2.C) Let $F = \mathbf{Q}(\sqrt[6]{5})$. Give the homomorphism $\Phi : F \longrightarrow F \otimes \mathbf{R}$ explicitly.

(2.D) Let F be a number field with $r_1 \geq 1$, i.e. F admits an embedding into $\mathbf{R}$. Show that the only roots of unity in F are ± 1.

(2.E) Let F be a number field of degree n and let $x \in F$. Show that for $q \in \mathbf{Q}$ on has that

$$\begin{aligned}
\mathrm{Tr}(qx) &= q\mathrm{Tr}(x),\\
\mathrm{Tr}(q) &= nq,\\
\mathrm{N}(q) &= q^n.
\end{aligned}$$

Show that the map $\mathrm{Tr} : F \longrightarrow \mathbf{Q}$ is surjective. Show that the analogous statement for the norm $\mathrm{N} : F^* \longrightarrow \mathbf{Q}^*$ is, in general, false.

(2.F) Let F be a number field of degree n and let $\alpha \in F$. Show that for $q \in \mathbf{Q}$ one has that $\mathrm{N}(\alpha - q) = f^{\alpha}_{\mathrm{char}}(q)$. Show that for $q, r \in \mathbf{Q}$ one has that $\mathrm{N}(q - r\alpha) = r^n f^{\alpha}_{\mathrm{char}}(q/r)$.

(2.G) Let $\alpha = \zeta_5 + \zeta_5^{-1} \in \mathbf{Q}(\zeta_5)$ where ζ_5 denotes a primitive 5th root of unity. Calculate the characteristic polynomial of $\alpha \in \mathbf{Q}(\zeta_5)$.

(2.H) Prove that $\mathrm{Disc}(T^n - a) = n^n a^{n-1}$. Compute $\mathrm{Disc}(T^2 + bT + c)$ and $\mathrm{Disc}(T^3 + bT + c)$.

(2.I) Let $f(T) = T^5 - T + 1 \in \mathbf{Z}[T]$. Show that f is irreducible. Determine r_1, r_2 and the discriminant of f.

(2.J) Consider the field $\mathbf{Q}(\sqrt{3}, \sqrt{5})$. Compute $\Delta(1, \sqrt{3}, \sqrt{5}, \sqrt{15})$ and $\Delta(1, \sqrt{3}, \sqrt{5}, \sqrt{3} + \sqrt{5})$.

(2.K) Let K be a field and let $f \in K[T]$. Show that f has a double zero if and only if $\mathrm{Disc}(f) = 0$. Let $h \in \mathbf{Z}[T]$ be a monic polynomial. Show that it has a double zero modulo a prime p if and only if p divides $\mathrm{Disc}(f)$.

(2.L) Let F be a number field of degree n. Let $\alpha \in F$. Show that

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \det((p_{i+j-2})_{i,j}).$$

Here p_k denotes the power sum $\phi_1(\alpha)^k + \ldots + \phi_n(\alpha)^k$. The ϕ_i denote the embeddings $F \hookrightarrow \mathbf{C}$.

(2.M) (*Newton's formulas*) Let K be a field and let $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. We define the *symmetric functions* s_k of the α_i by

$$\prod_{i=1}^{n}(T - \alpha_i) = T^n - s_1 T^{n-1} + s_2 T^{n-2} + \ldots + (-1)^n s_n.$$

We extend the definition by putting $s_k = 0$ whenever $k > n$. We define the *power sums* p_k by

$$p_k = \sum_{i=1}^{n} \alpha_i^k \qquad \text{for } k \geq 0.$$

Show that for every $k \geq 1$ one has that

$$(-1)^k k s_k = p_k - p_{k-1}s_1 + p_{k-2}s_2 - p_{k-3}s_3 + \ldots.$$

In particular

$$\begin{aligned}
s_1 &= p_1 \\
-2s_2 &= p_2 - p_1 s_1 \\
3s_3 &= p_3 - p_2 s_1 + p_1 s_2 \\
-4s_4 &= p_4 - p_3 s_1 + p_2 s_2 - p_1 s_3 \\
5s_5 &= \ldots
\end{aligned}$$

(Hint: Take the logarithmic derivative of $\prod_{i=1}^{n}(1 - \alpha_i T)$.)

(2.N) Show that the polynomial $T^5 + T^3 - 2T + 1 \in \mathbf{Z}[T]$ is irreducible. Compute its discriminant. (Hint: use Exer.2.M)

(2.O) (*Resultants*) Let K be a field and let $\alpha_1, \ldots, \alpha_r \in K$. Put $g = b\prod_{i=1}^{r}(T - \alpha_i)$ and let $h, h' \in K[T]$ be non-zero polynomials of degree s and s' respectively. Suppose that $h \equiv h' \pmod{g}$.

(i) Show that $\mathrm{Res}(g, h) = (-1)^{rs}\mathrm{Res}(h, g)$.

(ii) Show that $\mathrm{Res}(g, h) = b^s \prod_{\alpha : g(\alpha) = 0} h(\alpha)$.

(iii) Show that $b^{s'}\mathrm{Res}(g, h) = b^s \mathrm{Res}(g, h')$

(iv) Using parts (i) and (ii), find an efficient algorithm, similar to the Euclidean algorithm in the ring $K[T]$ to calculate resultants of polynomials.

(2.P) Consider the extension $L = \mathbf{F}_p(\sqrt[p]{X}, \sqrt[p]{Y})$ of the field $K = \mathbf{F}_p(X, Y)$. Show that the theorem of the primitive element does not hold in this case. Show that there are infinitely many distinct fields F with $K \subset F \subset L$.

(2.Q) Let K be a finite extension of degree n of a finite field $\mathbf{F}_q$. Show

(i) there exists $\alpha \in K$ such that $K = \mathbf{F}_q(\alpha)$.
(ii) there are precisely n distinct embeddings $\phi_i : K \longrightarrow \overline{\mathbf{F}_q}$.
(iii) the discriminant $\Delta(\omega_1, \ldots, \omega_n) = \det(\mathrm{Tr}(\omega_i\omega_j)_{i,j})$ is not zero if and only if $\omega_1, \ldots, \omega_n$ is an $\mathbf{F}_q$-basis for K. Here the definition of the trace $\mathrm{Tr}(\alpha)$ of an element $\alpha \in K$ is similar to Def.2.6. (Hint: copy the proof of Prop.2.9)

3. Rings of integers.

In section 2 we have introduced number fields F as finite extensions of $\mathbf{Q}$. They admit natural embedings into certain finite dimensional $\mathbf{R}$-algebras $F \otimes \mathbf{R}$, which are to be seen as generalizations of the embedding $\mathbf{Q} \hookrightarrow \mathbf{R}$. In this section we generalize the subring of integers $\mathbf{Z}$ of $\mathbf{Q}$: every number field F contains a unique subring O_F of *integral elements.*

Definition. *Let F be a number field. An element $x \in F$ is called integral if there exists a monic polynomial $f(T) \in \mathbf{Z}[T]$ with $f(x) = 0$. The set of integral elements of F is denoted by O_F.*

It is clear that the integrality of an element does not depend on the field F it contains. An example of an integral element is $i = \sqrt{-1}$, since it is a zero of the monic polynomial $T^2 + 1 \in \mathbf{Z}[T]$. Every n-th root of unity is integral, since it is a zero of $T^n - 1$. All ordinary integers $n \in \mathbf{Z}$ are integral in this new sense because they are zeroes of the polynomials $T - n$.

Lemma (3.1). *Let F be a number field and let $x \in F$. the following are equivalent*
(i) x is integral.
(ii) The minimum polynomial $f^x_{\mathrm{min}}(T)$ of x over $\mathbf{Q}$ is in $\mathbf{Z}[T]$.
(iii) The characteristic polynomial $f^x_{\mathrm{char}}(T)$ of x over $\mathbf{Q}$ is in $\mathbf{Z}[T]$.
(iv) There exists a finitely generated subgroup $M \neq 0$ of F such that $xM \subset M$.

Proof. *(i)⇒(ii)* Let x be integral and let $f(T) \in \mathbf{Z}[T]$ be a monic polynomial such that $f(x) = 0$. The minimum polynomial $f^x_{\mathrm{min}}(T)$ divides $f(T)$ in $\mathbf{Q}[T]$. Since the minimum polynomial of x is monic, we have that $f(T) = g(T)f^x_{\mathrm{min}}(T)$ with $g(T) \in \mathbf{Q}[T]$ monic. By Gauß' Lemma (Exer.3.A) we have that both $f^x_{\mathrm{min}}(T)$ and $g(T)$ are in $\mathbf{Z}[T]$ as required.
(ii)⇒(iii) This is immediate from Prop.2.7*(ii)*.
(iii)⇒(iv) Let n be the degree of $f^x_{\mathrm{char}}(T) = \sum_i a_i T^i$. Let M be the additive group generated by $1, x, x^2, \ldots, x^{n-1}$. The finitely generated group M satisfies $xM \subset M$ because $x \cdot x^{n-1} = x^n = -a_{n-1}x^{n-1} - \ldots - a_1 x - a_0 \in M$.
(iv)⇒(i) Let $M \neq 0$ be generated by $e_1, e_2, \ldots, e_m \in F$. Since $xM \subset M$ there exist $a_{ij} \in \mathbf{Z}$ such that

$$xe_i = \sum_{j=1}^{m} a_{ij} e_j \qquad \text{for all } 1 \leq i \leq m,$$

in other words

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mm} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix} = x \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix}.$$

Since $M \neq 0$, at least one of the e_i is not zero. This implies that the determinant $\det(a_{ij} - x \cdot \mathrm{Id}) = 0$ and that the monic polynomial

$$f(T) = \det(a_{ij} - T \cdot \mathrm{Id}) \in \mathbf{Z}[T]$$

vanishes in x. This proves the lemma.

Proposition (3.2). *The set O_F of integral elements of a number field F is a subring of F.*

Proof. It is easy to see that it suffices to show that $x+y$ and xy are integral whenever x and y are integral. Let therefore $x, y \in F$ be integral. By Lemma 3.1 there exist non-trivial finitely generated subgroups M_1 and M_2 of F, such that $xM_1 \subset M_1$ and $yM_2 \subset M_2$. Let $e_1, e_2, \ldots, e_l$ be generators of M_1 and let $f_1, f_2, \ldots, f_m$ be generators of M_2. Let M_3 be the additive subgroup of F generated by the products $e_i f_j$ for $1 \leq i \leq l$ and $1 \leq j \leq m$. It is easy to see that $(x+y)M_3 \subset M_3$ and that $xyM_3 \subset M_3$. This conludes the proof of Prop.3.2

In section 4 we will encounter a more general notion of "integrality": if $R \subset S$ is an extension of commutative rings, then $x \in S$ is said to be *integral over R,* if there exists a monic polynomial $f(T) \in R[T]$ such that $f(x) = 0$. Integers of rings of number fields are, in this sense, integral over $\mathbf{Z}$.

It is, in general, a difficult problem to determine the ring of integers of a given number field. According to Prop.2.1, every number field F can be written as $F = \mathbf{Q}(\alpha)$ for some $\alpha \in \mathbf{Z}$. A similar statement for rings of integers is, in general false: there exist number fields F such that $O_F \neq \mathbf{Z}[\alpha]$ for any $\alpha \in O_F$. For example, the field $\mathbf{Q}(\sqrt[3]{20})$ has $\mathbf{Z}[\sqrt[3]{20}, \sqrt[3]{50}]$ as a ring of integers and this ring is not of the form $\mathbf{Z}[\alpha]$ for any α (see Exer.6.G). There do, in fact, exist many number fields F for which O_F is not of the form $\mathbf{Z}[\alpha]$ for any α. For instance, it was recently shown by M.-N. Gras [28], that "most" proper subfields of the cyclotomic fields have this property.

For quadratic fields however, the rings of integrs are generated by one element and the calculations are rather easy:

Example (3.3). *Let F be a quadratic number field. Then*
(i) There exists a unique squarefree integer $d \in \mathbf{Z}$ such that $F = \mathbf{Q}(\sqrt{d})$.
(ii) Let d be a squarefree integer. The ring of integers O_F of $F = \mathbf{Q}(\sqrt{d})$ is given by

$$\begin{aligned} O_F &= \mathbf{Z}[\sqrt{d}] && \text{if } d \equiv 2 \text{ or } 3 \pmod 4, \\ &= \mathbf{Z}[\frac{1+\sqrt{d}}{2}] && \text{if } d \equiv 1 \pmod 4. \end{aligned}$$

Proof. *(i)* For any $\alpha \in F - \mathbf{Q}$ one has that $F = \mathbf{Q}(\alpha)$. The number α is a zero of an irreducible polynomial $f(T) \in \mathbf{Q}[T]$ of degree 2 and, obviously, $F = \mathbf{Q}(\sqrt{d})$ where d is the discriminant of f. The field $\mathbf{Q}(\sqrt{d})$ does not change if we divide or multiply d by squares of non-zero integers. We conclude that $F = \mathbf{Q}(\sqrt{d})$ for some squarefree integer d. The uniqueness of d will be proved after the proof of part *(ii)*.
(ii) Let $\alpha \in F = \mathbf{Q}(\sqrt{d})$. Then α can be written as $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbf{Q}$. It is easily verified that the characteristic polynomial is given by $f^x_{\text{char}}(T) = T^2 - 2aT + (a^2 - db^2)$ Therefore, a necessary and sufficient condition for $\alpha = a + b\sqrt{d}$ to be in O_F, is that $2a \in \mathbf{Z}$ and $a^2 - db^2 \in \mathbf{Z}$.

It follows that either $a \in \mathbf{Z}$ or $a \in \frac{1}{2} + \mathbf{Z}$. We write $b = u/v$ with $u, v \in \mathbf{Z}$, $v \neq 0$ and $\gcd(u,v) = 1$. If $a \in \mathbf{Z}$, then $b^2 d \in \mathbf{Z}$. and we see that v^2 divides $u^2 d$. Since $\gcd(u,v) = 1$, we conclude that v^2 divides d. Since d is squarefree, this implies that $v^2 = 1$ and that $b \in \mathbf{Z}$. If $a \in \frac{1}{2} + \mathbf{Z}$, then $4du^2/v^2 \in \mathbf{Z}$. Since $\gcd(u,v) = 1$ and d is squarefree this implies that v^2 divides 4. Since $a \in \frac{1}{2} + \mathbf{Z}$, we have that $b \notin \mathbf{Z}$ and $v^2 \neq 1$. Therefore $v^2 = 4$ and $b \in \frac{1}{2} + \mathbf{Z}$. Now we have that $a, b \in \frac{1}{2} + \mathbf{Z}$, and this together with the fact that $a^2 - db^2 \in \mathbf{Z}$ is easily seen to imply that $(d-1)/4 \in \mathbf{Z}$.

We conclude, that for $d \equiv 1 \pmod 4$ one has that $O_F = \{a + b\sqrt{d} : a, b \in \mathbf{Z} \text{ or } a, b \in \frac{1}{2} + \mathbf{Z}\}$. Equivalently, $O_F = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$. In the other cases one has that $O_F = \mathbf{Z}[\sqrt{d}]$.
$(i)^{\text{bis}}$ It remains to finish the proof of *(i)*. According to *(ii)* the smallest $b \in \mathbf{Q}_{>0}$ for which there exists an $a \in \mathbf{Q}$ such that $a + b\sqrt{d}$ is in the ring of integers of $\mathbf{Q}(\sqrt{d})$ is 1 if $d \equiv 2$ or 3 (mod 4) and

$1/2$ if $d \equiv 1 \pmod 4$. So the squarefree integer can be recovered from O_F. Therefore d characterizes the field F. This finishes the example.

Next we discuss *discriminants* of integral elements $\omega_1, \ldots, \omega_n \in F$.

Proposition (3.4). *Let F be a number field of degree n.*

(i) If $\omega_1, \ldots, \omega_n \in O_F$ then $\Delta(\omega_1, \ldots, \omega_n) \in \mathbf{Z}$.

(ii) Elements $\omega_1, \ldots, \omega_n \in O_F$ generate O_F as an abelian group if and only if $0 \neq \Delta(\omega_1, \ldots, \omega_n) \in \mathbf{Z}$ has minimal absolute value.

(iii) There exists $\omega_1, \ldots, \omega_n$ that generate O_F. For such a basis one has that $O_F \cong \oplus_{i=1}^n \omega_i \mathbf{Z}$. The value $\Delta(\omega_1, \ldots, \omega_n)$ is independent of the basis.

Proof. *(i)* Clearly the discriminant $\Delta(\omega_1, \ldots, \omega_n)$ is in O_F. By Prop.2.9*(i)* it is in $\mathbf{Q}$. Since $\mathbf{Z}$ is the ring of integers of $\mathbf{Q}$, we conclude that it is actually in $\mathbf{Z}$.
(ii) Suppose $\omega_1, \ldots, \omega_n$ generate O_F as an abelian group. Let $\omega_1', \ldots, \omega_n'$ be any n elements in O_F. There exist integers $\lambda_{ij} \in \mathbf{Z}$ such that $\omega_i' = \sum_{j=1}^n \lambda_{ij}\omega_j$ for $1 \leq j \leq n$. By Prop.2.9*(iii)* we have that $\Delta(\omega_1', \ldots, \omega_n') = \det(\lambda_{ij})^2 \Delta(\omega_1, \ldots, \omega_n)$. Since $\det(\lambda_{ij})^2$ is a positive integer, it follows that the discriminant $\Delta(\omega_1, \ldots, \omega_n)$ is minimal. Conversely, suppose $|\Delta(\omega_1, \ldots, \omega_n)|$ is minimal. If $\omega_1, \ldots, \omega_n$ do not generate the group O_F, there exists $x = \sum_i \lambda_i \omega_i \in O_F$, but not in the group generated by the ω_i. This implies that $\lambda_i \notin \mathbf{Z}$ for some i. After adding a suitable integral multiple of ω_i to x, we may assume that $0 \leq \lambda_i < 1$. Now we replace ω_i by x in our basis. One checks easily that $|\Delta(\omega_1, \ldots, x, \ldots, \omega_n)| = \lambda_i^2 |\Delta(\omega_1, \ldots, \omega_n)|$ which is integral by *(i)*, non-zero, but smaller than $\Delta(\omega_1, \ldots, \omega_n)$. This contradicts the minimality and proves *(ii)*.
(iii) There exists an integral basis $\omega_1, \ldots, \omega_n$ for F over $\mathbf{Q}$. This basis has a non-zero discriminant and by an *(i)* integral one. By *(ii)* it suffices to take such a basis with minimal $|\Delta(\omega_1, \ldots, \omega_n)|$. It follows that $O_F \cong \oplus_{i=1}^n \omega_i \mathbf{Z}$. The discriminant does not depend on the basis by Prop.2.9*(iii)*.

Corollary (3.5). *let F be a number field with ring of integers O_F. Then*

(i) Every ideal $I \neq 0$ of O_F has finite index $[O_F : I]$.

(ii) Every ideal I of O_F is a finitely generated abelian group.

(iii) Every prime ideal $I \neq 0$ of O_F is maximal.

Proof. Let $I \neq 0$ be an ideal of O_F. By Exer.3.E, the ideal I contains an integer $m \in \mathbf{Z}_{>0}$. Therefore $mO_F \subset I$. By Prop.3.4*(iii)*, the additive group of O_F is isomorphic to $\mathbf{Z}^n$, where n is the degree of F. It follows that O_F/I, being a quotient of $O_F/(m) \cong \mathbf{Z}^n/m\mathbf{Z}^n$ is finite.
(ii) Let I be an ideal of O_F. Since the statement is trivial when $I = 0$, we will assume that $I \neq 0$ and choose an integer $m \in \mathbf{Z}_{>0}$ in I. By *(i)*, the ring O_F/mO_F is finite and therefore the ideal $I \pmod{mO_F}$ can be generated, as an abelian group, by, say, $\alpha_1, \ldots, \alpha_k$. It follows easily that the ideal I is then generated by $\alpha_1, \ldots, \alpha_k$ and $m\omega_1, \ldots, m\omega_n$, where the ω_i are a $\mathbf{Z}$-basis for the ring of integers O_F.
(iii) Let $I \neq 0$ be a prime ideal of O_F. By *(i)*, the ring O_F/I is a finite domain. Since finite domains are fields, it follows that I is a maximal ideal.

As a consequence of Cor.3.5, the following definition is now justified:

Definition. *Let F be a number field and let $I \neq 0$ be an ideal of the ring of integers of O_F of F. We define the norm* $\mathrm{N}(I)$ *of the ideal I by*

$$\mathrm{N}(I) = [O_F : I] = \#(O_F/I).$$

Another application of Prop.3.4 is the following. Let F be a number field of degree n and let $\omega_1, \ldots, \omega_n \in F$. By Prop.2.9*(iii)* the discriminant $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ does not depend on $\omega_1, \ldots, \omega_n$, but merely on the additive group these numbers generate. This justifies the following definition.

Definition. Let F be a number field of degree n. the *discriminant* of F is the discriminant $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ of an integral basis $\omega_1, \omega_2, \ldots, \omega_n$ of O_F.

Since 1 is a $\mathbf{Z}$-basis for $\mathbf{Z}$, we see that the discriminant of $\mathbf{Q}$ is 1. As an example we calculate the discriminant of a quadratic field.

Example (3.6). Let F be aquadratic field. By Example 3.3 there exists a unique squarefree integer d such that $F = \mathbf{Q}(\sqrt{d})$. If $d \equiv 2$ or 3 (mod 4), the ring of integers of F is $\mathbf{Z}[\sqrt{d}]$. We take $\{1, \sqrt{d}\}$ as a $\mathbf{Z}$-base of O_F. Then

$$\Delta_{\mathbf{Q}(\sqrt{d})} = \det\begin{pmatrix} \mathrm{Tr}(1\cdot 1) & \mathrm{Tr}(1\cdot\sqrt{d}) \\ \mathrm{Tr}(1\cdot\sqrt{d}) & \mathrm{Tr}(\sqrt{d}\cdot\sqrt{d}) \end{pmatrix} = \det\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

If $d \equiv 1$ (mod 4), the ring of integers of F is $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$. We take $\{1, \frac{1+\sqrt{d}}{2}\}$ as a $\mathbf{Z}$-base of O_F. Then

$$\Delta_{\mathbf{Q}(\sqrt{d})} = \det\begin{pmatrix} \mathrm{Tr}(1\cdot 1) & \mathrm{Tr}(1\cdot\frac{1+\sqrt{d}}{2}) \\ \mathrm{Tr}(1\cdot\frac{1+\sqrt{d}}{2}) & \mathrm{Tr}(\frac{1+\sqrt{d}}{2}\cdot\frac{1+\sqrt{d}}{2}) \end{pmatrix} = \det\begin{pmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{pmatrix} = d.$$

In general, it is rather difficult to calculate the discriminant and the ring of integers of a number field. We will come back to this problem in section 6. The following proposition is often very useful.

Proposition 3.7. *Let F be a number field of degree n. Suppose $\omega_1, \omega_2, \ldots, \omega_n \in O_F$ have the property that $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ is a squarefree integer. Then $O_F = \sum_i \omega_i\mathbf{Z}$. In particular, if there exists $\alpha \in O_F$ such that the discriminant of $f^{\alpha}_{\mathrm{min}}(T)$ is squarefree, then $O_F = \mathbf{Z}[\alpha]$ and $\Delta_F = \Delta(1, \alpha, \ldots, \alpha^{n-1}) = \mathrm{Disc}(f^{\alpha}_{\mathrm{min}})$.*

Proof. It follows from Prop.2.9*(iii)* that $\Delta(\omega_1, \omega_2, \ldots, \omega_n) = \det(M)^2\Delta_F$, where $M \in \mathrm{GL}_2(\mathbf{Z})$ is the matrix expressing the ω_i in terms of a $\mathbf{Z}$-base of O_F. Since $\det(M)^2$ is the square of an integer, *(i)* follows.

If we take the powers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ for $\omega_1, \omega_2, \ldots, \omega_n$, the result in *(ii)* follows from *(i)* and the fact, proved in Prop.2.10, that $\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \mathrm{Disc}(f^{\alpha}_{\mathrm{min}})$.

Example. Let α be a zero of the polynomial $f(T) = T^3 - T - 1 \in \mathbf{Z}[T]$. Since $f(T)$ is irreducible modulo 2, it is irreducible over $\mathbf{Q}$. Put $F = \mathbf{Q}(\alpha)$. By Prop.2,7*(ii)*, the characteristic polynomial of α is also equal to $f(T)$. In order to calculate the discriminant of f, one can employ various methods. See Exer.2.O for an efficients algorithm involving resultants of polynomials. Here we just use the definition of the discriminant. Let's calculate

$$\Delta(1, \alpha, \alpha^2) = \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) \\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) & \mathrm{Tr}(\alpha^4) \end{pmatrix}.$$

The trace of 1 is 3. By Prop.2.7*(iii)*, we see that $\mathrm{Tr}(\alpha)$ is equal to the coefficient at T^2 and hence 0. In general, the traces $\mathrm{Tr}(\alpha^k)$ are equal to the power sums $p_k = \phi_1(\alpha)^k + \phi_2(\alpha)^k + \phi_3(\alpha)^k$ for $k \geq 0$. The Newton relations (see Exer.2.M) relate these sums to the coefficients s_k of the minimum polynomial of α.

We have that $\mathrm{Tr}(\alpha^2) = p_2 = -2s_2 + p_1 s - 1 = -2\cdot(-1) + 0 = 2$. We obtain the other values of $\mathrm{Tr}(\alpha^k)$ by using the additivity of the trace: $\mathrm{Tr}(\alpha^3) = \mathrm{Tr}(\alpha+1) = 0+3 = 3$ e $\mathrm{Tr}(\alpha^4) = \mathrm{Tr}(\alpha^2+\alpha) = 2+0 = 2$. Therefore

$$\Delta(1, \alpha, \alpha^2) = \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{pmatrix} = -23.$$

By Prop.3.7 we can now conclude that the ring of integers of $\mathbf{Q}(\alpha)$ is $\mathbf{Z}[\alpha]$ and that the discriminant $\Delta_{\mathbf{Q}(\boldsymbol{\alpha})}$ is equal to -23.

(3.A) Prove Gauß' Lemma: let R be a unique factorization domain with field of fractions K and let $f \in R[T]$ be a monic polynomial. If $f = g \cdot h$ in $K[T]$, with g and h monic polynomials, then $g, h \in R[T]$.

(3.B) Let F be a number field and let $\alpha \in F$. Show that there exist an integer $0 \neq m \in \mathbf{Z}$ such that $m\alpha \in O_F$.

(3.C) Show that for every number field F there exists an *integral* element $\alpha \in O_F$ such that $F = \mathbf{Q}(\alpha)$.

(3.D) Let F be a number field. Show that the field of fractions of O_F is F.

(3.E) Let F be a number field. Show that every ideal $I \neq 0$ of O_F contains a non-zero integer $m \in \mathbf{Z}$.

(3.F) Let F be a number field and let $\alpha \in O_F$. Show that $\mathrm{N}(\alpha) = \pm 1$ if and only if α is a unit of the ring O_F.

(3.G) Let $F \subset K$ be an extension of number fields. Show that $O_K \cap F = O_F$.

(3.H) Let F be a number field. Let r_1 be the number of distinct embeddings $F \hookrightarrow \mathbf{R}$ and let $2r_2$ be the number of remaining homomorphisms $F \hookrightarrow \mathbf{C}$. Show that the sign of Δ_F is $(-1)^{r_2}$.

(3.I) Determine the integers and the discriminant of the number field $\mathbf{Q}(\alpha)$ where α is given by $\alpha^3 + \alpha - 1 = 0$.

(3.J) Let F and K be two quadratic number fields. Show that if $\Delta_F = \Delta_K$, then $F \cong K$.

(3.K) Let $n \geq 1$ be an integer and let ζ_n denote a primitive n-th root of unity. Show that $\zeta_n - 1$ is a unit if and only if n is not the power of a prime. (Hint: substitute $T = 1$ in $(T^n - 1)/(T - 1) = \prod_{d|n, d \neq 1} \Phi(T)$ and use Example 2.11)

(3.L) *The goal of this exercise is to calculate the discriminant of the n-th cyclotomic polynomial $\Phi_n(T)$. For $n \in \mathbf{Z}_{\geq 1}$ let $\mu(n)$ denote the Möbius function: for squarefree integers n we have that $\mu(n)$ is the number of primes dividing n. For all other n one has that $\mu(n) = 0$.

(i) For $n \geq 1$ prove that $\sum_{d|n} d\mu(n/d) = \phi(n)$.

(ii) Show that

$$\Phi(T) = \prod_{d|m} (T^d - 1)^{\mu(m/d)}.$$

(iii) Let ζ denote a primitive m-th root of unity. Prove that

$$\Phi'_m(\zeta) \prod_{d|m, d \neq m} (\zeta^d - 1)^{-\mu(m/d)} = m\zeta^{-1}.$$

(Hint: write $T^m - 1 = \Phi_m(T)G(T)$, differentiate and put $T = \zeta$.)

(iv) Show that

$$\prod_{d|m, d \neq m} (\zeta^d - 1)^{-\mu(m/d)} = \prod_{p|m} (\zeta_p - 1)$$

where ζ_p denotes a primitive p-th root of unity in $\mathbf{Q}(\zeta_m)$. Show that

$$\mathrm{Disc}(\Phi_m(T)) = (-1)^{\frac{1}{2}\phi(m)} \left(\frac{m}{\prod_{p|m} p^{\frac{1}{p-1}}} \right)^{\phi(m)}.$$

(Hint: see Example 2.11.)

(3.M) *(Stickelberger 1923) Let F be a number field of degree n. Let $\{\omega_1, \omega_2, \ldots, \omega_n\}$ be a $\mathbf{Z}$-basis for the ring of integers of F. Let $\phi_i : F \hookrightarrow \mathbf{C}$ be the embeddings of F into $\mathbf{C}$. By S_n we denote the symmetric group on n symbols and by A_n the normal subgroup of *even* permutations. We define $\Delta^+ = \sum_{\tau \in A_n} \prod_{i=1}^n \sigma_i(\omega_{\tau(i)})$ and $\Delta^- = \sum_{\tau \in S_n - A_n} \prod_{i=1}^n \sigma_i(\omega_{\tau(i)})$. Prove, using Galois theory, that $\Delta^+ + \Delta^-$ e $\Delta^+\Delta^-$ are in $\mathbf{Z}$. Conclude that $\Delta_F = (\Delta^+ + \Delta^-)^2 - 4\Delta^+\Delta^- \equiv 0$ or $1 \pmod 4$.

4. Dedekind rings.

In this section we will introduce Dedekind rings (Richard Dedekind, German mathematician 1831–1916). Rings of integers of number fields are important examples of Dedekind rings. We will show that the *fractional ideals* of a Dedekind ring admit unique factorization into prime ideals.

Definition. *A commutative ring R is called Noetherian if every sequence of ideals of R*

$$I_1 \subset I_2 \subset \ldots \subset I_i \subset \ldots$$

stabilizes, i.e. if there exists an index i_0 such that $I_i = I_{i_0}$ for all $i \geq i_0$.

Lemma (4.1). *Let R be a commutative ring. The following are equivalent:*

(i) *Every R-ideal is finitely generated.*
(ii) *R is Noetherian.*
(iii) *Every non-empty collection Ω of R-ideals contains a maximal element i.e. an ideal I such that no ideal $J \in \Omega$ contains I properly.*

Proof. *(i) ⇒ (ii)* Let $I_1 \subset I_2 \subset \ldots \subset I_i \subset \ldots$ be a sequence of ideals of R. Suppose the union $I = \cup_{i \geq 1}$ is generated by $\alpha_1, \ldots, \alpha_m$. For every α_k there exists an index i such that $\alpha_k \in I_i$. Writing N for the maximum of the indices i, we see that $\alpha_k \in I_N$ for all k. Therefore $I = I_N$ and the sequences stabilizes.

(ii) ⇒ (iii) Suppose Ω is a non-empty collection without maximal elements. Pick $I = I_1 \in \Omega$. Since I_1 is not maximal, there exists an ideal $I_2 \in \Omega$ such that $I_1 \subset_{\neq} I_2$. Similarly, there exists an ideal $I_3 \in \Omega$ such that $I_2 \subset_{\neq} I_3$. In this way we obtain a sequence $I_1 \subset I_2 \subset \ldots \subset I_i \subset \ldots$ that does not stabilize. This contradicts the fact that R is Noetherian

(iii) ⇒ (i) Let I be an ideal of R and let Ω be the collection of ideals $J \subset I$ which are finitely generated. Since $(0) \in \Omega$, we see that $\Omega \neq \emptyset$ and hence contains a maximal element J. If $J \neq I$, we pick $x \in I - J$ and we see that the ideal $J + (x)$ properly contains J and is in Ω. This contradicts the maximality of J. We conclude that $I = J$ and the proof of the lemma is complete.

Almost all rings that appear in mathematics are Noetherian (Emmy Noether, German mathematician 1882-1955). Every principal ideal ring is clearly Noetherian, so fields and the ring $\mathbf{Z}$ are Noetherian rings. According to Exer.4.A., the quotient ring R/I of a Noetherian ring R is again Noetherian. Finite products of Noetherian rings are Noetherian. The famous "Basissatz" [33] of Hilbert (David Hilbert, German mathematician 1862–1943) affirms that the polynomial ring $R[T]$ is Noetherian whenever R is.

Non-Noetherian rings are often very large and sometimes pathological. For instance, the ring $R[X_1, X_1, X_3, \ldots]$ of polynomials in countably many variables over a commutative ring R is not Noetherian.

Definition. *Let $R \subset S$ be an extension of commutative rings. An element $x \in S$ is called integral over R, if there exists a monic polynomial $f(T) \in R[T]$ with $f(x) = 0$. A domain R is called integrally closed if every integral element in the field of fractions of R is in R.*

Using this terminology, one can say that the integers of number fields are, in fact, integers over $\mathbf{Z}$. Let F be a number field. By Exer.3.D, the field of fractions of the ring of integers O_F of F is precisely equal to F. Therefore, rings of integers are by definition integrally closed. Other examples of integrally closed rings are provided by Exer.4.C: every unique factorization domain is integrally closed.

Definition. *Let R be a commutative ring. The height of a prime ideal $P = P_0$ of R is the supremum of the integers n for which there exists a chain*

$$P_0 \subset P_1 \subset P_2 \subset \ldots \subset P_n \subset R$$

of distinct prime ideals in R. The Krull dimension of a ring is the supremum of the heights of the prime ideals of R.

For example, a field has Krull dimension 0 and the ring $\mathbf{Z}$ has dimension 1 (Wolfgang Krull, German mathematician 1899-1971). In general, principal ideal rings that are not fields, have dimension 1. It is easy to show that for every field K, the ring of polynomials $K[X_1, \ldots, X_n]$ has dimension at least n. The notion of dimension originates in algebraic geometry: the ring of regular functions on an affine variety of dimension n over a field K has Krull dimension equal to n.

Definition. *A Dedekind ring is a Noetherian, integrally closed domain of dimension at most 1.*

By Exer.4.H, every principal ideal domain R is a Dedekind ring. Its dimension is 0 if R is a field and 1 otherwise. The following proposition gives us many examples of Dedekind rings.

Proposition (4.2). *Let F be a number field. Then the ring of integers O_F of F is a Dedekind ring.*

Proof. The ring O_F is integrally closed by definition. By Cor.3.5*(ii)*, every ideal is a finitely generated abelian group. We conclude from Lemma(4.1) that O_F is a Noetherian ring. By Cor.3.5*(iii)* every non-zero prime ideal is maximal. This implies that the dimension of O_F is at most 1. This proves the proposition.

Definition. *Let R be a Dedekind ring with field of fractions K. A fractional ideal of R (or K) is an additive subgroup I of K for which there exists $\alpha \in K$ such that αI is a non-zero ideal of R.*

Proposition (4.3). *Let R be a Dedekind ring with field of fractions K. Then*
(i) Every non-zero ideal of R is a fractional ideal.
(ii) If I and J are fractional ideals, then $IJ = \{\sum_i^{<\infty} \alpha_i\beta_i : \alpha_i \in I, \beta_i \in J\}$ is a fractional ideal.
(iii) For every $\alpha \in K^*$ the set $(\alpha) = \alpha R = \{\alpha r : r \in R\}$ is a fractional ideal. Such a fractional ideal is called a principal fractional ideal.
(iv) For every fractional ideal I, the set $I^{-1} = \{\alpha \in K : \alpha I \subset R\}$ is a fractional ideal.

Proof. *(i)* is obvious.
(ii) If $\alpha I \subset R$ and $\beta J \in R$ then $\alpha\beta IJ \subset R$.
(iii) This follows from the fact that $\alpha^{-1} I = R$.
(iv) Let $\alpha \neq 0$ be any element in I. Then $\alpha I^{-1} \subset R$ is an ideal. This proves the proposition.

Theorem (4.4). *Let R be a Dedekind ring and let $Id(R)$ be the set of fractional ideals of R. Then*
(i) The set $Id(R)$ is, with the multiplication of Prop.4.3(i), an abelian group. The neutral element is R and the inverse of a fractional ideal I is I^{-1}.
(ii) We have

$$Id(R) \cong \bigoplus_{\mathfrak{p}} \mathbf{Z}$$

where $\mathfrak{p}$ runs over the non-zero prime ideals of R. More precisely: every fractional ideal can be written as a finite product of prime ideals (with exponents in $\mathbf{Z}$) in a unique way.

Proof. Since the theorem is obvious when R is a field, we will suppose that R is not a field. We suppose, in other words, that R has Krull dimension 1. The proof will be given in six steps:

(i) Every non-zero ideal of R contains a product of non-zero prime ideals of R.

Suppose that there exists an ideal that does not contain a product of non-zero prime ideals. So, the collection Ω of such ideals is not empty. Since R is Noetherian, we can, by Lemma 4.1 find an ideal $I \in \Omega$ such that every ideal J that properly contains I is not in Ω. Clearly I is not prime itself. Therefore there exist $x, y \notin I$ such that $xy \in I$. The ideals $I + (x)$ and $I + (y)$ are strictly larger than I and hence contain a product of non-zero prime ideals. Say $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset I + (x)$ and

$\mathfrak{p}'_1 \cdot \ldots \cdot \mathfrak{p}'_s \subset I + (y)$. Now we have $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \mathfrak{p}'_1 \cdot \ldots \cdot \mathfrak{p}'_s \subset (I + (x))(I + (y)) \subset I$ contradicting the fact that $I \in \Omega$.

(ii) For every ideal I with $0 \neq I \neq R$ one has that $R \subset_{\neq} I^{-1}$.

Let M be a maximal ideal with $i \subset M \subset R$. Since $I^{-1} \supset M^{1} \supset R^{-1} = R$ it suffices to prove the statement for $I = M$ a maximal ideal. Let $0 \neq a \in M$. By part *(i)* there exist prime ideals $\mathfrak{p}_i$ such that $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset (a) \subset M$. Let us assume that the number of prime ideals r in this product, is minimal. Since M itself is a prime ideal, one of the primes $\mathfrak{p}_i$, say $\mathfrak{p}_1$, is contained in M. Sinds R has Krull dimension 1, we conclude that $\mathfrak{p}_1 = M$. By minimality of r we see that $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \subset (a) \not\subset M$ and we can pick $b \in \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r$ but $b \notin (a)$. So, $b/a \in R$, but $b/a \in M^{-1}$ because $bM \subset \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r M \subset (a)$. This proves *(ii)*.

(iii) $MM^{-1} = R$ for every maximal ideal M of R.

Since $R \subset M^{-1}$ we have that $M \subset MM^{-1} \subset R$. If one would have that $M = MM^{-1}$ then every $x \in M^{-1}$ satisfies $xM \subset M$. Since M is finitely generated over R, it follows from Exer.4.E that x is integral over R. Since R is integrally closed this would imply that $M^{-1} \subset R$ contradicting *(ii)*. We conclude that $M \neq MM^{-1}$ and hence that $MM^{-1} = R$ as required.

(iv) $II^{-1} = R$ for every ideal $I \neq 0$ of R.

Suppose I is an ideal with $II^{-1} \neq R$. Suppose, moreover, that I is maximal with respect to this property. Let M be a maximal ideal containg I. Since $R \subset M^{-1}$, we have that $I \subset IM^{-1} \subset MM^{-1} \subset R$. We see that IM^{-1} is an ideal of R. If we would have that $IM^{-1} = I$, then, by Exer.4.G, M^{-1} would be integral, which is impossible. We conclude that $IM^{-1} = I$ is strictly larger than I. Therefore $IM^{-1}(IM^{-1})^{-1} = R$. This implies that $M^{-1}(IM^{-1})^{-1} \subset I^{-1}$. Finally: $R = IM^{-1}(IM^{-1})^{-1} \subset II^{-1} \subset R$ whence $II^{-1} = R$ contradicting the maximality of I. This proves *(iv)*.

(v) Every fractional ideal is a product of prime ideals with exponents in $\mathbf{Z}$.

Suppose $I \subset R$ is an ideal which cannot be written as a product of prime ideals. Suppose that I is maximal with respect to this property. Let M be maximal ideal $I \subset M \subset R$. Then $I \subset IM^{-1} \subset R$. Since $M^{-1} \not\subset R$ we see that IM^{-1} is strictly larger than I. So IM^{-1} is a product of primes and therefore, multiplying by M, so is I. This contradiction shows that every integral ideal I of R is a product of prime ideals. By definition, every fractional ideal is of the form $\alpha^{-1}I$ where $\alpha \in R$ and I is an ideal of R. We conclude that every fractional ideal is a product of prime ideals, with exponents in $\mathbf{Z}$.

(vi) The decomposition into prime ideals is unique.

Suppose $\prod \mathfrak{p}^{n_\mathfrak{p}}$ with $n_\mathfrak{p} \neq 0$. This gives us a relation $I\mathfrak{p} = J$ where I and J are ideals in R and J is a product of primes different from $\mathfrak{p}$. However, since $\mathfrak{p}$ is prime we have that $J \subset \mathfrak{p}$ and therefore $\mathfrak{p}$ contains a non-zero prime ideal different from itself. This is impossible and the proof of Theorem 3.4 is now complete.

It is easy to see that the ideals of R are precisely the fractional ideals that have a prime ideal decomposition $\prod \mathfrak{p}^{n_\mathfrak{p}}$ with non-negative exponents. When R is a Dedekind ring and $\mathfrak{p}$ is a non-zero prime ideal in R, we denote for every fractional ideal I by

$$\mathrm{ord}_\mathfrak{p}(I)$$

the exponent $n_\mathfrak{p}$ of $\mathfrak{p}$ in the prime decomposition of I. For $x \in F^*$ we denote by

$$\mathrm{ord}_\mathfrak{p}(x)$$

the exponent $\mathrm{ord}_\mathfrak{p}((x))$ occuring in the prime decomposition of the principal fractional ideal (x).

The following corollary is a generalization of the “Principle (P)” used in the introduction.

Corollary (4.5). *Let R be a Dedekind domain, let $N \in \mathbf{Z}_{>0}$ and let $I_1, I_2, \ldots, I_m$ be non-zero ideals of R which are mutually coprime i.e. for which $I_i + I_j = R$ whenever $i \neq j$. If*

$$I_1 \cdot I_2 \cdot \ldots \cdot I_m = J^N$$

for some ideal J of R, then there exists for every $1 \leq i \leq m$, an ideal J_i such that $J_i^N = I_i$.

Proof. By Theorem 4.4 we can decompose the ideals I_i into a product of distinct prime ideals $\mathfrak{p}_{i,j}$:

$$I_i = \prod_{j=1}^{n_i} \mathfrak{p}_{i,j}^{e_{i,j}}.$$

We have that

$$I_1 \cdot I_2 \cdot \ldots \cdot I_m = \prod_{i=1}^{m} \prod_{j=1}^{n_i} \mathfrak{p}_{i,j}^{e_{i,j}} = J^N$$

Since the ideals I_i are mutually coprime, all the prime ideals ideals $\mathfrak{p}_{i,j}$ are distinct. By Theorem 4.4, the group of fractional ideals is a sum of copies of $\mathbf{Z}$. We conclude that all the exponents $e_{i,j}$ are divisible by N and hence that the ideals I_i are N-th powers of ideals, as required.

Definition. Let R be a Dedekind ring with field of fractions K. We define a map

$$\theta : K^* \longrightarrow \mathrm{Id}(R)$$

by $\theta(\alpha) = (\alpha)$. The image of θ is the subgroup $PId(R)$ of principal fractional ideals and the kernel of θ is precisely the group of units R^* of R. The cokernel of θ is called the *class group* of R:

$$Cl(R) = \mathrm{cok}(\theta) = Id(R)/PId(R).$$

In other words, there is an exact sequence

$$0 \longrightarrow R^* \longrightarrow F^* \xrightarrow{\theta} Id(R) \longrightarrow Cl(R) \longrightarrow 0.$$

The class group of a Dedekind ring measures how far R is from being a principal ideal domain. Fields and, more generally, principal ideal domains have trivial class groups. The analogue of the class group in algebraic geometry is the *Picard group.*For a smooth algebraic curve this is the divisor group modulo its subgroup of principal divisors [30, p.143].

