2. Number fields.

In this section we discuss number fields. We introduce the norm and trace maps, discriminants, the $\mathbf{R}$-algebra $F_{\mathbf{R}}$ and the $\mathbf{C}$-algebra $F_{\mathbf{C}}$ associated to a number field F. No knowledge of Galois Theory is assumed. We prove the Theorem of the Primitive Element and this suffices for our purposes.

Definition 2.1. *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. Since the n-th cyclotomic polynomial is irreducible and has degree $\phi(n)$, we have $[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \phi(n)$. Here $\phi(n) = \#(\mathbf{Z}/n\mathbf{Z})^*$ denotes Euler's ϕ-function.

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

Definition 2.2. *Let F be a number field of degree n and let $x \in F$. The Norm $N(x)$ of x is $\det(M_x)$ while the Trace $Tr(x)$ is equal to the trace of the matrix M_x. The characteristic polynomial $f^x_{\mathrm{char}}(T) \in \mathbf{Q}[T]$ of x is*

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

Since the matrix M_x has rational entries, $f^x_{\mathrm{char}}(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0$ is in $\mathbf{Q}[T]$. Since we have $Tr(x) = -a_{n-1}$ and $N(x) = (-1)^n a_0$, the trace and the norm of x are in $\mathbf{Q}$. The characteristic polynomial, the trace and the norm of x are well defined since they do not depend on the basis with respect to which the matrix M_x has been defined. The norm and the trace have the following properties.

$$\begin{aligned} N(xy) &= N(x)N(y); \\ Tr(x+y) &= Tr(x) + Tr(y). \end{aligned} \qquad \text{for every } x, y \in F.$$

The characteristic polynomial $f^x_{\mathrm{char}}(T)$, and therefore the norm $N(x)$ and the trace $Tr(x)$ of an algebraic number x depend on the field F that contains x. Usually it is clear from the context what the relevant field F is. In order to avoid ambiguities we occasionally may write $Tr_F(x)$ for $Tr(x)$ and $N_F(x)$ for $N(x)$. See Exercise 2.11.

Definition 2.3. *Let F be a number field of degree n and let $\omega_1, \omega_2, \ldots, \omega_n \in F$. We define the discriminant $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ by*

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

Since traces are in $\mathbf{Q}$, so are discriminants. In the rest of this section we prove some basic properties of the characteristic polynomial, the norm and trace maps and discriminants. The following theorem says that every number field can be generated by one element only.

Theorem 2.4. *(Theorem of the primitive element.) Let F be a finite extension of $\mathbf{Q}$. Then there exists $\theta \in F$ such that $F = \mathbf{Q}(\theta)$.*

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 $f(T) = f^{\alpha}_{\min}(T)$ the minimum polynomial of β 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 $g(T) = f^{\beta}_{\min}(T)$ 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 $t \in \mathbf{Q}$ such that

$$t \neq \frac{\beta_i - \beta}{\alpha - \alpha_j} \qquad \text{for } 1 \leq i \leq m \text{ and for } 2 \leq j \leq n,$$

or equivalently,

$$t\alpha + \beta \neq t\alpha_j + \beta_i \qquad \text{for } 1 \leq i \leq n \text{ and for } 2 \leq j \leq m.$$

Put

$$\theta = t\alpha + \beta$$

The polynomials $h(T) = g(\theta - tT)$ and $f(T)$ are both in $\mathbf{Q}(\alpha)[T]$ and they both have α as a zero. The remaining zeroes of $f(T)$ are $\alpha_2, \ldots, \alpha_m$. If any of these were also a zero of $g(\theta - tT)$, then for some $j \geq 2$ the number $\theta - t\alpha_j$ would be equal to some zero β_i of g. This contradicts the choice of t.

