7. 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. It is of finite index by Cor.5.4. In this section we investigate under which conditions $\mathbf{Z}[\alpha]$ is equal to 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 7.1. *(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 that 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 $I_i \subset O_F$ be the ideal generated by p and $h_i(\alpha)$ and let $q = p^{\deg(h_i)}$. Then we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (p, h_i(\alpha)) & \longrightarrow & I_i & \longrightarrow & \text{cok} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbf{Z}[\alpha] & \longrightarrow & O_F & \longrightarrow & O_F/\mathbf{Z}[\alpha] & \longrightarrow & 0 \end{array}$$

It induces an exact sequence

$$\mathbf{F}_q \longrightarrow O_F/I \longrightarrow O_F/\mathbf{Z}[\alpha]/\text{cok} \longrightarrow 0$$

The leftmost map is a ring homomorphism. Since $\mathbf{F}_q$ is a field, it is therefore injective. The group in the middle is a finite dimensional $\mathbf{F}_p$-vector space. Since the order of its quotient $O_F/\mathbf{Z}[\alpha]/\text{cok}$ divides $[O_F : \mathbf{Z}[\alpha]]$, it must be 1. This shows that I_i is a prime ideal of O_F of norm q.

Therefore we have

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

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

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

Since $N((p)) = p^n$, the O_F-ideal (p) is equal to $\prod_i \mathfrak{p}_i$ 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. Since -23 is squarefree, 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 7.3.

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 7.4. *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 $I = \{g \in \mathbf{F}_p[T] : \frac{1}{p}g(\pi) \in O_F\}$. 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 it contains T^{n-1}, which means that $\frac{\pi^{n-1}}{p}$ 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

$$\pi\frac{\pi^{n-1}}{p} + \frac{a_{n-1}}{p}\pi^{n-1} + \ldots + \frac{a_1}{p}\pi + \frac{a_0}{p} = 0$$

it follows that π divides a_0/p in the ring O_F. Since a_0/p is prime to p, it follows that the O_F-ideal (π, p) is equal to O_F itself. But then we also have $(\pi, p)^n = O_F$, which is absurd, since $(\pi, p)^n \subset (p)$. We conclude that p does not divide the index $[O_F : \mathbf{Z}[\pi]]$ as required.

Example 7.5. *Let p be prime number and let $F = \mathbf{Q}(\zeta_p)$. The ring of integers of F is $\mathbf{Z}[\zeta_p]$.*

Proof. Clearly $\mathbf{Z}[\zeta_p]$ is contained in the ring of integers of $\mathbf{Q}(\zeta_p)$. The minimum polynomial of ζ_p is the p-th cyclotomic polynomial $\Phi_p(X) = (X^p - 1)/(X - 1) = X^{p-1} + \ldots + X + 1$. Indeed, the poltynomial

$$\Phi_p(T + 1) = \frac{(T + 1)^p - 1}{T} = T^{p-1} + pT^{p-2} + \ldots + p.$$

is Eisenstein at p. It follows that the trace of ζ_p^i is -1 when $i \not\equiv 0 \pmod{p}$, while it is $p - 1$ when $i \equiv 0 \pmod{p}$. Therefore the discriminant $\Delta(1, \zeta_p, \ldots, \zeta_p^{p-2})$ is equal to the determinant of the $p-1$ by $p-1$ matrix (a_{ij}) with entries $a_{ij} = -1$ when $i+j \not\equiv 2 \pmod{p}$, while $a_{ij} = p - 1$ when $i + j \equiv 2 \pmod{p}$. By Exercise 7.5 this determinant is equal to $\pm p^{p-2}$.

It follows that the discriminant of $\mathbf{Z}[\zeta_p]$ is $\pm p^{p-2}$. The only prime number that could divide the index $[O_F[\mathbf{Z}[\zeta_p]]$ is p. However, by Proposition 7.4 the prime p it doesn't. Therefore O_F is equal to the ring $\mathbf{Z}[\zeta_p]$ as required.