One can show [14], that *every* abelian group is isomorphic to the class group $Cl(R)$ of some Dedekind domain R. We will show in section 7 that the class groups of rings of integers of number fields are always *finite.*

Proposition (4.6). *let R be a Dedekind ring. The following are equivalent:*
(i) The class group $Cl(R)$ is trivial.
(ii) Every fractional ideal of R is principal.
(iii) R is a principal ideal domain.
(iv) R is a unique factorization domain.

Proof. The implications *(i)* ⇒ *(ii)* ⇒ *(iii)* ⇒ *(iv)* are easy or standard. To prove that *(iv)* ⇒ *(i)* we first note that by Theorem 4.4 it suffices to show that every *prime* ideal is principal. Let, therefore, $\mathfrak{p}$ be a non-zero prime ideal and let $0 \neq \pi \in \mathfrak{p}$. Writing π as a product of irreducible elements and observing that $\mathfrak{p}$ is prime, we see that $\mathfrak{p}$ contains an irreducible element π'. The ideal (π') is a prime ideal. Since the ring R is a Dedekind ring, it has Krull dimension 1 and we conclude that $\mathfrak{p} = (\pi')$ Writing [illegible] num al

Proposition (4.7). *Let F be a number field and let I, J be non-zero ideals of its ring of integers O_F. Then*

$$N(IJ) = N(I)N(J).$$

Proof. By Theorem 4.4 it suffices to prove that

$$N(IM) = N(I)N(M).$$

for a maximal ideal M of O_F. From the exact sequence

$$0 \longrightarrow I/IM \longrightarrow R/IM \longrightarrow R/I \longrightarrow 0$$

we deduce that all we have to show, is that $\#(I/IM) = \#(R/M)$. The group I/IM is a vector space over the field R/M. Since, by Theorem 4.4 one has that $MI \neq I$, it is a non-trivial vector space. Let W be a subspace of I/IM. The reciprocal image of W in R is an ideal J with $IM \subset J \subset I$. This implies that $M \subset JI^{-1} \subset R$ and hence that $JI^{-1} = M$ or $JI^{-1} = R$. In other words $J = IM$ or $J = I$ and hence $W = 0$ or $W = I/IM$. So, apparently the vector space I/IM has only trivial subspaces. It follows that its dimension is one. This proves the proposition.

The next proposition is a very useful application of the multiplicativity of the norm map.

Proposition (4.8). *Let F be a number field of degree n.*

(i) For every ideal $\mathfrak{p}$ of O_F there exists a prime number p such that $\mathfrak{p}$ divides p. The norm of $\mathfrak{p}$ is a power of p.

(ii) Let $\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g}$ be the prime decomposition of the ideal generated by p in O_F. Then

$$\sum_{i=1}^{g} e_i f_i = n$$

where for every i the number f_i is defined by $N(\mathfrak{p}_i) = p^{f_i}$.

(iii) For every prime number p there are at most n distinct prime ideals of O_F dividing p.

(iv) There are only finitely many ideals with bounded norm.

Proof. *(i)* Let $\mathfrak{p}$ be a prime ideal. By Exer.3.E there exists an integer $m \neq 0$ in $\mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, it follows that $\mathfrak{p}$ contains a prime number p. So $\mathfrak{p}$ divides p and by Prop.4.7 $N(\mathfrak{p})$ divides $N(p) = p^n$.

(ii) This follows at once from the multiplicativity of the norm, by taking the norm of the prime decomposition of (p) in O_F.

(iii) This is immediate from *(ii)*.

(iv) This follows from Theorem 4.4 and *(iii)*.

The numbers f_i and e_i are called the inertia- and ramification index respectively, of the prime ideal $\mathfrak{p}_i$. If for a prime p and a number field F of degree n one has that $e_i = f_i = 1$ for all g primes $\mathfrak{p}_i$ that divide p we say that *p is totally split in F*. In this case there are n different prime ideals dividing p. They all have norm p. If $g = 1$, there is only one prime ideal $\mathfrak{p}_1$ dividing p. If, in this case $f_1 = 1$, we say that p is *totally ramified* in F over $\mathbf{Q}$. If, on the other hand, $e_1 = 1$, the prime p "remains" prime i.e. (p) is also a prime ideal in O_F.

Example. Let $F = \mathbf{Q}(\sqrt{-5})$. By Example 3.6 the ring of integers of F is equal to $\mathbf{Z}[\sqrt{-5}]$. We will factor some small prime numbers into prime ideals.

First we study the prime 2: since $O_F/(2) = \mathbf{Z}[T]/(2, T^2+5) = \mathbf{F}_2[T]/((T+1)^2)$ is not a domain, the ideal (2) is not prime in O_F. The reciprocal image of the ideal $(T + 1) \subset \mathbf{F}_2[T]/((T + 1)^2)$ is just $\mathfrak{p}_2 = (2, 1+\sqrt{-5})$ in O_F. It is easily checked that $\mathfrak{p}_2^2 = (2)$. This is the decomposition of (2). We see that 2 is ramified.

Consider the ideal (3) in O_F. Since $O_F/(3) = \mathbf{Z}[T]/(2, T^2+5) = \mathbf{F}_3[T]/((T+1)(T-1))$ is not a domain, we see that (3) is not prime. In fact the reciprocal images of the ideals $(T+1)$ and $(T-1)$ are prime ideals that divide (3). We let $\mathfrak{p}_3 = (3, T+1)$ and $\mathfrak{p}'_3 = (3, T-1)$ denote these ideals. One verifies easily that $(3) = \mathfrak{p}_3\mathfrak{p}'_3$ which gives us the prime decomposition of (3) in O_F.

One checks that 7 decomposes in a way similar to 3. The prime 11 remains prime since $O_F/(11) \cong \mathbf{F}_{11}[T]/(T^2+5)$. The decomposition of the prime numbers less than or equal to 11 is given in the following table:

Table.

p	(p)	
2	$\mathfrak{p}_2^2$	$\mathfrak{p}_2 = (2, 1+\sqrt{-5})$
3	$\mathfrak{p}_3\mathfrak{p}'_3$	$\mathfrak{p}_3 = (3, 1+\sqrt{-5})$ and $\mathfrak{p}'_3 = (3, 1-\sqrt{-5})$
5	$\mathfrak{p}_5^2$	$\mathfrak{p}_5 = (\sqrt{-5})$
7	$\mathfrak{p}_7\mathfrak{p}'_7$	$\mathfrak{p}_7 = (7, 3+\sqrt{-5})$ and $\mathfrak{p}'_7 = (7, -3+\sqrt{-5})$
11	(11)	11 is inert.

The number 6 has in the ring $\mathbf{Z}[\sqrt{-5}]$ two distinct factorizations into irreducible elements:

$$\begin{aligned} 6 &= 2 \cdot 3, \\ &= (1+\sqrt{-5})(1-\sqrt{-5}). \end{aligned}$$

The factors have norms 4,9 or 6. They are irreducible, for if they were not, than their divisors $a + b\sqrt{-5}$ would necessarily have norm 2 or 3. But this is impossible because, for trivial reasons, the Diophantine equations $a^2 + 5b^2 = 2$ and $a^2 + 5b^2 = 3$ do not have any solutions $a, b \in \mathbf{Z}$. there exists, however, a unique factorization of the ideal (6) in "ideal" prime factors. These prime factors are non-principal ideals. The factorization refines the two factorizations above:

$$(6) = \mathfrak{p}^2\mathfrak{p}_3\mathfrak{p}'_3.$$

Indeed, one has that $\mathfrak{p}_2\mathfrak{p}_3 = (1+\sqrt{-5})$ and $\mathfrak{p}_2\mathfrak{p}'_3 = (1-\sqrt{-5})$.

Finally we will apply Theorem 4.4 to the ζ-function $\zeta_F(s)$ of a number field F. First we consider the ζ-function of Riemann:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad \text{for } s \in \mathbf{C},\ \mathrm{Re}(s) > 1.$$

L. Euler (Swiss mathematician who lived and worked in Berlin and Petersburg 1707–1783) found an expression for $\zeta(s)$ in terms of an infinite product:

$$\zeta(s) = \prod_{p \text{ prime}} (1 - \frac{1}{p^s})^{-1} \qquad \text{for } s \in \mathbf{C},\ \mathrm{Re}(s) > 1\ .$$

This implies at once that $\zeta(s)$ does not have any zeroes in $\mathbf{C}$ with real part larger than 1. The proof of Euler's formula is as follows: let $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. Observe that

$$(1 - \frac{1}{p^s})^{-1} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \ldots$$

Since every positive integer can be written as a product of primes *in a unique way*, we find that for every $X \in \mathbf{R}_{>0}$

$$\prod_{p \leq X} (1 - \frac{1}{p^s})^{-1} = \sum_n \frac{1}{n^s}$$

where n runs over the positive integers that have only prime factors less than X. Therefore

$$|\sum_{n=1}^{\infty} \frac{1}{n^s} - \prod_{p \leq X} (1 - \frac{1}{p^s})^{-1}| \leq \sum_{n > X} \frac{1}{n^{\mathrm{Re}(s)}} \to 0$$

when $X \to \infty$. This follows from the fact that the sum converges for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. This implies Euler's formula.

Definition. Let F be a number field. The Dedekind ζ-function $\zeta_F(s)$ is given by

$$\zeta_F(s) = \sum_{I \neq 0} \frac{1}{\mathrm{N}(I)^s}$$

where I runs over the non-zero ideals of O_F. We see that for $F = \mathbf{Q}$ the Dedekind ζ-function $\zeta_{\mathbf{Q}}(s)$ is just Riemann's ζ-function. We will now study for which $s \in \mathbf{C}$ this sum converges.

Proposition (4.9). *Let F be a number field. Then*

$$\zeta_F(s) = \sum_{I \neq 0} \frac{1}{\mathrm{N}(I)^s} = \prod_{\mathfrak{p}} (1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s})^{-1}$$

where I runs over the non-zero ideals of O_F and $\mathfrak{p}$ over the prime ideals of O_F. The sum and the product converge for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$.

Proof. Let m be the degree of F and let $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. By Prop 4.8*(iii)* there are at most m prime ideals dividing a fixed prime number p. Therefore

$$|\sum_{\mathrm{N}(\mathfrak{p}) \leq X} \frac{1}{\mathrm{N}(\mathfrak{p})^s}| \leq m \sum_{p \leq X} \frac{1}{p^{\mathrm{Re}(s)}} \leq m \sum_{n \leq X} \frac{1}{n^{\mathrm{Re}(s)}}$$

where $\mathfrak{p}$ runs over the primes of O_F of norm at most X, where p runs over the prime numbers at most X and where n runs over the integers from 1 to n. Since the last sum converges, the first sum converges absolutely. Hence, by Exer.4.S the product

$$\prod_{\mathfrak{p}} (1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s})^{-1}$$

converges. Now we take $s \in \mathbf{R}_{>1}$. By Theorem 4.4 the ideals I admit a unique factorization as a product of prime ideals. This implies

$$\sum_{\mathrm{N}(I) \leq X} \frac{1}{\mathrm{N}(I)^s} \leq \prod_{\mathfrak{p}} (1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s})^{-1}$$

and we see, since the terms $\frac{1}{N(I)^s}$ are positive, that the sum converges. Moreover

$$|\sum_{I \neq 0} \frac{1}{\mathrm{N}(I)^s} - \prod_{\mathrm{N}(\mathfrak{p}) \leq X} (1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s})^{-1}| \leq \sum_{\mathrm{N}(I) > X} \frac{1}{\mathrm{N}(I)^{\mathrm{Re}(s)}} \to 0$$

when $X \to \infty$. This concludes the proof.

(4.A) If R is a Noetherian ring, then R/I is Noetherian for every ideal I of R.
(4.B) Is the ring $C^\infty(\mathbf{R}) = \{f : \mathbf{R} \to \mathbf{R} : f \text{ is a } C^\infty\text{-function}\}$ Noetherian?
(4.C) Show that every unique factorization domain is integrally closed.
(4.D) Let R be an integrally closed ring and let $f \in R[X]$ be irreducible over K, the field of fractions of R. Then f is irreducible over R.
(4.E) Show: let $R \subset S$ be an extension of commutative rings. Then an element $x \in S$ is integral over R if and only if there exists an R-module M of finite type such that $xM \subset M$ (Hint: Copy Lemma(3.1)).
(4.F) Consider the properties "Noetherian", "integrally closed" and "of Krull dimension 1" that characterize Dedekind domains. Give examples of rings that have two of these properties, but not the third.
(4.G) Prove the Chinese Remainder Theorem: let R be a commutative ring and suppose that I and J are two ideals of R that are relatively prime i.e. $I + J = R$. Then the canonical homomorphism

$$R/IJ \longrightarrow R/I \times R/J$$

is an isomorphism.
(4.H) Prove that every principal ideal domain is a Dedekind domain.
(4.I) Let I and J be two fractional ideals of a Dedekind domain.
(i) Show that $I \cap J$ and $I + J$ are fractional ideals.
(ii) Show that $I^{-1} + J^{-1} = (I \cap J)^{-1}$ and that $I^{-1} \cap J^{-1} = (I + J)^{-1}$.
(iii) Show that $I \subset J$ if and only if $J^{-1} \subset I^{-1}$.
(4.J) Let R be a Dedekind ring. Show:
(i) a fractional ideal contained in R is an ideal of R.
(ii) for $\alpha \in R$ and a fractional ideal I one has that $\alpha I \subset I$.
(iii) every fractional ideal I is of the form $m^{-1}J$ where $m \in \mathbf{Z}$ and J is an ideal of R.
(iv) if $I = (x)$ is a principal fractional ideal, then $I^{-1} = (x^{-1})$.
(4.K) Let I and J be fractional ideals of a Dedekind domain R. Let $n_\mathfrak{p}$ and $m_\mathfrak{p}$ be the exponents in their respective prime decompositions. Show that $I \subset J \Leftrightarrow n_\mathfrak{p} \geq m_\mathfrak{p}$ for all primes $\mathfrak{p}$.
(4.L) Let R be a Dedekind ring with only finitely many prime ideals. Show that R is a principal ideal ring.
(4.M) Show that in a Dedekind ring every ideal can be generated by at most two elements.
(4.N) Let R be a Dedekind ring. Show that every class in $Cl(R)$ contains an ideal of R.
(4.O) Let R be a Dedekind ring. Let S be a set of prime ideals of R. Let R' be the subset of the quotient field K of R defined by

$$R' = \{x \in K^* : (x) = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}} \quad \text{with } n_\mathfrak{p} \geq 0 \text{ for all } \mathfrak{p} not \in S\} \cup \{0\}.$$

Show that R' is a Dedekind ring.
(4.P) Let R be a Dedekind ring and let $\mathfrak{p}$ and $\mathfrak{p}'$ be two different non-zero prime ideals of R. Then $\mathfrak{p}+\mathfrak{p}' = R$.
(4.Q) Let A be an additively written abelian group, which is free with basis $\{e_\lambda : \lambda \in \Lambda\}$. Let $a_1, a_2, \ldots, a_m \in A$. Define the integers $\alpha_{i,\lambda}$ by $a_i = \sum_{\lambda \in \Lambda} \alpha_{i,\lambda} e_\lambda$. Suppose that for all $i \neq j$, the sets $\{\lambda \in \Lambda : \alpha_{i,\lambda} \neq 0\}$ and $\{\lambda \in \Lambda : \alpha_{j,\lambda} \neq 0\}$ have empty intersection. Suppose that

$$\sum_{i=1}^{m} a_i = Nv$$

from some $N \in \mathbf{Z}_{>0}$ and $v \in A$. Show that N divides every $\alpha_{i,\lambda}$.
(4.R) Let $R \hookrightarrow S$ be an extension of Dedekind domains. Show that, if S is an R-module of finite type, the canonical map $Id(R) \longrightarrow Id(S)$ is injective.

(4.S) Let $a_i \in \mathbf{R}_{\geq 0}$ for $i = 1, 2, \ldots$. Show that $\sum_i a_i$ converges if and only if $\prod_i (1 + a_i)$ converges.

(4.T) Show that $\mathbf{Q}^*_{>0}$ and the additive group of the ring $\mathbf{Z}[T]$ are isomorphic as abelian groups.

(4.U) Let F be a number field of degree n. Show that for every $q \in \mathbf{Q}^*$, the fractional ideal generated by q has norm q^n.

(4.V) Let F be a number field and let I be a fractional ideal of F. Show that there is a positive integer m such that mI is an ideal.

(4.W) Let F be a number field. For an ideal $I \subset O_F$ we put $\Phi(I) = \#(O_F/I)^*$. Show that $\sum_{I \subset J \subset R} \Phi(J) = N(I)$ and that $\Phi(I) = N(I) \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-1})$. Here the product runs over the prime ideals $\mathfrak{p}$ with $I \subset \mathfrak{p} \subset R$.

(4.X) Show that the ideal $I = (2, 2i) \subset \mathbf{Z}[2i]$ is not invertible, i.e. $I^{-1}I \neq R$.

5. Finitely generated abelian groups and lattices.

The contents of this section are not of a number theoretical nature. The results will be very important in the sequel. Our first subject are finitely generated abelian groups. We will determine the structure of these groups. We will expain the relation between indices of finitely generated free groups and determinants.

The second part of this section concerns *lattices.* Lattices are finitely generated groups with additional structure. We will explain the relations between indices of free groups and certain volumes.

An abelian group is said to be *free of rank n,* if it is isomorphic to $\mathbf{Z}^n$. A subgroup A of a free group $F \cong \mathbf{Z}^n$ is said to have rank m if the $\mathbf{Q}$-vector space generated by A in $F \otimes \mathbf{Q} \cong \mathbf{Q}^n$ has dimension m.

For any two integers α and β, the notation $\alpha|\beta$ means that α divides β.

Theorem (5.1). *Let $F \cong \mathbf{Z}^n$ be a free group of rank n and let $A \subset F$ be a subgroup. Then*

(i) The group A is free of rank $m \leq n$.

(ii) There exists a $\mathbf{Z}$-basis $e_1, \ldots, e_n$ of F and integers $\alpha_1, \ldots, \alpha_m \in \mathbf{Z}_{\geq 0}$ such that $\alpha_1|\alpha_2|\ldots|\alpha_m$ and $\alpha_1 e_1, \ldots, \alpha_m e_m$ is a basis for A. The integers $\alpha_1, \ldots, \alpha_m$ are unique.

Proof. Suppose $0 \neq A \subset F$. Consider the functionals $f : F \longrightarrow \mathbf{Z}$. For every $f : F \longrightarrow \mathbf{Z}$ we have that $f(A)$ is an ideal in $\mathbf{Z}$. This ideal is principal and it is generated by a unique $\alpha_f \geq 0$. Since $\mathbf{Z}$ is Noetherian, there is a maximal ideal in the collection of ideals $\{f(A) : f : F \longrightarrow \mathbf{Z}\}$. Since $A \neq 0$, this ideal $f(A)$ is not 0. Let α denote a positive generator and let $a \in A$ be an element for which $f(a) = \alpha$.

Now α divides $g(a)$ for every $g : F \longrightarrow \mathbf{Z}$: for suppose that $d = \gcd(g(a), \alpha)$ and let $u, v \in \mathbf{Z}$ such that $u\alpha + vg(a) = d$. Then d is the value of the functional $uf + vg$ at a. Since d divides α, it follows from the maximality of α that $d = \alpha$ and hence that α divides $g(a)$.

In particular, α divides all coordinates of a. We let $b = \frac{1}{\alpha}a$. We see that $f(b) = 1$ and moreover that

$$F = b\mathbf{Z} \oplus \ker(f),$$
$$A = a\mathbf{Z} \oplus (\ker(f) \cap A).$$

This follows easily from the fact that for every $x \in F$ one has that $x = f(x) \cdot b + x - f(x) \cdot b$. If, moreover, $x \in A$, then $f(x) \in a\mathbf{Z}$ by definition of a. We leave the easy verifications to the reader.

Now we prove *(i)* by induction with respect to the rank m of A. If $m = 0$ the statement is trivially true. If $m > 0$, we can split F and A as we did in the discussion above. The group $\ker(f) \cap A$ obviously has rank at most m. Since $A = a\mathbf{Z} \oplus (\ker(f) \cap A)$ has clearly strictly larger rank, we conclude that the rank of $\ker(f) \cap A$ is at most $m - 1$. By induction we see that this is a free group and consequently A is free as well. This proves *(i)*

Part *(ii)* is proved by induction with respect to n. If $n = 0$ the statement is trivially true. If $n > 0$, either $A = 0$, in which case the result is clear, or $A > 0$. In the latter case we can split F and A as explained above:

$$F = b\mathbf{Z} \oplus \ker(f),$$
$$A = a\mathbf{Z} \oplus (\ker(f) \cap A).$$

The group $\ker(f)$ has rank at most $n-1$. By *(i)* it is *free* of rank at most $n-1$. By induction there exists a basis $e_2, \ldots, e_n$ of $\ker(f)$ and integers $\alpha_2, \ldots, \alpha_m$ such that $\alpha_2 e_2, \ldots, \alpha_m e_m$ is a basis for $\ker(f) \cap A$. We now take $e_1 = b$ and $\alpha_1 = \alpha$. To complete the proof it suffices to verify that α divides α_2. If there is no e_2, there is nothing to prove. If there is, we define a functional g by $g(e_1) = g(e_2) = 1$ and $g(e_i) = 0$ for $i > 2$. We see that $\alpha \in g(A)$ and therefore, by maximality of α, that $g(A) = (\alpha)$. Since $\alpha_2 \in g(A)$ the result follows.

Corollary (5.2).
(i) For any finitely generated abelian group A there exist unique integers $r \geq 0$ and $\alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbf{Z}_{>1}$ satisfying $\alpha_1 | \alpha_2 | \ldots | \alpha_t$ and such that

$$A \cong \mathbf{Z}^r \times \mathbf{Z}/\alpha_1\mathbf{Z} \times \ldots \mathbf{Z}/\alpha_t\mathbf{Z}.$$

(ii) For any finite abelian group A there exist unique integers $\alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbf{Z}_{>1}$ with the property that $\alpha_1 | \alpha_2 | \ldots | \alpha_t$, such that

$$A \cong \mathbf{Z}/\alpha_1\mathbf{Z} \times \ldots \mathbf{Z}/\alpha_t\mathbf{Z}.$$

(iii) Let $F \cong \mathbf{Z}^n$ be a free group of rank n and let $H \subset F$ be a subgroup of F. Then H has finite index in F if and only if $\mathrm{rk}(H) = \mathrm{rk}(F)$.

Proof. *(i)* Let A be a finitely generated group and let n be an integer such that there is a surjective map

$$\theta : \mathbf{Z}^n \longrightarrow A.$$

By Theorem 5.1 there is a basis $e_1, \ldots, e_n$ of $\mathbf{Z}^n$ and there exist positive integers $\alpha_1 | \alpha_2 | \ldots | \alpha_m$ such that $\alpha_1 e_1 \ldots, \alpha_m e_m$ is a basis for $B = \ker(\theta)$. It follows at once that

$$A \cong \mathbf{Z}^{n-m} \times \mathbf{Z}/\alpha_1\mathbf{Z} \times \ldots \times \mathbf{Z}/\alpha_m\mathbf{Z}$$

as required. The uniqueness of the α_i's follows easily by considering A modulo $\alpha_i A$ for various i.
(ii) This is just *(i)* for a *finite* abelian group.
(iii) Choose a basis $e_1, \ldots, e_n$ of F such that the subgroup H has $\alpha_1 e_1, \ldots, \alpha_m e_m$ as a basis. We have that

$$F/H \cong \mathbf{Z}^{n-m} \times \mathbf{Z}/\alpha_1\mathbf{Z} \times \ldots \times \mathbf{Z}/\alpha_m\mathbf{Z}$$

and clearly $\mathrm{rk}(H) = \mathrm{rk}(F)$ if and only if $n = m$ if and only if $[F : H] = \#(F/H)$ is finite. This proves *(ii)*.

Corollary (5.3). *Let A be a $n \times n$-matrix with integral coefficients. Let $F = \mathbf{Z}^n$ and $H = A(F) \subset F$. Then*
(i) The index of H in F is finite if and only if $\det(A) \neq 0$.
(ii) If $\det(A) \neq 0$ then $[F : H] = |\det(A)|$.

Proof. According to Theorem 5.1 we can choose a basis $e_1, e_2, \ldots, e_n$ for F such that $H = \alpha_1 e_1 \mathbf{Z} \oplus \ldots \oplus \alpha_m e_m \mathbf{Z}$. With respect to this basis the matrix A becomes

$$A = \begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \end{pmatrix}$$

and we see that F/H is infinite if and only if one of the α_i is zero. This proves *(i)*. Part *(ii)* follows from the fact that $\det(A) = \prod_i \alpha_i$.

Next we apply the results on finitely generated abelian groups to number theory.

Corollary (5.4). *Let $f \in \mathbf{Z}[T]$ be a monic irreducible polynomial. Let α denote a zero and $F = \mathbf{Q}(\alpha)$. Then the index $[O_F : \mathbf{Z}[\alpha]]$ is finite and*

$$\mathrm{Disc}(f) = [O_F : \mathbf{Z}[\alpha]]^2 \cdot \Delta_F.$$

Proof. Let $\omega_1, \ldots, \omega_n$ denote a $\mathbf{Z}$-basis for the ring of integers of F. There is then a matrix M with integral coefficients such that

$$M(\omega_1, \ldots, \omega_n) = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1}).$$

Therefore

$$(\det(M))^2 \Delta_F = \Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$$

and hence, by Cor.5.3 and Prop.2.10

$$[O_F : \mathbf{Z}[\alpha]]^2 \Delta_F = \mathrm{Disc}(f)$$

as required.

Corollary (5.5). *Let F be a number field and let $\alpha \in F$. Then the norm of the O_F-ideal generated by α is equal to the absolute value of the norm of α:*

$$\mathrm{N}((\alpha)) = |\mathrm{N}(\alpha)|.$$

Proof. Let M_α denote the matrix which expresses the multiplication by α with respect to a $\mathbf{Q}$-basis of F. We have

$$\begin{aligned} |\mathrm{N}(\alpha)| &= |\det(M_\alpha)| && \text{by definition,} \\ &= [O_F : \mathrm{im}(A)] && \text{by Cor.5.3,} \\ &= \#O_F/(\alpha) = N((\alpha)). \end{aligned}$$

Many of the finitely generated groups that arise in algebraic number theory are equipped with extra structure. Very often they are, in natural way, lattices. In the rest of this section we will study lattices. We will show that the ring of integers O_F of an algebraic number field F admits a natural lattice structure. In section 7 we will see that, in a certain sense, the unit group O_F^* admits a lattice structure as well.

Definition. *Let V be a vector space over $\mathbf{R}$. A subset $L \subset V$ is called a lattice if there exist $e_1, \ldots, e_n \in L$ such that (i) $L = \sum_i \mathbf{Z} e_i$, and (ii) The e_i are a basis for V over $\mathbf{R}$.*

An easy example of a lattice is the group $\mathbf{Z}^n$ contained in the vector space $\mathbf{R}^n$. The following example is very important.

Example (5.6). *Let F be a number field. The image under Φ of the ring of integers O_F of F in $F \otimes \mathbf{R} = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ is a lattice.*

Proof. By Lemma 2.5 the map Φ maps $\mathbf{Q}$-bases of F to $\mathbf{R}$-bases of $F \otimes \mathbf{R}$. In particular, every $\mathbf{Z}$-base of O_F is mapped to an $\mathbf{R}$-base of $F \otimes \mathbf{R}$. This implies that $\Phi(O_F)$ is a lattice in $F \otimes \mathbf{R}$.

Proposition (5.7). *Let V be a real vector space and let $L \subset V$ be a subgroup. Then*
(i) L is a lattice.
(ii) L is discrete and cocompact.
(iii) L generates V over $\mathbf{R}$ and for every bounded set $B \subset V$ one has that $B \cap L < \infty$.

Proof. *(i) $\Rightarrow$ (ii)* This is almost obvious. We have that $V = \sum_i e_i\mathbf{R}$ and therefore V/F, being a continuous image of the compact space $\sum_i e_i[0,1]$ is compact.
(ii) $\Rightarrow$ (iii) Suppose L is discrete and cocompact. If L generates $W \subset_{\neq} V$ then there is a continuous surjection $V/L \longrightarrow V/W$. The vector space V/W is not compact and this contradicts the fact that V/L is compact. If there would be a bounded set B with $B \cap L$ infinite, then L could not be discrete.
(iii) $\Rightarrow$ (i) Since L generates V over $\mathbf{R}$, there is an $\mathbf{R}$-basis $e_1, \ldots, e_n \in L$ of V. The set $B = \sum_i e_i[0,1]$ is bounded and therefore the following sum is finite:

$$L = \sum_{x \in B \cap L} (x + \sum_i e_i\mathbf{Z}).$$

We conclude that the index $[L : \sum_i e_i\mathbf{Z}] = m$ is finite and that $mL \subset \sum_i e_i\mathbf{Z}$. By Theorem 5.1 the group mL is free and by Cor.5.2 it is of rank n. We conclude that L is free of rank m as well. This proves the proposition.

Corollary (5.8). *Let F be a number field. The image of a fractional ideal I under $\Phi : F \longrightarrow V_F$ is a lattice.*

Proof. Let $n \neq 0$ be an integer such that nI is an ideal. Let $0 \neq m \in I$ be an integer. We have that

$$\frac{m}{n}O_F \subset I \subset \frac{1}{n}O_F$$

Since the image of O_F in V_F is a lattice, so is the image of qO_F for every $q \in \mathbf{Q}^*$. We conclude that $\frac{m}{n}O_F$ and therefore I is cocompact and that $\frac{1}{n}O_F$ and therefore I is discrete. By Prop.5.7 the image of I is a lattice, as required.

Definition. *Let V be a real vectore space provided with a Haar measure. Let $L \subset V$ be a lattice. The covolume* covol(L) of L is defined by

$$\mathrm{covol}(L) = \mathrm{vol}(V/L)$$

where the volume is taken with respect to the Haar measure induced on the quotient group V/L.

It is easy to see that the covolume of $L = \sum_i \mathbf{Z}v_i \subset \mathbf{R}^n$ is also the volume of a socalled *fundamental domain* of V for L:

$$\mathrm{covol}(L) = \mathrm{vol}(\{\sum_i \lambda_i v_i : 0 \leq \lambda_i < 1 \text{ for } 1 \leq i \leq n\}).$$

Lemma (5.9). *Let $e_1, \ldots, e_n$ be the standard basis of $\mathbf{R}^n$, provided with the usual Haar measure. Let M be an $n \times n$-matrix with real coefficients. Let L be the subgroup generated by the image $M(e_1 \ldots e_n)$ of the basis. Then*
(i) L is a lattice if and only if $\det(M) \neq 0$.
(ii) If L is a lattice, then $\mathrm{covol}(L) = |\det(M)|$.

Proof. Clearly $\det(M) \neq 0$ if and only if the vectors $M(e_1), \ldots, M(e_n)$ span $\mathbf{R}^n$ and, therefore, if and only if L is a lattice. This proves *(i)*. Part *(ii)* is a standard fact from linear algebra: For any n vectors $v_1, \ldots, v_n \in \mathbf{R}^n$ the paralellopepid $\{\sum \lambda_i v_i : 0 \leq \lambda_i < 1 \text{ for } 1 \leq i \leq n\}$ has volume $|\det(M)|$.

For instance, the lattice $\binom{2}{0}\mathbf{Z}+\binom{1}{-2}\mathbf{Z} \in \mathbf{R}^2$ has covolume $\left|\det\left(\begin{smallmatrix} 2 & 1 \\ 0 & -2 \end{smallmatrix}\right)\right| = 4$. The next proposition gives the covolumes of the lattices $\Phi(O_F)$ and $\Phi(I)$ in $F \otimes \mathbf{R}$.

Proposition (5.10). *Let F be a number field of degree n. Let r_1 denote the number of distinct homomorphisms $F \hookrightarrow \mathbf{R}$ and $2r_2$ number of remaining homomorphisms $F \hookrightarrow \mathbf{C}$.*
(i) The covolume of the lattice O_F or rather $\Phi(O_F)$ in $F \otimes \mathbf{R}$ is given by

$$\mathrm{covol}(O_F) = 2^{-r_2}|\Delta_F|^{1/2}.$$

(ii) Let I be a fractional ideal, the covolume of I in $F \otimes \mathbf{R}$ is given by

$$\mathrm{covol}(I) = \mathrm{N}(I)2^{-r_2}|\Delta_F|^{1/2}.$$

Proof. As usual we identify the 2-dimensional vector space $\mathbf{C}$ with $\mathbf{R}^2$ via $z \mapsto (\mathrm{Re}(z), \mathrm{Im}(z))$. In this way we have that $F \otimes \mathbf{R} \cong \mathbf{R}^n$ and we find that

$$\Phi(O_F) = \begin{pmatrix} \phi_1(\omega_1) & \ldots & \mathrm{Re}\,\phi_k(\omega_1) & \mathrm{Im}\,\phi_k(\omega_1) & \ldots & \\ \phi_1(\omega_2) & \ldots & \mathrm{Re}\,\phi_k(\omega_2) & \mathrm{Im}\,\phi_k(\omega_2) & \ldots & \\ \vdots & \vdots & & \vdots & \vdots & \end{pmatrix}$$

here $\omega_1, \ldots, \omega_n$ denotes a $\mathbf{Z}$-basis for O_F and the ϕ_j denote the embeddings $F \hookrightarrow \mathbf{C}$ upto complex conjugation. In the proof of Lemma 2.5 the determinant of this $n \times n$-matrix has been calculated:

$$\begin{aligned} |\det| &= |(2i)^{-r_2}\det(\phi_i(\omega_j))| \\ &= 2^{-r_2}|\Delta_F|^{1/2} \end{aligned}$$

and hence

$$\mathrm{covol}(O_F) = 2^{-r_2}|\Delta_F|^{1/2}.$$

(ii) Using the notation of part *(i)* let $I \neq 0$ be a fractional ideal in O_F. By Exer.4.J*(iii)* there exists a non-zero integer m such that mI is an ideal in O_F. The ideal mI, being a subgroup of finite index of the free group O_F, is free of rank n. Let A be a matrix with integral coefficients such that

$$mI = A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

By Cor.5.3*(ii)* the absolute value of the determinant of A is equal to $[O_F : mI] = \mathrm{N}(mI) = m^n\mathrm{N}(I)$. As in *(i)*, we have that

$$\mathrm{covol}(mI) = \det\left(A \cdot \Phi(O_F)\right) = m^n N(I)2^{-r_2}|\Delta_F|^{1/2}.$$

By Exer.5.D we have that $\mathrm{covol}(mI) = m^n\mathrm{covol}(I)$, and the result follows.

(5.A) Let $A = \binom{3}{0}\mathbf{Z} + \binom{0}{5}\mathbf{Z} \subset \mathbf{Z}^2$. Find a basis of $\mathbf{Z}^2$ as in Theorem 5.1.

(5.B) Let H in $\mathbf{Z}^3$ be the subgroup generated by $(1,1,2)$, $(5,1,1)$ abd $(-1,-5,-3)$, What is the structure of $\mathbf{Z}^3/H$?

(5.C) Let $L = \{(x,y,z) \in \mathbf{Z}^3 : 2x + 3y + 4z \equiv 0 \pmod 7\}$. Show that $L \subset \mathbf{R}^3$ is a lattice. Find a $\mathbf{Z}$-basis and calculate its covolume.

(5.D) Let $L \subset \mathbf{R}^n$ be a lattice. Let A be an invertible $n \times n$-matrix. Show that $A(L)$ is alattice. Show that $\mathrm{covol}(A(L)) = |\det(A)|\mathrm{covol}(L)$. Let $m \in \mathbf{Z}_{>0}$; show that $\mathrm{covol}(mL) = m^n\mathrm{covol}(L)$.

(5.E) Identify the quaternions with $\mathbf{R}^4$ by letting $1, i, j, k$ correspond to the standard basis vectors $e_1, \ldots, e_4$. What is the covolume of the ring of Hurwitz integers in $\mathbf{H} \cong \mathbf{R}^4$?

(5.F) Let F be a number field. Suppose $R \subset F$ is a subring with the property that its image in $F \otimes \mathbf{R}$ is a lattice. Show that $R \subset O_F$.

(5.G) *(Euclidean imaginary quadratic rings.)* Let F be an imaginary quadratic number field. We identify O_F with its Φ-image in $F \otimes \mathbf{R} = \mathbf{C}$.

(i) Show that O_F is Euclidean for the norm if and only if the closed circles with radius 1 and centers in O_F cover $\mathbf{C}$.

(ii) Show that O_F is Euclidean for the norm if and only if $\Delta_F = -3, -4, -7$ or -11.

(iii) For real quadratic fields F (with $F \otimes \mathbf{R} = \mathbf{R}^2$) there is a similar result. It is due to Chatland and Davenport [13] and much harder to prove. The following is easier: show that the rings of integers of the rings of integers of the quadratic fields F with $\Delta_F = 5, 8$ and 12 are Euclidean for the norm.

(5.H)*Let L be a free abelian group of rank r. Let $Q(x)$ be a positive definite quadratic form on L. Supppose that for every $B \in \mathbf{R}$ there are only finitely many $x \in L$ with $Q(x) < B$. Then there is an injective map $I : L \hookrightarrow \mathbf{R}^r$ such that $i(L)$ is a lattice and $\|i(x)\| = Q(x)$. Here $\|v\|$ denotes the usual length of a vector $v \in \mathbf{R}^r$.

(5.I) Let $L \subset \mathbf{R}^n$ be a lattice. Show that

$$\lim_{t\to\infty} \frac{1}{(t)^n} \#\{(v_1, \ldots, v_n) \in L : |a_i| \leq t \quad \text{for all } 1 \leq i \leq n\} = \frac{2^n}{\mathrm{covol}(L)}.$$

(5.J)**(H.W. Lenstra)* Show that the ring $\mathbf{Z}[\zeta_m]$ is Euclidean with respect to the norm for all m with $\phi(m) \leq 8$. (Hint: Read [47,48]).

6. Discriminants, integers and ramification.

Any number field F can be written as $\mathbf{Q}(\alpha)$ where α is an algebraic integer. Consequently, the ring $\mathbf{Z}[\alpha]$ is a subring of O_F, which is of finite index by Cor.5.4. In this section we investigate under which conditions $\mathbf{Z}[\alpha] = O_F$, or more generally, which primes divide the index $[O_F : \mathbf{Z}[\alpha]]$. For primes that do *not* divide this index, one can find the prime ideals of O_F that divide p, from the decomposition of the minimum polynomial $f(T)$ of α in the ring $\mathbf{F}_p[T]$. This is the content of the Factorization Lemma.

Theorem (6.1). *(Factorization Lemma) Suppose $f \in \mathbf{Z}[T]$ is an irreducible polynomial. Let α denote a zero of f and let $F = \mathbf{Q}(\alpha)$. Let p be a prime number not dividing the index $[O_F : \mathbf{Z}[\alpha]]$. Suppose the polynomial f factors in $\mathbf{F}_p[T]$ as*

$$f(T) = h_1(T)^{e_1} \cdot \ldots \cdot h_g(T)^{e_g}$$

where the polynomials $h_1, \ldots, h_g$ are the distinct irreducible factors of f modulo p. Then the prime factorization of the ideal (p) in O_F is given by

$$(p) = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g},$$

where $\mathfrak{p}_i = (h_i(\alpha), p)$ and $N(\mathfrak{p}_i) = p^{\deg(h_i)}$.

Proof. We observe first that for any prime p we have that

$$\mathbf{Z}[\alpha]/(h_i(\alpha),p) \cong \mathbf{F}_p[T]/(h_i(T),f(T),p) \cong \mathbf{F}_{p^{\deg(h_i)}}.$$

Let $d = [O_F : \mathbf{Z}[\alpha]]$ and suppose p is a prime not dividing d. Let $a, b \in \mathbf{Z}$ such that $ap + bd = 1$. We claim that the map

$$O_F/\mathfrak{p}_i \xrightarrow{*bd} \mathbf{Z}[\alpha]/(g_i(\alpha),p)$$

is an isomorphism of rings. Note that $\mathfrak{p}_i$ is the ideal generated by p and $g_i(\alpha)$ *in* O_F. To prove our claim we first observe that the map is clearly well defined. It is a homomorphism since $(bdx)(bdy) - bdxy = bdxy(1-bd) = bdxyap$ for $x, y \in O_F$ and this is 0 modulo the ideal $(g_i(\alpha),p) \subset \mathbf{Z}[\alpha]$. The map is injective since, whenever $bdx \in (g_i(\alpha),p)$ then $x = (ap+bd)x = apx + bdx \in \mathfrak{p}_i$. Finally, the map is surjective since any $x \in \mathbf{Z}[\alpha]$ satisfies $x = (ap+bd)x \equiv bdx$.

We conclude that $\mathfrak{p}_i$ is a prime ideal of norm $p^{\deg(h_i)}$. Therefore

$$\mathrm{N}(\prod_i \mathfrak{p}_i^{e_i}) = p^{\sum_i \deg(h_i)e_i} = p^n$$

where $n = \deg(f)$. On the other hand, we have that

$$\prod_i \mathfrak{p}_i^{e_i} = \prod_i (g_i(\alpha),p)^{e_i} \subset (p).$$

Since $\mathrm{N}((p)) = p^n$, we have that $(p) = \prod_i \mathfrak{p}_i$ as required.

Corollary (6.2). *Let F be a number field. If p is a prime number that ramifies in F, then p divides the discriminant Δ_F or p divides the index $[O_F : \mathbf{Z}[\alpha]]$ for some integral α which generates F over $\mathbf{Q}$. In particular, only finitely many primes p are ramified in F.*

Proof. Suppose p ramifies and does not divide the index $[O_F : \mathbf{Z}[\alpha]]$. By the Factorization Lemma 6.1 the prime (p) splits as

$$(p) = \prod (g_i(\alpha),p)^{e_i}$$

where the e_i are the exponents occurring in the prime decomposition of $f(T) = \prod_i h_i(T)^{e_i}$ in $\mathbf{F}_p[T]$. We conclude that $e_i > 1$ for some index i and hence that the polynomial $f(T) \in \mathbf{F}_p[T]$ is not squarefree. This implies that its discriminant is 0. In other words p divides $\mathrm{Disc}(f)$ as required.

Example. Let $F = \mathbf{Q}(\alpha)$ where α is a zero of the polynomial $f(T) = T^3 - T - 1$. We have seen in section 2 that the discriminant of f is -23. Therefore the ring of integers of F is just $\mathbf{Z}[\alpha]$. By the Factorization Lemma, prime numbers p factor in $O_F = \mathbf{Z}[\alpha]$ just as $f(T) = T^3 - T - 1$ factors in the ring $\mathbf{F}_p[T]$.

Modulo 2 and 3, the polynomial $f(T)$ is irreducible; we conclude that the ideals (2) and (3) in O_F are prime. Modulo 5 the polynomial $f(T)$ has a zero and f factors as $T^3 - T - 1 = (T-2)(T^2+2T-2)$ in $\mathbf{F}_5[T]$. We conclude that $(5) = \mathfrak{p}_5\mathfrak{p}_5'$ where $\mathfrak{p}_5 = (5, \alpha - 2)$ is a prime of norm 5 and $\mathfrak{p}_5' = (5, \alpha^2 + 2\alpha - 2)$ is a prime of norm 25. The prime 7 is again prime in O_F and the prime 11 splits, similar to 5, as a product of a prime of norm 11 and of norm 121.

The following table contains this and some more factorizations of prime numbers. Notice the only ramified prime: 23. There are also primes that split completely in F over $\mathbf{Q}$. The prime 59 is the smallest example.

Table.

p	(p)	
2	(2)	
3	(3)	
5	$\mathfrak{p}_5\mathfrak{p}_{25}$	$\mathfrak{p}_5 = (\alpha - 2, 5)$ and $\mathfrak{p}_{25} = (\alpha^2 + 2\alpha - 2, 5)$
7	(7)	
11	$\mathfrak{p}_{11}\mathfrak{p}_{121}$	$\mathfrak{p}_{11} = (\alpha + 5, 11)$ and $\mathfrak{p}_{121} = (\alpha^2 - 5\alpha + 2, 11)$
13	(13)	
17	$\mathfrak{p}_{17}\mathfrak{p}_{289}$	$\mathfrak{p}_{17} = (\alpha - 5, 17)$ and $\mathfrak{p}_{289} = (\alpha^2 + 5\alpha - 10, 17)$
19	$\mathfrak{p}_{19}\mathfrak{p}_{361}$	$\mathfrak{p}_{19} = (\alpha - 6, 19)$ and $\mathfrak{p}_{361} = (\alpha^2 + 6\alpha - 3, 19)$
23	$\mathfrak{p}_{23}^2\mathfrak{p}'_{23}$	$\mathfrak{p}_{23} = (\alpha - 10, 23)$ and $\mathfrak{p}'_{23} = (\alpha - 3, 23)$
59	$\mathfrak{p}_{59}\mathfrak{p}'_{59}\mathfrak{p}''_{59}$	$\mathfrak{p}_{59} = (\alpha - 4, 59)$, $\mathfrak{p}'_{59} = (\alpha - 13, 59)$ and $\mathfrak{p}''_{59} = (\alpha + 17, 59)$

Proposition (6.3). *Let p be a prime and let $f(T) \in \mathbf{Z}[T]$ be an Eisenstein polynomial for the prime p. Let π be a zero of f and let $F = \mathbf{Q}(\pi)$ be the number field generated by π. Then $\mathbf{Z}[\pi]$ has finite index in O_F and p does not* divide this index.