It follows that the gcd of f and g in the ring $\mathbf{Q}(\theta)$ has a single zero of multiplicity one and must therefore be equal to $c_0 + c_1 T$ for certain $c_0, c_1 \in \mathbf{Q}(\theta)$. It follows that $\alpha = -c_0/c_1$ is in $\mathbf{Q}(\theta)$. Then $\beta = \theta - t\alpha$ is also in $\mathbf{Q}(\theta)$ and the proof is complete.

Corollary 2.5. *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 2.4 the field F is of the form $\mathbf{Q}(\alpha)$ for some α. Let f be the minimum polynomial of α over $\mathbf{Q}$. Then the map $\mathbf{Q}[X]/(f) \to \mathbf{Q}(\alpha)$ given by evaluating polynomials in α is a well defined isomorphism of fields. Any ring homomorphism $\phi : \mathbf{Q}[X]/(f) \longrightarrow \mathbf{C}$ has the property that $\phi(q) = q$ for all $q \in \mathbf{Q}$. Since $f = 0$ in $\mathbf{Q}[X]/(f)$, the complex number $\phi(\alpha)$ must be a zero of f.

Conversely, evaluating in a complex zero of f is a homomorphism $\mathbf{Q}[X]/(f) \longrightarrow \mathbf{C}$. Since f is irredcible of degree n, it has n distinct zeroes in $\mathbf{C}$. Therefore there are exactly as many distinct homomorphism $F \longrightarrow \mathbf{C}$. This proves the corollary.

Definition 2.6. *Let F be a number field of degree n. The ring homomorphisms $F \longrightarrow \mathbf{C}$ whose images are contained in $\mathbf{R}$ are also called real embeddings. We denote their number by r_1. The ring homomorphisms $F \longrightarrow \mathbf{C}$ whose images are not in $\mathbf{R}$ are called complex embeddings. They come in complex conjugate pairs. We denote the number of pairs by r_2.*

We have

$$r_1 + 2r_2 = n.$$

Example. Consider the number field $F = \mathbf{Q}(\alpha)$, where $\alpha^4 = 2$. In other words, α is a zero of the irreducible polynomial $X^4 - 2 \in \mathbf{Q}[X]$. The field F is isomorphic to $\mathbf{Q}[X]/(X^4 - 2)$ and the four ring homomorphisms $\mathbf{Q}[X]/(X^4 - 2) \longrightarrow \mathbf{C}$ are given by evaluating polynomials in $\mathbf{Q}[X]$ in the four complex zeroes $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$ of f. Equivalently, these are the unique ring homomorphisms $\mathbf{Q}(\alpha) \longrightarrow \mathbf{C}$ that send α to $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$ respectively. We have $r_1 = 2$ and $r_2 = 1$.

The number field $\mathbf{Q}$ admits a unique field homomorphism into the field of complex numbers $\mathbf{C}$. It is the inclusion map. Its image is contained in the subfield $\mathbf{R}$. So, we have injective ring homomoprhisms

$$\mathbf{Q} \quad \hookrightarrow \quad \mathbf{R} \quad \hookrightarrow \quad \mathbf{C}. \tag{$*$}$$

By Corollary 2.5 a number field F admits in general several ring homomorphisms into $\mathbf{C}$. Their images are not necessarily contained in $\mathbf{R}$. The generalization of $(*)$ to an arbitrary number field F involves $\mathbf{R}$-algebras and $\mathbf{C}$-algebras that are not necessarily fields.

Let F be a number field. By Theorem 2.4 there is an element $\alpha \in F$ for which we have $F = \mathbf{Q}(\alpha)$. In other words $F = \mathbf{Q}[X]/(f)$ where $f \in \mathbf{Q}[X]$ denotes the minimum polynomial of α. We put $F_{\mathbf{R}} = \mathbf{R}[X]/(f)$ and $F_{\mathbf{C}} = \mathbf{C}[X]/(f)$. Here (f) denotes the principal ideal generated by f inside $\mathbf{Q}[X]$, $\mathbf{R}[X]$ and $\mathbf{C}[X]$ respectively. We have natural injective ring homomorphisms

$$F \quad \hookrightarrow \quad F_{\mathbf{R}} \quad \hookrightarrow \quad F_{\mathbf{C}}.$$

See Exercise 2.5 for the injectivity. The $\mathbf{R}$-algebra $F_{\mathbf{R}}$ is equal to the tensor product $F \otimes \mathbf{R}$ and, similarly, the $\mathbf{C}$-algebra $F_{\mathbf{C}}$ is the tensor product $F \otimes \mathbf{C}$. In these notes we avoid the language of tensor products.