Theorem 7.6. *(Dedekind's Criterion.) Suppose α is an algebraic integer with minimum polynomial over $f(T) \in \mathbf{Z}[T]$. Let $F = \mathbf{Q}(\alpha)$ and let p be a prime number. Then p divides the index $[O_F : \mathbf{Z}[\alpha]]$ if and only if there exists a maximal ideal $\mathfrak{m}$ of $\mathbf{Z}[X]$ with the property that $p \in \mathfrak{m}$ and $f(X) \in \mathfrak{m}^2$.*

Proof. *"if":* A maximal ideal $\mathfrak{m} \subset \mathbf{Z}[X]$ containing p and f has the form $\mathfrak{m} = (\phi, p)$ where $\phi \in \mathbf{Z}[X]$ is a a monic polynomial that is an irreducible divisor of f in $\mathbf{F}_p[X]$. If $f \in \mathfrak{m}^2$, we have

$$f = a\phi^2 + bp\phi + cp^2,$$

for certain polynomials $a, b, c \in \mathbf{Z}[X]$. Since $f \equiv a\phi^2 \pmod{p}$, the polynomial $a\phi \pmod{p}$ has degree $< \deg f$ and the element

$$x = \frac{a(\alpha)\phi(\alpha)}{p}$$

is not in $\mathbf{Z}[\alpha]$, but px is. Multiplying by x maps the $\mathbf{Z}[\alpha]$-ideal $(\phi(\alpha), p)$ to itself. Since $(\phi(\alpha), p)$ is finitely generated, the element x must be integral and hence in O_F. It follows that the image of x in the quotient group $O_F/\mathbf{Z}[\alpha]$ has order p.

The following diagram describes the situation. Here k denotes the finite field $\mathbf{Z}[X]/\mathfrak{m}$.

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & p\mathbf{Z}[X] & \longrightarrow & (\phi(\alpha), p) & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (f) & \longrightarrow & \mathbf{Z}[X] & \longrightarrow & \mathbf{Z}[\alpha] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (\phi) & \longrightarrow & \mathbf{F}_p[X] & \longrightarrow & k & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

"only if": Suppose that p divides the index of $\mathbf{Z}[\alpha]$ in O_F. Consider the $\mathbf{F}_p[X]$-ideal $J = \{h \in \mathbf{F}_p[X] : \frac{1}{p}h(\alpha) \in O_F\}$. The polynomial $f \pmod p$ is contained in J, but by assumption, it is not a generator. Let g be a generator of J and let $\phi \in \mathbf{Z}[X]$ be a a monic polynomial that is an irreducible divisor of f/g in $\mathbf{F}_p[X]$. Then f is an element of the maximal ideal $\mathfrak{m} = (\phi, p)$. So, we have $f = \phi u + ph$ for certain polynomials $u, h \in \mathbf{Z}[X]$. By construction, u modulo p is in the $\mathbf{F}_p[X]$-ideal J. This gives

$$\frac{u(\alpha)}{p} \cdot \phi(\alpha) = h(\alpha), \qquad \text{in } F.$$

Since $x = \frac{u(\alpha)}{p}$ is in O_F, it is is e zero of a polynomial of the form $X^m + a_{m-1}X^{m-1} + \ldots + a_1X + a_0 \in \mathbf{Z}[X]$. It follows that we have

$$h(\alpha)^m + a_{m-1}\phi(\alpha)h(\alpha)^{m-1} + \ldots + a_0\phi(\alpha)^m = 0.$$

Therefore $\phi(\alpha)$ divides $h(\alpha)^m$ in the ring $\mathbf{Z}[\alpha]$. So there exist polynomials $h_1, h_2 \in \mathbf{Z}[X]$ for which we have

$$h(X)^m = h_1(X)\phi(X) + h_2(X)f(X), \qquad \text{in } \mathbf{Z}[X].$$

This implies that ϕ divides h^m in $\mathbf{F}_p[X]$. Since ϕ is irreducible in $\mathbf{F}_p[X]$ it divides h in $\mathbf{F}_p[X]$. In other words, the polynomial h is contained in $\mathfrak{m}$. The relation $f = \phi u + ph$ implies that we also have $f = (\phi + p)u + (h - u)p$. Since $\phi - p$ is monic and congruent to ϕ modulo p, we may repeat the argument with ϕ replaced by $\phi - p$ and h by $h - u$. It follows that ϕ divides $h - u$ in $\mathbf{F}_p[X]$. This means that ϕ divides u in $\mathbf{F}_p[X]$, so that $u \in \mathfrak{m}$.

Since the polynomial f is equal to $\phi u + ph$ and both u and h are in $\mathfrak{m} = (\phi, p)$, also $f \in \mathfrak{m}^2$, as required.

Dedekind's criterion takes the following practical shape.