Proof. By Cor.5.4 the index $[O_F : \mathbf{Z}[\pi]]$ is finite. Suppose that p divides the index. Consider the $\mathbf{F}_p[T]$-ideal $I = \{g \in \mathbf{F}_p[T] : \frac{1}{p}g(\alpha) \in O_F\}$. Note that this ideal is well defined and that it contains $f(T) \equiv T^n \pmod{p}$. Since p divides the index $[O_F : \mathbf{Z}[\pi]]$, there exists a polynomial $g(T) \in \mathbf{Z}[T]$ of degree less than n and with not all its coefficients divisible by p, such that $x = \frac{1}{p}g(\alpha) \in O_F - \mathbf{Z}[\pi]$. This shows that the ideal I is a *proper* divisor of T^n. Therefore $\frac{\pi^{n-1}}{p}$ is in O_F.

Let $f(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_1T + a_0 \in \mathbf{Z}[T]$ be the Eisenstein polynomial. From

$$-\pi^n = p\left(\frac{a_{n-1}}{p}\pi^{n-1} + \ldots + \frac{a_1}{p}\pi + \frac{a_0}{p}\right)$$

and the fact that a_0/p is prime to p, it follows that π^n divides p. This gives a contradiction and we conclude that p does not divide the index $[O_F : \mathbf{Z}[\pi]]$ as required.

Example (6.4). *Let p^n be a power of a prime p and let $F = \mathbf{Q}(\zeta_{p^n})$. The ring of integers of F is $\mathbf{Z}[\zeta_{p^n}]$.*

Proof. Clearly $\mathbf{Z}[\zeta_p]$ is contained in the ring of integers of $\mathbf{Q}(\zeta_{p^n})$. By Example 2.11, the discriminant of $\Phi_{p^n}(T)$ is a power of p. By Cor.5.4 we see that the only prime that could divide the index $[O_F^* : \mathbf{Z}[\zeta_p]]$ is p. Consider the minimum polynomial of ζ_{p^n}:

$$f_{\min}^{\zeta_p}(T) = \Phi_{p^n}(T) = T^{(p-1)p^{n-1}} + \ldots + T^{p^{n-1}} + 1.$$

It is easy to see that $\Phi_{p^n}(T+1)$ is an Eisenstein polynomial. We conclude from Prop.6.3 that p does not divide the index $[O_F^* : \mathbf{Z}[\zeta_p]]$. This completes the example.

The following two theorems will not be used in the sequel. They are included because they give complete answers to natural questions and because the proofs can easily be given using only the theory we have developed sofar. Theorem 6.5 is an extension of Prop.6.3. Theorem 6.6 makes part of Cor.6.2 more precise.

Theorem (6.5). *(Dedekind's Criterion.) Suppose α is an algebraic integer with minimum polynomial over $f(T) \in \mathbf{Z}[T]$. Let $F = \mathbf{Q}(\alpha)$. For p be a prime number, let $f_1, \ldots, f_g \in \mathbf{Z}[T]$ and $e_1, \ldots, e_g \in \mathbf{Z}_{\geq 1}$ such that $f = f_1^{e_1} \cdot \ldots \cdot f_g^{e_g}$ is the decomposition of f into distinct irreducible polynomials f_i modulo p. Then*

p divides the index $[O_F : \mathbf{Z}[\alpha]]$

if and only if there is an index j such that

$$f_j \textit{ divides } \left(\frac{f(T) - \prod_j f_j(T)^{e_j}}{p}\right) \qquad \textit{in } \mathbf{F}_p[T] \qquad \textit{and} \qquad e_j \geq 2.$$

Proof. We put

$$u(T) = \frac{f(T) - \prod_j f_j(T)^{e_j}}{p} \in \mathbf{Z}[T]$$

and for every index j we define the polynomial $F_j(T) \in \mathbf{Z}[T]$ by

$$F_j(T) = \frac{1}{f_j(T)} \prod_{j=1}^{g} f_j(T)^{e_j}.$$

Finally we let

$$x_j = \frac{1}{p} F_j(\alpha) = \frac{u(\alpha)}{f_j(\alpha)} \in F.$$

"if": Suppose that $f_j(T)$ divides $u(T)$ in $\mathbf{F}_p[T]$ and that $e_j \geq 2$ for some index j. Consider $x = x_j$. Clearly $px \in \mathbf{Z}[\alpha]$, but since $\deg(F_j) < \deg(f)$, we have that $x \notin \mathbf{Z}[\alpha]$. To prove that p divides the index $[O_F : \mathbf{Z}[\alpha]]$ it suffices to show that $x \in O_F$.

Consider the ideal $I = (f_j(\alpha), p) \subset \mathbf{Z}[\alpha]$. We have that $xp = F_j(\alpha)$ which is a $\mathbf{Z}[\alpha]$-multiple of $f_j(\alpha)$ because $e_j \geq 2$. We have that $xf_j(\alpha) = u(\alpha)$ which is a $\mathbf{Z}[\alpha]$-multiple of $f_j(\alpha)$ by assumption. The ideal I is a finitely generated abelian group. Lemma 3.1*(iii)* implies that x is integral. This proves the sufficiency.

"only if": Suppose that p divides the index of $\mathbf{Z}[\alpha]$ in O_F. Consider the $\mathbf{F}_p[T]$-ideal $J = \{h \in \mathbf{F}_p[T] : \frac{1}{p}h(\alpha) \in O_F\}$. This ideal clearly contains $f(T)$, but, by our assumption on the index, it is strictly larger than (f). Let ϕ be a generator of J and let j be an index such that

$$f_j(T) \text{ divides } \frac{f(T)}{\phi(T)} \qquad \text{in } \mathbf{F}_p[T].$$

We claim that this index j satisfies the conditions of the theorem.

To show this we consider again

$$x = x_j = \frac{1}{p} F_j(\alpha) = \frac{u(\alpha)}{f_j(\alpha)}.$$

Since ϕ divides F_j, we have that $x \in O_F$. We conclude that there exists a monic polynomial in $\mathbf{Z}[T]$ with $u(\alpha)/f_j(\alpha)$ as a zero. Therefore $f_j(\alpha)$ divides $u(\alpha)^m$ in $\mathbf{Z}[\alpha]$ for some integer $m \geq 1$. We conclude that there exists polynomials $h_1, h_2 \in \mathbf{Z}[T]$ such that

$$u(T)^m = f_j(T)h_1(T) + f(T)h_2(T)$$

and hence that $f_j(T)$ divides $u(T)^m$ in the ring $\mathbf{F}_p[T]$. Since $f_j(T)$ is irreducible modulo p, this implies that $f_j(T)$ divides $u(T)$ modulo p.

It remains to prove that $e_j \geq 2$. From $f_j(\alpha)x = u(\alpha)$ one concludes that $F_j\alpha) + f_j(\alpha)x = F_j\alpha) + u(\alpha)$ and hence that

$$x = \frac{u(\alpha) + F_j(\alpha)}{p + f_j(\alpha)}.$$

Exactly the same proof as before, now gives that $f_j(T)$ divides $u(T) + F_j(T)$ modulo p. Therefore $f_j(T)$ divides $F_j(T)$ and $e_j \geq 2$ as required.

Theorem (6.6). *(R. Dedekind) Let F be a number field and let p be a prime. Then p is ramified in F over $\mathbf{Q}$ if and only if p divides Δ_F.*

Proof. We introduce a slightly more general concept of "discriminant": let K be a field and let A be an n-dimensional commutative K-algebra, that is, a vector space over K of dimension n which is also a commutative ring satisfying $\lambda(ab) = (\lambda a)b = a(\lambda b)$ for all $a, b \in A$ and $\lambda \in K$. In section 2 we have studied the special case $K = \mathbf{Q}$ and A a number field F.

On A we define the *trace* $\mathrm{Tr}(x)$ of an element $x \in A$ by $\mathrm{Tr}(x) = \mathrm{Tr}(M_x)$ where M_x denotes the matrix of the multiplication-by-x-map with respect to some K-base of A. For $\omega_1, \ldots, \omega_n \in A$ we let

$$\Delta(\omega_1, \ldots, \omega_n) = \det(\mathrm{Tr}(\omega_i \omega_j))_{1 \le i,j \le n}.$$

In contrast to the situation in section 2, or Exer.2.Q, it may happen, in general that $\Delta(\omega_1, \ldots, \omega_n) = 0$ even if the ω_i constitute a K-basis for A. However, if this happens, it happens for *every* basis of A: as in section 2, the discriminant $\Delta(\omega_1, \ldots, \omega_n)$ of a *basis* $\omega_1, \ldots, \omega_n$ depends on the basis, but whether the discriminant is zero or not doesn't: the discriminant differs by a multiplicative factor $\det(M)^2$ where $M \in \mathrm{GL}_n(K)$ is the matrix transforming one basis into the other.

Using the fact that the non-nullity of the discriminant of a basis does not depend on the basis, we define the *discriminant of* A by

$$\Delta(A/K) = \Delta(\omega_1, \ldots, \omega_n)$$

for some K-basis $\omega_1, \ldots, \omega_n$ of A. It is only well defined upto a unit in K^*.

In Exer.6.J it is shown that for two finite dimensional K-algebras A and B one has that

$$\Delta(A \times B/K) = \Delta(A/K)\Delta(B/K).$$

Now we start the proof. Let F be a number field of degree n and let p be a prime number. Consider the field $K = \mathbf{F}_p$ and the n-dimensional K-algebra $O_F/(p)$. We are going to calculate the discriminant of $O_F/(p)$. First by reducing a $\mathbf{Z}$-basis of the ring of integers O_F modulo p:

$$\Delta(O_F/(p)/\mathbf{F}_p) \equiv \Delta_F \pmod{p}.$$

Next we decompose $O_F/(p)$ into a product of $\mathbf{F}_p$-algebras. Suppose p factors in O_F as

$$(p) = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g}.$$

By the Chinese Remainder Theorem (Exer.4.G) we have that

$$O_F/(p) \cong O_F/\mathfrak{p}_1^{e_1} \times \ldots \times O_F/\mathfrak{p}_g^{e_g}$$

and hence that

$$\Delta(O_F/(p)) = \Delta((O_F/\mathfrak{p}_1^{e_1})/\mathbf{F}_p) \cdot \ldots \cdot \Delta((O_F/\mathfrak{p}_g^{e_g})/\mathbf{F}_p).$$

By Exer.2.Q the discriminant $\Delta(\mathbf{F}_q/\mathbf{F}_p)$ is non-zero for every finite field extension $\mathbf{F}_q$ of $\mathbf{F}_p$. This shows that p does not divide Δ_F whenever p is not ramified.

To show the converse, it suffices to show that $\Delta((O_F/\mathfrak{p}^e)/\mathbf{F}_p) = 0$ whenever $\mathfrak{p}$ divides p and $e > 1$. Let therefore $e > 1$ and put $A = O_F/\mathfrak{p}^e$ and let $\pi \in \mathfrak{p}$ but not in $\mathfrak{p}^2$. Then π is nilpotent. Since it is not zero, we can use it as the first element in an $\mathbf{F}_p$-basis $\omega_1, \ldots, \omega_k$ of A. Clearly $\pi\omega_i$ is nilpotent for every $\omega_i \in A$. Since a nilpotent endomorphism has only eigenvalues 0, we see that the first row of the matrix $(\mathrm{Tr}(\omega_i \omega_j))_{1 \le i,j \le n}$ is zero. This concludes the proof of the Theorem.

(6.A) Let $F = \mathbf{Q}(\alpha)$ where α be a zero of the polynomial $T^3 - T - 1$. Show that the ring of integers of F is $\mathbf{Z}[\alpha]$. Find the factorizations in $\mathbf{Z}[\alpha]$ of the primes less than 10.

(6.B) Let d be a squarefree integer and let $F = \mathbf{Q}(\sqrt{d})$ be a quadratic field. Show that for *odd* primes p one has that p splits (is inert, ramifies) in F over $\mathbf{Q}$ if and only if d is a square (non-square, zero) modulo p.

(6.C) Let ζ_5 denote a primitive 5th root of unity. Determine the decomposition into prime factors in $\mathbf{Q}(\zeta_5)$ of the primes less than 14.

(6.D) Show that the following three polynomials have the same discriminant:

$$T^3 - 18T - 6,$$
$$T^3 - 36T - 78,$$
$$T^3 - 54T - 150.$$

Let α, β and γ denote zeroes of the respective polynomials. Show that the fields $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\beta)$ and $\mathbf{Q}(\gamma)$ have the same discriminants, but are not isomorphic. (Hint: the splitting behavior of the primes is not the same.)

(6.E) Show that $\mathbf{Z}[\sqrt[3]{20}, \sqrt[3]{50}]$ is the ring of integers of $F = \mathbf{Q}(\sqrt[3]{20})$. Show there is no $\alpha \in O_F$ such that $O_F = \mathbf{Z}[\alpha]$.

(6.F)*(Samuel) Let $f(T) = T^3 + T^2 - 2T + 8 \in \mathbf{Z}[T]$. Show that f is irreducible.

(i) Show that $\mathrm{Disc}(f) = -4 \cdot 503$. Show that the ring of integers of $F = \mathbf{Q}(\alpha)$ admits $1, \alpha, \beta = (\alpha^2 - \alpha)/2$ as a $\mathbf{Z}$-basis.

(ii) Show that O_F has precisely three distinct ideals of index 2. Conclude that 2 splits completely in F over $\mathbf{Q}$.

(iii) Show that there is no $\alpha \in F$ such that $O_F = \mathbf{Z}[\alpha]$. Show that for every $\alpha \in O_F - \mathbf{Z}$, the prime 2 divides the index $[O_F : \mathbf{Z}[\alpha]]$.

(6.G)*Simplify the p-part of the proof of Theorem 6.4 in the case that f is an Eisenstein polynomial with respect to p.

(6.H)*Show that for $m > 2$, the discriminant of $\mathbf{Q}(\zeta_m)$ is given by

$$(-1)^{\frac{1}{2}\phi(m)} \left(\frac{m}{\prod_{p|m} p^{1/overp-1}} \right)^{\phi(m)}.$$

(Hint: Exercise (3.L).)

(6.I)*Let $m \in \mathbf{Z}_{>0}$. Let K be a field, let A be the K-algebra $K[T]/(T^m)$. Compute the discriminant of A.

(6.J)*Let K be a field and let A and B be two finite dimensional K-algebras. Show that $\Delta(A \times B) = \Delta(A) \times \Delta(B)$.

7. The Theorems of Minkowski and Dirichlet.

In this section we prove the two important finiteness results of algebraic number theory. We prove that the unit group of the ring of integers of a number field is a finitely generated group and that its class group is finite. Both these general results are due to to P. Lejeune Dirichlet (German mathematician 1805–1859) [45]. We will prove both by means of techniques from the "geometry of numbers" a subject created by Hermann Minkowski (German mathematician 1864–1909) [56,57]. For a very thorough discussion of the subject and its history see the book by Lekkerkerker and Gruber [46].

Theorem (7.1). *(Minkowski's convex body theorem) Let $V \cong \mathbf{R}^n$ be a real vector space and let $L \subset V$ be a lattice. Let X be a bounded, convex, symmetric subset of V. If*

$$\mathrm{vol}(X) > 2^n \mathrm{covol}(L)$$

then there exists a non-zero vector $\lambda \in L \cap X$.

Proof. Consider the measure preserving natural map

$$X \longrightarrow V/2L.$$

Since $\mathrm{covol}(2L) = 2^n\mathrm{covol}(L)$ we see that $\mathrm{vol}(X) > \mathrm{vol}(V/2L)$. Therefore there are two points $x_1 \neq x_2$ in X which have the same image in $V/2L$. In other words $x_1 - x_2 \in 2L$. We conclude that $0 \neq y = (x_1 - x_2)/2 \in L$. By symmetry we have that $-x_2 \in X$ and hence, by convexity, that $y = (x_1 - x_2)/2 \in X$. So $0 \neq y \in X \cap L$ as required.

In the proof of the following lemma, we will calculate a certain volume. This will be useful in the proof of Theorem 7.3.

Lemma (7.2). *Let $r_1, r_2 \in \mathbf{Z}_{>0}$ and put $n = r_1 + 2r_2$. For every $R \geq 0$ put*

$$W(r_1, r_2, R) = \{(x_1, \ldots, x_{r_1}, y_1, \ldots, y_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} : |x_1| + \ldots + |x_{r_1}| + 2|y_1| + \ldots + 2|y_{r_2}| \leq R\}.$$

Then

$$\mathrm{vol}(W(r_1, r_2, R)) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{R^n}{n!}.$$

Proof. The proof is by induction with respect to n. If $r_1 = 1$ and $r_2 = 0$ and if $r_1 = 0$ and $r_2 = 1$, the result is easily verified. We will next discuss the two steps $r_1 \to r_1 + 1$ and $r_2 \to r_2 + 1$.

Case $r_1 \to r_1 + 1$

$$\begin{aligned}\mathrm{vol}(W(r_1+1, r_2, R)) &= \int_{-R}^{R} \mathrm{vol}(r_1, r_2, R - |t|)dt\\ &= 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{1}{n!}\int_{-R}^{R}(R - |t|)^n dt\\ &= 2^{r_1+1}\left(\frac{\pi}{2}\right)^{r_2}\frac{1}{n!}\int_{0}^{R} t^n dt\\ &= 2^{r_1+1}\left(\frac{\pi}{2}\right)^{r_2}\frac{R^{n+1}}{(n+1)!}.\end{aligned}$$

Case $r_2 \to r_2 + 1$

$$\begin{aligned}
\mathrm{vol}(W(r_1, r_2+1, R)) &= \int_{\substack{z\in\mathbf{C}\\|z|\leq R/2}} \mathrm{vol}(r_1, r_2, R - |z|)d\mu(z) \\
&= \int_0^{2\pi}\int_0^{R/2} 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{1}{n!}(R-2\rho)^n\rho d\rho d\phi \\
&= 2\pi 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{1}{n!}\int_0^R t^n\frac{(R-t)}{2}\frac{dt}{2} \\
&= 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{R^{n+2}}{(n+2)!}
\end{aligned}$$

This proves the lemma.

Theorem (7.3). *(Minkowski) Let F be a number field of degree n. Let r_1 denote the number of embeddings $F \hookrightarrow \mathbf{R}$ and $2r_2$ the remaining number of embeddings $F \hookrightarrow \mathbf{C}$. Then every non-zero ideal I of O_F contains an element x with*

$$|\mathrm{N}(x)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|\Delta_F|^{1/2}\mathrm{N}(I).$$

Proof. We view the ideal I via the map $\Phi : O_F \longrightarrow V_F$ as a lattice in $V_F = \mathbf{R}^{r_1}\times\mathbf{C}^{r_2}$. By Prop.5.10*(ii)* the covolume of I in V_F is

$$\mathrm{covol}(I) = 2^{-r_2}\mathrm{N}(I)|\Delta_F|^{1/2}.$$

For any positive real number R we put

$$X(R) = \{(x_1,\ldots,x_{r_1},y_1,\ldots,y_{r_2}) \in \mathbf{R}^{r_1}\times\mathbf{C}^{r_2} : |x_1| + \ldots + |x_{r_1}| + 2|y_1| + \ldots + 2|y_{r_2}| \leq R\}.$$

Using the triangle inequality one easily verifies that $X(R)$ is a convex, symmetric and bounded set. By Lemma 7.2 its volume is given by

$$\mathrm{vol}(X(R)) = \frac{R^n}{n!}\left(\frac{\pi}{2}\right)^{r_2}2^{r_1}.$$

From Minkowski's convex body Theorem 7.1 we conclude that *if*

$$\frac{R^n}{n!}(\frac{\pi}{2})^{r_2}2^{r_1} > 2^n\cdot 2^{-r_2}\mathrm{N}(I)|\Delta_F|^{1/2}$$

then there exists a non-zero element $x \in I\cap X(R)$. Since for every R the set $X(R)$ is bounded, and since the set $I\cap X(R)$ is finite, it follows that there is a vector $x\in I$ such that $x\in X(R)$ for *every* R satisfying this inequality. This vector x is also contained in $X(R_0)$ where R_0 satisfies the equality

$$\frac{R_0^n}{n!}\left(\frac{\pi}{2}\right)^{r_2}2^{r_1} = 2^n\cdot 2^{-r_2}N(I)|\Delta_F|^{1/2}.$$

By Prop.2.7*(iii)* and the arithmetic-geometric-mean-inequality (Exer.7.D), we have that

$$\begin{aligned}
|\mathrm{N}(x)| &= |x_1|\cdot\ldots|x_{r_1}||y_1|^2\cdot\ldots\cdot|y_{r_2}|^2, \\
&\leq \left(\frac{|x_1| + \ldots + |x_{r_1}| + 2|y_1| + \ldots + 2|y_{r_2}|}{n}\right)^n, \\
&\leq \frac{R_0^n}{n^n} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|\Delta_F|^{1/2}\mathrm{N}(I)
\end{aligned}$$

as required.

Corollary (7.4). *Let F be a number field of degree n. Then*
(i)

$$|\Delta_F| \geq \left(\frac{n^n}{n!}(\frac{\pi}{4})^{r_2}\right)^2.$$

(ii) $|\Delta_F| \geq \frac{\pi^n}{4}$. *In particular,* $|\Delta_F| > 1$ *whenever* $F \neq \mathbf{Q}$.
(iii) Every ideal class contains an ideal I with

$$|N(I)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|\Delta_F|^{1/2}.$$

(iv) The class group $Cl(O_F)$ is finite.

Proof. *(i)* It follows from the multiplicativity of the norm (Prop.4.6) that for every ideal I and $x \in I$, one has that $|\mathrm{N}(x)| \geq \mathrm{N}(I)$. Combining this with Theorem 7.3 gives *(i)*
(ii) One verifies (by induction) that $n^n \geq 2^{n-1}n!$ for all $n \geq 1$. It follows from *(i)* that

$$|\Delta_F| \geq \left(\frac{n^n}{n!}\right)^2\left(\frac{\pi}{4}\right)^{2r_2} \geq (2^{n-1})^2\left(\frac{\pi}{4}\right)^n = \frac{\pi^n}{4}.$$

(iii) Let c be an ideal class. Every ideal class contains integral ideals. Pick an integral ideal J in the inverse of the class of I. By Theorem 7.3 there exists an element $x \in J$ with

$$\left|N(xJ^{-1})\right| \leq \frac{n!}{n^n}\left(\frac{\pi}{4}\right)^{-r_2}|\Delta_F|^{1/2}.$$

Since the ideal xJ^{-1} is integral and in c, the result follows.
(iv) By Prop.4.8*(iii)* there are only a finite number of prime ideals of a given norm. Therefore, for every number B, there are only a finite number of integral ideals of norm less than B. The result now follows from *(iii)*.

The cardinality of the class group $Cl(O_F)$ is called the *class number* of O_F, or of F. It is denoted by

$$h_F = \#Cl(O_F).$$

The expression

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_F|}$$

associated to a number field F, with the usual notations, is called the *Minkowski constant* associated to F. Although $n!/n^n \approx e^{-n}\sqrt{2\pi n}$, it grows rapidly with the degree n of F.

The estimate in Cor.7.4*(i)* can be drastically improved. We only mention the most recent *asymptotic* estimates, i.e. when $n \to \infty$, since these are the easiest to state. Using Stirling's formula is is easy to see that Cor.7.4*(i)* implies that

$$\begin{aligned}|\Delta_F|^{1/n} &\geq \left(\frac{e^2\pi}{4}\right)\left(\frac{4}{\pi}\right)^{\frac{r_1}{n}}\\ &\geq (5.803)(1.273)^{\frac{r_1}{n}}.\end{aligned}$$

Using the Dedekind ζ-function $\zeta_F(s)$ of the number field F and especially its functional equation (see section 9) these estimates were improved by A.M. Odlyzko in 1976:

$$\begin{aligned}|\Delta_F|^{1/n} &\geq (4\pi e^{\gamma})e^{\frac{r_1}{n}},\\ &\geq (22.37)(2.718)^{\frac{r_1}{n}}.\end{aligned}$$

here $\gamma = 0.57721566490153\ldots$ is Euler's constant: $\gamma = \lim_{n\to\infty}(\sum_{k=1}^{n}\frac{1}{k} - \log(n))$.

Odlyzko's estimates are even better if the truth of certain generalized Riemann hypotheses (GRH) is assumed. See Serre's Note [66] and Poitou's Bourbaki talk [60] for more details.

$$\begin{aligned} |\Delta_F|^{1/n} &\geq (8\pi e^{\gamma})(e^{\frac{\pi}{2}})^{\frac{r_1}{n}} \qquad \text{(GRH)},\\ &\geq (44.76)(4.810)^{\frac{r_1}{n}} \qquad \text{(GRH)}. \end{aligned}$$

J. Martinet [51] exhibited an infinite number of totally complex fields F (i.e. with $r_2 = 0$), with $|\Delta_F|^{1/n} = 2^{3/2}11^{4/5}23^{4/5} = 92.37\ldots$. This indicates that Odlyzko's bounds are close to being optimal. Odlyzko's methods can be used to obtain estimates for discriminants of number fields of *finite* degree as well. This has been done by F. Diaz y Diaz, who published his results in a table[20].

Minkowski's Theorem can be used to calculate class groups of rings of integers of number fields. In the next section we will give some elaborate examples. Here we give two small examples.

Examples. *(i)* Take $F = \mathbf{Q}(\alpha)$ where α is a zero of the polynomial $f(T) = T^3 - T - 1$. In section 2 we have calculated the discriminant Δ_F of F. We have that $\Delta_F = \mathrm{Disc}(f) = -23$. It is easily verified that the polynomial $T^3 - T - 1$ has precisely one real zero. So $r_1 = 1$ and $r_2 = 1$. The bound in Minkowski's Theorem is now

$$\frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{23} \approx 1.356942.$$

Therefore, by Cor.7.4*(iii)*, every ideal class contains an integral ideal of norm less than or equal to 1. This shows, at once, that the class group of F is trivial. (By Exer.7.R the ring of integers $\mathbf{Z}[\alpha]$ is even Euclidean!)

(ii) Take $F = \mathbf{Q}(\sqrt{-47})$. By the example in section 2, the ring of integers of F is $\mathbf{Z}[\frac{1+\sqrt{-47}}{2}]$ and the discriminant of F satisfies $\Delta_F = -47$. Since $r_1 = 0$ and $r_2 = 1$ we find that the Minkowski constant is equal to

$$\frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{47} \approx 4.36444.$$

Therefore the class group is generated by the prime ideals of norm less than or equal to 4. To find these prime ideals explicitly, we decompose the primes 2 and 3 in O_F. Let $\alpha = \frac{1+\sqrt{-47}}{2}$. Then $\alpha^2 - \alpha + 12 = 0$. By the Factorization Lemma (Theorem 6.1) we see that $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ where $\mathfrak{p}_2 = (2, \alpha)$ and $\mathfrak{p}_2' = (2, \alpha - 1)$. Similarly $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ where $\mathfrak{p}_3 = (3, \alpha)$ and $\mathfrak{p}_3' = (3, \alpha - 1)$. We conclude that the only ideals of O_F of norm less than 4.36444 are O_F, $\mathfrak{p}_2$, $\mathfrak{p}_2'$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$, $\mathfrak{p}_2^2$, $\mathfrak{p}_2'^2$, $\mathfrak{p}_2\mathfrak{p}_2'$. Therefore the class number is at most 8.

Since $(2) = \mathfrak{p}_2\mathfrak{p}_2'$, the ideal classes of $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ are each others inverses: $\mathfrak{p}_2' \sim \mathfrak{p}_2^{-1}$. Similarly $\mathfrak{p}_3' \sim \mathfrak{p}_3^{-1}$. We conclude that the class group is generated by the classe of $\mathfrak{p}_2$ and $\mathfrak{p}_3$.

In order to determine the class group, we decompose some principal ideals into prime factors. Principal ideals (β) can be factored, by first factoring their norm $N(\beta) \in \mathbf{Z}$ and then determining the prime ideal divisors of (β). For the sake of convenience we take elements β of the form $\beta = \alpha - k$ where $k \in \mathbf{Z}$ is a small integer. By Exer.2.F we have that $\mathrm{N}(\beta) = \mathrm{N}(k - \alpha) = k^2 - k + 12$.

We find

Table.

	k	β	$\mathrm{N}(\beta)$	(β)
(i)	1	$1-\alpha$	$12 = 2^2 \cdot 3$	${\mathfrak{p}_2'}^2\mathfrak{p}_3'$
(ii)	2	$2-\alpha$	$14 = 2 \cdot 7$	$\mathfrak{p}_2\mathfrak{p}_7$
(iii)	3	$3-\alpha$	$18 = 2 \cdot 3^2$	$\mathfrak{p}_2'{\mathfrak{p}_3}^2$
(iv)	4	$4-\alpha$	$24 = 2^3 \cdot 3$	${\mathfrak{p}_2}^3\mathfrak{p}_3$
(v)	5	$5-\alpha$	$32 = 2^5$	${\mathfrak{p}_2'}^5$

From entry (i), we see that the ideal class of ${\mathfrak{p}'_2}^2\mathfrak{p}'_3 \sim (1)$ is trivial. The relation implies that

$$\mathfrak{p}_3 \sim \mathfrak{p}_2^{-1}.$$

We conclude that the class group is *cyclic.* It is generated by the class of $\mathfrak{p}_2$. We will now determine the order of this class. The second entry tells us that $\mathfrak{p}_7 \sim \mathfrak{p}_2^{-1}$ and is not of much use to us. Relation (iii) implies that

$$\mathfrak{p}_2 \sim \mathfrak{p}_3^2.$$

Combining this with the relation obtained from the first entry of our table, gives at once that

$$\mathfrak{p}_2^5 \sim 1.$$

This relation can also be deduced directly from entry (v) of the table. It follows that the class group is cyclic of order 5 or 1. The latter case occurs if and only if the ideal $\mathfrak{p}_2$ is principal. Suppose that for $a, b \in \mathbf{Z}$ the element $\gamma = a + b(1+\sqrt{-47})/2 \in O_F$ is a generator of $\mathfrak{p}_2$. Since the norm of $\mathfrak{p}_2$ is 2, we must have that

$$2 = \mathrm{N}(\mathfrak{p}_2) = |\mathrm{N}(\gamma)| = a^2 + ab + 12b^2.$$

Writing this equation as $(2a+b)^2 + 47b^2 = 8$, it is immediate that there are no solutions $a, b \in \mathbf{Z}$. We conclude that $\mathfrak{p}_2$ is not principal and that $Cl_{\mathbf{Q}(\sqrt{-47})} \cong \mathbf{Z}/5\mathbf{Z}$.

Corollary (7.6). *(J. Hermite, French mathematician 1822-1901) For any integer Δ, there are upto isomorphism only finitely many number fields F with $|\Delta_F| = \Delta$.*

Proof. Let $\Delta \in \mathbf{Z}$. By Cor.7.4*(ii)* there are only finitely many possible values for the degree n of F. There is, therefore, no loss in assuming that the degree n is fixed. Let F be a number field of degree n and discriminant Δ. Consider the following, bounded, convex and symmetric box B in $F \otimes \mathbf{R} = \{\mathbf{x} = (x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}\}$:

$$B = \begin{cases} \{\mathbf{x} : |x_1| \le \sqrt{|\Delta|} + 1 \text{ and } |x_i| < 1 \text{ for } i \ne 1\} & \text{if } r_1 > 0, \\ \{\mathbf{x} : |\mathrm{Re}(z_1)| \le 1,\ |\mathrm{Im}(z_1)| \le \sqrt{|\Delta|} + 1 \text{ and } |z_i| < 1 \text{ for } i \ne 1\} & \text{if } r_1 = 0. \end{cases}.$$

It is easily checked that the volume of B is $\pi^{r_2-1}(\sqrt{|\Delta|}+1)$ if $r_1 = 0$ and $2^n(\sqrt{|\Delta|}+1)$ otherwise. In each case $\mathrm{vol}(B)$ exceeds $2^n\mathrm{covol}(O_F)$. By Minkowski's Theorem 7.1, there exists $0 \ne \alpha \in O_F \cap B$. Since $\alpha \ne 0$, we have that $\mathrm{N}(\alpha) \ge 1$. Since $\alpha \in B$, we have that $|\phi_i(\alpha)| < 1$ for all $i > 1$. We conclude that $|\phi_1(\alpha)| \ge 1$.

We claim that $\phi_1(\alpha) \ne \phi_i(\alpha)$ for all $i \ge 2$. This is immediate if $r_1 > 0$, for all $\phi_i(\alpha)$ have absolute values strictly larger than $|\phi_1(\alpha)|$. If $r_1 = 0$, only $\phi_{r_2+1}(\alpha) = \overline{\phi_1(\alpha)}$ has the same absolute value as $\phi_1(\alpha)$. But, if $\phi_{r_2+1}(\alpha) = \phi_1(\alpha)$, then $\phi_1(\alpha)$ would be in $\mathbf{R}$ and hence $|\phi_1(\alpha)| = |\mathrm{Re}(\phi_1(\alpha))| < 1$, which leads to a contradiction.

Let $f(T)$ denote the minimum polynomial $f_{\mathrm{char}}(T)$ of α. By Prop.2.7*(i)*, the polynomial f has no double zeroes and we conclude from part *(ii)* of the same proposition that $f = f_{\mathrm{min}}$ and that $F = \mathbf{Q}(\alpha)$.

Since the zeroes $\phi_i(\alpha)$ of $f(T) = f_{\mathrm{char}}(T) = \prod_i (T - \phi_i(\alpha))$ have absolute values bounded by $\sqrt{|\Delta|}+1$, the coefficients of f can be bounded as well. Since the coefficients are in $\mathbf{Z}$, there are only finitely many possibilities for f and therefore, upto isomorphism, for F. This proves the corollary.

The final result of this section is the Dirichlet Unit theorem (p. Lejeune Dirichlet, German mathematician 1805–1859). Dirichlet's original proof employed the so-called "box principle". We give a proof by means of Minkowski's convex body theorem.

We introduce *modified* absolute values $\|x\|$ on $\mathbf{R}$ and $\mathbf{C}$:

$$\|x\| = \begin{cases} |x|, & \text{on } \mathbf{R}; \\ |x|^2, & \text{on } \mathbf{C}. \end{cases}$$

Definition. Let F be a number field of degree n with r_1 embeddings $\phi_i : F \hookrightarrow \mathbf{R}$ and r_2 remaining embeddings $\phi_i : F \hookrightarrow \mathbf{C}$. Let the homomorphism Ψ be given by:

$$\begin{aligned} \Psi : O_F^* &\longrightarrow \mathbf{R}^{r_1+r_2} \\ \varepsilon &\mapsto (\log\|\phi_1(\varepsilon)\|, \ldots, \log\|\phi_{r_1+r_2}(\varepsilon)\|) \end{aligned}$$

where $\phi_1, \ldots, \phi_{r_1}$ denote the real embeddings and $\phi_{r_1+1}, \ldots, \phi_{r_1+r_2}$ denote a set of mutually non-conjugate complex embeddings.

Theorem (7.7). *(P. Lejeune-Dirichlet) Using the notation above:*
(i) The kernel of Ψ is finite and equal to μ_F, the group of the roots of unity of F.
(ii) The image of Ψ is a lattice in the space $\{x \in \mathbf{R}^{r_1+r_2} :$ the sum of the coordinates of x is zero$\}$, which is of codimension 1 in $\mathbf{R}^{r_1+r_2}$.

Proof. *(i)* Let $\zeta \in \mu_F$ be a root of unity in F. Then there is an integer $n \neq 0$ such that $\zeta^n = 1$. this implies that $n\Psi(\zeta) = 0$ and hence that $\Psi(\zeta) = 0$. This shows that the roots of unity are in the kernel. Next we show that the kernel of Ψ is finite. This implies that $\ker(\Psi) = \mu_F$.

For any $\varepsilon \in \ker(\Psi)$ we have that $\|\phi(\varepsilon)\| = 1$ for all embeddings $\phi : F \longrightarrow \mathbf{C}$. Viewing O_F via the map Φ of section 2 as a lattice inside the vector space V_F, we see that the kernel of Ψ is contained in the *bounded* set B of points $(x_1, \ldots, x_{r_1}, y_1, \ldots, y_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ for which

$$\begin{aligned} |x_i| &\leq 1 \qquad \text{for } 1 \leq i \leq r_1, \\ |y_i| &\leq 1 \qquad \text{for } 1 \leq i \leq r_2. \end{aligned}$$

Prop 5.7 implies that $B \cap \Phi(O_F)$ is finite and therefore that $\ker(\Psi)$ is finite as required.
(ii) Let B be any bounded set in $\mathbf{R}^{r_1+r_2}$. Let B' be the box

$$\{(x_1, \ldots, x_{r_1+r_2}) : \quad |x_i| \leq R \quad \text{for } 1 \leq i \leq r_1 + r_2\}$$

where R is so large that $B \subset B'$. The elements $\varepsilon \in O_F^*$ that have $\Psi(\varepsilon) \in B'$ satisfy

$$|\phi_i(\varepsilon)| \leq \begin{cases} \exp(A), & \text{for real immersions } \phi_i; \\ \exp(A/2), & \text{for complex immersions } \phi_i. \end{cases}$$

Viewing O_F via Φ as a lattice in $F \otimes \mathbf{R}$, we see that the elements $\varepsilon \in O_F^*$ that satsify $\Psi(\varepsilon) \in B'$ are in a bounded box in V_F. Therefore there are only finitely many such ε and a fortiori there are only finitely many elements in $B' \cap \Psi(O_F^*)$. We conclude that $\Psi(O_F^*)$ is *discrete.*

By Exer.3.F, every unit $\varepsilon \in O_F^*$ has $N(\varepsilon) = \pm 1$. Therefore

$$\begin{aligned} 1 = |N(\varepsilon)| &= \prod_{\sigma : F \to \mathbf{C}} |\sigma(\varepsilon)| \\ &= \prod_{i=1}^{r_1+r_2} \|\sigma_i(\varepsilon)\| \end{aligned} .$$

This easily implies that $\Psi(O_F^*)$ is contained in the subspace of $\mathbf{R}^{r_1+r_2}$ of vectors that have the sum of their coordinates equal to zero.

To complete the proof, we must show that $\Psi(O_F^*)$ spans this vector space. This will be done by invoking two lemmas that will be stated and proved *after* the proof of this theorem.

Let $1 \leq i \leq r_1 + r_2$. By lemma 7.8 there exist non-zero integral elements $x_1, x_2, x_3, \ldots \in O_F$, such that $|\mathrm{N}(x_i)|$ is bounded by $\sqrt{|\Delta_F|} + 1$ and

$$\|\phi_j(x_1)\| > \|\phi_j(x_2)\| > \|\phi_j(x_3)\| > \ldots \qquad \text{for all } j \neq i.$$

By Prop.4.8*(iii)* there are only finitely many ideals in O_F with bounded norm. This implies that the collection of principal ideals (x_k) is finite. Therefore there exist at least two indices $j < j'$ such that $(x_j) = (x_{j'})$. We define the unit ε_i by

$$\varepsilon_i = \frac{x_{j'}}{x_j}.$$

By construction, ε_i satisfies

$$\|\phi_j(\varepsilon_i)\| < 0 \qquad \text{for all } j \neq i.$$

Consider the matrix with entries $a_{ij} = \log\|\phi_j(\varepsilon_i)\|$ where $1 \leq i, j \leq r_1 + r_2$. It satisfies $a_{ij} < 0$ whenever $i \neq j$ and $\sum_j a_{ij} = 0$. Therefore Lemma 7.9 implies that any $(r_1 + r_2 - 1) \times (r_1 + r_2 - 1)$-minor is invertible. This implies that the rank of $(a_{ij})_{i,j}$ is $r_1 + r_2 - 1$ and the theorem is proved.

Lemma (7.8). *Let F be a number field of degree n. Let $\phi_1, \ldots, \phi_{r_1}$ denote the different homorphisms $F \longrightarrow \mathbf{R}$ and $\phi_{r_1+1}, \ldots, \phi_{r_1+r_2}$ the remaining, pairwise non-conjugate, embeddings $F \longrightarrow \mathbf{C}$. Then there exists for each index $1 \leq i \leq r_1 + r_2$ a sequence of integers $\alpha_1, \alpha_2, \alpha_3, \ldots \in O_F - \{0\}$, with $|\mathrm{N}(\alpha_j)| \leq \sqrt{|\Delta_F|} + 1$ and*

$$\|\phi_j(\alpha_1)\| > \|\phi_j(\alpha_2)\| > \|\phi_j(\alpha_3)\| > \ldots$$

for all indices $j \neq i$.

Proof. Let i be an index with $1 \leq i \leq r_1 + r_2$. The existence of the α_j is proved by applying Minkowski's theorem to boxes that are "thin" in every direction except in the direction of the i-th coordinate. In this direction the box is so large that its volume is larger than $2^n \mathrm{covol}(O_F)$. We will contruct the integers $\alpha_j \in O_F$ inductively. We take $\alpha_1 = 1$. Suppose that $\alpha_1, \ldots, \alpha_m$ have been constructed. Let $\beta_j = \frac{1}{2}\|\phi_j(x_m)\|$ for $j \neq i$ and let $\beta_i \in \mathbf{R}$ be defined by the relation $\prod_j \beta_j = \sqrt{|\Delta_F|} + 1$.

Consider the box

$$B = \{(x_1, \ldots, x_{r_1+r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} : \|x_j\| \leq \beta_j \text{ for all } j \neq i\}.$$

This is a bounded, symmetric and convex subset of $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$. It has volume

$$\mathrm{vol}(B) = \prod_{j=1}^{r_1} (2\beta_j) \prod_{j=r_1+1}^{r_1+r_2} (\pi\beta_j) = 2^{r_1}\pi^{r_2}\sqrt{|\Delta_F|}$$

which is easily seen to exceed $2^n 2^{-r_2}\sqrt{|\Delta_F|} = 2^n \mathrm{covol}(O_F)$.

By Minkowski's Theorem (7.1), there is a non-zero element x in $B \cap O_F$, where we view, as usual, O_F as a lattice in the vector space $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ via the map Φ of (2.4). We take $x_{m+1} = x$ and we verify that

$$|\mathrm{N}(x)| = \prod_{j=1}^{r_1+r_2} |\phi_j(x)| \leq \prod_{j=1}^{r_1+r_2} \beta_j = \sqrt{|\Delta_F|} + 1,$$

$$\|\phi_j(x)\| \leq \beta_j = \frac{1}{2}\|\phi_j(x_m)\| < \|\phi_j(x_m)\|$$

This proves the theorem.

Lemma (7.9). *Let $(a_{ij})_{i,j}$ be an $m \times m$-matrix with real entries. Suppose that*

$$\begin{aligned} a_{ij} &< 0 && \textit{when } i \neq j, \\ \sum_j a_{ij} &> 0 && \textit{for all } i. \end{aligned}$$

Then $(a_{ij})_{i,j}$ has rank m.

Proof. Suppose that the rank of $(a_{ij})_{i,j}$ is less than m. Then there is a non-trivial relation $\sum_j \lambda_j a_{ij} = 0$ with not all $\lambda_j \in \mathbf{R}$ equal to zero. Suppose λ_k has the largest absolute value of the λ_j. Since we can multiply the relation by -1, we may assume that $\lambda_k > 0$. We have that $\lambda_k \geq \lambda_j$ for all indices j. Therefore $\lambda_k a_{ik} \leq \lambda_i a_{ik}$ for *all* indices i, including $i = k$. Taking the sum over i, we find

$$0 < \lambda_k \sum_{i=1}^{m} a_{ik} = \sum_{i=1}^{m} \lambda_k a_{ik} \leq \sum_{i=1}^{m} \lambda_i a_{ik} = 0.$$

This contradiction proves the lemma.