We denote the ring homomorphisms $\mathbf{C}[X]/(f) \longrightarrow \mathbf{C}$ given by evaluating in the complex zeroes $\alpha_1, \ldots, \alpha_n$ of f by $\phi_1, \ldots, \phi_n$ respectively. Their restrictions to $F = \mathbf{Q}[X]/(f)$ are precisely the ring homomorphisms $F \longrightarrow \mathbf{C}$ that appear in the proof of Corollary 2.5. Let Φ denote the homomorphism $\mathbf{C}[X]/(f) \longrightarrow \prod_{i=1}^n \mathbf{C}$ given by $\Phi(y) = (\phi_1(y), \ldots, \phi_n(y))$ for $y \in \mathbf{C}[X]/(f)$. Since it is clearly injective, Φ is an isomorphism of $\mathbf{C}$-algebras. There are natural injective ring homomorphisms

$$\begin{array}{ccccc} F & \hookrightarrow & F_{\mathbf{R}} & \hookrightarrow & F_{\mathbf{C}} \\ & & & & \downarrow \Phi \\ & & & & \prod_{i=1}^n \mathbf{C} \end{array}$$

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

$$N(x) = \prod_{i=1}^{n} \phi_i(x) \qquad \text{and} \qquad Tr(x) = \sum_{i=1}^{n} \phi_i(x).$$

(b)

$$f^x_{\mathrm{char}}(T) = \prod_{i=1}^{n} (T - \phi_i(x)).$$

(c)

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

Proof. Let $x \in F$. Multiplying by $\Phi(x)$ is a $\mathbf{C}$-linear map from $F_{\mathbf{C}}$ to itself that restricts to the multiplication by x map $F \to F$. Let e_i denote the i-th vector in the canonical basis of $\prod_{i=1}^n \mathbf{C}$. It satisfies $e_i^2 = e_i$ and $e_i e_j = 0$ for every $j \neq i$. Therefore multiplication by $\Phi(x)$ is given by multiplication by a *diagonal* matrix with entries $\phi_i(x)$ for $i = 1, \ldots, n$. Its characteristic polynomial is therefore $\prod_{i=1}^n (T - \phi_i(x))$. Since may compute the characteristic polynomial of $x \in F$ also with respect to any $\mathbf{Q}$-basis of F, this is also the characteristic polynomial of x. This implies (b) and hence (a).

For part (c) let $g(T) \in \mathbf{Q}[T]$ be an irreducible divisor of $f^x_{\mathrm{char}}(T)$. By part *(b)* has one of the complex zeroes $\phi_i(x)$ as a zero of g. Since g has rational coefficients, we have that $\phi_i(g(x)) = g(\phi_i(x)) = 0$. Since ϕ_i is an injective field homomorphism, it follows that $g(x) = 0$. Therefore f^x_{min} divides g and by irreducibility we have that $g = f^x_{\mathrm{min}}$. Since g is an arbitrary irreducible divisor of the characteristic polynomial, it follows that $f^x_{\mathrm{char}}(T)$ 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 *(c)*.

Next we discuss the basic properties of discriminants.

Proposition 2.8. *Let F be a number field of degree n and let $\omega_1, \omega_2, \ldots, \omega_n \in F$. Then*
(a) we have

$$\Delta(\omega_1, \omega_2, \ldots, \omega_n) = \det(\phi_i(\omega_j)_{1 \leq i,j \leq n})^2.$$

(b) $\Delta(\omega_1, \omega_2, \ldots, \omega_n) \neq 0$ if and only if $\omega_1, \omega_2, \ldots, \omega_n$ is a basis for F as a vector space over $\mathbf{Q}$.