Corollary 7.7. *Let F be a number field, let $\alpha \in O_F$ and let p be a prime number. Suppose that*

$$f = \phi_1^{e_1} \cdot \ldots \cdot \phi_g^{e_g},$$

is the factorization of $f \in \mathbf{F}_p[X]$ in mutually distinct irreducible factors $\phi_i \in \mathbf{F}_p[X]$ and exponents $e_i \geq 1$. Then p divides the index $[O_F : \mathbf{Z}[\alpha]]$ if and only if for some $i = 1, \ldots, g$ we have $e_i \geq 2$ and

$$\frac{f - \tilde{\phi_1}^{e_1} \cdot \ldots \cdot \tilde{\phi_g}^{e_g}}{p} \equiv 0 \pmod{\phi_i}, \qquad \textit{in the ring } \mathbf{F}_p[X].$$

Here $\tilde{\phi}_i$ denotes any lift of the polynomial ϕ_i to $\mathbf{Z}[X]$.

In order to prove the last result of this section, we introduce a slightly more general concept of discriminant. Let K be a field and let A be an n-dimensional commutative K-algebra. In other words A is a ring equipped with a ring homomorphism $K \longrightarrow A$. In ths way A has the structure of a K-vector space, which we assume has dimension n. In section 2 we have studied the special case $K = \mathbf{Q}$ and A a number field F.

On A we define the *trace* $Tr(x)$ of an element $x \in A$ by $Tr(x) = Tr(M_x)$ 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 define the discriminant

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

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

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 either zero, or a well-defined element of the group K^*/K^{*2}. In particular, whether or not $\Delta(A/K)$ is zero does not depend on the choice of a K-basis of A.

Exercise 7.9 it devoted to a proof of the fact that

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

for two finite dimensional K-algebras A and B.

Theorem 7.8. *(R. Dedekind 1920) 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 the discriminant Δ_F.*

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 $O_F/(p)$ in two ways. 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 write $O_F/(p)$ as a product of $\mathbf{F}_p$-algebras as follows. Suppose p factors in O_F as

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

where the prime ideals $\mathfrak{p}^i$ are mutually distinct. By the Chinese Remainder Theorem 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 by Exercise 7.9 we get

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

By Exerc. 7.10 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 $A = O_F/\mathfrak{p}^e$. Let $\pi \in \mathfrak{p}$ but not in $\mathfrak{p}^2$. Then π is a non-zero nilpotent element. We can use it as the first element in an $\mathbf{F}_p$-basis $e_1, \ldots, e_k$ of A. Clearly πe_i is nilpotent for every $e_i \in A$. Since a nilpotent endomorphism has only eigenvalues 0, we see that the first row of the matrix $(Tr(e_i e_j))_{1 \le i,j \le n}$ is zero. This concludes the proof of the Theorem.

7.1. 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.

7.2. 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 respectively) in F over $\mathbf{Q}$ if and only if d is a square (non-square, zero respectively) modulo p.

7.3. 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.

7.4. 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.)

7.5 Let A be an $n \times n$ matrix with entries a_{ij} in a field k.

(a) Let $c \in k$. Suppose that $a_{ij} = c$ for all i, j. Show that the characteristic polynomial of A is equal to $X^{n-1}(X - nc)$.

(b) Suppose that $a_{ij} = c$ whenever $i \neq j$, while $a_{ij} = c - d$ when $i = j$. Prove that $\det A = d^{n-1}(d - nc)$.

7.6 Let $f(X) = X^3 - X^2 - 6X - 8 \in \mathbf{Z}[X]$. Show that f is irreducible.

(a) Show that $\mathrm{Disc}(f) = -4 \cdot 431$. Show that the ring of integers of $F = \mathbf{Q}(\alpha)$ admits $1, \alpha, \beta = (\alpha^2 - \alpha)/2$ as a $\mathbf{Z}$-basis.

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

(c) 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 $[O_F : \mathbf{Z}[\alpha]]$.

7.7 Let $\mathbf{F}_q$ be a finite field of q elements and let $\mathbf{F}_q \subset \mathbf{F}_{q^r}$ an extension of degree r. Dimostrare che $\Delta(\mathbf{F}_{q^r}/\mathbf{F}_q)$ is not zero.

7.8 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.

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

7.10 Show that for every number field F there is a prime that is ramified in F over $\mathbf{Q}$.