Corollary (7.10). *Let F be a number field with precisely r_1 distinct embeddings $F \hookrightarrow \mathbf{R}$ and $2r_2$ remaining embeddings $F \hookrightarrow \mathbf{C}$. Then*

(i) There exist a set of so-called fundamental units $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1} \in O_F^*$ such that

$$O_F^* = \{\zeta^m \varepsilon_1^{n_1} \cdot \ldots \cdot \varepsilon_{r_1+r_2-1}^{n_{r_1+r_2-1}} : n_1, \ldots, n_{r_1+r_2-1}, m \in \mathbf{Z}\}.$$

(ii) There is an isomorphism of abelian groups

$$O_F^* \cong (\mathbf{Z}/w_F\mathbf{Z}) \times \mathbf{Z}^{r_1+r_2-1}.$$

here w_F denotes the number of roots of unity in F.

Proof. By Theorem 7.6, we can choose $r_1 + r_2 - 1$ units ε_i in O_F^* such that the vectors $\Psi(\varepsilon_i)$ span the lattice $\Psi(O_F^*)$. For an arbitrary unit $u \in O_F^*$ there exist integers $n_1, \ldots, n_{r_1+r_2-1}$ such that

$$\Psi(u) = n_1\Psi(\varepsilon_1) + \ldots + n_{r_1+r_2-1}\Psi(\varepsilon_{r_1+r_2-1})$$

By Theorem 7.6*(i)* we see that $u\varepsilon^{-n_1} \cdot \ldots \cdot \varepsilon_{r_1+r_2-1}^{-n_{r_1+r_2-1}}$ is in the kernel of Ψ and therefore a root of unity. This proves *(i)*. Part *(ii)* follows from the fact that the roots of unity are algebraic integers and form a cyclic group.

Definition (7.11). Let F be a number field of degree n and let $\phi_1, \ldots, \phi_{r_1+r_2}$ be the homomorphisms $F \longrightarrow \mathbf{C}$ as in Lemma 7.8. The *regulator* R_F of F is defined by

$$|\det(\log\|\phi_j(\varepsilon_i)\|)_{i,j}|$$

where $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1}$ are a set of fundamental units and the ϕ_j run over the homomorphisms in the set $\{\phi_1, \ldots, \phi_{r_1+r_2}\}$ except one.

The regulator R_F of a number field F is well defined. See Exer.7.M for a proof that the value of R_F does not depend on the homomorphism ϕ_i that one leaves out in Definition.7.11.

Example. (7.12). Consider the field $F = \mathbf{Q}(\sqrt{257})$. We have that $r_1 = 2$ and $r_2 = 0$. Since F admits embeddings into $\mathbf{R}$, the group of roots of unity in F is $\{\pm 1\}$. By Dirichlet's Unit Theorem we therefore have that

$$O_F^* \cong \varepsilon^{\mathbf{Z}} \times \{\pm 1\}.$$

We will determine the class group $Cl(O_F)$ and the unit group of O_F together. By Example 3.3, the ring of integers of F is equal to $\mathbf{Z}[\alpha]$ where $\alpha = (1+\sqrt{257})/2$. By Example 3.6, the discriminant of F is 257. Minkowski's constant for F is easily calculated to be equal to

$$\frac{2^2}{2!}\sqrt{257} \approx 8.01.$$

The minimum polynomial of α is easily seen to be $f(T) = T^2 - T - 64$. We first substitute a few integers n into f. In order to obtain small values of $f(n)$, we choose n close to the zero $(1+\sqrt{257})/2 \approx 8.5 \in \mathbf{R}$:

Table.

	n	β	$f(n) = \mathrm{N}(\beta)$	(β)
(i)	5	$\alpha - 5$	$-44 = -4 \cdot 11$	$\mathfrak{p}_2'^{\,2}\mathfrak{p}_{11}'$
(ii)	6	$\alpha - 6$	$-34 = -2 \cdot 17$	$\mathfrak{p}_2\mathfrak{p}_{17}$
(iii)	7	$\alpha - 7$	$-22 = -2 \cdot 11$	$\mathfrak{p}_2'\mathfrak{p}_{11}$
(iv)	8	$\alpha - 8$	$-8 = -2^3$	${\mathfrak{p}_2}^3$
(v)	9	$\alpha - 9$	$8 = 2^3$	$\mathfrak{p}_2'^{\,3}$
(vi)	10	$\alpha - 10$	$26 = 2 \cdot 13$	$\mathfrak{p}_2'\mathfrak{p}_{13}$
(vii)	11	$\alpha - 11$	$46 = 2 \cdot 23$	$\mathfrak{p}_2'\mathfrak{p}_{23}$

Since non of the numbers $f(n)$ is divisible by 3,5 or 7, we conclude that f has no zeroes modulo 3,5 or 7. By the Factorization Lemma 6.1, we conclude that the ideals (3), (5) and (7) are prime in O_F. Therefore, the only primes having norm less than 8.01 in O_F are the prime divisors $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ of 2. From the Factorization Lemma we deduce that $\mathfrak{p}_2 = (\alpha, 2)$ and $\mathfrak{p}_2' = (\alpha - 1, 2)$.

Since the classes of $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ are inverse to one another in the class group, we conclude that the class group of O_F is cyclic. It is generated by the class of $\mathfrak{p}_2$. From entry (iv) or (v) of the table, it is immediate that

$$\mathfrak{p}_2^3 \sim 1$$

and we see that $Cl(O_F)$ is cylic of order 3 or 1. The class group is trivial if and only if $\mathfrak{p}_2$ is principal. If $\mathfrak{p}_2$ were principal and $\gamma = a + b(1+\sqrt{257})/2$, with $a, b \in \mathbf{Z}$ would be a generator, we would have the following equation:

$$\pm 2 = \mathrm{N}(\gamma) = a^2 + ab - 64b^2.$$

This Diophantine equation is not so easy to solve directly, so we proceed in a different way. We will need to know the unit group O_F^* first.

From the 4th and 5th line of the table we deduce the following decomposition into prime ideals:

$$((\alpha - 8)(\alpha - 9)) = {\mathfrak{p}_2}^3\mathfrak{p}_2'^{\,3}$$

Since we also have that $(8) = {\mathfrak{p}_2}^3\mathfrak{p}_2'^{\,3}$, we see that the principal ideals $((\alpha - 8)(\alpha - 9))$ and (8) are equal. Therefore their generators differ by a unit $\varepsilon \in O_F$. Taking norms, we see that $\mathrm{N}(\varepsilon) = -1$ and we conclude that $\varepsilon \neq \pm 1$. We find, in fact, that

$$\varepsilon = \frac{(\alpha - 8)(\alpha - 9)}{8} = -2\alpha + 17 = 16 - \sqrt{257}.$$

However, it is not yet clear that ε is a fundamental unit in the sense of Dirichlet's Unit Theorem. It could be that there is another unit $u \in O_F^*$ such that $\varepsilon = \pm u^k$ form some $k \geq 2$. We will show that this is not the case and that, actually, $O_F^* = \pm\varepsilon^{\mathbf{Z}}$. But in order to determine the class group of O_F it is not necessary to know this. It appears to be sufficient to know that ε generates O_F^* *modulo cubes.* This is, in general, much easier to check. In this case we check it by considering ε modulo the prime ideal $(5) \subset O_F$: the multiplicative group of the residue class field has 24 elements and $x \in O_F/(5)$ is a cube if and only if $x^8 \equiv 1$. We have that

$$\varepsilon^8 \equiv (16 - \sqrt{257})^3(16 + \sqrt{257}) \equiv \mathrm{N}(\varepsilon)(1 - \sqrt{2})^2 = -(3 - 2\sqrt{2}) \not\equiv 1.$$

This shows that ε is not a cube mod 5 and therefore not a cube in O_F. We conclude that ε generates O_F^* modulo cubes.

First we will determine the class group of O_F, and then the unit group O_F^*.

Suppose the class group $Cl(O_F)$ is trivial. We then have that $\mathfrak{p}_2 = (\gamma)$ and by entry (iv) of the table that $\gamma^3 = u(\alpha - 8)$ for some unit u. Here γ is only determined upto a unit and, consequently, the unit u is only determined upto a cube of a unit. Therefore we may assume that

$$\gamma^3 = \varepsilon^k(\alpha - 8) \qquad \text{for some } k \in \mathbf{Z}.$$

This implies that for every ideal $I \subset O_F$, which is prime to $\mathfrak{p}_2$, we have that

$$\alpha - 8 \equiv 1 \in (O_F/I)^*/H$$

where H is the subgroup generated by $((O_F/I)^*)^3$ and the image of O_F^* modulo I. We check this modulo the ideal $I = (13)$. The prime 13 splits as $(13) = \mathfrak{p}_{13}\mathfrak{p}'_{13}$, where $\mathfrak{p}_{13} = (13, \alpha - 4)$ and $\mathfrak{p}'_{13} = (13, \alpha + 3)$.

We have the following isomorphism of groups

$$(O_F/I)^*/((O_F/I)^*)^3 \cong \mathbf{F}_{13}^*/(\mathbf{F}_{13}^*)^3 \times \mathbf{F}_{13}^*/(\mathbf{F}_{13}^*)^3 \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}.$$

given by $z \mapsto (z \pmod{\mathfrak{p}_{13}}), z \pmod{\mathfrak{p}'_{13}})$ and $(2^x, 2^y) \mapsto (x \pmod 3), y \pmod 3))$ respectively.

The image of $\varepsilon = -2\alpha + 17$ in the ring is $(-2 \cdot (-4) + 17, -2 \cdot (3) + 17) = (8, 11) \mapsto (0, 1) \in \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. The image of $\alpha - 8$, however is $(4 - 8, -3 - 8) = (9, 2) \mapsto (2, 1)$. We conclude that $\alpha - 8$ and ε generate distinct subspaces. Therefore $\alpha \notin H$ and the class group $Cl(O_F)$ has order 3.

Finally we determine the unit group of O_F. We will show that $O_F^* = \{\pm\varepsilon^k : k \in \mathbf{Z}\}$. Consider $\varepsilon \in F \subset F \otimes \mathbf{R} \cong \mathbf{R} \times \mathbf{R}$. The absolute values of $|\phi_1(\varepsilon)|$ and $|\phi_2(\varepsilon)|$ are $32.0312\ldots$ and $0.0312\ldots$ respectively. If ε would not be a fundamental unit in the sense of Dirichlet's Unit Theorem, then there would be a unit u with $\varepsilon = \pm u^k$ for $|k| \geq 2$. This would imply that the absolute values of u satisfy $|\phi_{1,2}(u)| \leq \sqrt{32.04} \leq 5.7$. It is easily checked, that there are no units in O_F satisfying these conditions. This completes the example.

(7.A) Show that $\mathbf{Z}[\sqrt{-163}]$ has trivial class group and that $\mathbf{Z}[\sqrt{-71}]$ has class group isomorphic to $\mathbf{Z}/7\mathbf{Z}$.

(7.B) Show that the class group of $\mathbf{Q}(\alpha)$ where α is a zero of the polynomial $T^3 + T - 1$ is trivial.

(7.C) Compute the class group of $F = \mathbf{Q}(\sqrt{229})$. Find the units of O_F.

(7.D) Prove the arithmetic-geometric-mean inequality: let $a_1, \ldots, a_n \in \mathbf{R}_{\geq 0}$ then

$$(a_1 \cdot \ldots \cdot a_n)^{1/n} \leq \frac{a_1 + \ldots + a_n}{n}.$$

The equality holds if and only if $a_1 = \ldots = a_n$.(Hint: let $A = \frac{a_1 + \ldots + a_n}{n}$. Show that $e^{\frac{a_i}{A} - 1} \geq \frac{a_i}{A}$ for every i, with equality if and only if $a_i = A$.)

(7.E) Let F be a number field of degree n. Show that $R_F\sqrt{n} = \mathrm{covol}(O_F^*)$. here we view O_F^* via the map Ψ as a lattice in the subspace of vectors in $\mathbf{R}^{r_1+r_2}$ that have the sum of their coordinates equal to 0.

(7.F) Show that the class group of $\mathbf{Q}(\zeta_{11})$ is trivial.

(7.G) Let $f(T) \in \mathbf{Z}[T]$. Show: if $\mathrm{Disc}(f) = 1$, then $f(T) = (T-k)(T-k-1)$ for some $k \in \mathbf{Z}$.

(7.H) Show that if the rank of the unit group O_F^* of a number field F is 1, then $[F : \mathbf{Q}] = 2$, 3 or 4.

(7.I) Show that the ring $\mathbf{Z}[(1+\sqrt{19})/2]$ is *not* Euclidean, but admits unique factorization.

(7.J) (*Pell's equation.*) Show that for every positive integer d the equation

$$X^2 - dY^2 = 1$$

has solutions $X, Y \in \mathbf{Z}_{>0}$.

(7.K) Let $f(T) \in \mathbf{Z}[T]$ be a polynomial all of whose roots in $\mathbf{C}$ are on the unit circle. Show that all roots of f are roots of unity.

(7.L) Let $\eta \in \mathbf{C}$ be a sum of roots of unity. Show that if $|\eta| = 1$, then η is a root of unity.

(7.M) Let F be a number field.

(i) Show that the regulator R_F is well defined, i.e. it does not depend on the choice of the embedding $\phi_i : F \to \mathbf{C}$ that was left out in Definiton.7.11.

(ii) For $1 \leq i \leq r_1 + r_2$, let π_i denote the projection of $\mathbf{R}^{r_1+r_2}$ onto the subspace generated by all basis vectors except the i-th. Show that π_i restricted to $\Psi(O_F^*)$ is injective.

(7.N) Show that the ring $\mathbf{Z}[\sqrt{-61}]$ that was encountered in the introduction, has class number 6.

(7.O) Show that the Diophantine equation $Y^2 = X^3 - 5$ has no solutions $X, Y \in \mathbf{Z}$. (Hint: show that $\mathbf{Z}[\sqrt{-5}]$ has class number 2.)

(4.P) Show that $\mathbf{Q}(\sqrt{2})^*$ and $\mathbf{Q}(\sqrt[3]{2})^*$ are isomorphic abelian groups.

(7.Q)*Show that for every number field F there is a prime that is ramified in F over $\mathbf{Q}$.

(7.R)*Let F be a number field. Show that if

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |\Delta_F|^{1/2} < 2$$

then the ring of integers O_F is a Euclidean for the norm $|\mathrm{N}(x)|$. (Hint: Let $x \in F \otimes \mathbf{R}$. Show, using the notation of the proof of Theorem 7.3, that the set $X(R) \cup (X(R) + x)$ with $R = n$ has a volume which is larger than $2^n\mathrm{covol}(O_F)$. Show that it contains a lattice point.)

8. Examples.

In this section we illustrate the theory of the preceding sections by means of three elaborate examples.

Example (8.1). (*The Number Field Sieve*) Let $F = \mathbf{Q}(\sqrt[5]{2})$. The discriminant of the minimum polynomial $T^5 - 2$ of $\sqrt[5]{2}$ is easily seen to be equal to $50\,000 = 2^4 5^5$. Since $T^5 - 2$ is an Eisenstein polynomial for the prime 2 and $(T + 2)^5 - 2$ is Eisenstein for 5, we conclude from Prop.6.3 that $\mathbf{Z}[\sqrt[5]{2}]$ is the ring of integers of F.

Since the roots of $T^5 - 2$ differ by 5th roots of unity, there is only one embedding $F \hookrightarrow \mathbf{R}$. Therefore $r_1 = 1$ and $r_2 = 2$. Minkowski's constant is equal to

$$\frac{5!}{5^5}\left(\frac{4}{\pi}\right)^2 \sqrt{50\,000} = 13.919\ldots.$$

By Cor.7.4*(iii)*, the class group of F is generated by the ideal classes of the primes of norm less than 13.919. We use the Factorization Lemma 6.1 to determine those primes: we already observed that $T^5 - 2$ and $(T - 2)^5 - 2$ are Eisenstein polynomials with respect to the primes 2 and 5 respectively. We conclude that both 2 and 5 are totally ramified in F over $\mathbf{Q}$:

$$(2) = \mathfrak{p}_2^5 \qquad \text{and} \qquad (5) = \mathfrak{p}_5^5.$$

To study the decomposition of the other primes p in F, we consider the map $\mathbf{F}_p^* \longrightarrow \mathbf{F}_p^*$ given by $x \mapsto x^5$. If $p \not\equiv 1 \pmod 5$, this is a bijection. This implies that in this case the polynomial $T^5 - 2$ has precisely one zero in $\mathbf{F}_p$.In fact,

$$(p) = \begin{cases} \mathfrak{p}_p\mathfrak{p}_{p^2}\mathfrak{p}'_{p^2}, & \text{if } p \equiv -1 \pmod 5. \\ \mathfrak{p}_p\mathfrak{p}_{p^4}, & \text{if } p \equiv 2, 3 \pmod 5. \end{cases}$$

Here $\mathfrak{p}_{p^k}$ denotes a prime ideal of norm p^k.

On the other hand, if $p \equiv 1 \pmod 5$, the map $x \mapsto x^5$ is not bijective. If 2 is a 5th power in $\mathbf{F}_p^*$, then $T^5 - 2$ decomposes as a product of linear factors modulo p. If not, $T^5 - 2$ is irreducible. For instance, $T^5 - 2$ is irreducible mod 11.

We conclude that there are prime ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_7$ and $\mathfrak{p}_{13}$ of norm 2,3,5,7 and 13 respectively. These are all primes of norm less than 13.919. They generate the class group. In order to determine the structure of the class group, we factor some prime ideals of small norm.

Table.

	p/q	$\beta = p - q\alpha$	$\mathrm{N}(\beta) = p^5 - 2q^5$	(β)
(i)	0	α	-2	$\mathfrak{p}_2$
(ii)	1	$1 - \alpha$	-1	(1)
(iii)	-1	$1 + \alpha$	-3	$\mathfrak{p}_3$
(iv)	2	$2 - \alpha$	$-30 = -2 \cdot 3 \cdot 5$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$
(v)	-2	$2 + \alpha$	$34 = 2 \cdot 17$	$\mathfrak{p}_2\mathfrak{p}_{17}$
(vi)	3	$3 - \alpha$	241	$\mathfrak{p}_{241}$
(v)	-3	$3 + \alpha$	$-245 = -5^2 7$	$\mathfrak{p}_5{}^2\mathfrak{p}_7$
(vii)	$1/2$	$1 - 2\alpha$	$-63 = -3^2 7$	$\mathfrak{p}_3{}^2\mathfrak{p}_7$
(viii)	$-1/2$	$1 + 2\alpha$	$65 = 5 \cdot 13$	$\mathfrak{p}_5\mathfrak{p}_{13}$

By relation (viii), the ideal $\mathfrak{p}_{13}\mathfrak{p}_5$ is principal. This implies that

$$\mathfrak{p}_{13} \sim \mathfrak{p}_5^{-1}$$

i.e. the ideal class of $\mathfrak{p}_{13}$ is equal to the class of $\mathfrak{p}_5^{-1}$. Therefore, the ideal class group of F is already generated by the classes of $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_5$ and $\mathfrak{p}_7$. In a similar way, by considering the relations (vii) and (iv), we see that $Cl(O_F)$ is, in fact, generated by $\mathfrak{p}_2$ and $\mathfrak{p}_3$. But both these ideals are principal: it follows form entries (i) and (iii) that they are generated by α and $\alpha + 1$ respectively. We conclude that the class group of O_F is trivial.

By Dirichlet's Unit Theorem the unit group O_F^* has rank $r_1 + r_2 - 1 = 1 + 2 - 1 = 2$. From the table we obtain one unit $\alpha - 1 = \sqrt[5]{2} - 1$. It does not seem easy to obtain independent units with small absolute values by extending the table further. Therefore we will search among elements of the form $x =$

Using the ρ-method of Pollard, Brent and Pollard found in 1980 a rather small factor of the 8th Fermat number. They found that

$$2^{256} + 1 = 1238926361552897 \cdot p_{62}$$

here the cofactor

$$p_{62} = 93461639715357977769163558199606896584051237541638188580280321$$

is prime. The ninth Fermat number F_9 had been the main challenge since 1980. It was known that F_9 had a small factor. The factor p_7 was already found by A. Western in 1903. It was also well known that the remaining factor of F_9 was not a prime number. A new factoring algorithm, due to J.M. Pollard was used: The Number Field Sieve. It took from january to may of 1991 of calculations in the ring $\mathbf{Z}[\sqrt[5]{2}]$ on hundreds of computers all over the world to find the factors. These computers were each collecting rows of a gigantic 200 000 by 200 000 matrix over $\mathbf{F}_2$. Solving the linear equations was done on a special machine and took only two hours. For more details on the algorithm and the actual calculations, see [50]. The 10th Fermat number has not yet been factored completely. It is divisible by 11131 and 395937. The remaining factor is not prime and has 299 decimal digits.

Example (8.2). Consider the following (randomly selected) polynomial

$$f(T) = T^4 - 2T^2 + 3T - 7 \qquad \in \mathbf{Z}[T].$$

This polynomial is irreducible modulo 2. This follows from the fact that it is an Artin-Schreier polynomial, but it can also, easily, be checked directly. We will study the number field $F = \mathbf{Q}(\alpha)$, where α is a zero of $f(T)$.

First of all we substitute all integers n with $-18 \leq n \leq 18$ in $f(T)$ and factor the result into a product of prime numbers:

Table I.

n	$f(n) = \mathrm{N}(n - \alpha)$
0	-7
1	-5
2	7
3	$5 \cdot 13$
4	229
5	$11 \cdot 53$
6	$5 \cdot 13 \cdot 19$
7	$7 \cdot 331$
8	$5 \cdot 797$
9	$7^2 \cdot 131$
10	$11 \cdot 19 \cdot 47$
11	$5^2 \cdot 577$
12	20477
13	$5 \cdot 5651$
14	$7 \cdot 5437$
15	$149 \cdot 337$

n	$f(n) = \mathrm{N}(n - \alpha)$
0	-7
-1	-11
-2	-5
-3	47
-4	$5 \cdot 41$
-5	$7 \cdot 79$
-6	$11 \cdot 109$
-7	$5^2 \cdot 7 \cdot 13$
-8	$31 \cdot 127$
-9	$5 \cdot 19 \cdot 67$
-10	$13 \cdot 751$
-11	$83 \cdot 173$
-12	$5 \cdot 7 \cdot 11 \cdot 53$
-13	$19 \cdot 1483$
-14	$5^2 \cdot 7^2 \cdot 31$
-15	50123

To evaluate the discriminant of $f(T)$, we compute the sums p_i of the ith powers of its roots in $\mathbf{C}$ using Newton's relations (Exer.2.M):

$$\begin{aligned}
p_1 &= 0\\
p_2 &= -2s_2 + p_1 s_1 = -2\cdot 2 + 0 = 4\\
p_3 &= 3s_3 + p_2 s_1 - p_1 s_2 = 3\cdot(-3) + 0 + 0 = -9\\
p_4 &= 2p_2 - 3p_1 + 7p_0 = 2\cdot 4 - 0 + 7\cdot 4 = 36\\
p_5 &= 2p_3 - 3p_2 + 7p_1 = 2\cdot(-9) - 3\cdot 4 + 0 = -30\\
p_6 &= 2p_4 - 3p_3 + 7p_2 = 2\cdot 36 - 3\cdot(-9) + 7\cdot 4 = 127
\end{aligned}$$

We have that

$$\mathrm{Disc}(f) = \det\begin{pmatrix} 4 & 0 & 4 & -9\\ 0 & 4 & -9 & 36\\ 4 & -9 & 36 & -30\\ -9 & 36 & -30 & 127\end{pmatrix} = -98443$$

which is a prime number. We conclude from Prop.3.7 that $\Delta_F = -98443$ and that $O_F = \mathbf{Z}[\alpha]$. From Exer.3.H we deduce that $(-1)^{r_2} = -1$ and we conclude that $r_2 = 1$ and hence that $r_1 = 2$. Minkowski's constant is equal to

$$\frac{4!}{4^4}\frac{4}{\pi}\sqrt{98443} = 37.45189\ldots.$$

By Minkowski's Theorem, the ideal class group $Cl(O_F)$ is generated by the primes of norm less than $37.451\ldots$. In order to calculate the class group, we determine the primes of small norm first.

We see in Table I that the polynomial $f(T)$ has no zeroes modulo p for the primes $p = 2, 3, 17, 23$ and 29. We leave the verification that $f(T)$ has no zeroes modulo 37 either, to the reader. By the Factorization Lemma we conclude that there are no prime ideals of norm p for these primes p. It is easily checked that $f(T)$ is irreducible modulo 2 and 3 and that $f(T) \equiv (T-1)(T+2)(T^2 - T + 1) \pmod 5$. The polynomial $T^2 - T + 1$ is irreducible mod 5.

This gives us the following list of all prime ideals of norm less than $37.45\ldots$: the ideals (2) and (3) are prime and $(5) = \mathfrak{p}_5\mathfrak{p}'_5\mathfrak{p}_{25}$, where $\mathfrak{p}_5$ and $\mathfrak{p}'_5$ have norm 5 and $\mathfrak{p}_{25}$ is a prime of norm 25. The other primes $\mathfrak{p}_p$ and $\mathfrak{p}'_p$ of norm less $37.45\ldots$ have prime norm p. They are listed in Table II and are easily computed from Table I.

Table II.

$\mathfrak{p}_5 = (5, \alpha - 1)$	$\mathfrak{p}'_5 = (5, \alpha + 2)$
$\mathfrak{p}_7 = (7, \alpha)$	$\mathfrak{p}'_7 = (7, \alpha - 2)$
$\mathfrak{p}_{11} = (11, \alpha + 1)$	$\mathfrak{p}'_{11} = (11, \alpha - 5)$
$\mathfrak{p}_{13} = (13, \alpha - 3)$	$\mathfrak{p}'_{13} = (13, \alpha - 6)$
$\mathfrak{p}_{19} = (19, \alpha - 6)$	$\mathfrak{p}'_{19} = (19, \alpha + 9)$
$\mathfrak{p}_{31} = (31, \alpha + 8)$	$\mathfrak{p}'_{31} = (31, \alpha + 14)$

The class group is generated by the classes of these primes and the class of $\mathfrak{p}_{25}$. There exist, however, many relations between these classes. In the following table we list the factorizations of some numbers of the form $q - p\alpha$, where $p, q \in \mathbf{Z}$. We have chosen numbers of this form because $\mathrm{N}(q - p\alpha) = p^4 f(q/p)$ can be computed so easily. The factorizations into prime ideals of the principal ideals $(q - p\alpha)$ give rise to relations in the class group. For instance $\mathrm{N}(1 - 4\alpha) = -2015 = -5\cdot 13\cdot 31$

and $(1-4\alpha)=\mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{p}_{31}$. This shows that the ideal class of $\mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{p}_{31}$ is trivial. Therefore the class of $\mathfrak{p}_{31}$ can be xepressed in terms of classes of prime ideals of smaller norm:

$$\mathfrak{p}_{31} \sim \mathfrak{p}_5^{-1}\mathfrak{p}_{13}^{-1}.$$

We conclude that the ideal $\mathfrak{p}_{31}$ is not needed to generate the ideal class group. In a similar way one deduces from Table III below that the ideal classes of the primes of norm 31,19,13 and 11, can all be expressed in terms of ideal classes of primes of smaller norm.

Table III.

	β	$\mathrm{N}(\beta)$	(β)
(i)	$4\alpha+1$	$-5\cdot 31\cdot 13$	$\mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{p}_{31}$
(ii)	$3\alpha-2$	-31	$\mathfrak{p}'_{31}$
(iii)	$\alpha-6$	$5\cdot 13\cdot 19$	$\mathfrak{p}_5\mathfrak{p}'_{13}\mathfrak{p}_{19}$
(iv)	$2\alpha-1$	$-5\cdot 19$	$\mathfrak{p}'_5\mathfrak{p}'_{19}$
(v)	$\alpha+7$	$5^2\cdot 7\cdot 13$	${\mathfrak{p}'_5}^2\mathfrak{p}'_7\mathfrak{p}'_{13}$
(vi)	$3\alpha-5$	13	$\mathfrak{p}'_{13}$
(vii)	$\alpha-3$	$-5\cdot 13$	$\mathfrak{p}'_5\mathfrak{p}_{13}$
(viii)	$\alpha+1$	-11	$\mathfrak{p}_{11}$
(ix)	$3\alpha-4$	$5^2\cdot 11$	${\mathfrak{p}'_5}^2\mathfrak{p}'_{11}$

We conclude that $Cl(O_F)$ is generated by the primes $\mathfrak{p}_5$, $\mathfrak{p}'_5$, $\mathfrak{p}_7$, $\mathfrak{p}'_7$ and $\mathfrak{p}_{25}$. One does not need entry (vi) to conclude this, but this entry will be useful later.

The primes of norm 5 and 7 are all principal. This follows form the first few lines of Table I. Finally, since $\mathfrak{p}_5\mathfrak{p}'_5\mathfrak{p}_{25}=(5)$, one concludes that $\mathfrak{p}_{25}$ is principal. We have proved that the class group of $\mathbf{Q}(\alpha)$ is trivial.

By Dirichlet's Unit Theorem, the unit group has rank $r_1+r_2-1=2+1-1=2$. The group of roots of unity is just $\{\pm 1\}$. In all our calculations, we have not encountered a single unit yet! To find units, it is convenient to calculate the norms of some elements of the form $a+b\alpha+c\alpha^2$ with $a,b,c\in\mathbf{Z}$. This can be done as follows: one calculates approximations of the roots $\alpha_1,\alpha_2,\alpha_3,\overline{\alpha_3}$ of f in $\mathbf{C}$:

$$\begin{aligned}\alpha_1&=-2.195251731\ldots\\ \alpha_2&=1.655743097\ldots\\ \alpha_3&=.269754317\ldots\pm 1.361277001\ldots i\end{aligned}$$

By Prop.2.7*(iii)* one has that

$$\mathrm{N}(a+b\alpha+c\alpha^2)=\left(a+b\alpha_1+c\alpha_1^2\right)\left(a+b\alpha_2+c\alpha_2^2\right)\left|a+b\alpha_3+c\alpha_3^2\right|^2.$$

Calculating norms of some small elements of the form $a+b\alpha+c\alpha^2$ one soon finds that $\mathrm{N}(1+\alpha-\alpha^2)=5$. This shows that the ideals $1+\alpha-\alpha^2$ and $\mathfrak{p}'_5$ are equal. In Table I, we read that $\mathfrak{p}'_5=(\alpha+2)$. We conclude that

$$\varepsilon_1=\frac{1+\alpha-\alpha^2}{\alpha+2}=\alpha^3-2\alpha^2+3\alpha-4$$

is a unit. Similarly one finds that $\mathrm{N}(2-2\alpha+\alpha^2)=65$. One easily checks that $(2-2\alpha+\alpha^2)=\mathfrak{p}'_5\mathfrak{p}'_{13}$. In Table III(vi) we see that $\mathfrak{p}'_{13}=(3\alpha-5)$. We conclude that the principal ideals $(2-2\alpha+\alpha^2)$ and $((\alpha+2)(3\alpha-5))$ are equal. This implies that

$$\epsilon_2=\frac{2-2\alpha+\alpha^2}{(3\alpha-5)(\alpha+2)}=\alpha^3+\alpha^2+\alpha+3$$

is a unit.

Rather then proving that the units ϵ_1, ϵ_2 and -1 generate the unit group, we "verify" in another way that these units generate the whole group. For this we will use the main results of the *next* section. We will use the ζ-function of the field F. Theorem 9.4 gives us an expression for the residue of the Dedekind ζ-function $\zeta_F(s)$ associated to F at $s = 1$. Since the Riemann ζ-function $\zeta_{\mathbf{Q}}(s)$ has a residue equal to 1 at $s = 1$, one can express the content of Theorem 9.4 as follows

$$\lim_{s\to 1} \frac{\zeta_F(s)}{\zeta_{\mathbf{Q}}(s)} = \frac{2^{r_1}(2\pi)^{r_2} h_F R_F}{w_F\sqrt{|\Delta|}}.$$

Using the Euler product formula for the ζ-functions and ignoring problems of convergence this gives rise to

$$\prod_p \frac{\prod_{\mathfrak{p}|p}\left(1-\frac{1}{\mathrm{N}(\mathfrak{p})}\right)^{-1}}{\left(1-\frac{1}{p}\right)^{-1}} = \frac{2^{r_1}(2\pi)^{r_2} h_F R_F}{w_F\sqrt{|\Delta|}}.$$

We can compute the right hand side: $r_1 = 2$, $r_2 = 1$, $w_F = 2$ and $\Delta = -98443$. By the calculation above we have that $h_F = 1$. Assuming that the units $\varepsilon_1, \varepsilon_2$ are fundamental, we compute the regulator using the two real embeddings $\phi_1, \phi_2 : F \hookrightarrow \mathbf{R}$ given by $\alpha \mapsto \alpha_1$ and $\alpha \mapsto \alpha_2$ respectively. This gives

$$R_F = \det\begin{pmatrix} \log|\phi_1(\varepsilon_1)| & \log|\phi_1(\varepsilon_2)| \\ \log|\phi_2(\varepsilon_1)| & \log|\phi_2(\varepsilon_2)| \end{pmatrix} \approx \det\begin{pmatrix} 3.427619209 & 1.600462837 \\ -3.752710586 & 2.479594524 \end{pmatrix} \approx 14.50597965$$

So, assuming that the units $\varepsilon_1, \varepsilon_2$ are fundamental we find that the residue of $\zeta_F(s)$ is equal to

$$\frac{2^2(2\pi)\cdot 1\cdot 14.50597965}{2\cdot\sqrt{98443}} \approx 0.5809524077.$$

Next we calculate an approximation to the slowly converging Euler product on the left hand side. We'll do this by simply evaluating the contribution of the primes less than a certain moderately large number. In order to evaluate the product we must, for a given prime p, find the terms

$$\prod_{\mathfrak{p}|p}\left(1-\frac{1}{\mathrm{N}(\mathfrak{p})}\right)^{-1},$$

i.e. we must determine the way a prime p splits in the extension F over $\mathbf{Q}$. Apart from the ramified prime 98443, there are five possibilities. Using the Factorization Lemma they can be distinguished by the factorization of $f(T) \in \mathbf{F}_p[T]$:

$$(p) = \begin{cases} \textit{(i)} \quad \mathfrak{p}_p\mathfrak{p}'_p\mathfrak{p}''_p\mathfrak{p}'''_p, & \text{if } f(T) \text{ has 4 zeroes mod } p, \\ \textit{(ii)} \quad \mathfrak{p}_p\mathfrak{p}'_p\mathfrak{p}_{p^2}, & \text{if } f(T) \text{ has exactly 2 zeroes mod } p, \\ \textit{(iii)} \quad \mathfrak{p}_p\mathfrak{p}_{p^3}, & \text{if } f(T) \text{ has only one zero mod } p, \\ \textit{(iv)} \quad \mathfrak{p}_{p^2}\mathfrak{p}'_{p^2} & \text{if } f(T) \text{ has two irreducible quadratic factors mod } p, \\ \textit{(v)} \quad (p), & \text{if } f(T) \text{ is irreducible mod } p. \end{cases}$$

here $\mathfrak{p}_p$, $\mathfrak{p}_{p^2}$, etc. denote primes of norm p, p^2 etc. One has that

$$\lim_{s\to 1} \frac{\zeta_F(s)}{\zeta_{\mathbf{Q}}(s)} = \prod_p F(p)^{-1}$$

where

$$\begin{aligned} F(p) &= \left(1-\frac{1}{p}\right)^3 && \text{in case } \textit{(i)},\\ &= \left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right) && \text{in case } \textit{(ii)},\\ &= \left(1-\frac{1}{p^3}\right) && \text{in case } \textit{(iii)},\\ &= \left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}\right) && \text{in case } \textit{(iv)},\\ &= \left(1+\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right) && \text{in case } \textit{(v)}. \end{aligned}$$

A simple computer program enables one to evaluate this product with some precision. It suffices to count the zeroes of $f(T)$ modulo p. To distinguish between cases *(iv)* and *(v)* one observes that the T^3-coefficient of $f(T)$ is 0 and that the constant term is 7. This implies that a factorization of $f(T)$ as a product of two quadratic terms must be of the form

$$f(T) = T^4 - 2T^2 + 3T - 7 = (T^2 - aT + b)(T^2 + aT - \frac{7}{b}).$$

Comparing coefficients one finds that $(b - 7/b)a = 3$ and $b - 7/b = a^2 - 2$. Eliminating a gives that

$$(b^2 - 7)(b^2 + 7)^2 + 18b^3 = 0.$$

We see that, when $f(T)$ has no zeroes mod p, we are in case *(v)* if and only if the polynomial $(Y^2 - 7)(Y^2 + 7)^2 + 18Y^3$ has a zero in $\mathbf{F}_p$. This can be tested easily.

Using the primes less than 1657 one finds .5815983 for the value of the Euler product. This is close to the number 0.5809524077 that we found above. In view of the slow convergence of the Euler product, the error is not unusually large. It is rather unlikely that the final value will be twice or more as small. This indicates, but does not prove, that the units ε_1 and ε_2 are indeed fundamental. To *prove* that they are fundamental, one should employ different techniques, related to methods to search for short vectors in lattices.

Example (8.3). Let $g(T) \in \mathbf{Z}[T]$ be given by $g(T) = T^3 + T^2 + 5T - 16$. From the third column of Table V below, it follows that g has no zeroes modulo 11. Therefore it is irreducible mod 11 and hence also over $\mathbf{Z}$. Let $F = \mathbf{Q}(\alpha)$ where α denotes a zero of $g(T)$. We want to calculate the ring of integers O_F of F, its unit group and its class group.

Using Newton's formulas we find that $p_0 = 3$, $p_1 = -1$, $p_2 = 1 \cdot 1 - 10 = -9$. Using the relation

$$p_{n+3} = -p_{n+2} - 5p_{n+1} + 16p_n$$

we obtain $p_3 = 9 + 5 + 16 \cdot 3 = 62$ and $p_4 = -62 - 5 \cdot (-9) - 16 = -33$. This gives us

$$\det \begin{pmatrix} 3 & -1 & -9 \\ -1 & -9 & 62 \\ -9 & 62 & -33 \end{pmatrix} = -8763 = -3 \cdot 23 \cdot 127$$

Since 8763 is squarefree, $\Delta_F = -8763$, and the ring of itegers O_F is equal to $\mathbf{Z}[\alpha]$. Exer.3.H implies that $(-1)^{r_2} = -1$ and hence that $r_2 = 1$. Minkowski's constant is equal to

$$\frac{3!}{3^3}\frac{4}{\pi}\sqrt{8763} = 26.4864\ldots$$

The class group is generated by the classes of the prime ideals of norm less than 26.5. With the aid of the values of the polynomial $g(T)$ at the first few integers, given in table V below, it is easy to deduce the following factorizations of prime numbers in O_F:

Table IV.

p	(p)	
2	$\mathfrak{p}_2\mathfrak{p}_4$	$\mathfrak{p}_2 = (\alpha, 2)$
3	$\mathfrak{p}_3^2\mathfrak{p}_3'$	$\mathfrak{p}_3 = (\alpha+1, 3)$ and $\mathfrak{p}_3' = (\alpha-1, 3)$
5	$\mathfrak{p}_5\mathfrak{p}_{25}$	$\mathfrak{p}_5 = (\alpha+2, 5)$
7	$\mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7''$	$\mathfrak{p}_7 = (\alpha+1, 7)$, $\mathfrak{p}_7' = (\alpha-3, 7)$ and $\mathfrak{p}_7'' = (\alpha+3, 7)$
11	(11)	
13	(13)	
17	(17)	
19	$\mathfrak{p}_{19}\mathfrak{p}_{361}$	$\mathfrak{p}_{19} = (\alpha-6, 19)$
23	$\mathfrak{p}_{23}^2\mathfrak{p}_{23}'$	$\mathfrak{p}_{23} = (\alpha+7, 23)$ and $\mathfrak{p}_{23}' = (\alpha+10, 23)$

The following table contains the values of $g(T)$ at the integers k with $-10 \leq k \leq 9$ or, equivalently, the norms of the principal ideals $(k-\alpha)$. Using these norms and the explicit descriptions of the prime ideals of O_F, given in Table IV, it is easy to find the factorization of the principal ideals $(k-\alpha)$. It is given in the fourth column of the table.

Table V.

	k	$\mathrm{N}(k-\alpha)$	
(i)	0	-2^4	$\mathfrak{p}_2^4$
(ii)	1	-3^2	${\mathfrak{p}_3'}^2$
(iii)	2	$2\cdot 3$	$\mathfrak{p}_2\mathfrak{p}_3$
(iv)	3	$5\cdot 7$	$\mathfrak{p}_5\mathfrak{p}_7'$
(v)	4	$2^2\cdot 3\cdot 7$	$\mathfrak{p}_2^2\mathfrak{p}_3'\mathfrak{p}_7''$
(vi)	5	$3\cdot 53$	
(vii)	6	$2\cdot 7\cdot 19$	$\mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{19}$
(viii)	7	$3\cdot 137$	
(ix)	8	$2^3\cdot 3\cdot 5^2$	$\mathfrak{p}_2^3\mathfrak{p}_3{\mathfrak{p}_5}^2$
(x)	9	839	

	k	$\mathrm{N}(k-\alpha)$	
(xi)	-1	$-3\cdot 7$	$\mathfrak{p}_3\mathfrak{p}_7$
(xii)	-2	$-2\cdot 3\cdot 5$	$\mathfrak{p}_2\mathfrak{p}_3'\mathfrak{p}_5$
(xiii)	-3	-7^2	${\mathfrak{p}_7''}^2$
(xiv)	-4	$-2^2\cdot 3\cdot 7$	$\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_7'$
(xv)	-5	$-3\cdot 47$	
(xvi)	-6	$-2\cdot 113$	
(xvii)	-7	$-3\cdot 5\cdot 23$	$\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{23}$
(xviii)	-8	$-2^3\cdot 3^2\cdot 7$	$\mathfrak{p}_2^3{\mathfrak{p}_3'}^2\mathfrak{p}_7$
(xix)	-9	-709	
(xx)	-10	$-2\cdot 3\cdot 7\cdot 23$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7''\mathfrak{p}_{23}'$

the class group is generated by the classes of the prime ideals of norm less than or equal to 23. Using the relations that are implied by the factorizations of the principal ideals $(\alpha - k)$, we can reduce the number of generators of the class group. For example, entry (xx) tells us that

$$\mathfrak{p}_{23}' \sim (\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7'')^{-1}.$$

This implies that the class of $\mathfrak{p}_{23}'$ is in the group generated by the classes of $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_7''$. Similarly, entry (xvii) says that

$$\mathfrak{p}_{23} \sim (\mathfrak{p}_3\mathfrak{p}_5)^{-1}.$$

We conclude that the class group is already generated by the classes of the prime ideals of norm at most 19. Continuing in this way, we can eliminate many of the generators, each time expressing the class of a prime ideal as a product of classes of primes of smaller norm.

By entry (vi), we eliminate $\mathfrak{p}_{19}$; by means of the entries (iii), (iv) and (xi) we eliminate the primes over 7. Entry (xii) implies that $\mathfrak{p}_5$ can be missed as a generator. Since $\mathfrak{p}_{25} \sim \mathfrak{p}_5^{-1}$, we see that $\mathfrak{p}_{25}$ can be missed as well. The prime $\mathfrak{p}_3$ is taken care of by the relation implied by entry (ii). Since $\mathfrak{p}'_3 \sim \mathfrak{p}_3^{-2}$ we don't need the prime $\mathfrak{p}'_3$ either.

We conclude that the class group of O_F is generated by the class of the prime $\mathfrak{p}_2$. Entry (i) implies that

$$\mathfrak{p}_2^4 \sim (1).$$

This shows that the class group is a quotient of $\mathbf{Z}/4\mathbf{Z}$. To prove that the class group is actually *isomorphic* to $\mathbf{Z}/4\mathbf{Z}$, it suffices to show that the ideal $\mathfrak{p}_2^2$ is not principal. Since, by entry (ii) $\mathfrak{p}'_3 \sim \mathfrak{p}_3^{-2} \sim \mathfrak{p}_2^2$, this is equivalent to showing that the ideal $\mathfrak{p}'_3$ is nor principal. Before we can show this, we need to know the units of O_F^*, or, at least, the unit group modulo squares.

Consider the principal ideals generated by $(\alpha-1)(\alpha-2)^4$ and 9α. Entries (i), (ii) and (iii) of the table imply that both these ideals factor as

$$\mathfrak{p}_2^4\mathfrak{p}_3^4{\mathfrak{p}'_3}^2.$$

Therefore $((\alpha-1)(\alpha-2)^4) = (9\alpha)$ and

$$\varepsilon = \frac{(\alpha-1)(\alpha-2)^4}{9\alpha} = 4\alpha^2 + \alpha - 13.$$

is a unit. Modulo $\mathfrak{p}_3 = (\alpha+1, 3)$ we have that $\varepsilon \equiv 4 - 1 - 13 \equiv -1 \pmod 3$. In particular, ε is not a square modulo $\mathfrak{p}_3$. We conclude that ε generates $O_F^*/(O_F^*)^2$.