(c) If $\omega_i' = \sum_{j=1}^n \lambda_{ij}\omega_j$ with $\lambda_{ij} \in \mathbf{Q}$ for $1 \leq i, j \leq n$, 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. *(a)* Proposition 2.6 implies that for every $i, j = 1, \ldots, n$ we have $\sum_{k=1}^n \phi_k(\omega_i\omega_j) = \mathrm{Tr}(\omega_i\omega_j)$. Therefore we have the following equality of matrices

$$(\phi_i(\omega_k))(\phi_i(\omega_k)) = (Tr(\omega_i\omega_j))$$

and *(a)* easily follows.
(b) The monomials 1, $X \ldots, X^{n-1}$ form a a basis of the $\mathbf{Q}$-vector space $F = \mathbf{Q}[X]/(f)$. They are *also* an $\mathbf{R}$-basis of the real vector space $F_{\mathbf{R}} = \mathbf{R}[X]/(f)$ and a $\mathbf{C}$-basis of the complex vector space $F = \mathbf{C}[X]/(f)$. Therefore, n elements $\omega_1, \ldots, \omega_n$ in F form a basis of the $\mathbf{Q}$-vector space F if and only if their images in $F_{\mathbf{R}}$ are an $\mathbf{R}$-basis of the real vector space $F_{\mathbf{R}} = \mathbf{R}[X]/(f)$ and if and oly if their images in $F_{\mathbf{C}}$ are a $\mathbf{C}$-basis of the complex vector space $F = \mathbf{C}[X]/(f)$.

For $j = 1, \ldots, n$ the image of ω_j in $F_{\mathbf{C}} \cong \prod_{i=1}^n \mathbf{C}$ is the vector $\phi_i(\omega_j)$. Therefore the elements $\omega_1, \ldots, \omega_n$ form a $\mathbf{Q}$-basis of F if and only if the vectors $\phi_i(\omega_j)$, for $j = 1, \ldots, n$, are a $\mathbf{C}$-basis of $F_{\mathbf{C}}$. By linear algebra this happens precisely when the determinant of the square matrix $(\phi_j(\omega_i))$ is not zero. Part (b) now follows from (a).

(c) We have the following matrix product

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

and *(c)* follows from *(a)*.

This finishes the proof of the proposition.

Corollary 2.9. *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 $\det(\phi_j(\omega_i)) \neq 0$ if and only if $\Delta(\omega_1, \omega_2, \ldots, \omega_n) \neq 0$.*

Proof. *This is clear.*

The rest of this section is devoted to the $\mathbf{R}$-algebra $F_{\mathbf{R}}$. As before we have $F = \mathbf{Q}(\alpha)$. Let $f \in \mathbf{Q}[X]$ denote the minimum polynomial of α. It has r_1 real zeroes and r_2 pairs of complex conjugate zeroes in $\mathbf{C} - \mathbf{R}$. They correspond to the r_1 real embeddings $F \hookrightarrow \mathbf{R}$ and r_2 pairs of complex conjugate embeddings $F \hookrightarrow \mathbf{C}$. The Chinese remainder Theorem implies that evaluating in the r_1 real zeroes and in one of each of the r_2 pairs of non-real zeroes is an isomorphism of rings

$$F_{\mathbf{R}} = \mathbf{R}[X]/(f) \xrightarrow{\cong} \prod_{i=1}^{r_1} \mathbf{R} \times \prod_{i=1}^{r_2} \mathbf{C}.$$

We have the following commutative diagram of ring homomorphisms

$$\begin{array}{ccccc} F & \hookrightarrow & F_{\mathbf{R}} & \hookrightarrow & F_{\mathbf{C}} \\ \| & & \downarrow & & \downarrow \Phi \\ F & \hookrightarrow & \prod_{i=1}^{r_1} \mathbf{R} \times \prod_{i=1}^{r_2} \mathbf{C} & \hookrightarrow & \prod_{i=1}^{n} \mathbf{C} \end{array}$$

The image of F is dense in $F_{\mathbf{R}}$. The homomorphism $F \hookrightarrow \prod_{i=1}^{r_1} \mathbf{R} \times \prod_{i=1}^{r_2} \mathbf{C}$ is given as follows. The real coordinates are obtained by applying the *real*embedding ϕ while the complex ones are obtained by applying one of each of the r_2 pairs of complex conjugate embeddings. Here our choice should agree with the choice made above. The homomorphism $\prod_{i=1}^{r_1} \mathbf{R} \times \prod_{i=1}^{r_2} \mathbf{C} \hookrightarrow \prod_{i=1}^{n} \mathbf{C}$ is the inclusion map $\mathbf{R} \subset \mathbf{C}$ on the real coordinates while it is the map $z \mapsto (z, \overline{z})$ on the complex ones.

Example. Let $\alpha = \sqrt[4]{2}$ 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 $\pm i\sqrt[4]{2}$. Therefore we have $r_1 = 2$ and $r_2 = 1$. The $\mathbf{R}$-algebra $F_{\mathbf{R}}$ is isomorphic to $\mathbf{R} \times \mathbf{R} \times \mathbf{C}$

Let ϕ_1 and ϕ_2 denote the two *real* embeddings. They are given by $\phi_1(\alpha) = \sqrt[4]{2}$ and $\phi_2(\alpha) = -\sqrt[4]{2}$. The non-real complex conjugate embeddings are ϕ_3 and ϕ_4, given by $\phi_3(\alpha) = i\sqrt[4]{2}$ and $\phi_4(\alpha) = -i\sqrt[4]{2}$. The map

$$F \longrightarrow F_{\mathbf{R}} = \mathbf{R} \times \mathbf{R} \times \mathbf{C}$$

is, given by $x \mapsto (\phi_1(x), \phi_2(x), \phi_3(x))$ for $x \in F$.

Exercises.

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

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

2.3 Let $F = \mathbf{Q}(\sqrt[6]{5})$. Describe the homomorphism $F \longrightarrow F_{\mathbf{R}}$ explicitly.

2.4 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.

2.5 Let K be a subfield of a field L and let $g \in K[X]$. Show that the natural homomorphism $K[X]/(g) \to L[X]/(g)$ is injective. Here (g) denotes the ideal generated by g in $K[X]$ and $L[X]$ respectively.

2.6 Let F be a number field of degree n and let $x \in F$. Show that for $q \in \mathbf{Q}$ one has that

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

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

2.7 Let $F \subset K$ be number fields. Let $x \in F$ and put $d = [K : F]$. Show that $N_K(x) = N_F(x)^d$ and $Tr_K(x) = dTr_F(x)$.

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

2.9 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 $\alpha \in \mathbf{Q}(\zeta_5)$.

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

2.11 Let $F = \mathbf{Q}(\sqrt[4]{2})$ and let $x = \sqrt{2} = (\sqrt[4]{2})^2 \in F$.

(a) Show that the characteristic polynomial of x is $f^x_{\text{char}}(T) = T^4 - 4T^2 + 4$, that its norm is $N_F(x) = 4$ and its trace is $Tr_F(x) = 0$.

(b) The element x is cointained in the subfield $F' = \mathbf{Q}(\sqrt{2})$. Compute the characteristic polynomial of x as an element of F'. Compute $N_{F'}(x)$ and $Tr_{F'}(x)$.

2.12 Let F be a number field. Let $\omega_1, \ldots, \omega_n \in F$ be a $\mathbf{Q}$-basis of F. Show $\Delta(\omega_1, \ldots, \omega_n)$ has sign $(-1)^{r_2}$. As usual, r_2 denotes half the number of embeddings $F \hookrightarrow \mathbf{C}$ whose image is not in $\mathbf{R}$.