Now we verify that $\mathfrak{p}'_3$ is not principal. Suppose $\mathfrak{p}'_3 = (\gamma)$ for some $\gamma \in O_F^*$. By entry (ii) of Table V, we would have that $(\gamma)^2 = (\alpha - 1)$. Therefore

$$\gamma^2 \cdot u = \alpha - 1 \qquad \text{for some unit } u.$$

Consider this relation in the group

$$(O_F/\mathfrak{p}_3)^* \times (O_F/\mathfrak{p}_5)^*/(O_F/\mathfrak{p}_5)^{*2} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/\mathbf{Z}.$$

We saw already that $\varepsilon \equiv -1 \pmod{\mathfrak{p}_3}$. We also have that $\varepsilon \equiv 4(-2)^2 + (-2) - 1 \equiv -2 \pmod{\mathfrak{p}_5}$. Since -2 is not a square mod 5, the image of ε in $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/\mathbf{Z}$ is the vector $(1,1)$. On the other hand, $\alpha - 1 \equiv -1 - 1 \equiv 1 \pmod{\mathfrak{p}_3}$ and $\alpha - 1 \equiv -2 - 1 \equiv 2 \pmod{\mathfrak{p}_5}$. This implies that the image of $\alpha - 1$ in $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/\mathbf{Z}$ is the vector $(0,1)$.

This shows that $\alpha - 1$ and ε are independent in the group $(O_F/\mathfrak{p}_3)^* \times (O_F/\mathfrak{p}_5)^*$ modulo squares. Therefore the relation $\gamma^2 \cdot u = \alpha - 1$ is impossible. We conclude that $\mathfrak{p}'_3$ is not principal and hence that $Cl(O_F) \cong \mathbf{Z}/4\mathbf{Z}$.

By Dirichlet's Unit Theorem, the group O_F^* has rank $r_1 + r_2 - 1 = 1 + 1 - 1 = 1$. Since F admits an embedding into $\mathbf{R}$, the group of roots of unity of F is just $\{\pm 1\}$. We conclude that $O_F^* \cong \mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})$ or, in other words, that $O_F^* = \pm u^{\mathbf{Z}}$ for some fundamental unit u. By means of a search in certain lattices, one can show that the unit $\varepsilon = 4\alpha^2 + \alpha - 13$ is actually a fundamental unit. We do not prove it here.

(8.A) Pick integers $A, B, C, D \in \mathbf{Z}$, satisfying $|A|, |B|, |C|, |D| \leq 4$ until the polynomial $(f(T) = T^4 + AT^3 + BT^3 + CT + D$ is irreducible. Let α denote a zero of $F(T)$. Determine the class group of $\mathbf{Q}(\alpha)$.

(8.B) Determine which of the prime ideals in table IV are in which of the four ideal classes of O_F of example 8.3.

(8.C) (H.W. Lenstra) Determine the class group of the field generated by a zero of the polynomial $T^4 + +3T^2 + 7T + 4$.

9. Zeta functions.

In this section we will compute the residue of the Dedekind ζ-function $\zeta_F(s)$ associated to a number field F in $s = 1$. The techniques will be analytical in nature. See Heilbronn's article in [12] or Davenport's book [17] for similar techniques. For the Γ-function see Artin's booklet [4].

First we discuss the Riemann ζ-function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, which is just the Dedekind ζ-function associated to $\mathbf{Q}$. To study it we need to know some properties of the Γ-function.

Definition. The Γ-function $\Gamma(s)$ is for $s \in \mathbf{C}$, $\mathrm{Re}(s) > 0$ is defined by

$$\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{dt}{t}.$$

Proposition (9.1).

(i) For every $s \in \mathbf{C}$, $\mathrm{Re}(s) > 0$ one has that $\Gamma(s+1) = s\Gamma(s)$.

(ii) The Γ-function admits a meromorphic extension to $\mathbf{C}$ with poles at $0, -1, -2, \ldots$ of order 1. The residue at $-k$ is $(-1)^k/k!$.

(iii) $\Gamma(s)\Gamma(1-s) = \pi/\sin(\pi s)$ for $s \in \mathbf{C} - \mathbf{Z}$.

Proof. The first part follows easily by partial integration. Using the functional equation $\Gamma(s+1) = s\Gamma(s)$ one can extend $\Gamma(s)$ meromorphically to all of $\mathbf{C}$. For every $k \in \mathbf{Z}_{\geq 0}$ one has that

$$\Gamma(s) = \frac{1}{(s+(k-1)) \cdot \ldots \cdot (s-1)s} \Gamma(s+k)$$

which easily implies *(ii)*.

(iii) Write $F(s) = \Gamma(s)\Gamma(1-s)$. By *(ii)* the function $F(s)$ has poles of order 1 at the integers. For $s \in \mathbf{C}$, $0 < \mathrm{Re}(s) < 1$ one has that

$$F(s) = \int_0^\infty \int_0^\infty e^{-t-x} \left(\frac{t}{x}\right)^s dx \frac{dt}{t}$$

and, making the substitution $t = zx$, we find that

$$F(s) = \int_0^\infty z^s \int_0^\infty e^{-(z+1)x} dx \frac{dz}{z} = \int_0^\infty \frac{z^{s-1}}{z+1} dz.$$

Using the Residue Theorem it is rather easy to show that the last integral is equal to $\pi/\sin(\pi s)$. See Exer.9.A for the details. This proves the proposition.

Definition. For $x \in \mathbf{R}_{>0}$ we let

$$\theta(x) = \sum_{n \in \mathbf{Z}} e^{-\pi n^2 x}$$

denote the θ-function.

This θ-function is a minor modification of the well known Jacobi Θ-function $\Theta(z) = \theta(-2iz)$ (Carl Gustav Jacob Jacobi, German mathematician 1804–1851). The Θ-function is defined for z in the upper halfplane. It is a modular form. See the books by N. Koblitz [36] and S. Lang [40] for more about Θ-series and modular forms.

Proposition (9.2). *(C.G.J. Jacobi) Let $x \in \mathbf{R}_{>0}$. Then*

$$\theta\left(\frac{1}{x}\right) = \sqrt{x}\theta(x).$$

Proof. Let $f : \mathbf{R} \longrightarrow \mathbf{C}$ be a rapidly decreasing C^∞-function i.e. for all $n \in \mathbf{Z}$ one has that $f(x)x^n \to 0$ when $x \to \pm\infty$. The basic example will be $e^{-\pi A x^2}$ for $A > 0$. We define the Fourier transform of f by

$$\hat{f}(t) = \int_{\mathbf{R}} f(x)e^{2\pi i t x}dx.$$

The proof will be a consequence of the *Poisson summation formula:*

$$\sum_{n\in\mathbf{Z}} f(n) = \sum_{n\in\mathbf{Z}} \hat{f}(n).$$

This formula can be deduced as follows: consider

$$\begin{aligned} g(x) &= \sum_{k\in\mathbf{Z}} f(k+x) \\ &= \sum_{m\in\mathbf{Z}} c_m e^{2\pi i m x} \end{aligned}$$

The second expression is the Fourier expansion of the *periodic* function $g(x)$. The Fourier coefficients c_m are given by

$$c_m = \int_0^1 g(x)e^{-2\pi i m x}dx \qquad \text{for all } m \in \mathbf{Z}.$$

The coefficients c_m can be evaluated explicitly as follows:

$$\begin{aligned} c_m &= \int_0^1 \sum_{k\in\mathbf{Z}} f(k+x)e^{-2\pi i m x}dx = \int_0^1 \sum_{k\in\mathbf{Z}} f(x)e^{-2\pi i m(x-k)}dx \\ &= \int_{\mathbf{R}} f(x)e^{-2\pi i m x}dx = \hat{f}(m) \end{aligned}$$

We conclude that

$$\sum_{k\in\mathbf{Z}} f(k) = g(0) = \sum_{m\in\mathbf{Z}} c_m = \sum_{m\in\mathbf{Z}} \hat{f}(m)$$

as required.

Now we give the proof of Prop.9.2: consider the, rapidly decreasing, function $h(y) = e^{-\pi y^2}$. It is well-known and easily checked that $\hat{h}(y) = h(y)$. It is convenient to calculate the Fourier transform of $h_b(y) = h(by)$ for $b \in \mathbf{R}$. the result is that $\hat{h_b}(y) = \frac{1}{b}\hat{h}(\frac{y}{b})$. By the Poisson summation formula we have that

$$\begin{aligned} \theta(x) &= \sum_{n\in\mathbf{Z}} e^{-\pi n^2 x} = \sum_{n\in\mathbf{Z}} h_{\sqrt{x}}(n) = \sum_{n\in\mathbf{Z}} \widehat{h_{\sqrt{x}}}(n), \\ &= \sum_{n\in\mathbf{Z}} \frac{1}{\sqrt{x}}\hat{h}(\frac{n}{\sqrt{x}}) = \frac{1}{\sqrt{x}}\sum_{n\in\mathbf{Z}} e^{-\pi(\frac{n}{\sqrt{x}})^2} \\ &= \frac{1}{\sqrt{x}}\theta\left(\frac{1}{x}\right), \end{aligned}$$

as required.

Proposition (9.3). *The Riemann ζ-function (G.B. Riemann, German mathematician 1826–1866) has the following properties:*

(i) *(Euler product.)*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

for $s \in \mathbf{C}$, $\mathrm{Re}\, s > 1$. Here the product runs over the primes p.

(ii) *(Analytic continuation.) The function $\zeta(s)$ admits a meromorphic extension to $\mathbf{C}$. It has only a pole at $s = 1$. This pole is of order 1 with residue 1.*

(iii) *(Functional equation.) The function*

$$Z(s) = \Gamma\left(\frac{s}{2}\right) \pi^{\frac{s}{2}} \zeta(s)$$

satisfies $Z(s) = Z(1-s)$.

(iv) *(Zeroes) If ρ is a zero of $\zeta(s)$ then either ρ is a trivial* zero, i.e. ρ is a negative even integer, or $0 \le \rho \le 1$

(v) (*Special values.*) Let m be an even positive integer. Then

$$\zeta(m) = \frac{(2\pi i)^m}{2 \cdot m!} B_m,$$
$$\zeta(1-m) = \frac{B_m}{m}.$$

here the B_m denote *Bernoulli numbers. They are defined by*

$$\frac{T}{e^T - 1} = \sum_{m=1}^{\infty} \frac{B_m}{m!} T^m.$$

Finally we have that $\zeta(0) = -\frac{1}{2}$.

Proof. Part *(i)* has been proved in section 4. We prove *(ii)* and *(iii)* at the same time. For $s \in \mathbf{C}$, $\mathrm{Re}(s) \ge 1$, consider the Z-function

$$Z(s) = \Gamma\left(\frac{s}{2}\right) \pi^{\frac{s}{2}} \zeta(s)$$

We can write

$$Z(s) = \int_0^{\infty} e^{-t} t^{s/2} \frac{dt}{t} \pi^{-s/2} \sum_{n \ge 1} n^{-s} = \int_0^{\infty} e^{-t} \sum_{n \ge 1} t^{s/2} \pi^{-s/2} n^{-s} \frac{dt}{t}.$$

Substituting $t = x\pi n^2$ in every term of the sum, we find

$$Z(s) = \int_0^{\infty} x^{s/2} \sum_{n \ge 1} e^{-x\pi n^2} \frac{dx}{x} = \int_0^{\infty} \frac{\theta(x) - 1}{2} x^{s/2} \frac{dx}{x}.$$

Next, we split the integral in two pieces: a piece from 0 to 1 and another from 1 to ∞. In the first piece we change the variable x to $1/x$ and we find, using Prop.9.2, that

$$\begin{aligned} Z(s) &= \int_1^{\infty} \frac{\theta(x) - 1}{2} x^{s/2} \frac{dx}{x} + \int_{\infty}^{1} \frac{\theta(1/x) - 1}{2} x^{-s/2} \frac{d(1/x)}{1/x}, \\ &= \int_1^{\infty} \frac{\theta(x) - 1}{2} x^{s/2} \frac{dx}{x} + \int_1^{\infty} \sqrt{x}\theta(x) - 1/2 x^{-s/2} \frac{dx}{x}, \\ &= \int_1^{\infty} \frac{\theta(x) - 1}{2} \left(x^{s/2} + x^{(1-s)/2}\right) dx + \int_1^{\infty} \frac{x^{(1-s)/2} - x^{-s/2}}{2} \frac{dx}{x}, \\ &= \int_1^{\infty} \frac{\theta(x) - 1}{2} \left(x^{s/2} + x^{(1-s)/2}\right) dx - \frac{1}{s} - \frac{1}{1-s}. \end{aligned}$$

Now we have an expression for $Z(s)$ which converges for all $s \in \mathbf{C}$. We clearly have that $Z(s) = Z(1-s)$. The Z function has poles at 0 and 1, both with residue 1. Since the function $\pi^{-s/2}\Gamma(s/2)$ has a zero at 0, but not at 1. It follows that the ζ-function has only a pole at 1. From Prop.9.1*(iii)* we see that $\Gamma(1/2) = \sqrt{\pi}$. Therefore the residue of $\zeta(s)$ at 1 is 1.

(iv) Suppose ρ is a zero of the Riemann ζ-function. By *(i)* we have that $\mathrm{Re}(s) < 1$. Suppose $\mathrm{Re}(s) < 0$ and that ρ is *not* an even negative integer. We have that $Z(\rho) = \Gamma(\rho)\pi^{-\rho/2}\zeta(\rho)$. By Prop.9.1, the function $\Gamma(s/2)$ does not have a pole at ρ. Therefore $Z(\rho) = 0$ and by *(iii)* we see that $Z(1-\rho) = 0$. It is immediate from Prop.9.1*(iii)* that the Γ-function has no zeroes. We conclude that $\zeta(1-\rho) = 0$. This contradicts the fact that $\mathrm{Re}(\rho) > 1$ and the result follows.

(v) Let $R \in \frac{1}{2} + \mathbf{Z}$ be a large number and let C_R be a big square in $\mathbf{C}$ with corners $\pm R \pm iR$. The contour integral

$$\int_{C_R} \frac{z^{-m}}{e^z - 1} dz \qquad \text{for } m \geq 2$$

approaches 0 as $R \to \infty$. Calculating the residues of the function, one finds for *even* values of m that

$$\sum_{n=1}^{\infty} \frac{1}{(2\pi i n)^m} = -\frac{1}{2}\frac{B_m}{m!}.$$

This gives the values of $\zeta(m)$ for even positive integers m. The values of $\zeta(1-m)$ follow from the functional equation proved in *(ii)*. Finally one obtains that $\zeta(0) = -1/2$ by observing that both $Z(s)$ and $\pi^{-s/2}\Gamma(s/2)$ have a simple pole at 0. The Z-function has a residue equal to -1 and the function $\pi^{-s/2}\Gamma(s/2)$ has a residue -2, because $\Gamma(s/2) = (2/s)\Gamma(s/2+1)$. This proves Proposition 9.3.

The Riemann ζ-function is one of the most studied mathematical objects [22]. The results in Prop.9.3 were all proved by Euler and Riemann. Riemann observed that many zeroes ρ of $\zeta(s)$ satisfy $\mathrm{Re}(\rho) = 1/2$ and conjectured that this is true for all non-trivial zeroes. This is the celebrated Riemann Hypothesis which is still unproven. Its truth is considered very likely and would have important consequences. A very weak version of it has been proved by Hadamard and De la Vallée Poussin in 1899. They showed that $\mathrm{Re}\,\rho \neq 1$ for every zero ρ of $\zeta(s)$. An immediate consequence is the Prime Number Theorem:

$$\#\{p < X : \ p \text{ prime}\} \approx \frac{X}{\log X}.$$

The Riemann Hypothesis has been numerically verified [77]: The "first" 10^{12} zeroes ρ all have their real part equal to 1/2. There are analogues of the Riemann ζ-function in algebraic geometry. For some of these functions the analogue of the Riemann Hypothesis has been proved e.g. for zeta functions of curves over finite fields by A. Weil [82] in 1948. This result was extended by P. Deligne [19] in 1973.

Much less is known about the values of the ζ-function at odd integers. It was proved by Apéry in 1976 that $\zeta(3) \approx 1.2020569031 \notin \mathbf{Q}$. His proof does not seem to generalize well [3,78]. Just recently expressions for $\zeta(3)$ involving the dilogarithm function have been obtained by Zagier [84].

Dedekind ζ-functions are analogues of the Riemann ζ-function. Nowadays one can prove the analogue of Proposition 9.3. for these functions.

The main result of this section is the calculation of the residue of the ζ-function $\zeta(s)$ at $s = 1$. Strictly speaking, we do not prove that $\zeta(s)$ extends to a meromorphic function in a neighborhood of $s = 1$. We merely calculate the limit $\lim_{s\to 1}(s-1)\zeta(s)$ but this will be sufficient for our purposes.

Theorem (9.4). *Let F be a number field and let $\zeta_F(s)$ denote its Dedekind ζ-function. Then*

$$\lim_{s\to 1}(s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}h_F R_F}{w_F\sqrt{|\Delta_F|}}$$

Here r_1 is the number of homomorphism $F \hookrightarrow \mathbf{C}$ which have their image in $\mathbf{R}$ and $2r_2$ the remaining number of homomorphism $F \hookrightarrow \mathbf{C}$. By h_F we denote the class number of F, by R_F its regulator, by Δ_F, the discriminant and, finally, by w_F, the number of roots of unity in F.

Proof. Let $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. By Prop.4.9, the sum

$$\zeta_F(s) = \sum_{J\neq 0}\frac{1}{\mathrm{N}(J)^s}$$

is absolutely convergent. We rewrite it as

$$\zeta_F(s) = \sum_{C\in Cl(O_F)}\zeta_C(s)$$

where

$$\zeta_C(s) = \sum_{J\in C}\frac{1}{\mathrm{N}(J)^s}.$$

Let C be an ideal class and let $I \in C^{-1}$. The map $J \mapsto IJ$ gives a bijection between the class C and the set of principal ideals (α) contained in I. Therefore we can write

$$\zeta_C(s) = \sum_{(\alpha)\subset I}\frac{1}{\mathrm{N}(\alpha I^{-1})^s} = \mathrm{N}(I)\sum_{(\alpha)\subset I}\frac{1}{|\mathrm{N}\alpha|^s}.$$

In order to calculate this sum, we view the ideal I via the map $\Phi : F \longrightarrow F\otimes\mathbf{R}$ as a lattice in the $\mathbf{R}$-algebra $F\otimes\mathbf{R} = \mathbf{R}^{r_1}\times\mathbf{C}^{r_2}$.

The units of the algebra $F\otimes\mathbf{R}$ are precisely the vectors that have all their coordinates non-zero. We extend the map $\Psi : O_F^* \longrightarrow \mathbf{R}^{r_1+r_2}$ to $(F\otimes\mathbf{R})^*$:

$$\Psi : (\mathbf{R}^{r_1}\times\mathbf{C}^{r_2})^* \longrightarrow \mathbf{R}^{r_1+r_2}$$

by

$$\Psi(x_1,\ldots,x_{r_1},z_1,\ldots,z_{r_2}) = (\log\|x_1\|,\ldots,\log\|x_{r_1}\|,\log\|z_1\|,\ldots\log\|z_{r_2}\|)$$

and we extend the norm $\mathrm{N} : F \longrightarrow \mathbf{R}$ to $F\otimes\mathbf{R}$ by

$$\mathrm{N}(x_1,\ldots,x_{r_1},z_1,\ldots,z_{r_2}) = |x_1|\cdot\ldots\cdot|x_{r_1}|\cdot|z_1|^2\cdot\ldots\cdot|z_{r_2}|^2.$$

The norm is a homogenous polynomial of degree n. Clearly it does not vanish on $(F\otimes\mathbf{R})^*$.

We choose a basis E for the real vector space $\mathbf{R}^{r_1+r_2}$. Choose a system of fundamental units $\varepsilon_1,\ldots,\varepsilon_{r_1+r_2-1}$ and apply the map Ψ. This gives us r_1+r_2-1 independent vectors $\Psi(\varepsilon_i)$ that span the subspace of vectors that have the sum of their coordinates equal to zero. The basis E will consist of the vectors $\Psi(\varepsilon_i)$ plus the vector $\mathbf{v} = (1,1,\ldots,1,2,2,\ldots,2)$ that has 1's on the real coordinates and 2's on the complex coordinates.

The proof will be a fairly straightforward consequence of three lemmas that will be stated and proved after the proof of Theorem 9.4.

Consider the following set $\Gamma \subset \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$:

$$\Gamma = \{\mathbf{x} \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} : \text{the coordinates } \xi_i \text{ of the vectors } \Psi(\mathbf{x}) \text{ with respect to the basis } E \text{ satisfy } 0 \leq \xi_i < 1 \text{ for } 1 \leq i \leq r_1 + r_2 - 1; \text{ the first coordinate } x_1 \text{ of } \mathbf{x} \text{ satisfies } 0 \leq \arg(x_1) < \tfrac{2\pi}{w_F}\}.$$

If $r_1 > 0$, i.e. if the first coordinate x_1 is real, the condition $0 \leq \arg(x_1) < \frac{2\pi}{w_F}$ should be interpreted as $x_1 > 0$. By Lemma 9.5, we have that

$$\zeta_C = \mathrm{N}(I)^s \sum_{\alpha \in I \cap \Gamma} \frac{1}{|\mathrm{N}(\alpha)|^s} \qquad \text{for } s \in \mathbf{C},\ \mathrm{Re}(s) \geq 1.$$

The set Γ is a *cone,* i.e. for all $\mathbf{x} \in \Gamma$ and $\lambda > 0$ also $\lambda\mathbf{x} \in \Gamma$. This can be seen as follows: From

$$\Psi(\lambda\mathbf{x}) = \Psi(\lambda) + \Psi(\mathbf{x}) = \lambda\mathbf{v} + \Psi(\mathbf{x})$$

it follows that, with respect to the basis E, the coordinates of $\Psi(\lambda\mathbf{x})$ and $\Psi(\mathbf{x})$ are equal, except possibly the last. Since $\lambda > 0$, the argument of the first coordinate of $\mathbf{x}$ is also unchanged. This shows that Γ is a cone.

The subset $\Gamma_1 = \{\gamma \in \Gamma : |\mathrm{N}(\gamma)| \leq 1\}$ is bounded and has finite volume. Therefore, by Lemmas 9.6 and 9.7, we have that

$$\begin{aligned}\lim_{s \to 1}(s-1)\zeta_C(s) &= \lim_{s \to 1}(s-1)\mathrm{N}(I)^s \sum_{\alpha \in I \cap \Gamma} \frac{1}{|\mathrm{N}(\alpha)|^s} \\ &= \mathrm{N}(I)\frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(I)} = \mathrm{N}(I)\frac{2^{r_1}\pi^{r_2}R_F}{w_F}\frac{2^{r_2}}{\mathrm{N}(I)\sqrt{|\Delta_F|}}.\end{aligned}$$

We see that the result does *not* depend on the ideal class C. Therefore, since there are h_F different ideal classes, we find that

$$\lim_{s \to 1}(s-1)\zeta_F(s) = \sum_C \lim_{s \to 1}(s-1)\zeta_C(s) = h_F\frac{2^{r_1}\pi^{r_2}R_F}{w_F\sqrt{|\Delta|}}$$

as required

Lemma (9.5). *Let F be a number field and let $\Gamma \subset F \otimes \mathbf{R}$ be the cone defined above. Then for a fractional ideal I of F we have that*

$$\sum_{(\alpha) \subset I} \frac{1}{|\mathrm{N}(\alpha)|^s} = \sum_{\alpha \in I \cap \Gamma} \frac{1}{|\mathrm{N}(\alpha)|^s}.$$

(Note that the first sum runs over the principal ideals (α), while the second runs over *elements* α.)

Proof. We show first that $(F \otimes \mathbf{R})* = O_F^* \cdot \Gamma$: let $(\mathbf{x} \in F \otimes \mathbf{R})^*$. Write $\Psi(\mathbf{x})$ with respect to the besis E introduced above.

$$\Psi(\mathbf{x}) = \xi_1\Psi(\varepsilon_1) + \ldots + \xi_{r_1+r_2-1}\Psi(\varepsilon_{r_1+r_2-1}) + \xi_{r_1+r_2}\mathbf{v}.$$

Define the unit ε by

$$\varepsilon = \varepsilon_1^{m_i} \ldots \varepsilon_{r_1+r_2}^{m_{r_1+r_2}},$$

where m_i denotes the integral part of ξ_i. As a consequence, the first r_1+r_2-1 coordinates of $\Psi(\varepsilon^{-1}\mathbf{x})$ are between 0 and 1. Next consider the first coordinate y_1 of $\varepsilon^{-1}\mathbf{x}$. Pick a root of unity $\zeta \in F^*$, such that the argument ϕ of ζy_1 satisfies $0 \leq \phi < 2\pi/w_F$. We conclude that $\zeta\varepsilon^{-1}\mathbf{x} \in \Gamma$ and hence that $\mathbf{x} \in O_F^* \cdot \Gamma$ as required.

Moreover, this representation of $\mathbf{x} \in (F \otimes \mathbf{R})^*$ is unique: suppose that $\varepsilon\gamma = \varepsilon'\gamma'$ for $\varepsilon\varepsilon' \in O_F^*$ and $\gamma, \gamma' \in \Gamma$. Then $u = \varepsilon/\varepsilon' = \gamma'/\gamma \in O_F^* \cap \Gamma$. This implies at once that the first r_1+r_2-1 coeficients of $\Psi(u)$ are zero. Since u is a unit, the sum of the coefficients is zero and therefore the last coefficient is also zero. this implies that $u \in \ker(\Psi) = \mu_F$. Since the arguments of the first coordinate in $F \otimes \mathbf{R}$ of both γ and γ' are between 0 and $2\pi/w_F$, we conclude that $u = 1$ and the unicity follows.

The lemma now follows from the fact that every principal ideal $(\alpha) \subset F \otimes \mathbf{R}$ has precisely one generator in Γ. Indeed, $\alpha \in (F \otimes \mathbf{R})^*$, so by the above, there is a unique unit ε such that $\varepsilon\alpha \in \Gamma$.

Lemma (9.6). *Let L be a lattice in $\mathbf{R}^n$ and let $\Gamma \subset \mathbf{R}^n$ be a cone. Let N be a homogeneous polynomial of degree, that does not vanish on Γ. Assume that $\Gamma_1 = \{\gamma \in \Gamma : |\mathrm{N}(\gamma)| \leq 1\}$ is bounded and has finite volume. Then*

$$\lim_{s\to 1} \sum_{x \in L\cap\Gamma} \frac{1}{|\mathrm{N}(x)|^s} = \frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)}.$$

Proof. Let

$$\nu(r) = \#(\frac{1}{r}L \cap \Gamma_1) = \#\{x \in L : |\mathrm{N}(x)| \leq r^n\}.$$

Since Γ_1 is bounded, $\nu(r)$ is finite. The equality follows from the fact that $\mathrm{N}(x)$ is homogeneous of degree n. By the definiton of the Riemann integral we have that

$$\mathrm{vol}(\Gamma_1) = \lim_{r\to\infty} \nu(r)\mathrm{covol}(\frac{1}{r}L)$$

and, equivalenlty

$$\lim_{r\to\infty} \frac{\nu(r)}{r^n} = \frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)}.$$

Next, we enumerate the vectors $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_3 \ldots$ in $\Gamma \cap L$:

$$0 < |\mathrm{N}(\mathbf{x}_1)| \leq |\mathrm{N}(\mathbf{x}_2)| \leq |\mathrm{N}(\mathbf{x}_3)| \leq \ldots$$

and for $k \geq 1$ we put

$$r_k = |\mathrm{N}(\mathbf{x}_k)|^{\frac{1}{n}}.$$

It is immediate that $k \leq \nu(r_k)$ and that for every $\varepsilon > 0$ one has that $\nu(r_k - \varepsilon) \leq k-1 < k$. Therefore

$$\frac{\nu(r_k-\varepsilon)}{(r_k-\varepsilon)^n}\left(\frac{r_k-\varepsilon}{r_k}\right)^n < \frac{k}{r_k^n} \leq \frac{\nu(r_k)}{r_k^n}$$

and letting $\varepsilon \to 0$ we find that

$$\lim_{k\to\infty} \frac{k}{r_k^n} = \lim_{k\to\infty} \frac{k}{r_k^n} = \lim_{k\to\infty} \frac{v(r_k)}{r_k^n} = \frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} > 0.$$

It follows that for $\varepsilon > 0$ suficiently small and $k_0 \in \mathbf{Z}_{>0}$ sufficiently large, we have for all $k \geq k_0$ that

$$\left(\frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} - \varepsilon\right)\frac{1}{k} < \frac{1}{|\mathrm{N}(\mathbf{x}_k)|} < \left(\frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} + \varepsilon\right)\frac{1}{k}$$

and hence for $s \in \mathbf{R}_{>1}$ that

$$\left(\frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} - \varepsilon\right)^s (s-1)\sum_{k\geq k_0}\frac{1}{k^s} < (s-1)\sum_{k\geq k_0}\frac{1}{|\mathrm{N}(\mathbf{x}_k)|^s} < \left(\frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} + \varepsilon\right)^s (s-1)\sum_{k\geq k_0}\frac{1}{k^s}.$$

Now we let s tend to 1. Since $\lim_{s\to 1}(s-1)\sum_{1\leq k<k_0} 1/k^s = 0$, and the fact that the Riemann ζ-function $\zeta(s) = \sum_{k=1}^{\infty} 1/k^s$ has a pole of order 1 at $s=1$ with residue 1, we obtain that for sufficiently small $\varepsilon > 0$

$$\frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} - \varepsilon < \lim_{s\to 1}\sum_{k=1}^{\infty}\frac{1}{|\mathrm{N}(\mathbf{x}_k)|^s} < \frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)} + \varepsilon.$$

This proves the lemma.

Lemma (9.7). *Let F be a number field and let $\Gamma \subset F \otimes \mathbf{R}$ be the cone defined above. Then*
(i)

$$\mathrm{vol}(\Gamma_1) = \frac{2^{r_1}\pi^{r_2}R_F}{w_F}.$$

(ii) Let I be a fractional ideal in F, then the image of I in $F \otimes \mathbf{R}$ satisfies

$$\mathrm{covol}(I) = 2^{-r_2}\mathrm{N}(I)\sqrt{|\Delta_F|}.$$

Proof. The set Γ_1 consists of those vectors $\mathbf{x} = (x_1, \ldots, x_{r_1}, y_1, \ldots, y_{r_2}) \in (F \otimes \mathbf{R})^*$, for which $0 \leq \arg(x_1) < \pi/w_F$, for which $\mathrm{N}(\mathbf{x}) \leq 1$ and for which $0 \leq \xi_1, \ldots, \xi_{r_1+r_2-1} \leq 1$, where the ξ_i are defined by

$$\Psi(\mathbf{x}) = \xi_1\Psi(\varepsilon_1) + \ldots + \xi_{r_1+r_2-1}\Psi(\varepsilon_{r_1+r_2-1}) + \xi_{r_1+r_2}\mathbf{v}.$$

It is clear that, if we drop the condition that $0 \leq \arg(x_1) < \pi/w_F$, the volume of Γ_1 is multiplied by w_F. If, moreover, we add the conditions that $x_i > 0$ for all real coordinates i, i.e. for $1 \leq i \leq r_1$, the volume is multiplied by 2^{-r_1}:

$$\begin{aligned}\mathrm{vol}(\Gamma_1) = \frac{2^{r_1}}{w_F}\mathrm{vol}\{\mathbf{x} \in (F \otimes \mathbf{R})^* : & 0 \leq \xi_1, \ldots, \xi_{r_1+r_2-1} \leq 1 \text{ and } x_1, \ldots, x_{r_1} > 0 \\ & |x_1| \cdot \ldots \cdot |x_{r_1}| \|y_1\| \cdot \ldots \cdot \|y_{r_2}\| \leq 1\}.\end{aligned}$$

We use polar coordinates for the complex coordinates: write $z_k = \rho_k e^{i\phi_k}$ and it is convenient to work with $x_{r_1+k} = \rho_k^2$ rather than ρ_k. We find that

$$\mathrm{vol}(\Gamma_1) = \frac{2^{r_1}\pi^{r_2}}{w_F}\int_W dx_1 \cdot \ldots \cdot dx_{r_1+r_2-1}$$

where W is the set of vectors $\mathbf{x} = (x_1, \ldots, x_{r_1+r_2}) \in (F \otimes \mathbf{R})^*$ for which $x_1, \ldots, x_{r_1+r_2} > 0$ and $\sum_{i=1}^{r_1+r_2}\log(x_i) < 0$ and for which

$$\begin{pmatrix}\log(x_1)\\ \vdots \\ \log(x_{r_1+r_2})\end{pmatrix} = \xi_1\Psi(\varepsilon_1) + \ldots + \xi_{r_1+r_2-1}\Psi(\varepsilon_{r_1+r_2-1}) + \xi_{r_1+r_2}\mathbf{v}$$

with $0 \leq \xi_1, \ldots, \xi_{r_1+r_2-1} < 1$.

Observe that $\xi_{r_1+r_2-1} = -\sum_i \log(x_i)$. Clearly, the above integral is most conveniently evaluated by integration with respect to the variables ξ_i. So, we make the change of variables according to the formulas given in the description of the set W. It is not difficult to calculate the Jacobian J of this transformation. One finds

$$\mathrm{vol}(\Gamma_1) = \frac{2^{r_1}\pi^{r_2}}{w_F}\int_0^1 \ldots \int_0^1 \int_{-\infty}^0 |\det(J)| d\xi_1 \ldots d\xi_{r_1+r_2}$$

where

$$J = \begin{pmatrix} x_1 \log\|\phi_1(\varepsilon_1)\| & \ldots & x_1 \log\|\phi_1(\varepsilon_{r_1+r_2-1})\| & x_1 \\ \vdots & & \vdots & \vdots \\ x_{r_1+r_2}\log\|\phi_{r_1+r_2}(\varepsilon_1)\| & \ldots & x_{r_1+r_2}\log\|\phi_{r_1+r_2}(\varepsilon_{r_1+r_2-1})\| & 2x_{r_1+r_2} \end{pmatrix}.$$

We conclude that

$$\begin{aligned} \mathrm{vol}(\Gamma_1) &= \frac{2^{r_1}\pi^{r_2}}{w_F} R_F \int_0^1 \ldots \int_0^1 \int_{-\infty}^0 n x_1 \cdot \ldots \cdot x_{r_1+r-2} d\xi_1 \ldots d\xi_{r_1+r_2} \\ &= \frac{2^{r_1}\pi^{r_2}}{w_F} R_F n \int_{-\infty}^0 e^{n\xi_{r_1+r_2}} d\xi_{r_1+r_2} = \frac{2^{r_1}\pi^{r_2} R_F}{w_F}. \end{aligned}$$

as required.

Finally, we give, without proof, the analog of Theorem 8.4. for the Dedekind ζ-functions. This result is due to E. Hecke (German mathematician 1887–1947) [31,32]. Hecke's proof is elaborate, but similar to the proof of Proposition 9.3. It exploits Θ-functions and their functional equations. Later in 1959, J.T. Tate gave a simpler proof, based on harmonic analysis on adelic groups [12,p.305].

Theorem (9.10). *(E. Hecke 1917) Let F be a number field and let $\zeta_F(s)$ denote its Dedekind ζ-function.*

(i) (Euler product.)

$$\zeta_F(s) = \sum_{0 \neq I} \frac{1}{\mathrm{N}(I)^s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right)$$

for $s \in \mathbf{C}$, $\mathrm{Re}(s) > 1$. Here the sum runs over the non-zero ideals of the ring of integers O_F and the product runs over the non-zero prime ideals $\mathfrak{p}$ of this ring.

(ii) (Analytic continuation.) the function $\zeta_F(s)$ admits a meromorphic extension to $\mathbf{C}$. It has only a pole at $s = 1$. The residue is

$$\frac{2^{r_1}(2\pi)^{r_2} h_F R_F}{w_F \sqrt{|\Delta}}$$

where the notation is as in Theorem 9.4.

(iii) (Functional equation.) The function

$$Z(s) = |\Delta_F|^{s/2} \left(\Gamma(\frac{s}{2})\pi^{-s/2}\right)^{r_1} \left(\Gamma(s)(2\pi)^{-s}\right)^{r_2} \zeta_F(s)$$

satisfies $Z(s) = Z(1-s)$.

(iv) (Zeroes.) The ζ-function has zeroes at the negative integers: at the odd ones with multiplicity R_2 and at the even ones with multiplicity $r_1 + r_2$. At $s = 0$ it has a zero of order $r_1 + r_2 - 1$ with leading coefficient of the Taylor expansion at 0 equal to $-h_F R_F / w_F$. These are the so-called trivial zeroes. All other zeroes ρ satisfy $0 \leq \mathrm{Re}(\rho) \leq 1$.

Proof. We have proved *(i)* in section 4. For a proof of *(ii)* and *(iii)* we refer to Lang's book. Part *(iv)* is a rather easy consequence of the properties of the Γ-function that are listed in Prop.9.1. There is also a theory of special values of Dedekind ζ-functions. See Tate's book on Stark's conjectures [74] for more details. The Generalized Riemann Hypothesis is the statement that all non-trivial zeroes of $\zeta_F(s)$ have their real parts equal to $1/2$. This important conjecture conjecture has not been proved.

(9.A) Let $\log(z)$ denote the branch of the logarithm with argument ϕ satisfying $0 \leq \phi < 2\pi$. Let $C_{\varepsilon,R}$ be the contour in $\mathbf{C}$, from ε to R, then counterclockwise on a large circle of radius R via $-R$ back to R with argument 2π, then to ε (with argument 2π) and clockwise back to ε (with argument 0) via a small circle of radius ε. Show that for $s \in \mathbf{C}$, $0 < \mathrm{Re}(s) < 1$

$$\int_{C_{\varepsilon,R}} \frac{z^{s-1}}{z+1} dz = -e^{s\pi i} 2\pi i.$$

Show that the contributions to the integral of the parts over the circles of radius ε and R tend to 0 as $\varepsilon \to 0$ and $R \to \infty$ respectively. Conclude that

$$\int_0^\infty \frac{x^{s-1}}{x+1} dx = \frac{\pi}{\sin(\pi s)}.$$

(9.B) Verify the entries of the following table

$$\begin{array}{lll}
\zeta(-4) = 0 & \zeta(-1) = -1/12 & \zeta(2) = \pi^2/6 \\
\zeta(-3) = 1/120 & \zeta(0) = -1/2 & \zeta(3) = 1.2020569\ldots \\
\zeta(-2) = 0 & \zeta(1) = \infty & \zeta(4) = \pi^4/90
\end{array}$$

(9.C) Verify Theorem 9.4 for the Dedekind ζ-function of $\mathbf{Q}$.

(9.D) Verify that the set Γ_1 occurring in the proof of Theorem 9.4, is bounded.

(9.E)*Let $\mathbf{F}_q$ be a finite field with q elements. Let $\zeta(s)$ denote the ζ-function of the ring $\mathbf{F}_q[T]$:

$$\zeta_{\mathbf{F}_q(T)}(s) = \sum_{I \neq 0} \frac{1}{\mathrm{N}(I)^s}.$$

s (Here the product runs over the non-zero ideals I and $\mathrm{N}(I) = [\mathbf{F}_q[T] : I]$.) Show that

$$\zeta_{\mathbf{F}_q(T)}(s) = \frac{1}{1 - q^{1-s}}.$$

What is the ζ-function of the ring $\mathbf{F}_q[X,Y]/(X^2+Y^2+1)$? (Hint: conclude from Exer.1.L that the conic $X^2+Y^2+1 = 0$ is isomorphic to the projective line over $\mathbf{F}_q$.)

(9.K)*Show that

$$\Gamma(2s) = \frac{1}{\sqrt{2\pi}} 2^{2s-1/2} \Gamma(s)\Gamma(s+\frac{1}{2}).$$

(9.M) Show that

$$\Theta(z) + \Theta(z+\frac{1}{2}) = 2\Theta(4z).$$

10. Hilbert Theory.

From now on we will assume that the reader knows the main results of Galois theory. These can be found in Stewart's book [71] or in Lang's *Algebra* [41].

When a number field F is a *Galois* extension of $\mathbf{Q}$, the Galois group $G = \mathrm{Gal}(F/\mathbf{Q})$ acts on many of the objects that we have introduced. This gives rise to additional structure and symmetry. In this section we discuss the action of the Galois group on the primes of F that divide a fixed prime number p. Many of the concepts that we mention were introduced by D. Hilbert (German mathematician (1862–1943)) in his *Zahlbericht* [34].

Suppose F is a number field which is a Galois extension of $\mathbf{Q}$ with $G = \mathrm{Gal}(F/\mathbf{Q})$. The Galois group G acts on F, but it also acts naturally on many objects associated to F. It is, for instance, easily verified that for every $\sigma \in G$ one has that $\sigma(x)$ is integral whenever x is. This implies that G acts on the ring of integers O_F of F. Similarly, for every ideal I of O_F and every $\sigma \in G$ the set $\{\sigma(x) : x \in I\}$ is again an ideal. The same is true for any fractional ideal I. We see that G acts on the ideal group.

In a similar way, it is easily checked that the group G acts on the unit group O_F^* and on the class group $Cl(O_F)$. For every prime ideal $\mathfrak{p}$ of O_F and every $\sigma \in G$, the ideal $\sigma(\mathfrak{p})$ is again prime. A final useful observation is the following: By Prop.4.8 every prime ideal of O_F divides a unique prime number p. This prime number p is contained in the prime ideal $\mathfrak{p} \cap \mathbf{Z}$ and therefore $\mathfrak{p} \cap \mathbf{Z} = (p)$.

Proposition (10.1). *Let F be a number field with $G = \mathrm{Gal}(F/\mathbf{Q})$. Then*

(i) The Galois group G acts simply transitively on the embeddings $\phi : F \longrightarrow \mathbf{C}$ via $\sigma(\phi)(x) = \phi(\sigma^{-1}(x))$.

(ii) The group G acts transitively on the primes $\mathfrak{p}$ of O_F that divide a fixed prime number p.

(iii) Let $x \in F$. We have that $\mathrm{N}(x) = \prod_{\sigma \in G} \sigma(x)$ and $\mathrm{Tr}(x) = \sum_{\sigma \in g} \sigma(x)$.

Proof. *(i)* Let $\phi : F \longrightarrow \mathbf{C}$ be any embedding of F into $\mathbf{C}$. Suppose $\sigma, \tau \in G$ and $\sigma(\phi) = \tau(\phi)$. This implies that $= \phi(\sigma^{-1}(x)) = \phi(\tau^{-1}(x))$ for all $x \in F$. Since ϕ is injective, it follows that $\sigma = \tau$. We deduce that there are at least $\#G$ embeddings of the form $\sigma(\phi)$. On the other hand, there are, by Cor.2.2, exactly $[F : \mathbf{Q}] = \#G$ embeddings $F \hookrightarrow \mathbf{C}$ at all. Therefore the group G acts simply transitively on the set of embeddings $F \hookrightarrow \mathbf{C}$.

(iii) Let $x \in F$ and let $\phi : F \longrightarrow \mathbf{C}$ be an embedding of F into $\mathbf{C}$. We have $\phi(\prod_{\sigma \in G} \sigma(x)) = \prod_{\sigma \in G} \phi(\sigma^{-1}(x))$. By *(i)* this is equal to $\prod_{\phi' : F \hookrightarrow \mathbf{C}} \phi'(x)$ and by Prop.2.5*(iii)* this is equal to $\mathrm{N}(x)$. since $\mathrm{N}(x) \in \mathbf{Q}$, we conclude that $\phi(\prod_{\sigma \in G} \sigma(x)) = \phi(\mathrm{N}(x))$. Part *(iii)* now follows from the fact that ϕ is injective.

(ii) Let $\mathfrak{p}$ be a prime ideal of O_F. If $\mathfrak{p}$ divides p for a prime number p, we have, for every $\sigma \in G$, that $\sigma(\mathfrak{p})$ divides $\sigma(p) = p$. So G acts on the primes dividing $\mathfrak{p}$. Suppose $\mathfrak{p}'$ is a prime dividing p which is *not* of the form $\sigma(\mathfrak{p})$ for any $\sigma \in G$. By the Chinese Remainder Theorem (Exer.4.G) we can find an $x \in O_F$ such that

$$\begin{aligned} x &\equiv 0 \pmod{\mathfrak{p}'}, \\ &\equiv 1 \pmod{\sigma(\mathfrak{p})} \qquad \text{for all } \sigma \in G. \end{aligned}$$

From *(ii)* and the first congruence we deduce that $\mathrm{N}(x) \in \mathfrak{p} \cap \mathbf{Z} = (p)$. The second congruence implies that $\sigma^{-1}(x) \notin \mathfrak{p}$ for every $\sigma \in G$. Since $\mathfrak{p}$ is prime this implies that $\mathrm{N}(x) = \prod_{\sigma \in g} \sigma(x) \notin \mathfrak{p} \cap \mathbf{Z} = (p)$. This contradiction shows that G acts transitively on the prime ideals that divide p.