2.13 Let F be a number field of degree n. Let $T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0$ be the characteristic polynomial of $\alpha \in F$. For $k \geq 0$ let p_k denotes the *power sum* $\phi_1(\alpha)^k + \ldots + \phi_n(\alpha)^k$. Here The ϕ_i denote the embeddings $F \hookrightarrow \mathbf{C}$.

(a) Show that $p_{m+n} + a_{m+n-1}p_{n-1} + \ldots + a_1 p_{m+1} + p_m = 0$ for every $m \geq 0$

(b) Show

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

2.14 (*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

$$s_1 = p_1, \quad -2s_2 = p_2 - p_1 s_1, \quad 3s_3 = p_3 - p_2 s_1 + p_1 s_2, \quad -4s_4 = p_4 - p_3 s_1 + p_2 s_2 - p_1 s_3, \ldots$$

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

2.15 Let $f(T) = T^4 + T + 1 \in \mathbf{Q}[T]$.
- (a) Show that f is irreducible.
- (b) Show that the power sums $p_0, p_1, p_2, p_3, p_4, p_5, p_6$ are equal to $4, 0, 0, -3, -4, 0, 3$ respectively.
- (c) Compute the discriminant of $f(T)$.

2.16 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.

2.17 (Vandermonde) Let A be a commutative ring and let $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$. Prove the equality

$$\det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{pmatrix} = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i).$$

2.18 Let K be a field and let $f \in K[T]$ be a polynomial of degree n. Suppose that we have $f(T) = \prod_{i=1}^{n}(T - \alpha_i) \in K[T]$ for certain elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ in some splitting field of f Then the *discriminant* $\mathrm{Disc}(f)$ of f is defined by

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

Suppose $F = \mathbf{Q}(\alpha)$ is a number field. Let f denote the minimum polynomial of α. Show

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

(Hint: Differentiate the relation $f(T) = \prod_{i=1}^{n}(T - \alpha_i)$ and substitute $T = \alpha_j$.)

2.19 Let K be a field and let $a, b, c \in K$.
- (a) Prove that $\mathrm{Disc}(T^n - a) = n^n a^{n-1}$.
- (b) Compute $\mathrm{Disc}(T^2 + bT + c)$ and $\mathrm{Disc}(T^3 + bT + c)$.

2.20 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

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

Show that for any $f \in K[X]$ we have

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

2.21 (*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 $h \equiv h' \pmod{g}$.
(a) Show that $\mathrm{Res}(g,h) = (-1)^{rs}\mathrm{Res}(h,g)$.
b) Show that $\mathrm{Res}(g,h) = b^s \prod_{\alpha:g(\alpha)=0} h(\alpha)$.
(c) Show that $b^{s'}\mathrm{Res}(g,h) = b^s\mathrm{Res}(g,h')$
(d) Using parts (i) and (ii), describe an efficient algorithm, similar to the Euclidean algorithm in the ring $K[T]$ to calculate resultants of polynomials.

2.22 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 in $\overline{\mathbf{F}}_p$ if and only if the prime p divides $\mathrm{Disc}(f)$.

2.23 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 $K \subset F \subset L$.

2.24 Let $\mathbf{F}_q$ be a finite field of q elements. Let K be a finite extension of degree n of $\mathbf{F}_q$. Show
(a) there exists $\alpha \in K$ such that $K = \mathbf{F}_q(\alpha)$.
(b) there are precisely n distinct embeddings $\phi_i : K \longrightarrow \overline{\mathbf{F}}_q$.
(c) the discriminant $\Delta(\omega_1, \ldots, \omega_n) = \det(Tr(\omega_i\omega_j))$ is not zero if and only if the elements $\omega_1, \ldots, \omega_n$ form an $\mathbf{F}_q$-basis for K. Here the trace $Tr(\alpha)$ of an element $\alpha \in K$ is $\sum_{i=1}^{n}\phi_i(\alpha)$. (Hint: copy the proof of Prop.2.9)