Definition. *Let F be a finite Galois extension of $\mathbf{Q}$ with $G = \mathrm{Gal}(F/\mathbf{Q})$. Let p be a prime number. For every prime ideal $\mathfrak{p}$ of F dividing p we put*

$$\begin{aligned} G_{\mathfrak{p}} &= \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\}, \\ I_{\mathfrak{p}} &= \{\sigma \in G_{\mathfrak{p}} : \sigma \equiv \mathrm{id} \pmod{\mathfrak{p}}\}. \end{aligned}$$

The group $G_{\mathfrak{p}}$ is called the decomposition group of the prime ideal $\mathfrak{p}$. The group $I_{\mathfrak{p}}$ is a normal subgroup of $G_{\mathfrak{p}}$; it is called the inertia group of $\mathfrak{p}$.

Proposition (10.2). *Let F be a finite Galois extension of $\mathbf{Q}$ with $G = \mathrm{Gal}(F/\mathbf{Q})$. Let p be a prime number and let $\mathfrak{p}$ be a prime of O_F dividing p.*
(i) For every $\sigma \in G$ one has that

$$G_{\sigma(\mathfrak{p})} = \sigma G_{\mathfrak{p}} \sigma^{-1}.$$

(ii) There is an exact sequence

$$0 \longrightarrow I_{\mathfrak{p}} \longrightarrow G_{\mathfrak{p}} \longrightarrow \mathrm{Gal}((O_F/\mathfrak{p})/\mathbf{F}_p) \longrightarrow 0.$$

Proof. *(i)* We have that $\tau \in G_{\sigma(\mathfrak{p})}$ if and only if $\tau\sigma(\mathfrak{p}) = \sigma(\mathfrak{p})$ i.e. if and only if $\sigma^{-1}\tau\sigma \in G_{\mathfrak{p}}$. This proves *(i)*.
(ii) It is only necessary to prove the surjectivity of the map $G_{\mathfrak{p}} \longrightarrow \mathrm{Gal}((O_F/\mathfrak{p})/\mathbf{F}_p)$: pick a generator ζ of the multiplicative group $(O_F/\mathfrak{p})^*$. By the Chinese Remainder Theorem, we can find $\alpha \in O_F$ such that

$$\alpha \equiv \begin{cases} \zeta \pmod{\mathfrak{p}} \\ 0 \pmod{\mathfrak{p}'} & \text{for the other primes } \mathfrak{p}' \text{ dividing } p. \end{cases}$$

Let $g(T) = \prod_{\sigma\in G}(T - \sigma(\alpha)) \in \mathbf{Z}[T]$. We have that

$$g(T) \equiv T^{n-\#G_{\mathfrak{p}}} \prod_{\sigma\in G} (T - \sigma(\alpha)) \pmod{\mathfrak{p}}$$

and, since $g(T) \in \mathbf{Z}[T]$, we have the same congruence modulo p as well. Let $h(T) \in \mathbf{F}_p[T]$ be the minimum polynomial of ζ over $\mathbf{F}_p$. Since $g(\alpha) = 0$, but $\alpha \equiv \zeta \not\equiv 0 \pmod{\mathfrak{p}}$, we have that $h(T)$ divides $g(T)$ in $\mathbf{F}_p[T]$. Therefore α^p is a zero of $g(T)$ and we conclude that there is a $\sigma \in G_{\mathfrak{p}}$ such that $\sigma(\zeta) = \zeta^p$. So the image of σ generates the Galois group of $O_F/\mathfrak{p}$ over $\mathbf{F}_p$. This proves *(ii)*.

Let F be a finite Galois extension of $\mathbf{Q}$ with Galois group G. By Prop.10.2*(i)*, the cardinalities of their decompostion groups are the same. Since G permutes the prime ideals that divide a fixed prime number p, we see that the norms of all these ideals are equal, and hence by Prop.10.2*(ii)* that $e_{\mathfrak{p}} = \#I_{\mathfrak{p}}$, and that $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ are the same for every prime $\mathfrak{p}$ dividing p. Since these numbers only depend on p, we sometimes write e_p for $e_{\mathfrak{p}}$ and f_p for $f_{\mathfrak{p}}$. We have that $g_p f_p e_p = n$, where g_p is the number of primes ideals dividing p.

When p is *unramified* in F over $\mathbf{Q}$, the inertia groups $I_{\mathfrak{p}}$ are trivial for all primes $\mathfrak{p}$ dividing p. In this case the map

$$G_{\mathfrak{p}} \longrightarrow \mathrm{Gal}((O_F/\mathfrak{p})/\mathbf{F}_p)$$

is an isomorphism. We define $\phi_{\mathfrak{p}}$ to be the automorphism in $G_{\mathfrak{p}}$ that corresponds to the automorphism of O_F given by $x \mapsto x^p$. The map $\phi_{\mathfrak{p}}$ is called the *Frobenius automorphism of* $\mathfrak{p}$ (G. Frobenius, German mathematician 1849–1917). It depends on the ideal $\mathfrak{p}$, but it is easy to check that its conjugacy class depends only on p.

Next we study an extension $\mathbf{Q} \subset K \subset F$ of number fields. We describe how the decomposition and inertia groups corresponding to the different extensions are related.

Proposition (10.3). *Let F be a number field with $G = \mathrm{Gal}(F/\mathbf{Q})$ and let K be a Galois extension of $\mathbf{Q}$ with $\mathbf{Q} \subset K \subset F$ and $H = \mathrm{Gal}(F/K)$. Let p be a prime number, let $\mathfrak{p}$ be a prime ideal of K dividing p and let $\mathfrak{p}'$ be a prime ideal of F dividing $\mathfrak{p}$.*
(i) For the decomposition group of $\mathfrak{p}'$ we have that $(G/H)_{\mathfrak{p}} = G_{\mathfrak{p}'} \pmod{H}$

(ii) The inertia group of $\mathfrak{p}$ in G/H is just the inertia group of $I_{\mathfrak{p}'}$ modulo H.

(iii) We have that

$$p \text{ splits completely in } K \Leftrightarrow G_{\mathfrak{p}'} \subset H,$$
$$p \text{ is unramified in } K \Leftrightarrow I_{\mathfrak{p}'} \subset H.$$

Proof. Since $\mathfrak{p}'$ divides $\mathfrak{p}$ in O_F, one has that $\mathfrak{p}' \cap O_K = \mathfrak{p}$. From this observation parts *(i)* and *(ii)* are immediate. Part *(ii)* is the special case where $(G/H)_{\mathfrak{p}}$ and the inertia groiup of $\mathfrak{p}$ in G/H are trivial. This completes the proof of the proposition.

In the rest of this section we will illustrate Propositions (10.1)–(10.3) by the cyclotomic fields $\mathbf{Q}(\zeta_m)$. The cyclotomic fields are Galois extensions of $\mathbf{Q}$. Every σ in the Galois group of $\mathbf{Q}(\zeta_m)$ over $\mathbf{Q}$ is determined by its image $\sigma(\zeta_m)$ of ζ_m. Since the Galois group maps *primitive* m-th roots of unity to *primitive* m-th roots of unity, we get an injective natural map

$$\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}) \longrightarrow (\mathbf{Z}/m\mathbf{Z})^*.$$

In the next proposition we show that this natural map is, in fact, an isomorphism.

Theorem (10.4). *The cyclotomic polynomial $\Phi_m(T) \in \mathbf{Z}[T]$ is irreducible. The Galois group of $\mathbf{Q}(\zeta_m)$ over $\mathbf{Q}$ is canonically isomorphic to $(\mathbf{Z}/m\mathbf{Z})^*$.*

Proof. Since $\deg(\Phi_m(T)) = \phi(m) = \#((\mathbf{Z}/m\mathbf{Z})^*)$, the surjectivity will follow from the irreducibility of the cyclotomic polyniomial $\Phi_m(T)$.

Let $g(T) \in \mathbf{Z}[T]$ be an irreducible factor of $\Phi(T)$ and write $\Phi(T) = g(T)h(T)$. Let p be a prime not dividing m. Suppose α is a zero of g. Then α is a zero of $T^m - 1$ and so is α^p. If $g(\alpha^p) \neq 0$, then $h(\alpha^p) = 0$ and therefore $g(T)$ divides $h(T^p)$. This implies that $g(T)$ divides $h(T)^p$ in the ring $\mathbf{F}_p[T]$. Let $\phi(T)$ denote the minimum polynomial of α over $\mathbf{F}_p$. Then $\phi(T)$ divides both $g(T)$ and $h(T)$ modulo p. this implies that $T^m - 1$ has a double zero mod p. But this is impossible because the derivative mT^{m-1} has, since $m \not\equiv 0 \pmod p$, no zeroes in common with $T^m - 1$.

Therefore $g(\alpha^p) = 0$. We conclude that for *every* prime not dividing m, one has that $g(\alpha^p) = 0$ whenever $g(\alpha) = 0$. This implies that $g(\alpha^k) = 0$ for every integer k which is coprime to m. This shows that $\Phi_m(T)$ and $g(T)$ have the same zeroes and the result follows.

Proposition (10.5). *Let $m \in \mathbf{Z}$ with $m \not\equiv 2 \pmod 4$ and let p be a prime number. Then*

(i) If p does not divide m then p is not ramified in $\mathbf{Q}(\zeta_m)$ over $\mathbf{Q}$. Moreover, identifying $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ with $(\mathbf{Z}/m\mathbf{Z})^*$, we have that

$$G_{\mathfrak{p}} =< p >\subset (\mathbf{Z}/m\mathbf{Z})^*.$$

(ii) If p divides m then p ramifies in $\mathbf{Q}(\zeta_m)$ over $\mathbf{Q}$. Writing $m = p^k m'$ where p does not divide m' we have that

$$I_p = \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}(\zeta_{m'}))$$

while G_p contains I_p and

$$G_P/I_p =< p >\subset (\mathbf{Z}/m'\mathbf{Z})^*.$$

Proof. *(i)* The proof is by induction with respect to the number of primes dividing m. Suppose l is a prime dividing m. Say $m = m'l^n$ where l does not divide m'. We have the following diagram

$$\begin{tikzcd}
 & \mathbf{Q}(\zeta_m) & \\
\mathbf{Q}(\zeta_{m'}) & & \mathbf{Q}(\zeta_{l^n}) \\
 & \mathbf{Q} &
\end{tikzcd}$$

We put $H_1 = \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}(\zeta_{m'}))$ and $H_2 = \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}(\zeta_{l^n}))$. We have that $H_1 \cap H_2 = \{1\}$ and that $H_1H_2 = \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$. By Example 6.4 the ring of integers of $\mathbf{Q}(\zeta_{l^n})$ is precisely $\mathbf{Z}[\zeta_{l^n}]$ and we can apply the Factorization Lemma to determine the splitting behaviour of any prime number p. The minimum polynomial of ζ_{l^n} is the cyclotomic polynomial $\Phi_{l^n}(T)$, which divides $X^{l^n} - 1$. Therefore, only the prime l ramifies. Since p does not divide m, we have that $p \neq l$ and hence that p is not ramified in $\mathbf{Q}(\zeta_{l^n})$. Therefore, by Lemma (7.3), we have that $I_p \subset H_1$. By induction also $I_p \subset H_2$ and hence $I_p \subset H_1 \cap H_2 = \{1\}$. This implies that I_p is trivial and hence that p is unramified in $\mathbf{Q}(\zeta_m)$.

(ii) Consider the following diagram

$$\begin{tikzcd}
 & \mathbf{Q}(\zeta_m) & \\
\mathbf{Q}(\zeta_{m'}) & & \mathbf{Q}(\zeta_{p^k}) \\
 & \mathbf{Q} &
\end{tikzcd}$$

By Example 6.4, the ring $\mathbf{Z}[\zeta_{p^k}]$ is the ring of integers of $\mathbf{Q}(\zeta_{p^k})$. Since the cyclotomic polynomial $\Phi_{p^k}(T) \equiv (T-1)^{\phi(p^k)} \pmod{p}$, we see that p is totally ramified in the extension $\mathbf{Q}(\zeta_{p^k})$ over $\mathbf{Q}$. Therefore the ramification index of p in the extension $\mathbf{Q}(\zeta_m)$ over $\mathbf{Q}$ is at least $\phi(p^k)$. By *(i)*, the prime p is unramified in the extension $\mathbf{Q}(\zeta_{m'})$. Therefore, by Prop.10.3, the inertia group of p is contained in $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}(\zeta_{m'}))$, which has cardinality $\phi(p^k)$. We conclude that I_p is equal to $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}(\zeta_{m'}))$. The rest of *(ii)* follows from *(i)*, applied to the field $\mathbf{Q}(\zeta_{m'})$.

As an illustration of the theory of decomposition and inertia groups, we will prove the law of Quadratic Reciprocity. For an odd prime p, we introduce the *Legendre symbol* (A.M. Legendre, French Mathematician 1752–1833). For $x \in \mathbf{Z}$ we put

$$\left(\frac{x}{p}\right) = \begin{cases} -1, & \text{if } x \text{ is a not a square modulo } p, \\ 0, & \text{if } x = 0, \\ 1, & \text{otherwise.} \end{cases}$$

The induced map $(\frac{x}{p}) : (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \{\pm 1\}$ is easily seen to be a surjective homomorphism. Its kernel is the subgroup of squares. Since the homomorphism $(\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \{\pm 1\} \subset (\mathbf{Z}/p\mathbf{Z})^*$ given by $x \mapsto x^{(p-1)/2}$ has the same kernel, they must agree and we obtain *Euler's Formula:*

$$\left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \pmod{p} \qquad \text{for all } x \in \mathbf{Z}.$$

The following Lemma is the principal ingredient in the proof of the Law of quadratic reciprocity. Part *(iii)* is of interest in itself. This statement can be seen as a reformulation of the law of quadratic reciprocity. This formulation is better suited for generalizations.

Lemma (10.6).

(i) We have that $\sqrt{-1} \in \mathbf{Q}(\zeta_4)$ and $\sqrt{2}, \sqrt{-2} \in \mathbf{Q}(\zeta_8)$.

(ii) Let p be an odd prime then

$$\begin{aligned} \sqrt{p} &\in \mathbf{Q}(\zeta_p) \qquad \text{for} \quad p \equiv 1 \pmod{4}, \\ \sqrt{-p} &\in \mathbf{Q}(\zeta_p) \qquad \text{for} \quad p \equiv 3 \pmod{4}. \end{aligned}$$

(iii) Let F be a quadratic field with discriminant Δ. Then $F \subset \mathbf{Q}(\zeta_{|\Delta|})$.

Proof. *(i)* We have that $i = \zeta_4$ is a square root of -1 and that $\zeta_8 \pm \zeta_8^{-1}$ is a square root of ± 2.
(ii) Let

$$\tau = -\sum_{x \in \mathbf{F}_p^*} \left(\frac{x}{p}\right) \zeta_p^x$$

be the *Gaussian sum* associated to the homomorphism $(\frac{x}{p}) : (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \{\pm 1\}$. We view τ in the complex numbers via one of the embeddings $\phi : \mathbf{Q}(\zeta_p) \hookrightarrow \mathbf{C}$. Since $\zeta^{-1} = \bar{\zeta}$ for every root of unity ζ, one has that

$$\bar{\tau} = \left(\frac{-1}{p}\right) \tau.$$

We compute the absolute value bfn √e bthe e e √ee∑e fe bf7 ∯ i e e e fi e e

(ii)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

(iii) Let q be an odd prime different from p. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof. *(i)* is immediate from Euler's formula. To prove *(ii)* we take an 8th root of unity in $\alpha = \zeta_8 \in \overline{\mathbf{F}_p}$. We have that $\zeta_8^4 = -1$ and hence that $\alpha^2 = 2$. Using this relation we see that

$$\alpha^p = \zeta_8^p + \zeta_8^{-p} = \begin{cases} \zeta_8 + \zeta_8^{-1} = \alpha, & \text{if } p \equiv \pm 1 \pmod 8, \\ \zeta_8^3 + \zeta_8^{-3} = -\alpha, & \text{if } p \equiv \pm 3 \pmod 8, \end{cases}$$

This implies that $\sqrt{2} = \alpha$ is in the field $\mathbf{F}_p$ if and only if $p \equiv \pm 1 \pmod 8$. this proves *(ii)*. *(iii)* Consider the quadratic subfield $F = \mathbf{Q}(\sqrt{(\frac{-1}{p})p})$ of $\mathbf{Q}(\zeta_p)$. The discriminant of the minimum polynomial of $(\frac{-1}{p})p$ is $\pm 4p$. By the Factorization Lemma (Theorem 6.1), we have that

$$q \text{ splits in } F \quad\Longleftrightarrow\quad \left(\tfrac{-1}{p}\right) p \text{ is a square mod } q$$

or, using Euler's formula

$$q \text{ splits in } F \quad\Longleftrightarrow\quad \left(\frac{(-1)^{(p-1)/2}p}{q}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1.$$

On the other hand, we use Hilbert's theory to see when q splits in F. The Galois group of $\mathbf{Q}(\zeta_p)$ over F is the unique subgroup of index 2 in $(\mathbf{Z}/p\mathbf{Z})^*$. Therefore it is the subgroup of squares. By Prop.10.5, we conclude that

$$q \text{ splits in } F \quad\Longleftrightarrow\quad q \in ((\mathbf{Z}/p\mathbf{Z})^*)^2$$

equivalently

$$q \text{ splits in } F \quad\Longleftrightarrow\quad \left(\frac{q}{p}\right) = 1.$$

This proves the theorem.

C.F. Gauß (German mathematician, 1777–1855) [26] gave several proofs of his reciprocity law. The "law" can be used to calculate the value of $(\frac{x}{p})$ efficiently. For these purposes it is important to have a Legendre symbol for composite numbers as well. This is discussed in Exer.10.E.

w ing theorem is due tc H. Weber (German mathematician 1 is very subtle and is peculiar for $\mathbf{Q}$: i field.

Theorem (10.8). *(Kronecker-Webe integer m such that*

We do not give a proof of this theorem. There is a huge generalization of it to base fields other than **Q**: *Class Field Theory* gives a description of the finite abelian extensions of a number field F in terms of the "internal" arithmetic of F. This theory was developed by Hilbert (1862–1943), Furtwängler (1800–1900), Takagi (1875–1960), Artin (1898–1962) and Hasse (1898–1979) in the period 1910–1930. For classical expositions of class field theory see Lang's [42], or Janusz' [35] book ; for a cohomological approach see the Artin-Tate notes [5] or the volume by Cassels and Fröhlich [12].

The Kronecker-Weber theorem is actually more precise than the general theorems of class field theory: it gives explicit generators for the abelian extensions of **Q**, viz. roots of unity. Such a precise statem

11. Dirichlet L-series.

In this section we will factorize the Dedekind ζ-function associated to a cyclotomic field $\mathbf{Q}(\zeta_m)$ into a product of so-called Dirichlet L-series. As a consequence we obtain another expression for the "residue" of the ζ-function $\zeta_F(s)$ at $s=1$ that has been computed in section 6. A rather straightforward application is the famous theorem of Dirichlet on the existence of primes in arithmetic progressions.

Definition. *Let G be a group. A character* χ of G is a homomorphism $\chi : G \longrightarrow \mathbf{C}^*$. The characters of G form a group under multiplication: $(\chi_1\chi_2)(x) = \chi_1(x)\chi_2(x)$. This group is called the *dual group* or *character group* of G and is denoted by $\widehat{G}$. The neutral element of $\widehat{G}$ is the homomorphism that maps every element to 1. It is denoted by 1.

For any homomorphism $f : G_1 \longrightarrow G_2$ of groups there is a natural homomorphism $\widehat{f} : \widehat{G_2} \longrightarrow \widehat{G_1}$ given by $\widehat{f}(\chi)(x) = \chi(f(x))$. It is easy to see that for an exact sequence of groups

$$1 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 1$$

the associated "dual" sequence

$$1 \longrightarrow \widehat{G/H} \longrightarrow \widehat{G} \longrightarrow \widehat{H}$$

is also exact (Exer.11.B). In general the homomorphism $\widehat{G} \longrightarrow \widehat{H}$ is not surjective. For finite abelian groups, however, one has the following.

Proposition (11.1).

(i) For any finite abelian group G, the dual group $\widehat{G}$ is isomorphic to G.

(ii) The canonical homomorphism $G \longrightarrow \widehat{\widehat{G}}$ given by $x \mapsto \Xi$, where Ξ is defined by $\Xi(\chi) = \chi(x)$, is an isomorphism.

(iii) For any exact sequence of finite abelian groups

$$1 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 1$$

the dual sequence

$$1 \longrightarrow \widehat{G/H} \longrightarrow \widehat{G} \longrightarrow \widehat{H} \longrightarrow 1$$

is also exact.

(iv) (Orthogonality relations.) For any $\chi \in \widehat{G}$ one has that

$$\sum_{g \in G} \chi(g) = \begin{cases} \#G, & \text{if } \chi = 1, \\ 0, & \text{if } \chi \neq 1. \end{cases}$$

For any $g \in G$ one has that

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} \#G, & \text{if } g = 1, \\ 0, & \text{if } g \neq 1. \end{cases}$$

Proof. *(i)* It is easy to verify that the map $h : \widehat{G_1} \times \widehat{G_2} \longrightarrow \widehat{G_1 \times G_2}$ given by $h(\chi_1, \chi_2)(x, y) = \chi_1(x)\chi_2(y)$ is an isomorphism. Since, by Cor.5.2*(ii)*, every finite abelian group is a product of cyclic groups, it suffices to show that the dual of a cyclic group of order m is also cyclic of order m.

This is immediate: let G be cyclic of order m, generated by g. Any homomorphism $\chi : G \longrightarrow \mathbf{C}^*$ is determined by $\chi(g)$. Since $(\chi(g))^m = \chi(g^m) = 1$, we see that $\chi(g)$ is necessarily an m-th

root of unity. Conversely, for any m-th root of unity ζ, the map $\chi : G \longrightarrow \mathbf{C}^*$ given by $\chi(g^a) = \zeta^a$ is a homomorphism. This proves *(i)*.
(ii) Suppose Ξ is trivial. This means that $\Xi(\chi) = \chi(x) = 1$ for all characters χ or, equivalently, that $x \in \ker(\chi)$ for all characters χ. Therefore, the injection $G/\widehat{<x>} \hookrightarrow \widehat{G}$ is surjective. Since G is finite, we must have that $x = 1$ and we conclude that $G \longrightarrow \widehat{\widehat{G}}$ is injective, as required.
(iii) Suppose

$$1 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 1$$

is exact. The dual sequence is exact, except, possibly for the surjectivity of $\widehat{G} \longrightarrow \widehat{H}$. For finite abelian groups the surjectivity follows from *(i)* and by counting cardinalities.
(iv) If $\chi = 1$ on has that $\sum_g \chi(g) = \sum_g 1 = \#G$. If $\chi \neq 1$, we pick $h \in G$ such that $\chi(h) \neq 1$. Let $S = \sum_g \chi(g)$. Then $\chi(h)S = \sum_g \chi(hg) = \sum_g \chi(g) = S$. Therefore $(\chi(h) - 1)S = 0$ and $S = 0$ as required. The other statement follows by duality, but can also be proved in a similar way.

Lemma (11.2). *(Partial summation) Let $a_n, b_n \in \mathbf{C}$ for $n = 1, 2, \ldots$. Put $A_n = \sum_{k=1}^n a_k$ and $B_n = \sum_{k=1}^n b_k$. Then*

$$\sum_{n=M+1}^{N} a_n b_n = A_N b_N - A_M b_{M+1} + \sum_{M+1}^{N-1} A_n (b_n - b_{n+1}).$$

Proof.

$$\sum_{n=M+1}^{N} a_n b_n = \sum_{M+1}^{N} (A_n - A_{n-1}) b_n = \sum_{M+1}^{N} A_n b_n - \sum_{M}^{N-1} A_n b_{n+1},$$
$$= A_N b_N - A_M b_{M+1} + \sum_{M+1}^{N-1} A_n (b_n - b_{n+1}).$$

as required.

We are mainly interested in the finite abelian groups $G = (\mathbf{Z}/m\mathbf{Z})^*$. In this case the characters of G are often called *Dirichlet characters.* Whenever f divides m, the canonical surjection $(\mathbf{Z}/m\mathbf{Z})^* \longrightarrow (\mathbf{Z}/f\mathbf{Z})^*$ gives rise to an injective dual map:

$$\widehat{(\mathbf{Z}/f\mathbf{Z})^*} \hookrightarrow \widehat{(\mathbf{Z}/m\mathbf{Z})^*}.$$

In this way we can view the characters of $(\mathbf{Z}/f\mathbf{Z})^*$ as a subset of the characters of $(\mathbf{Z}/m\mathbf{Z})^*$.

De e

Here χ_k has conductor k.

It is sometimes convenient to view a character χ of $(\mathbf{Z}/m\mathbf{Z})^*$ as a function on $\mathbf{Z}$. This can be done by lifting χ to the integers that are prime to m and extending χ to all of $\mathbf{Z}$ by 0. However, some care must be taken. The resulting function χ on $\mathbf{Z}$ vanishes on all integers that are not coprime to m, even if they *are* coprime to the conductor of χ. We will *always* assume that characters χ are lifted "from" $(\mathbf{Z}/f\mathbf{Z})^*$, where f is the conductor of χ. As a consequence $\chi(k) = 0$ if and only if k is not coprime to the conductor of χ. This kind of characters are called *primitive* in the literature. Note that the resulting functions on $\mathbf{Z}$ are not homomorphisms, but they are multiplicative: $\chi(xy) = \chi(x)\chi(y)$ for *all* $x, y \in \mathbf{Z}$.

Definition. *Let $\chi : (\mathbf{Z}/m\mathbf{Z})^* \longrightarrow \mathbf{C}^*$ be a character. We define the Dirichlet L-series* associated to χ by

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \qquad \text{for } s \in \mathbf{C},\ \mathrm{Re}(s) > 1.$$

(Remember how χ has been lifted to $\mathbf{Z}$!)

Proposition (11.3). *Let $\chi : (\mathbf{Z}/m\mathbf{Z})^* \longrightarrow \mathbf{C}^*$ be a Dirichlet character.*

(i) If $\chi \neq 1$ then $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges for $s \in \mathbf{C}$, $\mathrm{Re}(s) > 0$.

(ii) One has that

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \qquad \textit{for } s \in \mathbf{C},\ \mathrm{Re}(s) > 1.$$

where the product runs over the prime numbers.

Proof. We apply partial summation (Lemma 11.2) to the series $\sum_n a_n b_n$ with $a_n = \chi(n)$ and $b_n = 1/n^s$. We find for $N > M > 0$ that

$$\sum_{n=M+1}^{N} \frac{\chi(n)}{n^s} = \frac{\sum_{n=1}^{N}\chi(n)}{N^s} - \frac{\sum_{n=1}^{M}\chi(n)}{(M+1)^s} + \sum_{n=M+1}^{N-1}\left(\sum_{k=1}^{n}\chi(k)\right)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right).$$

The character χ is periodic modulo m. Since it is not trivial, we have, by Prop.11.1, that $\sum_{k \pmod f}\chi(k) = 0$. Therefore any sum $\sum_{k=a}^{b}\chi(k)$ has an absolute value at most m, where m is a period of χ, and usually much less. Using this, plus the fact that

$$\frac{1}{n^s} - \frac{1}{(n+1)^s} = -s\int_n^{n+1}\frac{dx}{x^{s+1}}$$

we find that

$$\left|\sum_{n=M+1}^{N}\frac{\chi(n)}{n^s}\right| \le \frac{m}{N^{\mathrm{Re}(s)}} + \frac{m}{(M+1)^{\mathrm{Re}(s)}} + m|s|\int_{M+1}^{\infty}\frac{dx}{x^{\mathrm{Re}(s)+1}}$$

Letting $N \to \infty$ we get

$$\left|\sum_{n=M+1}^{\infty}\frac{\chi(n)}{n^s}\right| \le \frac{m}{(M+1)^{\mathrm{Re}(s)}} + m\left|\frac{s}{\mathrm{Re}(s)}\right|\frac{1}{(M+1)^{\mathrm{Re}(s)}}$$

Since $\mathrm{Re}(s) > 0$, the right hand side tends to 0 when $M \to \infty$. This implies that the L-series converges as required.

(ii) This is immmediate from the fact that χ is multiplicative on $\mathbf{Z}$. The proof is similar to the one given at the end of section 4 for the Riemann ζ-function.

The following theorem is the main result of this section. It is a rather easy consequence of the work we did in sections 7–10.

Theorem (11.4). *Let* $\mathbf{Q}(\zeta_m)$ *be a cyclotomic field. Then*

(i)

$$\zeta_{\mathbf{Q}(\zeta_m)}(s) = \prod_{\chi} L(s,\chi) \qquad \text{for } s \in \mathbf{C},\ \mathrm{Re}(s) > 1.$$

Here χ *runs over all characters of* $(\mathbf{Z}/m\mathbf{Z})^*$.

(ii) Let F *be a subfield of* $\mathbf{Q}(\zeta_m)$. *Then*

$$\zeta_F(s) = \prod_{\substack{\chi \\ H \subset \ker(\chi)}} L(s,\chi) \qquad \text{for } s \in \mathbf{C},\ \mathrm{Re}(s) > 1.$$

(iii) Let F *be a subfield of* $\mathbf{Q}(\zeta_m)$. *Then*

$$\frac{2^{r_1}(2\pi)^{r_2} h_F R_F}{\sqrt{|\Delta_F|}w_F} = \prod_{\substack{\chi \neq 1 \\ H \subset \ker(\chi)}} L(1,\chi).$$

(iv) For every character $\chi \neq 1$ *one has that*

$$L(1,\chi) \neq 0.$$

Proof. Obviously *(i)* is a special case of *(ii)*. We will give the proof of *(i)* and briefly indicate how to modify this proof to obtain a proof of *(ii)*.

(i) Note that both the left hand side and the right hand side converge absolutely for $s \in \mathbf{C}$, $\mathrm{Re}(s) > 1$. By Prop.4.8 and the fact (Prop.4.7(*(i)*) that every prime ideal $\mathfrak{p}$ of the ring of integers of $\mathbf{Q}(\zeta_m)$ divides a prime number p, it suffices to show that for every prime p, one has that

$$\prod_{\mathfrak{p}|p} \left(1 - \frac{1}{\mathrm{N}\mathfrak{p}^s}\right)^{-1} = \prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

where the left hand product runs over the prime ideals $\mathfrak{p}$ that divide p and the right hand one over the characters of $(\mathbf{Z}/m\mathbf{Z})^*$. Since $\mathbf{Q}(\zeta_m)$ is a Galois extension of $\mathbf{Q}$ of degree $n = \phi(m)$, we can, by the remarks after Prop.10.2, for every prime p, write $n = efg$, where g is the number of primes dividing p. All these primes have norm p^f and they divide p with multiplicity e. It follows that the left hand side is equal to

$$\left(1 - \frac{1}{p^{fs}}\right)^{-g}.$$

It is now clear that it suffices to verify the following equality of polynomials in $\mathbf{C}[X]$:

$$\prod_{\chi}(1 - \chi(p)X) = (1 - X^f)^g.$$

If p does not divide m, we see that the product depends only on the images of the characters χ of the map $\widehat{(\mathbf{Z}/m\mathbf{Z})^*} \longrightarrow \widehat{<p>}$. From Prop.10.5, we conclude that the cardinality of the group generated by p in $(\mathbf{Z}/m\mathbf{Z})^*$ is precisely f. It follows that the kernel of this map has order g, and therefore

$$\prod_{\chi}(1 - \chi(p)X) = \left(\prod_{\chi}(1 - \chi(p)X)\right)^g$$

where, this time, the product runs over the characters of the cyclic group $< p >$. Since

$$\prod_{\chi}(1-\chi(p)X)=\prod_{\zeta^f=1}(1-\zeta X)=1-X^f$$

the result follows.

If p divides m, we write $m=p^km'$ where p does not divide m'. Let χ be a characters of $(\mathbf{Z}/m\mathbf{Z})^*$. Then $\chi(p)=0$ if and only if p divides the conductor of χ if and only if χ is *not* a character of $(\mathbf{Z}/m'\mathbf{Z})^*$. Therefore

$$\prod_{\chi}(1-\chi(p)X)=\prod_{\chi\in(\mathbf{Z}/m'\mathbf{Z})^*}(1-\chi(p)X)$$

By Prop.10.5, the inertia group of p in $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ is precisley the Galois group of $\mathbf{Q}(\zeta_m)$ over $\mathbf{Q}(\zeta_{m'})$. This implies that the ramification index e is equal to the index $[\mathbf{Q}(\zeta_m):\mathbf{Q}(\zeta_{m'})]$ and that the values of f and g that one has for $\mathbf{Q}(\zeta_{m'})$, are equal to the ones for $\mathbf{Q}(\zeta_m)$. the result now follows from the case $p\not|m$. This proves *(i)*.

(ii) From the proof of *(i)* it is clear that it suffices to show for every prime p the following identity

$$\prod_{\substack{\chi\\ H\subset\ker(\chi)}}(1-\chi(p)X)=(1-X^f)^g$$

in $\mathbf{C}[X]$, where g is the number of primes of F over p. The norms of these primes are all equal to p^f. Write $m=m'p^k$ where p does not divide m'. We have that

$$\prod_{\substack{\chi\\ H\subset\ker(\chi)}}(1-\chi(p)X)=\prod_{\chi}(1-\chi(p)X)$$

where the second product runs over the characters that are trivial on both H and the inertia group $I=\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}(\zeta_{m'}))$. By Prop.10.5*(ii)*, the group I is precisely the inertia group of p in the Galois group of $\mathbf{Q}(\zeta_m)$ over $\mathbf{Q}$. It follows from Prop.10.3*(ii)*, that the second product runs over the fg characters of F that vanish on the inertia group of p in $\mathrm{Gal}(F/\mathbf{Q})$.

As in *(i)*, the product only depends on the values of the characters on p. The result now follows as in *(i)*.

(iii) Consider the formula proved in *(ii)*. Divide by the Riemann ζ-function $\zeta(s)=L(1,s)$ and let s tend to 1. The result now follows from Theorem 9.4.

(iv) This is immediate from *(iii)*.

By the Kronecker-Weber Theorem, every finite abelian extension F of $\mathbf{Q}$ is contained in $\mathbf{Q}(\zeta_m)$ for some m. We conclude from Thm.11.4*(ii)* that the Dedekind ζ-function of every such extension F can be decomposed as a product of Dirichlet L-series. When $G=\mathrm{Gal}(F/\mathbf{Q})$ is not abelian, there is a similar decomposition of $\zeta_F(s)$ due to E. Artin (German mathematician 1898–1962). In this case one associates to each irreducible representation of G a so-called *Artin L-series* [12,Ch.8]. In the case where G is abelian, all the irreducible representations of G are 1-dimensional and the Artin L-series are just Dirichlet L-series.

The following theorem on “primes in arithmetical progressions” due to P. Lejeune-Dirichlet is a famous consequence of the mere fact that $L(1,\chi)\neq 0$ stated in Theorem 11.4*(iv)*.

Theorem (11.5). *(P.G. Lejeune-Dirichlet) Let $m \in \mathbf{Z}_{\geq 1}$ and let $a \in (\mathbf{Z}/m\mathbf{Z})^*$. There exist infinitely many primes $p \equiv a \pmod{m}$. More precisely their natural density is $1/\phi(m)$:*

$$\lim_{X\to\infty} \frac{\#\{p \leq X : p \textit{ prime and } p \equiv a \pmod{p}\}}{\#\{p \leq X : p \textit{ prime }\}} = \frac{1}{\phi(m)}.$$

Proof. Consider, for each character χ of $(\mathbf{Z}/m\mathbf{Z})^*$ the logarithm of $L(s,\chi)$ and of its product expansion. The resulting series are *absolutely convergent* for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$:

$$\log(L(s,\chi)) = -\sum_p \log\left(1 - \frac{\chi(p)}{p^s}\right) = \sum_p \frac{\chi(p)}{p^s} + O(1)$$

The $O(1)$ follows from the Taylor series expansion of the logarithm and the following estimates

$$\left|\sum_p \left(\frac{\chi(p)^2}{2p^{2s}} + \frac{\chi(p)^3}{3p^{3s}} + \ldots\right)\right| \leq \frac{1}{2}\sum_p \left(\frac{1}{p^{2\mathrm{Re}(s)}} + \frac{1}{p^{3\mathrm{Re}(s)}} + \ldots\right),$$

$$\leq \sum_p \frac{1}{p(p-1)} \leq \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1.$$

Introducing, for every $b \in (\mathbf{Z}/m\mathbf{Z})^*$ the functions

$$f_b(s) = \sum_{p\equiv b \pmod{m}} \frac{1}{p^s} \qquad s \in \mathbf{C} \text{ with } \mathrm{Re}(s) > 1.$$

we can write

$$\log(L(s,\chi)) = \sum_{b\in(\mathbf{Z}/m\mathbf{Z})^*} \chi(b) f_b(s) + O(1).$$

The orthogonality relations imply that

$$\begin{aligned} \sum_\chi \chi(a)^{-1}\log(L(s,\chi)) &= \sum_\chi \sum_b \chi(ba^{-1}) f_b(s) + O(1) \\ &= \sum_b f_b(s) \sum_\chi \chi(ba^{-1}) + O(1) \\ &= \phi(m) f_a(s) + O(1). \end{aligned}$$

Here χ runs over all characters of $(\mathbf{Z}/m\mathbf{Z})^*$.

Now we let s tend to 1. By Theorem 11.4*(iv)*, we have that $L(1,\chi) \neq 0$ for all characters $\chi \neq 1$. Since the Riemann ζ-function has a simple pole at 1 with residue 1, we see that

$$-\log(s-1) = \phi(m) f_a(s) + O(1) \qquad \text{for } s \to 1.$$

In other words

$$\lim_{s\to 1} \frac{\sum_{p\equiv a \pmod{m}} \frac{1}{p^s}}{\sum_p \frac{1}{p^s}} = \frac{1}{\phi(m)}.$$

This shows that the so-called analytic density is $1/\phi(m)$. One can show that in this case, the analytic density is equal to the "natural" density, that occurs in the statement of the theorem. See [67].

In the special case where $a = 1$, there is an easy proof, due to Euler, of the fact that there exist infinitely many primes congruent to $a \pmod{m}$. This proof is indicated in Exer.11.A. The following is an amusing corollary of this, easier, result.

Corollary (11.6). *For every finite abelian group G, there exists an extension F ~~of~~ $\mathbf{Q}$ with $A \sim$* Gal$(F/\mathbf{Q})$.

Proof. By Cor.5.2*(iii)*, we have that

$$A \cong \mathbf{Z}/a_1\mathbf{Z} \times \mathbf{Z}/a_2\mathbf{Z} \times \ldots \times \mathbf{Z}/a_t\mathbf{Z}$$

for certain integers $a_1, a_2, \ldots, a_t$ and t in $\mathbf{Z}_{\geq 1}$. Therefore it suffices to show that for all integers $N, t \in \mathbf{Z}_{\geq 1}$, there exists a number field F with $\text{Gal}(F/\mathbf{Q}) \cong (\mathbf{Z}/N\mathbf{Z})^t$. To show this, we pick t primes $l_1, l_2, \ldots, l_t \equiv 1 \pmod{N}$. We have that $\mathbf{Q}(\zeta_{l_1}, \ldots, \zeta_{l_t}) = \mathbf{Q}(\zeta_m)$ where $m = l_1 \cdot \ldots \cdot l_t$. By Theorem 10.4, the Galois group of $\mathbf{Q}(\zeta_m) \cong (\mathbf{Z}/m\mathbf{Z})^*$. The latter group is isomorphic to $(\mathbf{Z}/l_1\mathbf{Z})^* \times \ldots \times (\mathbf{Z}/l_t\mathbf{Z})^*$, a group which is a product of t cyclic groups of cardinality divisible by N. Therefore there is a surjective homomorphism

$$\text{Gal}(\mathbf{Q}(\zeta_m)\mathbf{Q}) \longrightarrow (\mathbf{Z}/N\mathbf{Z})^t$$

and the corresponding subfield F of $\mathbf{Q}(\zeta_m)$ has the required Galois group over $\mathbf{Q}$.

There is a conjecture stating that *every* finite group G occurs as $\text{Gal}(F/\mathbf{Q})$ for some number field F. The general problem is called the *Inverse Problem of Galois Theory.* It appears to be of a rather arithmetical nature. It has been proved by Šafarevich in 1960 that every finite solvable group occurs as a Galois group of a number field [64]. In the past few years, many of the sporadic simple groups have been realized as Galois groups over $\mathbf{Q}$. See [52] and especially Serre's Bourbaki talk [68].

Theorem (11.7). *Let χ be a Dirichlet character of conductor m.*

(i) The absolute value of the Gaussian sum

$$\tau(\chi) = \sum_{x \in (\mathbf{Z}/m\mathbf{Z})^*} \chi(x)\zeta_m^x$$

is m.

(ii) The value at 1 of the L-series associated to χ is given by

$$\begin{aligned} L(1,\chi) &= -\frac{\tau(\chi)}{m} \sum_{a \in (\mathbf{Z}/m\mathbf{Z})^*} \chi^{-1}(a) \log|\sin(\frac{\pi a}{m})| && \textit{for } \chi \textit{ even,} \\ &= \frac{\pi i \tau(\chi)}{m} B_{1,\chi^{-1}} && \textit{for } \chi \textit{ odd.} \end{aligned}$$

Here the generalized Bernoulli number $B_{1,\psi}$ associated to a character ψ of conductor m, is defined by

$$B_{1,\psi} = \sum_{0 \leq a \leq m} \psi(a)\frac{a}{m}.$$

Proof. Let ζ denote a fixed m-th root of unity. Consider the following "modified" Gaussian sum:

$$\tau_a(\chi) = \sum_{x \in (\mathbf{Z}/m\mathbf{Z})^*} \chi(x)\zeta^{ax}$$

We have that

$$\tau_a(\chi) = \begin{cases} 0, & \text{if } \gcd(a,m) > 0, \\ \chi^{-1}(a)\tau(\chi), & \text{otherwise.} \end{cases}$$

Proof. The second case follows from an easy change of summation variable. Let us therefore consider the first case and assume that $1 < d = \gcd(a,m)$. Since χ has conductor m, we can find $z \equiv 1 \pmod{m/d}$ with $\chi(z) \neq 1$. We have that

$$\tau_a(\chi) = \sum_{x \in (\mathbf{Z}/m\mathbf{Z})^*} \chi(xz)\zeta^{azx} = \chi(z) \sum_{x \in (\mathbf{Z}/m\mathbf{Z})^*} \tau_a(\chi)$$

and this shows that $\tau_a(\chi) = 0$ as required.
(i) We have that

$$\begin{aligned} \tau(\chi)\tau(\chi^{-1}) &= \sum_{x,y \in (\mathbf{Z}/m\mathbf{Z})^*} \chi(xy^{-1})\zeta^{x-y} = \sum_{z,y \in (\mathbf{Z}/m\mathbf{Z})^*} \chi(z)\zeta^{(z-1)y}, \\ &= \sum_{y \in (\mathbf{Z}/m\mathbf{Z})^*} \zeta^y \tau_y(\chi) = \sum_{z,y \in \mathbf{Z}/m\mathbf{Z}} \chi(z)\zeta^{(z-1)y}. \end{aligned}$$

The last equality follows from the fact that $\tau_y(\chi) = 0$ whenever $y \notin (\mathbf{Z}/m\mathbf{Z})^*$ and the fact that $\chi(z) = 0$ for $z \notin (\mathbf{Z}/m\mathbf{Z})^*$. Finally we find

$$\tau(\chi)\tau(\chi^{-1}) = \sum_{z \in \mathbf{Z}/m\mathbf{Z}} \chi(z) \sum_{y \in \mathbf{Z}/m\mathbf{Z}} \zeta^{(z-1)y} = m + \sum_{z \neq 1} \chi(z) \sum_{y} \zeta^{(z-1)y} = m.$$

here the final inner sums are zero by the orthogonality relations applied to the characters $y \mapsto \zeta^{(z-1)y}$ of the additive group $\mathbf{Z}/m\mathbf{Z}$.
(ii) By *(i)* we can write for $s \in \mathbf{C}$, $\mathrm{Re}(s) > 1$,

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\tau_n(\chi^{-1})/\tau(\chi^{-1})}{n^s} = \frac{1}{\tau(\chi^{-1})} \sum_{a \in (\mathbf{Z}/m\mathbf{Z})^*} \chi^{-1}(a) \sum_{n=1}^{\infty} \frac{\zeta^{an}}{n^s}.$$

Since all infinite series converge at 1, we obtain the relation

$$L(1,\chi) = -\frac{1}{\tau(\chi^{-1})} \sum_{a \in (\mathbf{Z}/m\mathbf{Z})^*} \chi^{-1}(a)\log(1-\zeta^a)$$

where the argument ϕ of the logarithm should satisfy $-\pi < \phi < \pi$. It is easily seen that $\overline{\tau(\chi)} = \chi^{-1}(-1)\tau(\chi^{-1})$. Therefore we conclude from *(i)* that $1/\tau(\chi^{-1}) = \chi(-1)\tau(\chi)/m$. Distinguishing the cases where χ is even or odd, we find that

$$\begin{aligned} L(1,\chi) &= -\frac{\tau(\chi)}{m} \sum_{a \in (\mathbf{Z}/m\mathbf{Z})^*} \chi^{-1}(a)\log|1-\zeta^a| && \text{for } \chi \text{ even,} \\ &= \frac{\tau(\chi)}{m} \sum_{0 \leq a \leq m} \chi^{-1}(a)\frac{\pi a i}{m} && \text{for } \chi \text{ odd.} \end{aligned}$$

The result now follows upon writing $|1-\zeta^a| = 2|\sin(a\pi/m)|$ and by using the fact that $\sum_a \chi^{-1}(a) = 0$.

Finally we give, without proof, the analog of Theorem 9.10 for Dirichlet L-series. Like Thm.9.10, this result is due to Hecke[31,32] and a proof based on harmonic analysis on the adeles can be found in Tate's thesis [12,p.403].

Theorem (11.8). *Let χ be a Dirichlet character of conductor m. Then*

(i) (Euler product.)

$$L(s,\chi)=\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1}\qquad \textit{for } s\in\mathbf{C},\ \mathrm{Re}(s)>1.$$

where the product runs over the prime numbers.

(ii) (Analytic continuation.) The L-functions admit a meromorphic extension to $\mathbf{C}$. When $\chi\neq 1$, this extension is actually holomorphic. When $\chi=1$, the L-series is equal to the Riemann ζ-function and has a pole of order 1 at $s=1$ with residue 1. The values of the L-functions at 1 are given in Thm.11.6.

(iii) (Functional equation.) The function

$$\begin{aligned}\Lambda(s)&=\left(\frac{m}{\pi}\right)^{\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)L(s,\chi)\qquad &&\textit{when } \chi \textit{ is even,}\\ &=\left(\frac{m}{\pi}\right)^{\frac{s}{2}}\Gamma\left(\frac{s+1}{2}\right)L(s,\chi)\qquad &&\textit{when } \chi \textit{ is odd.}\end{aligned}$$

satisfies $\Lambda(s)=W_\chi\Lambda(1-s)$ where the root number W_χ is a complex number of absolute value 1. It is given by $W_\chi=\tau(\chi)/\sqrt{m}$ or $-i\tau(\chi)/\sqrt{m}$ depending on whether χ is even or odd.

(iv) (Zeroes.) $L(s,\chi)$ has zeroes at the non-positive integers that have the same parity as χ. These are the trivial zeroes. All other zeroes ρ satisfy $0\le\mathrm{Re}(\rho)\le 1$.

(v) (Special values.) When $n\in\mathbf{Z}_{\geq 0}$ of the same parity as χ, then

$$L(s,1-n)=-\frac{B_{n,\chi}}{n}.$$

here the Generalized Bernoulli numbers $B_{n,\chi}$ are defined by

$$\sum_{a=1}^{m}\frac{\chi(a)Te^{aT}}{e^{fT}-1}=\sum_{n=0}^{\infty}B_{n,\chi}\frac{T^n}{n!}.$$

Proof. Part *(i)* is in Prop.10.3.

A Dirichlet characters $\chi:(\mathbf{Z}/m\mathbf{Z})^*\longrightarrow\mathbf{C}^*$ can be viewed as a one dimensional representation of $\mathrm{Gal}(\mathbf{Q}(\zeta_m/\mathbf{Q})$ and hence of the" absolute" Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. For the Artin L-series associated to higher dimensional representations, much less is known. A famous conjecture of Artin asserts that all Artin L-functions can be extended holomorphically to all of $\mathbf{C}$. An important result in this direction is due to R. Brauer [11]. He showed, by means of his results in representation theory of finite groups, that Artin L-functions are, at least, always meromorphic. All Artin L-series are conjectured to satisfy certain generalized Riemann Hypotheses.

Artin L-series are believed to intimately related to L-series associated to automorphic forms. The "Langlands Philosophy" says, in fact, that every Artin L-series should arise in this way. Establishing these conjectures is part of the so-called Langlands Program. It is a very active area of research [6].

(11.A) Let m be a positive integer and suppose p is a prime that does not divide m. Show that if for some integer x one has that $p|\Phi_m(x)$, then x has order m modulo p. Show that there exist infinitely many primes $l\equiv 1 \pmod{m}$. (Hint: any prime dividing $\Phi_m(Mm)$ is 1 (mod m) and does *not* divide mM.)

(11.B) For any homomorphism $f : A \longrightarrow B$ of abelian groups and let Q be an abelian group. We let $\widehat{f} : \mathrm{Hom}(B, Q) \longrightarrow \mathrm{Hom}(A, Q)$ denote the natural homomorphism given by $\widehat{f}(g)(a) = g(f(a))$. Show that for every exact sequence of abelian groups.

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

and every abelian group Q, the associated sequence

$$0 \longrightarrow \mathrm{Hom}(C, Q) \longrightarrow \mathrm{Hom}(B, Q) \longrightarrow \mathrm{Hom}(A, Q)$$

is also exact. Show that, in general, the map $\mathrm{Hom}(B, Q) \longrightarrow \mathrm{Hom}(A, Q)$ is not surjective. Show that it is surjective if Q is free.

(11.D) Let $l_1, l_2, \ldots, l_r$ be a set of mutually disticnt primes. Let $q_1, q_2, \ldots, q_s$ be a second such set, disjoint form the first. Show that there exist infnitely many primes p, which are squares modulo every l_i and non-squares modulo every q_i.

(11.C) Show: if a set of primes P has a natural density, then it also has a natural density and the densities are equal. Show that the set P of primes whose first decimal digit is 1, does not have a natural density. (It has analytic density equal to $\log(2)/\log(10)$ (Bombieri)).

(11.E) Let $U(m) =$ the number of characters of conductor m. Show that $\sum_{d|m} U(d) = \phi(m)$ and show that U is multiplicative. Show that $U(m) = \sum_{d|m} \mu(\frac{m}{d})\phi(d)$.

12. Cyclotomic fields of prime conductor.

In this section we will investigate the arithmetical structure of the number fields $\mathbf{Q}(\zeta_p)$ where $p \neq$ is a prime and ζ_p is a primitive p-th root of unity. Our results will be applied in the next section in our proof of Kummer's Theorem 1.6. The fields $\mathbf{Q}(\zeta_p)$ are cyclotomic fields. For these fields there is a very rich theory, initiated by Kummer [39]. See the books by Lang [43] and Washington [80] for the recent developments in the theory of cyclotomic fields and Iwasawa theory.

The field $\mathbf{Q}(\zeta_p)$ is a Galois extension of $\mathbf{Q}$. Its Galois group is canonically isomorphic to the cyclic group $(\mathbf{Z}/p\mathbf{Z})^*$. By $\mathbf{Q}(\zeta_p)^+$ we denote the subfield of $\mathbf{Q}(\zeta_p)$ which is fixed under the automorphism $-1 \in (\mathbf{Z}/p\mathbf{Z})^*$. Clearly $\zeta_p + \zeta_p^{-1} \in \mathbf{Q}(\zeta_p)^+$. Since ζ_p is a zero of the polynomial $T^2 - (\zeta_p + \zeta_p^{-1})T - 1$, we conclude that $\mathbf{Q}(\zeta_p)^+ = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$. The subfield $\mathbf{Q}(\zeta_p)^+$ of $\mathbf{Q}(\zeta_p)$ will play an important role in this and the next chapter.

Since $\mathbf{Q}(\zeta_p)$ contains non-trivial roots of unity, none of its embeddings $\mathbf{Q}(\zeta_p) \hookrightarrow \mathbf{C}$ has its image contained in $\mathbf{R}$. Therefore $r_1 = 0$ and $r_2 = p - 1$ for $\mathbf{Q}(\zeta_p)$. The map $\zeta_p + \zeta_p^{-1} \mapsto 2\cos(2\pi/p)$ induces an immersion of $\mathbf{Q}(\zeta_p)^+$ into $\mathbf{R}$. By Prop.10.1*(i)*, all the embeddings $\mathbf{Q}(\zeta_p)^+ \hookrightarrow \mathbf{C}$ have their images in $\mathbf{R}$. This shows that $r_1 = (p-1)/2$ and $r_2 = 0$ for this field.

Our first proposition gives some information about the rings of integers of $\mathbf{Q}(\zeta_p)$ and $\mathbf{Q}(\zeta_p)^+$:

Proposition (12.1). *Let $p \neq 2$ be a prime. Let $F = \mathbf{Q}(\zeta_p)$ and $F^+ = \mathbf{Q}(\zeta_p)^+$. Writing ζ for ζ_p, we ahve that*

(i) For every $i \not\equiv 0 \pmod p$ we have that

$$\frac{\zeta^i - 1}{\zeta - 1} \quad \text{is a unit.}$$

(ii) The prime p is totally ramified in $\mathbf{Q}(\zeta_p)$. We have the following decomposition of ideals in O_F:

$$(p) = (\zeta - 1)^{p-1}.$$

(iii) The ring of integers O_F of F is equal to $\mathbf{Z}[\zeta_p]$ and the discriminant of F is equal to $\Delta_F = (-1)^{(p-1)/2}p^{p-2}$.

(iv) The ring of integers O_{F^+} of F^+ is equal to $\mathbf{Z}[\zeta_p + \zeta_p^{-1}]$ and the discriminant of F^+ is equal to $\Delta_{F^+} = p^{(p-3)/2}$.

Proof. *(i)* Let $j \in \mathbf{Z}$ such that $ij \equiv 1 \pmod p$. Then

$$\frac{\zeta - 1}{\zeta^i - 1} = \frac{\zeta^{ij} - 1}{\zeta^i - 1} = \zeta^{i(j-1)} + \ldots + \zeta^i + 1$$

is an algebraic integer. We conclude that $(\zeta^i - 1)/(\zeta - 1)$ is a unit.
(ii) We have that

$$p = \Phi_p(1) = \prod_{i=1}^{p-1}(1 - \zeta^i) = (\zeta - 1)^{p-1}\prod_{i=1}^{p-1}(\zeta^i - 1)/(\zeta - 1)$$

and the result follows from *(i)*.
(iii) By Example 6.4, the ring of integers of F is $\mathbf{Z}[\zeta_p]$. By Example 2.11, the discriminant of F is $(-1)^{(p-1)/2}\mathrm{N}(\Phi_p'(\zeta)) = (-1)^{(p-1)/2}p^{p-2}$ as required.
(iv) By Prop. 2.10, the discriminant of the basis of the powers $1, \alpha, \alpha^2, \ldots, \alpha^{(p-3)/2}$ of $\alpha = \zeta + \zeta^{-1}$ is equal to

$$\prod_{1 \le i < j \le (p-1)/2} ((\zeta^i + \zeta^{-i}) - (\zeta^j + \zeta^{-j}))^2.$$

Since $(\zeta^i + \zeta^{-i}) - (\zeta^j + \zeta^{-j}) = (\zeta^i - \zeta^{-j})(1 - \zeta^{j-i})$, we see by *(i)*, that, upto a unit, every factor in the product is equal to $(\zeta - 1)^2$. Therefore the discriminant of this basis is, upto a unit, equal to

$$(\zeta - 1)^{2\frac{p-1}{2}\frac{p-3}{2}}$$

which is, again upto a unit, equal to $p^{(p-3)/2}$.

As in part *(iii)*, we conclude that the only possible primes dividing the index of $\mathbf{Z}[\zeta + \zeta^{-1}]$ in O_{F^+} is p. However $\beta = \zeta + \zeta^{-1} - 2$ generates the same ring as $\zeta + \zeta^{-1}$ and by Exer.12.A, its minimum polynomial is, in fact, an Eisenstein polynomial. We conclude from Prop.6.3 that $O_{F^+} = \mathbf{Z}[\zeta + \zeta^{-1}]$ and that, upto a unit, the discriminant of F^+ is equal to $p^{(p-3)/2}$. By Exerc.3.H it is equal to $p^{(p-3)/2}$. This proves the Proposition.

The units that have been mentioned in part *(i)* of the previous proposition play an important role. The multiplicative group generated by the roots of unity in $F = \mathbf{Q}(\zeta_p)$ and these units is called the group of *cyclotomic units* and is denoted by Cyc_F:

$$\begin{aligned} Cyc_F &= \left\langle \pm\zeta_p^j, \frac{\zeta^i - 1}{\zeta - 1} \text{ for } i \not\equiv 0 \pmod p \right\rangle \\ &= O_F^* \cap \left\langle \pm\zeta_p^j, \zeta^i - 1 \text{ for } i \not\equiv 0 \pmod p \right\rangle. \end{aligned}$$

It is easy to verify the last description of Cyc_F; it shows that the group of cyclotomic units is stable under the action of the Galois group of F over $\mathbf{Q}$. We define the group of "real" cyclotomic units Cyc_{F^+} by $Cyc_{F^+} = Cyc_F \cap F^+$. It too is stable under the action of the Galois group. We have the following alternative descriptions of Cyc_{F^+}:

Lemma (12.2). *Let p be an odd prime, let ζ be a primitive p-th root of unity and let $F = \mathbf{Q}(\zeta)$. Then*

$$\begin{aligned} Cyc_{F^+} &= \left\langle \pm 1, \frac{\zeta^j - \zeta^{-j}}{\zeta - \zeta^{-1}} \text{ for } j \not\equiv 0 \pmod p \right\rangle \\ &= \langle \pm 1, \sigma_a(\eta) \text{ for } 1 \le a \le (p-1)/2 \rangle \end{aligned}$$

where

$$\eta = \frac{\zeta^g - \zeta^{-g}}{\zeta - \zeta^{-1}}$$

for some primitive root g modulo p, and where σ_a denotes the automorphism of F determined by $\sigma_a(\zeta) = \zeta^a$. Moreover, Cyc_F is the direct product of Cyc_{F^+} and μ_F.

Proof. Since

$$\frac{\zeta^j-\zeta^{-j}}{\zeta-\zeta^{-1}}=\zeta^{-j+1}\frac{\zeta^{2j}-1}{\zeta^2-1}=\zeta^{-j+1}\sigma_2\left(\frac{\zeta^j-1}{\zeta-1}\right)$$

and Cyc_{F^+} is stable under the Galois group, every $(\zeta^j-\zeta^{-j})/(zeta-\zeta^{-1})$ is contained in Cyc_{F^+}. Vice versa,let $\varepsilon\in Cyc_{F^+}$. We have that

$$\varepsilon=\pm\zeta^a\prod_j\frac{\zeta^j-1}{\zeta-1}=\pm\zeta^a\prod_j\frac{\zeta^{2j}-1}{\zeta^2-1}=\pm\zeta^{a'}\prod_j\frac{\zeta^j-\zeta^{-j}}{\zeta-\zeta^{-1}}.$$

Since $\varepsilon\in F^+$, we must have that $a'=0$ and the fisrt equality follows.

To show that $Cyc_{F^+}=\langle\pm1,\sigma_a(\eta)$ for $1\le a\le(p-1)/2\rangle$, we observe that it is clear that $\eta\in Cyc_{F^+}$ and hence that $\sigma_a(\eta)\in Cyc_{F^+}$ for all a. The opposite inclusion is proved as follows: let g be a primitive root mod p. Then

$$\frac{\zeta^{g^{i+1}}-\zeta^{-g^{i+1}}}{\zeta-\zeta^{-1}}=\sigma_{g^i}(\eta)\cdot\frac{\zeta^{g^i}-\zeta^{-g^i}}{\zeta-\zeta^{-1}}.$$

This implies the result by induction.

Example. For $p=11$ and $\zeta=\zeta_{11}$, we have that

$$\begin{aligned}CyC_{F^+}&=\left\langle\pm1,\frac{\zeta^2-\zeta^{-2}}{\zeta-\zeta^{-1}},\frac{\zeta^3-\zeta^{-3}}{\zeta-\zeta^{-1}},\frac{\zeta^4-\zeta^{-4}}{\zeta-\zeta^{-1}},\frac{\zeta^5-\zeta^{-5}}{\zeta-\zeta^{-1}},\right\rangle\\&=\left\langle\pm1,\eta=\frac{\zeta^2-\zeta^{-2}}{\zeta-\zeta^{-1}},\eta_2=\frac{\zeta^4-\zeta^{-4}}{\zeta^2-\zeta^{-2}},\eta_3=\frac{\zeta^6-\zeta^{-6}}{\zeta^3-\zeta^{-3}},\eta_4=\frac{\zeta^8-\zeta^{-8}}{\zeta^4-\zeta^{-4}},\right\rangle\end{aligned}$$

Here we have listed a set of generators. The missing $\frac{\zeta^j-\zeta^{-j}}{\zeta-\zeta^{-1}}$ and η_a can be expressed in terms of these.

Proposition (12.3). *Let $p\neq2$ be a prime. Let $F=\mathbf{Q}(\zeta_p)$ and $F^+=\mathbf{Q}(\zeta_p)^+$. Then*

(i) The group of roots of unity μ_F of F is equal to μ_{2p}.

(ii) For the group of units O_F^* of O_F, one has that

$$O_F^*=\mu_pO_F$$

(iii) The canonical map $Cl_{F^+}\longrightarrow Cl_F$ is injective.

(iv) The subgroup of cyclotomic units Cyc_F has index

$$\frac{1}{2^{(p-3)/2}R_F}\left|\prod_{\chi\neq1}\sum_{a\in(\mathbf{Z}/m\mathbf{Z})^*}\chi^{-1}(a)\log|\sin\left(\frac{\pi a}{p}\right)|\right|$$

in $O_{F^+}^*$. Here the product runs over the even non-trivial characters χ of $(\mathbf{Z}/p\mathbf{Z})^*$.

Proof. *(i)* Obviously we have that $\mu_{2p}\subset F^*$. If $\mu_{2mp}\subset F^*$ for some $m\in\mathbf{Z}_{\geq1}$, then $\mathbf{Q}(\zeta_{2mp})\subset F=\mathbf{Q}(\zeta_p)$ and hence $\phi(2mp)$ divides $\phi(p)$. This is easily seen to imply that $m=1$, as required.
(ii) Let $\zeta=\zeta_p$ and let $\varepsilon\in O_F^*$. By $x\mapsto\bar{x}$ we denote the automorphism of F determined by $\zeta\mapsto\zeta^{-1}$. It corresponds to the element $-1\in(\mathbf{Z}/p\mathbf{Z})^*=\mathrm{Gal}(F/\mathbf{Q})$. For any embedding $\phi:F\hookrightarrow\mathbf{C}$, we have that $\phi(\bar{x})=\overline{\phi(x)}$, where the right hand side "bar" denotes ordinary complex conjugation. We have

$$\begin{aligned}|\phi(\varepsilon/\bar{\varepsilon})|^2&=\phi(\varepsilon/\bar{\varepsilon})\overline{\phi(\varepsilon/\bar{\varepsilon})},\\&=\phi(\varepsilon/\bar{\varepsilon}\cdot\bar{\varepsilon}/\varepsilon)=1.\end{aligned}$$

We conclude that $\varepsilon/\bar{\varepsilon}$ is in the kernel of the map $\Psi : O_F^* \longrightarrow \mathbf{R}^{r_1+r_2}$ of Theorem 7.8. It follows from Part *(i)* of this theorem that

$$\varepsilon/\bar{\varepsilon} = \xi \qquad \text{for some } \xi \in \mu_F.$$

By *(i)* we have that $\xi = \pm\zeta$ for some p-th root of unity ζ. To determine the sign, we compute this relation modulo π, where $\pi = \zeta - 1$ is a prime divisor of p. It has norm p. We obviously have that $\zeta \equiv 1 \pmod{\pi}$ and by Prop.12*(i)* that $(\bar{\pi}) = (\pi)$. We conclude that $\varepsilon/\bar{\varepsilon} \equiv 1 \pmod{\pi}$ and therefore that

$$\varepsilon/\bar{\varepsilon} = \zeta \qquad \text{for some } \zeta \in \mu_p.$$

Since p is odd, we can write $\zeta = \zeta'^2$ for some $\zeta' \in \mu_p$. It follows that $u = \varepsilon\zeta'^{-1}$ satisfies $\bar{u} = u$. Therefore $u \in O_{F^+}^*$ and the result follows.
(iii) Let $c \in Cl_{F^+}$ be in the kernel of the map $Cl_{F^+} \longrightarrow Cl_F$ and let $I \in c$ be an ideal. Then the ideal $O_F I$ generated by I in the ring O_F is principal and generated by $\alpha \in O_F$, say. Since I is an ideal of O_{F^+}, the ideal $(\alpha) = O_F I$ satisfies $(\bar{\alpha}) = (\alpha)$. Therefore $\alpha/\bar{\alpha}$ is a unit and one shows, as in part *(ii)* that it is even a root of unity:

$$\alpha/\bar{\alpha} = \pm\zeta \qquad \text{for some } \zeta \in \mu_p.$$

To determine the sign, we do a calculation mod π where $\pi = \zeta - 1$ is a prime of norm p. Write $\alpha = \beta\pi^k$ where $\mathrm{ord}_\pi(\beta) = 0$. Since I is an ideal of F^+ we have, by Exer.12.B, that $k = \mathrm{ord}_\pi(I)$ is *even.* Since $\bar{\pi} = -\zeta^{-1}\pi$ we find, as in *(ii)*, that

$$\frac{\alpha}{\bar{\alpha}} = \frac{\beta\pi^k}{\bar{\beta}(-\zeta^{-1})^k\pi^k} = \frac{\beta}{\bar{\beta}}\zeta^k \equiv 1 \pmod{\pi}$$

We conclude that $\alpha/\bar{\alpha} = \zeta$ for some $\zeta \in \mu_p$. Since p is odd, we can write $\zeta = \zeta'^2$ for some $\zeta' \in \mu_p$. It follows that $\alpha' = \alpha\zeta'^{-1}$ satisfies $\bar{\alpha'} = \alpha'$ and hence that $\alpha' \in F^+$.

We see that the ideals I and (α') of F^+ are, when extended to ideals of O_F both equal to (α). Since the canonical map $Id(O_{F^+}) \longrightarrow Id(O_F)$ is injective by Exer.4.R, we conclude that $(\alpha') = I$ and the result follows.
(iv) For F^+ we have that $r_1 = (p-1)/2$ and $r_2 = 0$. We study the image $\Psi(Cyc_{F^+})$ of the map Ψ of Theorem 7.7, in the $(p-1)/2$-dimensional real vector space $\mathbf{R}^{r_1+r-2}$. By Lemma 12.2, the group $\Psi(Cyc_{F^+})$ is generated by vectors

$$\Psi(\sigma_a(\eta) = \begin{pmatrix} \log|\phi_1(\sigma_a(\eta))| \\ \vdots \\ \log|\phi_{(p-1)/2}(\sigma_a(\eta))| \end{pmatrix} \qquad \text{for } 1 \leq a \leq (p-1)/2.$$

These vectors are not independent. For instance $|\prod_a \sigma_a(\eta)| = |\mathrm{N}(\eta_a)| = 1$, so the sum of the $\Psi(\eta)$ is zero. Alternatively, the sum of the coordinates of each $\Psi(\eta_a)$ is 0.

We will calculate the determinant of a $(p-3)/2 \times (p-3)/2$-minor of the matrix

$$(\log|\phi_i(\sigma_a(\eta))|)_{i,a}$$

where $0 \leq a, i \leq (p-3)/2$. In order to do this, we choose a primitive root g modulo p. We take $a = 1, g, g^2, \ldots, g^{(p-5)/2}$ and $\phi_i = \phi \cdot \sigma_{g^i}$ for $0 \leq i \leq (p-5)/2$ and $\phi : F^+ \hookrightarrow \mathbf{R}$ given by $\zeta + \zeta^{-1} \mapsto 2\cos(2\pi/p)$. This gives the determinant

$$\det\left(\log|\phi(\sigma_{g^{i+j}}(\eta))|\right)_{0\leq i,j\leq(p-5)/2} = \det(a_{i+j+1} - a_{i+j})_{0\leq i,j\leq(p-5)/2}$$

where

$$a_k = \log|\phi\left(\zeta^{g^k} - \zeta^{-g^k}\right)|$$

By Lemma 12.4, which will be proved after the proof of this proposition, this determinant is equal to

$$\prod_{\chi \neq 1} \sum_{i=0}^{(p-3)/2} \chi^{-1}(g^i)\log|\phi\left(\zeta^{g^i} - \zeta^{-g^i}\right)|$$

Here the product runs over the non-trivial characters of the group $(\mathbf{Z}/p\mathbf{Z})^*/\{\pm 1\}$. Using the orthogonality relations the determinant is seen to be equal to

$$2^{-\frac{p-3}{2}} \prod_{\substack{\chi \neq 1 \\ \chi \text{ even}}} \sum_{a \in (\mathbf{Z}/p\mathbf{Z})^*} \chi^{-1}(a)\log|\sin(\frac{\pi a}{p})|.$$

By Theorem 11.7, the factors in this product are equal to $L(1,\chi)$ times a non-zero constant. Since $L(1,\chi) \neq 0$, we conclude that the the determinant we have just calculated is not zero.

We left out the last coordinate of the vectors $\Psi(\sigma_a(\eta))$. This corresponds to projecting $\mathbf{R}^{(p-1)/2}$ onto the subspace of codimension 1 spanned by the first $(p-3)/2$ basis vectors. It follows that the projection of the image $\Psi(Cyc_{F^+})$ of the cyclotomic units has finite index in the projection of $\Psi(O_{F^+})$. The index is precisely the regulator R_{F^+} divided by the absolute value of the determinant above.

By Exer.7.M, the projection is injective on $\Psi(O^*_{F^+})$. Since $\ker(\Psi) = \{\pm 1\}$, we see that the index is also equal to the index $[O^*_{F^+} : Cyc_{F^+}]$ as required.

Lemma (12.4). *Let $a_0, \ldots, a_{n-1} \in \mathbf{C}$. Then*
(i)

$$\det\begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_1 & a_2 & \ldots & a_0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_0 & \ldots & a_{n-2} \end{pmatrix} = \prod_{\chi} \sum_{i=0}^{n-1} \chi^{-1}(g^i)a_i$$

where the product runs over the characters of a cyclic group G of order n generated by g.
(ii)

$$\det\begin{pmatrix} a_1 - a_0 & a_2 - a_1 & \ldots & a_{n-1} - a_{n-2} \\ a_2 - a_1 & a_3 - a_2 & \ldots & a_{n-2} - a_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} - a_{n-2} & a_{n-2} - a_{n-3} & \ldots & a_0 - a_{n-1} \end{pmatrix} = \prod_{\chi \neq 1} \sum_{i=0}^{n-1} \chi^{-1}(g^i)a_i$$

where the product runs over the non-trivial characters of a cyclic group G of order n generated by g.

Proof. Consider the group ring $\mathbf{C}[G]$ and $x = \sum_{i=1}^{n} a_i[g^{-i}] \in \mathbf{C}[G]$. Multiplying by x is a $\mathbf{C}$-linear map. Expressing its effect with respect to the standard basis $[1], [g], \ldots, [g^{n-1}]$ of $\mathbf{C}[G]$ gives the matrix in *(i)*. To evaluate its determinant we take the basis of idempotents:

$$e_\chi = \sum_{i=0}^{n-1} \chi^{-1}(g^i)[g^i] \qquad \text{for } \chi : G \to \mathbf{C}^*.$$

The orthogonality relations (Prop.11.1*(iv)*) imply that the e_χ are orthogonal with respect to the scalar product $< \mathbf{v}, \mathbf{w} >= \sum_i \alpha_i \bar{\beta}_i$ for $\mathbf{v} = \sum_i \alpha_i [g^i]$ and $\mathbf{w} = \sum_i \beta_i [g^i]$. Therefore they form a $\mathbf{C}$-basis for the group ring $\mathbf{C}[G]$.

The e_χ are eigenvectors for the multiplication-by-x-map. The eigenvalues are

$$\sum_{i=0}^{n-1} \chi(g^{-i}) a_i.$$

Since the determinant is equal to the product of the eigenvalues, *(i)* follows.

(ii) Taking the sum of the coefficients of $\mathbf{v} = \sum_i \alpha_i [g^i]$ is a homomorphism of $\mathbf{C}[G]$ to $\mathbf{C}$. We define the *augmentation ideal* I by the exact sequence

$$0 \longrightarrow I \longrightarrow \mathbf{C}[G] \longrightarrow \mathbf{C} \longrightarrow 0.$$

A $\mathbf{C}$-basis for I is given by the elements $g^i - 1$ for $1 \le i \le n-1$. The multiplication-by-x-map respects the ideal I. Expressing this map with respect to the basis $g^i - 1$ gives the matrix in part *(ii)* of the Lemma. To evaluate its determinant, we remark that all idempotents e_χ except the one with $\chi = 1$, are in I. Therefore the vectors e_χ with $\chi \neq 1$ form an orthogonal basis for I.

Since the determinant is equal to the product of the eigenvalues, *(ii)* follows.

We will write $h(p)$ for the class number of $\mathbf{Q}(\zeta_p)$ and $h^+(p)$ for the class number of $\mathbf{Q}(\zeta_p)^+$. By Prop.12.3*(ii)* we see that $h^+(p)$ divides $h(p)$. We define the *minus class number* $h^-(p)$ by

$$h(p) = h(p)^+ \cdot h^-(p).$$

In Theorem 12.5 we will give formulas for $h(p)^+$ and $h(p)^-$. These will follow from Theorem 11.8 and the results in this section. In order to prove this theorem, we need one further ingredient which is of interest in itself:

Proposition (12.5). *(The sign of the Gaussian sum.) Let $p \neq 2$ be a prime number and let χ be the quadratic character modulo p. Let ζ be the primitive p-th root of unity $e^{(2\pi i)/p}$ in $\mathbf{C}$. Then the Gaussian sum $\tau(\chi)$ satisfies*

$$\tau(\chi) = \sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} \left(\frac{x}{p}\right) \zeta^x = \begin{cases} i\sqrt{p}; & \text{if } p \equiv 1 \pmod 4, \\ \sqrt{p}. & \text{if } p \equiv 3 \pmod 4). \end{cases}$$

Proof. We introduce

$$\tau' = \prod_{k=1}^{(p-1)/2} (\zeta^k - \zeta^{-k})$$

One has that

$$\tau'^2 = \prod_{k=1}^{(p-1)/2} (\zeta^k - \zeta^{-k})^2 = (-1)^{(p-1)/2} \prod_{k=1}^{p-1} (\zeta^k - \zeta^{-k})$$
$$= (-1)^{(p-1)/2} \zeta^{\sum_{k=1}^{p-1} k} \prod_{k=1}^{p-1} (1 - \zeta^{-2k}) = (-1)^{(p-1)/2} p.$$

The last equality folows from the fact that $\prod_{k=1}^{p-1}(1-\zeta^{-2k}) = \prod_{k=1}^{p-1}(1-\zeta^k) = \Phi_p(1) = p$. On the other hand, since

$$\tau' = \prod_{k=1}^{(p-1)/2} 2i \sin(\frac{2\pi k}{p}) = i^{\frac{p-1}{2}} \times (\text{something positive})$$

we conclude that

$$\tau' = i^{\frac{p-1}{2}}\sqrt{p} \qquad \text{in } \mathbf{C}.$$

By Lemma 10.G, the Gaussian sum $\tau = \tau(\chi)$ also satisfies

$$\tau^2 = (-1)^{(p-1)/2}p.$$

We conclude that

$$\tau = \pm\tau'$$

and we see that it suffices to determine the correct sign of this equation. We will do this by viewing τ and τ' in $\mathbf{Q}(\zeta_p) \subset \mathbf{C}$ via $\zeta_p \mapsto \zeta$ and by calculating each side modulo a sufficiently high power of the prime element $\pi = \zeta_p - 1$. Since $p = O(\pi^{p-1})$ we have that

$$\begin{aligned}\tau' = &\prod_{k=1}^{(p-1)/2} \left((1+\pi)^k - (1+\pi)^{p-k}\right) = \prod_{k=1}^{(p-1)/2} (k - (p-k)\pi + O(\pi^2)),\\ \equiv &2^{\frac{p-1}{2}}(\frac{p-1}{2})!\pi^{\frac{p-1}{2}} + O(\pi^{\frac{p+1}{2}}) \equiv \left(\frac{2}{p}\right)\left(\frac{p-1}{2}\right)!\pi^{\frac{p-1}{2}} \pmod{\pi^{\frac{p+1}{2}}}.\end{aligned}$$

The last equality follows form Euler's formula. For the Gaussian sum we have that

$$\begin{aligned}\tau = &\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)(1+\pi)^x = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\sum_{i=0}^{\infty}\binom{x}{i}\pi^i\\ \equiv &\sum_{i=0}^{\infty}\pi^i \sum_{x\in(\mathbf{Z}/p\mathbf{Z})^*} x^{\frac{p-1}{2}}\binom{x}{i} \equiv \pi^{\frac{p-1}{2}}\frac{1}{(\frac{p-1}{2})!}(-1) \pmod{\pi^{\frac{p+1}{2}}}\end{aligned}$$

The last line follows from Euler's formula and the "orthogonality" relations

$$\sum_{x\in(\mathbf{Z}/p\mathbf{Z})^*} x^i \equiv \begin{cases} -1 \pmod{p} & \text{if } i \equiv 0 \pmod{(p-1)},\\ 0 \pmod{p} & \text{otherwise.}\end{cases}$$

Finally we use the fact that

$$-1 \equiv (p-1)! \equiv (-1)^{(p-1)/2}\left(\frac{p-1}{2}\right)!^2 \pmod{p}$$

to obtain

$$\tau \equiv (-1)^{\frac{p-1}{2}}(\frac{p-1}{2})!\pi^{(p-1)/2} \pmod{\pi^{(p+1)/2}}.$$

Comparing this with the congruence for τ' we see that

$$\tau \equiv (-1)^{(p-1)/2}\left(\frac{2}{p}\right)\tau'$$

and combining this with the explicit expression for τ' that was derived above, we obtain the desired formulas for τ. This completes the proof of the proposition.

Theorem (12.6). *Let $p \neq 2$ be a prime number. Let $F = \mathbf{Q}(\zeta_p)$ and let $F^+ = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then*
(i)

$$h^+(p) = [O_F^* : Cyc_F],$$

(ii)

$$h^-(p) = 2p \prod_{\chi \text{ odd}} -\frac{1}{2} B_{1,\chi}.$$

Proof. *(i)* Let $H = \mathrm{Gal}(F/F^+)$. Identifying the Galois group of F over $\mathbf{Q}$ with $(\mathbf{Z}/p\mathbf{Z})^*$, we have that $H = \{\pm 1\}$ and we see that the characters χ of $(\mathbf{Z}/p\mathbf{Z})^*$ with $H \subset \ker(\chi)$ are precisely the even characters.

From Theorem 11.4*(iii)* applied to F^+ and the explicit expressions for $L(1,\chi)$ of Theorem 12.6, we deduce that

$$\frac{2^{(p-1)/2} h^+(p) R_{F^+}}{2p^{(p-3)/4}} = \prod_{\substack{\chi \neq 1 \\ \chi \text{ even}}} \frac{-\tau(\chi)}{p} \sum_{a \in (\mathbf{Z}/p\mathbf{Z})^*} \chi^{-1}(a) \log|\sin(\frac{a\pi}{p})|.$$

Here we have used Prop.12.1*(iv)* to calculate the discriminant of F^+. Now take absolute values. Using the fact that the Gaussian sums $\tau(\chi)$ have absolute value $\sqrt{p}$ and using Prop.12.3*(iv)* for the index $[O_{F^+}^* : Cyc_{F^+}]$ we find, after many cancellations, the required result.
(ii) We take the quotients of the formulas of Theorem 11.4*(iii)* applied to F and F^+ respectively. We find that

$$\frac{2\pi^{(p-1)/2} h_F R_F}{2p \cdot p^{(p-2)/2}} \frac{2p^{(p-3)/4}}{2^{(p-1)/2} h^+(p) R_{F^+}} = \prod_{\chi \text{ odd}} L(1,\chi).$$

Next we substitute the value for $L(1,\chi)$ from Theorem 12.6:

$$L(1,\chi) = \frac{\pi i \tau(\chi)}{p} B_{1,\chi^{-1}}$$

To evaluate the product, it is useful to combine the Gaussian sums $\tau(\chi)$ and $\tau(\chi^{-1})$. For odd characters χ one has that

$$\overline{\tau(\chi)} = \chi(-1)\tau(\chi^{-1}) = -\tau(\chi^{-1}),$$

so that $\tau(\chi)\tau(\chi^{-1}) = -p$ or rather $i\tau(\chi) \cdot i\tau(\chi^{-1}) = p$. There is an odd character χ for which $\chi = \chi^{-1}$, or equivalently, for which $\chi^2 = 1$, if and only if $p \equiv 3 \pmod 4$. In this case we use Prop.12.5, which says that $\tau(\chi) = i\sqrt{p}$. We find that

$$\prod_{\chi \text{ odd}} L(1,\chi) = \frac{\pi^{(p-1)/2}}{p^{(p-1)/2}} (-1)^{(p-1)/2} \prod_{\chi \text{ odd}} B_{1,\chi}.$$

Combining this with the formula above, one finds, after many cancellations, the required result.

Table (12.7).

p	$h^-(p)$
3	1
5	1
7	1
11	1
13	1
17	1
19	1
23	3
29	8
31	9
37	37
41	121
43	211
47	695
53	4889
59	41421
61	76301
67	853513
71	3882809
73	11957417
79	100146415
83	838216959
89	13379363737
97	411322842001

The minus class numbers $h^-(p)$ have been computed upto 521. They grow very fast with p. The minus class number of $\mathbf{Q}(\zeta_{509})$ has 145 decimal digits [44]. About the plus class numbers $h^+(p)$ much less is known. It has been proved by Van der Linden [76] that $h^+(p) = 1$ for all primes upto 67. Assuming the Generalized Riemann Hypothesis for the ζ-functions of $\mathbf{Q}(\zeta_p)$, one can show that $h^+(p) = 1$ for $p < 163$, while $h^+(163) = 4$. These results have been obtained using the discriminant bounds of Odlyzko, that have been mentioned in section 7. At present it seems rather hopeless to compute the numbers $h^+(p)$ where p is larger than 163. The class numbers are not always small. There are examples where $h^+(p)$ is a lot larger than p:

$$h^+(28654) \geq 283198643235353.$$

Although the results *(i)* and *(ii)* of Theorem 2.4 are purely *algebraic* statements, we have proved them with methods from *analysis:* we have exploited certain properties of the Dedekind ζ-function and its decomposition into Dirichlet L-series to obtain this result. In fact, upto very few years ago, no algebraic proofs of these formulas were known. Only very recently, in 1986, first the Brazilian Thaine [63,75] and then the Soviet mathematician V. B. Kolyvagin [37,59] proved certain theorems, that, combined with the work of Mazur and Wiles [55] from 1984, seems to lead to a *purely algebraic* proof of Theorem 12.6. The proof of Mazur and Wiles generalizes Ribet's paper [62] and involves a lot of arithmetical algebraic geometry.

Another surprising feature of Theorem 12.6 is that it does give the equality of the cardinalities of certain groups, without indicating any relation, like an *isomorphism,* between these groups. Even more surprising is the fact that, actually, there is no such isomorphism! For instance, for $p = 32009$, it is known that the groups Cl_{F+} and O_{F^+}/Cyc_{F^+} have the same cardinality, but are *not* isomorphic.

There are analogues of Theorem 12.6 for cyclotomic fields $\mathbf{Q}(\zeta_m)$ where m is not prime. The formula for the minus class number $h^-(m)$ is actually very similar and can be proved with the methods we have used in this section. The formula for $h^+(m)$ is, in general, more subtle. The best results have been obtained by W.B. Sinnott [70] in 1978. He showed that the index of his group of cyclotomic units inside the group of all units of $\mathbf{Q}(\zeta_m)^+$ is, upto a well-determined power of 2, equal to the plus class number $h^+(m)$.

(12.A) Let p be a prime. Show that the minimum polynomial of $\beta = \zeta_p + \zeta_p^{-1} - 2$ is Eisenstein with respect to p. (Hint: β is conjugate to $(\zeta_p - \zeta_p^{-1})^2$.

(12.B) Let p be a prime and let $\pi = \zeta_p - 1 \in \mathbf{Z}[\zeta_p]$. If $y \in \mathbf{Q}(\zeta_p)^+$, then $\mathrm{ord}_\pi(y)$ is even. (Hint: find a generator of the only prime in $\mathbf{Q}(\zeta_p)^+$ dividing p.)

(12.C) Let $\alpha \in \mathbf{Z}[\zeta_p]$. Show that α^p is congruent to an integer modulo (p). Show that if for some $n, m \in$ on has that $\alpha^n \equiv m \pmod{p}$, then $alpha \equiv m' \pmod{p}$ for some $m' \in \mathbf{Z}$ or p divides n.

13. Fermat's Last Theorem.

In this section we will use our knowledge of the number field $\mathbf{Q}(\zeta_p)$ gained in section 12, to prove Kummer's Theorem 1.6 regarding Fermat's last Theorem. Under the condition that p does not divide the class number of $\mathbf{Q}(\zeta_p)$, we first prove the so-called *first case* of Fermat's Last Theorem. The general case is a bit harder. We explain Kummer's method to relate p-adic properties of cyclotomic units to generalized Bernoulli numbers using logarithmic derivatives. Then we show that under the assumption that p does not divide the class number of $\mathbf{Q}(\zeta_p)$, the "second case" of Fermat's last Theorem follows. Finally we discuss the so-called Kummer congruences, which are satisfied by Bernoulli numbers. As a consequence we obtain a proof of Theorem 1.6.

Proposition (13.1). *("The first case.") Let $p \neq 2$ be a prime. If the class number of the cyclotomic field $\mathbf{Q}(\zeta_p)$ is not divisible by p, then the equation*

$$X^p + Y^p = Z^p$$

has no solutions $X, Y, Z \in \mathbf{Z}$ with $XYZ \not\equiv 0 \pmod{p}$.

Proof. Suppose $X, Y, Z \in \mathbf{Z}$ is a solution. We may and do assume that $\gcd(X, Y, Z) = 1$. Let first $p = 3$. In this case X^3, Y^3 and Z^3 are each congruent to $\pm 1 \pmod{9}$. Since $(\pm 1) + (\pm 1) \not\equiv (\pm 1) \pmod{9}$ we see that no solution can exist when $p = 3$.

From now on we suppose that $p \geq 5$. Since $T^p + 1 = \prod_{i=0}^{p-1}(T + \zeta^i)$ where ζ denotes a primitive p-th root of unity, we obtain from a solution X, Y, Z the following equality of ideals:

$$\prod_{i=0}^{p-1}(X + \zeta^i Y) = (Z)^p.$$

Suppose we have that $\mathfrak{p}$ is a common prime divisor of $X + \zeta^i Y$ and $X + \zeta^j Y$ for $i \neq j$. Then $\mathfrak{p}$ divides $\zeta^i - \zeta^j$ or Y. If $\mathfrak{p}|Y$, then $\mathfrak{p}|X$ and therefore $\mathfrak{p}$ divides Z, which is impossible since $\gcd(X, Y, Z) = 1$. If $\mathfrak{p}$ divides $\zeta^i - \zeta^j$, then, by Prop.11.1*(i)*, we have that $\mathfrak{p} = (\zeta - 1)$. We conclude that $\zeta - 1$ divides Z and hence that p divides Z, which is also impossible. Therefore the factors $(X + \zeta^i Y)$ are mutually coprime and, by Theorem 4.6, we obtain

$$(X + \zeta Y) = I^p$$

for some ideal I of the ring of integers $\mathbf{Z}[\zeta]$ of $\mathbf{Q}(\zeta)$. We see that the p-th power of I is principal and hence, since p does not divide the class number of $\mathbf{Q}(\zeta_p)$, that I itself is principal. Say $I = (\alpha)$. We now have that

$$X + \zeta Y = u\alpha^p$$

for some unit u. By Prop.12.1*(iii)*, the ring of integers of $\mathbf{Q}(\zeta)$ is $\mathbf{Z}[\zeta]$. We conclude that α and u are both in $\mathbf{Z}[\zeta]$. By Prop.11.2*(ii)*, we have that $u = \zeta^j \varepsilon$ for some integer j and some unit $\varepsilon \in \mathbf{Q}(\zeta_p)^+$.

Writing $\pi = \zeta - 1$, we have that $\mathbf{Z}[\zeta]/(\pi) \cong \mathbf{F}_p$. Therefore, $\alpha = a + \beta\pi$ for some $a \in \mathbf{Z}$ and $\beta \in \mathbf{Z}[\zeta]$. Using Prop.12.3*(ii)* and Exer.12.C, it follows that $\alpha^p \equiv a \pmod{p}$. So we have that

$$X + \zeta Y \equiv \varepsilon\zeta^j a \pmod{p}.$$

Applying complex conjugation we find

$$X + \zeta^{-1} Y \equiv \varepsilon\zeta^{-j} a \pmod{p}.$$

and eliminating the factor εa, we get that

$$\zeta^{-j}(X+\zeta Y) \equiv \zeta^{j}(X+\zeta^{-1}Y) \pmod p$$

and

$$X\zeta^{-j} - X\zeta^{j} - Y\zeta^{j-1} + Y\zeta^{1-j} = 0 \qquad \text{in } \mathbf{Z}[\zeta]/(p).$$

Since $p \geq 5$, the ring $\mathbf{Z}[\zeta]/(p)$ is an $\mathbf{F}_p$-vector space of dimenion at least 4. It admits $1, \zeta, \ldots, \zeta^{p-2}$ as an $\mathbf{F}_p$-basis. Since $X, Y \not\equiv 0 \pmod p$, some of the roots of unity ζ^{j}, ζ^{-j}, ζ^{j-1}, ζ^{1-j} must agree. This is easily seen to imply that $j \equiv 0, 1$ or $1/2 \pmod p$. This, in turn implies that Y, X or $Z \equiv 0 \pmod p$ respectively. Since this contradicts the assumptions, the proof of the lemma is complete.

The first case of Fermat's Last Theorem is much easier to prove than the general statement. It can, for instance, be shown that the first case of Fermat's Last Theorem is true for a prime p, whenever $2^{p-1} \not\equiv 1 \pmod{p^2}$. This condition, which can be checked rather easily, is verified by all primes less than $6 \cdot 10^9$ except 1093 and 3511. For these two primes Fermat's Last Theorem is also true by similar criteria obtained by Sophie Germain, Mirimanoff etc. see [80, Ch.I].Recently it has been proved that the first case of Fermat's Last Theorem is true for an infinite set of primes [2].

We will prove the second case after some preliminary considerations. Let $p \neq 2$ be a prime and let Δ denote the Galois group of $F = \mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$. The group ring $\mathbf{F}_p[\Delta] = \{\sum_{i=1}^{p-1} a_i[i] : a_i \in \mathbf{F}_p\}$ will play an important role in the sequel. For every character $\chi : \Delta \to \mathbf{F}_p^*$ it contains the *idempotent* e_χ given by

$$e_\chi = -\sum_{a=1}^{p-1} \chi^{-1}(a)[a] \in \mathbf{F}_p[\Delta].$$

Proposition (13.2). *Let p be a prime and let $\Delta = (\mathbf{Z}/p\mathbf{Z})^*$.*
(i) The elements $e_\chi \in \mathbf{F}_p[\Delta]$ form a set of orthogonal idempotents in the group ring:

$$\begin{aligned} e_\chi^2 &= e_\chi && \textit{for every } \chi, \\ e_\chi e_{\chi'} &= 0 && \textit{when } \chi \neq \chi', \\ \sum_\chi e_\chi &= 1. \end{aligned}$$

(ii) Let M be an $\mathbf{F}_p[\Delta]$-module and for every character $\chi : \Delta \longrightarrow \mathbf{F}_p^*$ let $M(\chi)$ denote the "χ-eigenspace" $e_\chi M$. Then

$$M = \bigoplus_\chi M(\chi)$$

and

$$\sigma(e_\chi m) = \chi(\sigma) e_\chi m \qquad \textit{for all } \sigma \in \Delta,\ m \in M(\chi).$$

Proof. *(i)* This is well-known and easy. We leave the verifications to the reader.
(ii) This is immediate from *(i)*.

Example. *(i)* We decompose the group ring $\mathbf{F}_p[\Delta]$ itself into a product of χ-eigenspaces. For every character χ, the idempotent e_χ is not trivial. By Prop.13.2*(ii)* one has that the eigenspace $e_\chi \mathbf{F}_p[\Delta]$ is simply equal to $\mathbf{F}_p e_\chi$. Therefore

$$\mathbf{F}_p[\Delta] = \bigoplus_\chi \mathbf{F}_p e_\chi.$$

We define the *Teichmüller character* $\omega : \Delta \longrightarrow \mathbf{F}_p^*$ to be the homomorphism given by $\omega(a) = a$, where we have identified Δ, as usual, with the group $(\mathbf{Z}/p\mathbf{Z})^*$. The Teichmüller character is a canonical generator of the character group. All other homomorphisms from Δ to $\mathbf{F}_p^*$ are powers of ω:

$$\mathrm{Hom}(\Delta, \mathbf{F}_p^*) = \{\omega^k : 0 \leq k \leq p-2\}.$$

(ii) By way of example, we find the eigenspaces of two more $\mathbf{F}_p[\Delta]$-modules. First consider $\mathbf{F}_p$, i.e. the vectorspace $\mathbf{F}_p$ with trivial Δ-action. It, obviously, is itself an eigenspace, viz. the eigenspace corresponding to the trivial character. All other eigenspaces are zero.

Next consider μ_p, the group of p-th roots of unity with the natural action of the Galois group Δ. We identify, as usual, $(\mathbf{Z}/p\mathbf{Z})^*$ with Δ via $a \leftrightarrow \sigma_a$, where $\sigma_a(\zeta) = \zeta^a$. Since $\omega(a) \equiv a \pmod{p}$, we see that Δ acts "via" ω. That is, μ_p is itself equal to the ω-eigenspace and all other eigenspaces are zero.

In the next proposition we determine the decomposition into eigenspaces of some $\mathbf{F}_p[\Delta]$-modules associated to the number fields $\mathbf{Q}(\zeta_p)$ and $\mathbf{Q}(\zeta_p)^+$.

Lemma (13.3). *Let $p \neq 2$ be a prime and let Δ denote the Galois group of $F = \mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$.*

(i) The map

$$\mathbf{F}_p[\Delta] \longrightarrow O_F/(p)$$

given by $\sigma_a \mapsto \sigma_a(\zeta_p)$ is an isomorphism of $\mathbf{F}_p[\Delta]$-modules. The ideal $(1-\zeta_p)^{p-2} \subset O_F/(p)$ is equal to the ω^{-1} eigenspace.

(ii)

$$Cyc_F/Cyc_F^p \cong \mu_p \times \prod_{\substack{\chi \text{ even} \\ \chi \neq 1}} \eta_\chi^{\mathbf{Z}/p\mathbf{Z}}.$$

$$Cyc_{F^+}/Cyc_{F^+}^p \cong \prod_{\substack{\chi \text{ even} \\ \chi \neq 1}} \eta_\chi^{\mathbf{Z}/p\mathbf{Z}}.$$

Here η_χ is a generator of the χ-eigenspace. It is given by

$$\eta_\chi = \prod_{a \in (\mathbf{Z}/p\mathbf{Z})^*} (1-\zeta_p^a)^{\chi^{-1}(a)} \qquad \text{for } \chi \text{ even but } \chi \neq 1.$$

Proof. *(i)* The $\mathbf{F}_p[\Delta]$-morphism $\mathbf{F}_p[\Delta]\zeta_p \longrightarrow O_F/(p)$ induced by the $\zeta_p \in O_F$, is obviously surjective. Since the $\mathbf{F}_p$-dimensions of both vector spaces are both equal to $p-1$, it is actually an isomorphism. The decomposition now follows from the discussion above. It remains to check the statement about the ω^{-1} eigenspace: we have that $\sigma_a((\zeta_p - 1)^i) = (\zeta_p^a - 1)^i = (\zeta_p - 1)^i((\zeta_p^a - 1)/(\zeta_p - 1))^i \equiv (\zeta_p - 1)^i a^i \pmod{(\zeta_p - 1)^{i+1}}$. In particular, with $i = p-2$, we find that σ_a acts by multiplication with a^{-1} on $(1-\zeta_p)^{p-2}/(1-\zeta_p)^{p-1}$.

(ii) We use the description of Lemma 12.2: the cyclotomic units Cyc_F are the units inside the multiplicative group generated by $\zeta = \zeta_p$ and $\zeta_b - 1$, for $b \not\equiv 0 \pmod{p}$ inside F^*. The group Cyc_{F^+} are the units that are also invariant under complex conjugation σ_{-1}.

Claim: The following canonical maps are all injective.

$$Cyc_{F^+}/(Cyc_{F^+})^p \hookrightarrow Cyc_F/(Cyc_F)^p \hookrightarrow \left\langle \zeta^a, 1-\zeta^b \right\rangle \text{ mod } p\text{-th powers.}$$

This allows us to view both Cyc_F/Cyc_F^p and $Cyc_{F^+}/(Cyc_{F^+})^p$ as subsets of

$$V = \left\langle \zeta^a, 1-\zeta^b : a \in \mathbf{Z}, \quad b \not\equiv \pmod{p} \right\rangle \text{ mod } p\text{-th powers.}$$

Proof. Suppose $\varepsilon \in Cyc_F$ is a p-th power of an element $\eta \in \langle \zeta^a, 1-\zeta^b-1\rangle$. This implies that η is a unit and therefore that $\eta \in Cyc_F$. This shows that the rightmost map is an injection.

Next, suppose that $\varepsilon \in Cyc_{F^+}$ is a p-th power of an element $\eta \in \langle \zeta^a, 1-\zeta^b-1\rangle$. As before this implies that η is a unit. It remains to show that we can find a unit η that is invariant under σ_{-1}. Since $\varepsilon \in F^+$, we have that $\sigma_{-1}(\eta)^p = \eta^p$. This shows that $\sigma_{-1}(\eta) = \xi\eta$ for some root of unity ξ. Since p is odd, $\xi = \xi'^2$ for some other p-th root of unity ξ'. It is easy to see that $\eta' = \xi'^{-1}\eta$ satisfies $\eta'^p = \varepsilon$ and $\sigma_{-1}(\eta') = \eta'$. This proves the claim.

Now we decompose the Δ-module V into eigenspaces. Note, that V is generated, as a Δ-module by just two elements: ζ and $1-\zeta$. To find the eigenspaces it suffices to calculate ζ^{e_χ} and $(1-\zeta)^{e_\chi}$. We have that

$$\sigma_{-1}\left((1-\zeta)^{e_\chi}\right) = (1-\zeta^{-1})^{e_\chi} = (\zeta^{-1})^{e_\chi}(1-\zeta)^{e_\chi}.$$

When $\chi = \omega$, this says that

$$\left((1-\zeta)^{e_\omega}\right)^{-1} = (\zeta^{-1})^{e_\omega}(1-\zeta)^{e_\omega} = \zeta^{-1}(1-\zeta)^{e_\omega}.$$

Since Δ acts on μ_F via the Teichmüller character ω, this implies that the ω-eigenspaces is just $\mu_p \subset V$. When χ is odd, $\chi \neq \omega$, then the formula implies that

$$\left((1-\zeta)^{e_\chi}\right)^{-1} = (\zeta^{-1})^{e_\chi}(1-\zeta)^{e_\chi} = (1-\zeta)^{e_\chi}$$

and hence that all the χ-eigenspaces are trivial for odd characters $\chi \neq \omega$.

Now let χ be even. In this case $\zeta^{e_\chi} = 1$. This implies that the χ-eigenspace is a cyclic group generated by $\eta_\chi = \eta^{e_\chi}$. When $\chi = 1$ one has that $\eta^{e_\chi} = \prod_{a=1}^{p-1}(1-\zeta^a) = p$.

This completes the description of the decomposition of V into a product of eigenspaces for the action of Δ. It easily implies part *(ii)* of the lemma: Since $Cyc_F/(Cyc_F)^p$ and $Cyc_{F^+}/(Cyc_{F^+})^p$ are Δ-modules, they each are product of a number of the one-dimensional eigenspaces that make up V. The only eigenspace which is not generated by a unit is the one corresponding to $\chi = 1$. The only eigenspace which is not invariant under complex conjugation is μ_p. This proves the lemma.

As we have seen in the proof of Theorem 13.1, it is, when studying Fermat's Last Theorem, important to know when the class number of $\mathbf{Q}(\zeta_p)$ is divisible by p or not. In section 12 we have decomposed this class number as a product of two factors:

$$h_{\mathbf{Q}(\zeta_p)} = h^+(p)h^-(p).$$

For the minus class number $h^-(p)$, Theorem 12.5*(ii)* gives an expression in terms of generalized Bernoulli numbers $B_{1,\chi}$. We have

$$h^-(p) = 2p \prod_{\chi \text{ odd}} -\frac{1}{2}B_{1,\chi}.$$

In order to study this formula "modulo p", we choose, once and for all, a prime ideal $\mathfrak{p}$ in $\mathbf{Z}[\zeta_{p-1}]$ over p. Since $p \equiv 1 \pmod{p-1}$, the residue class field of $\mathfrak{p}$ is $\mathbf{F}_p$. The map $\zeta \mapsto \zeta \pmod{\mathfrak{p}}$ is an isomorphism from μ_{p-1} to $(\mathbf{Z}[\zeta_{p-1}]/\mathfrak{p})^* \cong \mathbf{F}_p^*$. We define another "Teichmüller character" $\omega : \Delta \longrightarrow \mu_{p-1}$, closely related to the first, by $\omega(\sigma_a) \equiv a \pmod{\mathfrak{p}}$. As before, all characters $\Delta \longrightarrow \mu_{p-1}$ are powers of ω.

We study the generalized Bernoulli numbers $B_{1,\chi}$ modulo $\mathfrak{p}$. For an odd character $\chi : \Delta \longrightarrow \mu_{p-1}$ we have for $b \in (\mathbf{Z}/p\mathbf{Z})^*$ that

$$\begin{aligned}(\chi^{-1}(b) - b)B_{1,\chi} &= \sum_{a=1}^{p-1} \left(\frac{'a'}{p}\chi(b^{-1}a) - b\frac{'a'}{p}\chi(a) \right), \\ &= \sum_{a=1}^{p-1} \frac{'ab' - b'a'}{p}\chi(a) \in \mathbf{Z}[\zeta_{p-1}].\end{aligned}$$

Here, for an integer a, we define $'a'$ by the relations $a \equiv {'a'} \pmod{p}$ and $0 \leq {'a'} < p$. When $\chi \neq \omega^{-1}$ there exists an integer b such that $\chi^{-1}(b) \not\equiv b \pmod{\mathfrak{p}}$. We conclude that

$$B_{1,\chi} \text{ is } \mathfrak{p}\text{-integral when } \chi \neq \omega^{-1}.$$

We have that $pB_{1,\omega^{-1}} = \sum_{a=1}^{p-1} x\omega^{-1}(x) \equiv -1 \pmod{\mathfrak{p}}$ and therefore, upto a factor which is a unit modulo $\mathfrak{p}$:

$$h^-(p) = \prod_{\substack{\chi \text{ odd} \\ \chi \neq \omega^{-1}}} B_{1,\chi}.$$

Proposition (13.4). *Let $p \neq$ be a prime. And let $\mathfrak{p}$ be a fixed prime over p in the ring $\mathbf{Z}[\zeta_{p-1}]$ as above. Then*

$$\begin{aligned} h^-(p) \equiv 0 \pmod{p} \quad &\Longleftrightarrow \quad B_{1,\chi} \equiv 0 \pmod{\mathfrak{p}} \quad \textit{for some } \chi \neq \omega^{-1}, \\ h^+(p) \equiv 0 \pmod{p} \quad &\Longleftrightarrow \quad \eta_\chi \textit{ is a } p\textit{-th power of a unit for some } \chi \neq 1. \end{aligned}$$

Proof. *(i)* From the discussion above, it follows that $h^-(p) \equiv 0 \pmod{\mathfrak{p}}$ whenever $B_{1,\chi} \equiv 0 \pmod{\mathfrak{p}}$ for some character $\chi \neq \omega^{-1}$. Since $h^-(p) \in \mathbf{Z}$, the result follows.
(ii) By Lemma 13.3, the cyclotomic units Cyc_{F^+} are generated, modulo p-th powers, by the η_χ. If, for some character $\chi \neq 1$, the unit η_χ is a p-th power, (or rather: if η_χ is trivial in $O_{F^+}^*/(O_{F^+}^*)^p$,) then p divides the index $[O_{F^+}^* : Cyc_{F^+}]$ and the result follows from Theorem 12.6.

The following theorem is due to Kummer [23,39]. It is a key result in the proof of Fermat's Last theorem for regular primes p. It has long been a rather mysterious mechanism, relating the p-part of the class group of $\mathbf{Q}(\zeta_p)^+$ to the p-part of the minus class number $h^-(p)$. Only recently Kummer's construction has been understood better and generalized, e.g. by J. Coates and A. Wiles in [15] and by R. Coleman in [16].

Theorem (13.5). *Let $p \neq 2$ be a prime. Let $\chi : \Delta \longrightarrow \mathbf{F}_p^*$ be a non-trivial even character and let η_χ denote $\prod_a (1 - \zeta_p)^{\chi^{-1}(a)}$ in the group of cyclotomic units modulo p-th powers. Then*

$$\textit{if} \quad \eta_\chi \equiv m \pmod{p} \quad \textit{for some } m \in \mathbf{Z}, \qquad \textit{then} \quad B_{1,\omega\chi^{-1}} \equiv 0 \pmod{\mathfrak{p}}.$$

Proof. Notice that it makes sense to affirm that η_χ is congruent to an integer mod p, because, by Exer.12.C, p-th powers of elements in $\mathbf{Z}[\zeta_p]$ are congruent to integers mod p. Let $F = \mathbf{Q}(\zeta_p)$ and let $\pi = \zeta_p - 1$. We define a homomorphism

$$\Lambda : \mathbf{Z}[\zeta_p]^*/(\mathbf{Z}[\zeta_p]^*)^p \longrightarrow \mathbf{Z}[\zeta_p]/(\pi^{p-2})$$

as follows: for $h(T) = \sum_{i=0}^{p-2} a_i T^i \in \mathbf{Z}[T]$ and $h\zeta_p)$ a unit, we let

$$\Lambda : h(\zeta_p) \mapsto \frac{h'(\zeta_p)}{h(\zeta_p)}.$$

This is well defined since $\Phi_p'(\zeta_p)\pi = p\zeta_p^{p-1}$ as follows easily by differentiating the relation $\Phi_p(T)(T-1) = T^p - 1$ and by substituting $T = \zeta_p$.

Since $\eta_\chi \equiv m \pmod{p}$, for some $m \in \mathbf{Z}$, we obtain that

$$\Lambda(\eta_\chi) = \sum_{a=1}^{p-1} \frac{\chi^{-1} a\zeta_p^{a-1}}{1-\zeta_p^a} \equiv 0 \pmod{\pi^{p-2}}$$

and therefore

$$\left(\sum_{a=1}^{p-1} \chi^{-1}(a)a[a]\right)\left(\frac{\zeta}{1-\zeta}\right) \equiv 0 \pmod{\pi^{p-2}}.$$

We have $\zeta/(1-\zeta) = 1 - 1/\pi$. Since $\chi \neq \omega$ we have that $\left(\sum_{a=1}^{p-1} \chi^{-1}(a)a[a]\right)\left(\frac{\zeta}{1-\zeta}\right)(1) \equiv 0 \pmod{p}$ and hence that

$$\left(\sum_{a=1}^{p-1} \chi^{-1}(a)a[a]\right)\left(\frac{1}{\pi}\right) \equiv 0 \pmod{\pi^{p-2}}.$$

Since $\Phi_p'(\zeta_p) = p\zeta_p^{p-1}$ we have that $\sum_{a=1}^{p-1} a\zeta_p^{a-1} = p\zeta_p^{-1}$ and, equivalently, $(\sum_{a=1}^{p-1} a[a])(\zeta_p/p) = 1/\pi$. We obtain

$$\left(\sum_{a=1}^{p-1} \chi^{-1}(a)a[a]\right)\left(\sum_{a=1}^{p-1} \frac{a}{p}[a]\right)(\zeta_p) \equiv 0 \pmod{\pi^{p-2}}.$$

Replacing ζ_p by ζ_p^i we see that this implies that

$$\left(\sum_{a=1}^{p-1} \chi^{-1}(a)a[a]\right)\left(\sum_{a=1}^{p-1} \frac{a}{p}[a]\right)(\mathbf{Z}[\zeta_p]) \equiv 0 \pmod{\pi^{p-2}}.$$

Now we restrict our attention to the $\omega^{-1}\chi$-eigenspace of $\mathbf{Z}[\zeta_p]/(p)$. Since Δ acts via $\omega^{-1}\chi$, and since $(\sum_{a=1}^{p-1} \chi^{-1}(a)a\omega^{-1}\chi(a)) \equiv -1$, we see that $B_{1,\omega^{-1}\chi} \pmod{\mathfrak{p}}$ annihilates the $\omega^{-1}\chi$-eigenspace. By Lemma 13.2 these eigenspaces are non-trivial except possibly when $\omega^{-1}\chi = \omega^{-1}$. Since $\chi \neq 1$,this does not matter and we conclude that $B_{1,\omega^{-1}\chi} \equiv 0 \pmod{\mathfrak{p}}$, as required.

Corollary (13.6). *Let $p \neq 2$ be a prime. If p divides $h^+(p)$ then p divides $h^-(p)$ as well.*

Proof. Suppose p divides $h^+(p)$. By Prop.13.4 we must have that η_χ is a p-th power for some non-trivial even character χ. By Exer.12.C, this implies that η_χ is congruent to some integer m modulo p. Theorem 13.5 implies then that $B_{1,\omega\chi^{-1}} \equiv 0 \pmod{\mathfrak{p}}$. Since $\omega\chi^{-1} \neq \omega$, it follows from Prop.13.4 that $h^-(p) \equiv 0 \pmod{p}$. This proves the corollary.

There is not a single prime p known for which p divides $h^+(p)$! The statement that p does not divide $h^+(p)$ for any prime p, is called *Vandiver's Conjecture* [80]. It has been verified for all primes $p < 150000$. The experts do not quite agree on whether to believe Vandiver's Conjecture or not.

Corollary (13.7). *Let $p \neq 2$ be a prime and suppose that p does not divide $h^-(p)$. Then, if ε is a unit for which $\varepsilon \equiv m \pmod{p}$, for some integer m, then ε is a p-th power.*

Proof. Since p does not divide $h^-(p)$, we conclude from Cor.13.4 that p does not divide $h^+(p)$. Therefore, by Theorem 12.5*(i)*, there is an integer h not divisible by p such that $\varepsilon^h \in Cyc_F$. So

$$\varepsilon^h = \pm\zeta_p^{n_\omega} \prod_{\chi\neq 1} \eta_\chi^{n_\chi}.$$

Now we take eigenspaces. For every non-trivial character χ of Δ we have that ε^{e_χ} is congruent to an integer modulo p. Therefore, $\zeta_p^{n_\omega}$ and the $\eta_\chi^{n_\chi}$, for every non-trivial even character χ, are congruent to integers modulo p. A calculation mod π^2 shows that that $n_\omega \equiv 0 \pmod{p}$. Since p does not divide $h^-(p)$ we have, for every

Eliminating the ideal $\mathbf{d}$, we get

$$(X+Y)J_i^p = (X+\zeta^i Y)(\pi)^{(m-1)p}J_0^p \qquad \text{for } 1 \le i \le p-1$$

We conclude that the fractional ideals $(J_i/J_0)^p$ are principal and therefore, since p does not divide the class number of $\mathbf{Q}(\zeta_p)$, that $J_i/J_0 = (\gamma_i)$ for certain $\gamma_i \in \mathbf{Q}(\zeta_p)^*$. Note that $\mathrm{ord}_\pi(\gamma) = 0$. The equation becomes

$$(X+Y)\varepsilon_i\gamma_i^p = (X+\zeta^i Y)\pi^{(m-1)p} \qquad \text{for } 1 \le i \le p-1$$

for certain units ε_i in $\mathbf{Z}[\zeta_p]^*$.

Our task is now to construct another solution of the original equation by means of this equation. This is done as folows. We multiply the identity

$$(X+\zeta Y)(1+\zeta) - (X+\zeta^2 Y) = \zeta(X+Y)$$

by $\pi^{(m-1)p}$:

$$(X+\zeta Y)\pi^{(m-1)p}(1+\zeta) - (X+\zeta^2 Y)\pi^{(m-1)p} = \zeta(X+Y)\pi^{(m-1)p}.$$

Using the equation above this becomes

$$(X+Y)\gamma_1^p(1+\zeta)\varepsilon_1 - (X+Y)\gamma_2^p\varepsilon_2 = \zeta(X+Y)\pi^{(m-1)p}$$

and hence

$$\gamma_1^p - \left(\frac{\varepsilon_2}{\varepsilon_1(1+\zeta)}\right)\gamma_2^p = \frac{\zeta}{\varepsilon_1(1+\zeta)}\pi^{(m-1)p}.$$

Finally, writing $\gamma_1 = \alpha_1/\beta_1$ and $\gamma_2 = \alpha_2/\beta_2$ with π not dividing $\alpha_1, \alpha_2, \beta_1, \beta_2$, we obtain

$$(x^p + \varepsilon y^p) = (z)^p$$

where $x = \alpha_1\beta_2$, $y = \alpha_2\beta_1$ and $z = \beta_1\beta_2\pi^{m-1}$. The unit ε is equal to $\varepsilon_2/\varepsilon_2(1+\zeta)$.

The unit ε is congruent to $(-x/y)^p$ modulo π^p. In particular, $\varepsilon \equiv m \pmod{p}$, for some integer m. Cor.13.5 implies that ε is a p-th power. Since $\mathrm{ord}_\pi(z) = m-1 > 0$ is smaller than m, we obtain a contradiction and we conclude that the original equation of ideals, does not have any solutions.

In the rest of this section we will discuss the arithmetical properties of Bernoulli numbers and generalized Bernoulli numbers. As a result we will obtain an elementary way of expressing the fact that $h^-(p) \not\equiv 0 \pmod{p}$ for a prime p. This will give us a proof of Kummer's Theorem 1.6.

Theorem (13.9). *(Kummer's Congruences.) Let $p \neq 2$ be a prime. Let the Bernoulli numbers B_k for $k \ge 0$ be defined by*

$$\frac{T}{e^T - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!}T^k.$$

Then

(i)

$$\frac{B_k}{k} \quad \text{is } p\text{-integral when } k \not\equiv 0 \pmod{p-1}.$$

i.e. B_k/k can be written as a rational number with denominator not divisible by p.

$$p\frac{B_k}{k} \quad \textit{is } p\textit{-integral when } k \equiv 0 \pmod{p-1}.$$

(ii)

$$\frac{B_k}{k} \equiv \frac{B_{k'}}{k'} \quad \textit{if } k \equiv k' \pmod{p-1}.$$

(iii) For every $k, Y \in \mathbf{Z}_{\geq 0}$

$$1^k + 2^k + \ldots + Y^k = \frac{1}{k+1}\sum_{i=0}^{k+1}\binom{k+1}{i}B_{k+1-i}(Y+1)^i$$

(iv) Let $\mathfrak{p}$ be a fixed prime over p in $\mathbf{Z}[\zeta_{p-1}]$ and let $\omega : (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \mu_{p-1}$ be the Teichmüeller associated to $\mathfrak{p}$.

$$B_{1,\omega^k} \equiv \frac{B_{k+1}}{k+1} \pmod{\mathfrak{p}} \quad \textit{for } k = 1, 3, 5, \ldots, p-4.$$

Proof. Fix an integer $a \in \mathbf{Z}_{>0}$ not divisible by p. We have that

$$\sum_{k=0}^{\infty}\frac{(a^k-a)B_k}{k!}T^k = \frac{aT}{e^{aT}-1} - \frac{T}{e^T-1}.$$

Writing $u = e^T - 1$, we see that this is equal to

$$T\left(\frac{a}{(u+1)^a-1} - \frac{1}{u}\right) = \frac{T}{u}\left(\frac{1}{1+\frac{1}{a}\binom{a}{2}u+\ldots+\frac{1}{a}u^a} - 1\right)$$

$$= \frac{T}{u}\sum_{i\geq 1}\left(\frac{1}{a}\binom{a}{2}u+\ldots+\frac{1}{a}u^a\right)^i$$

$$= T\sum_{i\geq 0}A_i u^j$$

where, since p does not divide a, the A_i are p-integral. This shows that

$$\sum_{k=0}^{\infty}\frac{(a^k-a)B_k}{k!}T^k = T\sum_{i\geq 0}A_i(e^T-1)^i = T\sum_{k\geq 0}\frac{A_k'}{k!}T^k$$

where the A_i' are p-integral, because the series $\sum_{i\geq 0}A_i(e^T-1)^i$ is a p-integral combination of series of the form $e^{iT} = \sum_{j\geq 0}^{\infty}\frac{i^j}{j!}T^j$.

It follows that $(a^k-1)B_k/k = A_k'$ is p-integral. If $k \not\equiv 0 \pmod{p-1}$ we can choose a such that $a^k - 1 \not\equiv 0 \pmod{p}$. If $k \equiv 0 \pmod{p-1}$, then one can choose $a = p+1$. One checks that $(p+1)^k - 1 = kp + \binom{k}{2}p^2 + \ldots + p^k$ contains exactly $\mathrm{ord}_p(k)+1$ factors p. This proves *(i)*.

To prove *(ii)* we observe that $i^j \equiv i^{j'} \pmod{p}$ whenever $j \equiv j' \pmod{p-1}$. This implies that the coefficients A_i' above have the same property: $A_j \equiv A_{j'} \pmod{p}$ whenever $j \equiv j' \pmod{p-1}$. Part *(ii)* now follows from the fact that $(a^k-1)B_k/k = A_k'$.

(iii) One has that

$$\sum_{k=0}^{\infty}\left(1^k+2^k+\ldots+Y^k\right)T^k=\sum_{x=1}^{Y}\sum_{k=0}^{\infty}\frac{(xT)^k}{k!}=\sum_{x=1}^{Y}e^{xT}=\frac{e^{(Y+1)T}-1}{e^T-1}$$

Since one has that

$$\frac{e^{(Y+1)T}-1}{e^T-1}=\frac{e^{(Y+1)T}-1}{T}\frac{T}{e^T-1}=\left(\frac{1}{T}\sum_{i\geq 0}\frac{((Y+1)T)^i}{i!}\right)\left(\sum_{j=0}^{\infty}\frac{B_j}{j!}T^j\right)=$$

the result follows by evaluating the coefficients of the product of the power series.
(iv) Let k be an odd integer between 1 and $p-4$. We will need to know the values of the Teichmüller character ω modulo $\mathfrak{p}^2$. Since $\omega(x)\equiv x \pmod{\mathfrak{p}}$ for all x, one finds that

$$\omega(x)-x^p=\omega(x)^p-x^p=(\omega(x)-x^p)(\omega^{p-1}(x)+\omega^{p-2}(x)x+\ldots+x^{p-1})\equiv 0 \pmod{\mathfrak{p}^2}.$$

Therefore

$$pB_{1,\omega^k}=\sum_{x=1}^{p-1}x\omega^k(x)\equiv\sum_{x=1}^{p-1}x^{pk+1} \pmod{\mathfrak{p}^2}$$

By *(iii)* we have that

$$\sum_{x=1}^{p-1}x^{pk+1}=\frac{1}{pk+2}\sum_{i=0}^{pk+2}\binom{pk+2}{i}B_{pk+2-i}(pk)^i.$$

Since $k\leq p-4$, there are no indices i such that $pk+2-i\equiv 0 \pmod{p(p-1)}$. The smallest i for which $pk=2-i\equiv 0 \pmod{p-1}$ is $k+2$ and hence at least 3. Therefore

$$B_{pk+2-i}(pk)^i\equiv 0 \pmod{p^2}\quad\text{for } i\geq 2.$$

This implies that

$$\sum_{x=1}^{p-1}x^{pk+1}\equiv\frac{1}{pk+2}B_{pk+2}+B_{pk+1}p \pmod{p^2}.$$

Since k is odd, B_{pk+2} is zero. Finally

$$B_{1,\omega^k}\equiv B_{pk+1}\equiv\frac{pk+1}{k+1}B_{k+1}\equiv\frac{B_{k+1}}{k+1} \pmod{\mathfrak{p}}$$

as required.

Theorem (13.10). *Let $p\neq 2$ be a prime. If p does not divide the Bernoulli numbers B_2, B_4, $\ldots,B_{(p-3)/2}$, then Fermat's Last theorem is true for the exponent p. In other words, the equation*

$$X^p+Y^p=Z^p$$

does not have any solutions in integers X,Y,Z with $XYZ\neq 0$.

Proof. Since p does not divide $B_2, B_4, \ldots, B_{(p-3)/2)}$, we conclude from Theorem 13.9 that $\mathfrak{p}$ does not divide $B_{1,\chi}$ for every odd character $\chi \neq \omega^{-1}$ of the Galois group of $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$. By Prop.13.4*(i)* we conclude that $h^-(p)$ is not divisible by p. Cor.13.6 implies that p does not divide $h^+(p)$ and therefore that p does not divide the class number of $\mathbf{Q}(\zeta_p)$.

Now we can apply Prop.13.1 and Prop.13.8: the equation $X^p + Y^p = Z^p$ cannot have any solutions $X, Y, Z \in \mathbf{Z}$ with p not dividing XYZ by Prop.13.1. Suppose we have a solution X, Y, Z with $\gcd(X, Y, Z) = 1$ but with p dividing XYZ. Clearly we may assume that p divides Z, but not X or Y. We conclude at once from Prop.13.8 that this is impossible. This concludes the proof of the theorem.

(13.A) Prove that the equation $X^5 + Y^5 = Z^5$ does not have any solutions $X, Y, Z \in \mathbf{Z}/25\mathbf{Z}$ with 5 not dividing X, Y and Z.

(13.B) Let $p \equiv 1 \pmod 3$ be a prime. Show that for every $n \geq 1$, there are solutions $X, Y, Z \in \mathbf{Z}/p^n\mathbf{Z}$ of Fermat's equation $X^p + Y^p = Z^p$ satisfying $X, Y, Z \not\equiv 0 \pmod p$. (Hint: Let $z \in (\mathbf{Z}/p^n\mathbf{Z})^*$ have order 3. Show that $1^p + z^p = z^{2p}$ in the ring $\mathbf{Z}/p^n\mathbf{Z}$.

Bibliography

[1] Abrahamowitz, M. and Stegun, I.A.: *Handbook of Mathematical Functions*, Dover Publ. New York 1965.

[2] Adleman, L. and Fouvry, : *Inventiones Math.*

[3] Apéry, R.: Interpolation de fractions continues et irrationalité de certaines constantres, *Bull. Section de Sciences du C.T.H.S*, **3** (1978), 37–53.

[4] Artin, E.: *The Gamma function*, Holt, Rinehart& Winston 1964.

[5] Artin, E. and Tate J.T.: *Class Field Theory*, Benjamin, New York 1967.

[6] Bloch, S.: The proof of the Mordell conjecture, *Math. Intelligencer*, **6**, (1983) 41–47.

[7] Bombieri, E.: (Mordell) To appear.

[8] Borevič, Z. and Shafarevič, I.: *Number Theory*, Academic Press, London 1966.

[9] Bourbaki, N.: *Algèbre*, Hermann, Paris 1970. Masson, Paris 1981.

[10] Bourbaki, N.: *Eléments d'histoire des mathématiques*, Coll. Histoire de la pensée **4**, Hermann, Paris 1969.

[11] Brauer, R.: On Artin's L-series with generalized group characters, *Ann. of Math.* **48** (1947), 502–514.

[12] Cassels, J.W.S and Fröhlich, A.: *Algebraic Number Theory*, Academic Press, London 1967.

[13] Chatland and Davenport, H.: Euclids algorithm in real quadratic fields, *Canadian J. of Math.*, **2** (1950), 289–296. In: Davenport, H.: *Collected works I*, Academic Press, London 1977, 366–373.

[14] Claborn, L.: Every abelian group is a class group, *Pacific J. of Math.*, **18** (1966), 219–222.

[15] Coates, J. and Wiles, A.: On p-adic L-functions and elliptic units, *J. Austral. Math. Soc., Ser A.*, **26** (1978), 1–25.

[16] Coleman, R.: Division values in local fields, *Invent. Math.*, **53** (1979), 91–116.

[17] Davenport, H.:*Multiplicative number theory, 2nd Ed.*, Grad. Texts in Math. **74**, Springer-verlag, New York 1980.

[18] Dedekind, R.: *Gesammelte mathematische Werke*, Vieweg, Braunschweig 1932.

[19] Deligne, P.: La Conjecture de Weil I., *Publ. Math. I.H.E.S.*, **43** (1973), 273–307.

[20] Diaz y Diaz, F.: Tables minorant la racine n-ième du discriminant d'un corps de degré n. *Publ. Math.*, Orsay 1980.

[21] *Diophanti Alexandrini Opera Omnia ...*, éd. P. Tannery, Teubner, Lipsiae 1893–1895.

[22] Edwards, H.M.: *Riemann's zeta function*, Academic Press, New York 1974.

[23] Edwards, H.: *Fermat's last theorem, a genetic introduction to algebraic number theory*, Grad. Texts in Math. **50**, Springer-Verlag, New York 1977.

[24] Faltings, G.: Endlichkeitssätze für Abelsche Varietäten über Zahlkörpern, *Invent. Math.*, **73**, (1983) 349–366.

[25] Fermat, P. de: *Œuvres*, Gauthier-Villars, Paris 1891–1922.

[26] Gauß, C.F.: *Disquisitiones Arithmeticae*,Fleischer, Leipzig 1801.

[27] Gelbart, Bulletin

[28] Gras, M.-N.: Non monogénité de l'anneau des entiers des extensions cycliques de **Q** de degré premier $l \geq 5$. *J. of Number Theory*, **23** (1986), 347–353.

[29] Hardy, G.H. and Wright, E.M.: *An Introduction to the Theory of numbers*, (4th ed.), Oxford Univ. Press, Oxford 1960.

[30] Hartshorne, R: *Algebraic geometry*, Grad. Texts in Math. **52**, Springer-Verlag, New York 1977.

[31] Hecke, E.: *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923. Chelsea, New York 1970.

[32] Hecke, E.: *Mathematische Werke* , VandenHoeck & Ruprecht, Göttingen 1983.

[33] Hilbert, D.: *Gesammelte Abhandlungen*, Chelsea, New York 1965.

[34] Hilbert, D.: Die theorie der algebraischen Zahlkörper, *Jahresbericht Deutsce. math.-Verein*, **4** (1897), 175–546. *Gesammelte Anhandlungen I*, Chelsea, New York 1965, 63–363.

[35] Janusz, G.J.: *Algebraic Number Fields*, Pure and Appl. Math. **55**, Ac. Press, New York 1973.

[36] Koblitz, N.:*Introduction to Elliptic Curves and Modular forms*, Grad. Texts in Math. **97**, Springer-verlag, New York 1984.

[37] Kolyvagin, V.A.: Euler systems. To appear in Grothendieck festschrift, Birkhäuser 1991.

[38] Kronecker, L.: Über die algebraisch auflösbaren Gleichungen. *Monatsber. Kö. Preuß. Akad. Wiss. Berlin*, (1853), 365–374. *Mathematische Werke* , Chelsea, new York, 1968, Vol.4, 3–11.

[39] Kummer, E.E.: *Collected Papers* (ed. by A. Weil), Springer-verlag, New York 1975.

[40] Lang, S.: *Elliptic functions*, Addison-Wesley, Reading 1973.

[41] Lang, S.: *Algebra* (2nd edition), Addison-Wesley, Menlo Park (Ca) 1984.

[42] Lang S.: *Algebraic Number Theory*, Addison-Wesley, Reading 1980.

[43] Lang, S.: *Cyclotomic Fields* 2^{nd} *ed.*, Graduate Texts in Math. **100**, Springer-Verlag, New York 1990.

[44] Lehmer, D.H. and Masley, J.: Table of the cyclotomic class numbers $h^*(p)$ and their factors for $200 < p < 521$, *Math.Comp* **32**, (1978), 577–582, microfiche supplement.

[45] Lejeune-Dirichlet, P.G.: *Werke*, Reimer, Berlin 1889–1897.

[46] Lekkerkerker, C.G. and Gruber, P.: *Geometry of Numbers, 2nd Ed.*, North-Holland 1988.

[47] Lenstra, H.W.: Euclidean number fields. *Math. Intelligencer*, **2** (1979), 6–15 and (1980) 73–77, 99–103.

[48] Lenstra, H.W.: Euclid's algorithm in cyclotomic fields. *J. London Math. Soc*, **10**,(1975), 457–465.

[49] Lenstra, H.W.: *Elementaire Algebraïsche getaltheorie*, Syllabus, Univ. van Amsterdam 1982.

[50] Lenstra, A.K., Lenstra, H.W., Manasse, M., Pollard, J.:

[51] Martinet, J.: Tours de corps de classes et estimations de discrimiants, *Invent. Math.*, **44** (1978), 65–73..

[52] Matzat, B.H.: *Manuscripta Math.*, **51** (1985), 253–265.

[53] Mazur, B.: Modular curves and the Eisenstein ideal, *IHES Publ. Math.*, **47** (1977), 33–186.

[54] Mazur., B.: Rational points of Abelian varieties with values in towers of number fields, s Invent. Math., **18** (1972), 183–266.

[55] Mazur, B. and Wiles, A.: Class fields of abelian extensions of **Q**, *Invent. Math.* **76**, (1984), 179–330.

[56] Minkowski, H.: *Geometrie der Zahlen.*, Teubner, Leipzig 1896.

[57] Minkowski, H.: *gesammelte Abhandlungen*, Teubner, Leipzig 1896.

[58] Ono, T.: *An introduction to algebraic number theory*, Plenum Press, New York 1990.

[59] Perrin-Riou, B.: Travaux de Kolyvagin et Rubin, *Sém. Bourbaki*, **717**, Paris Novembre 1989.

[60] Poitou, G.: Minorations de discriminants (d'après Odlyzko). Sém. Bourbaki 1975/1976, Exp. 479, In: Springer Lecture Notes in Math. **567**,(1977), 136–153.

[61] Ribet, K.: On modular representations of Gal($\overline{\mathbf{Q}}/\mathbf{Q}$) arising from modular forms,
Invent. Math. (1990)

[62] Ribet, K.: A modular construction of unramified p-extensions of $\mathbf{Q}(\mu_p)$, *Invent. Math.* **34**, (1976), 151–162.

[63] Rubin, K.: Global units and ideal class groups, *Invent. Math.*, **89** (1987), 511–526.

[64] Shafarevič, I.R.: *Collected Mathematical papers*, Springer-Verlag, Berlin 1989.

[65] Samuel, P.: *Théorie algebrique des nombres*, Hermann, Paris 1971.

[66] Serre, J.-P.: *Œuvres*, Springer-Verlag, Berlin 1986.

[67] Serre, J.-P.: *A corse in Arithmetic*, Grad. Texts in Math., **7** Springer-Verlag, New York 1973.

[68] Serre, J.-P,, on Matzat etc. Sém. Bourbaki

[69] Shimura, G. and Taniyama, Y.: Complex Multiplication of abelian varieties and its application to number theory, *Publ. Math. Soc. japan*, **6** (1961).

[70] Sinnott, W.B.: On the Stickelberger ideal and the circular units of a cyclotomic field, *Ann. of Math.*, **108** (1978), 107–134.

[71] Stewart, I.N.: *Galois Theory, 2nd Ed.*, Chapman and Hall, London 1989.

[72] Stewart, I.N. and Tall, D.O.: *Algebraic number theory*, Chapman and Hall, London 1987.

[73] Tanner, J.W. and Wagstaff, S.S.: New congruences for the Bernoulli numbers, *Math. of Comp.*, **48** (1987), 341–350.

[74] Tate, J.T.: *Les conjectures de Stark sur les fonctions L d'Artin en* $s = 0$. *(Notes d'un cours à Orsay rédigées par D. Bernardi et N. Schappacher)*, Birkhäuser, Boston 1984.

[75] Thaine, F.: On the ideal class groups of real abelian number fields, *Ann. of Math.*, **128**

[76] Van der Linden, F.: Class number computations of real abelian number fields, *Math. Comp.* **39**, (1982), 693–707.

[77] Van der Lune, J. and Te Riele, H.: On the zeroes of the Riemann Zeta function in the critical strip, III, *Math.Comp.*, **41** (1983), 759–767.

[78] Van der Poorten, A proof that Euler missed ... Apéry's proof of the irrationality of $\zeta(3)$, *Math. Intelligencer*, **1** (1979), 195–203.

[79] Wagstaff, S.S.: The irregular primes to 125,000, *Math. of Comp.*, **32** (1978), 583–591.

[80] Washington, L.: *Introduction to cyclotomic fields*, Grad. Texts in Math. **83**, Springer-verlag, New York 1982.

[81] Weber H.: Theorie der Abelschen Zahlkörper, *Acta Math.*, **8** (1866), 193–263.

[82] Weil, A.: *Sur les courbes algébriques et les variétés qui s'en déduissent*, Hermann, Paris 1948.

[83] Weil, A.: *Number Theory, an approach through history*, Birkäuser, Boston 1984.

[84] Zagier, D.B.: Hyperbolic manifolds and special values of Dedekind zeta-functions, *Invent. Math.* **83**, (1986), 285–301.