Number Fields

Prerequisites: • Some knowledge of rings, fields, vector spaces and rudiments of Galois Theory.
• Also, shall assume basic topics in Discrete Maths.
• Shall appeal at the beginning to:

Symmetric Function Theorem: Let R be any ring. Every symmetric polynomial in $R[x_1,..,x_n]$ is expressible as a polynomial over R in the elementary symmetric functions $s_1,..,s_n$, where $(t+x_1)\cdot\cdot(t+x_n) = t^n + s_1t^{n-1} + \cdots + s_n$. ie, $s_1 = x_1+\cdots+x_n$, $s_2 = x_1x_2+\cdots+x_{n-1}x_n$, .., $s_n = x_1\cdots x_n$.
Thus the symmetric polynomials form a ~~ring in~~ polynomial ring in $R[s_1,..,s_n]$.
Proof: See, for example, P.M. Cohn, "Algebra, vol I" (Wiley 1982), P.178

Frequently, one refers to the division algorithm. For integers, this states that if a,b are positive integers, then $\exists$ integers q,r ~~st~~ such that $a = bq+r$ with $0 \le r < b$.
For polynomials it states that if $a(x), b(x)$ are polynomials over a field k, then $\exists$ polynomials $q(x), r(x)$ over k such that $a(x) = b(x)q(x)+r(x)$, with $\deg r(x) < \deg b(x)$.

1. Foundations

1.1. Algebraic Number.

An algebraic number α is a zero of a polynomial $p(x)$ with rational coefficients. The minimal polynomial for α is the polynomial p as above of least degree and with leading coefficient of 1, ie, the polynomial is monic.
The conjugates of α are the zeroes $\alpha_1,..,\alpha_n$ of p, the minimal polynomial for α. Here the polynomial is considered to be defined over $\mathbb{C}$, the complex numbers, so the degree of p is n.
We call n the degree of α.

Notes: (i) The minimal polynomial p for α is also the minimal polynomial for α_j $(j=1,..,n)$.
Proof: Let p_j be the minimal polynomial for α_j. Then by the division algorithm, p_j divides p. Hence α is a zero of either p_j or p/p_j, so that $p = p_j$ by the minimal property of p.
(ii) All the α_j $(j=1,..,n)$ are distinct.
Proof: by (i) we have $(p,p')=1$, where p' is the derivative of p. Hence p cannot have a squared linear factor, ie the α_j are distinct.
(iii) If $R(x)$ is a polynomial such that $R(\alpha_j)=0$ for some j, then $R(\alpha_j)=0$ $\forall j$.
[Here, R has rational coefficients, thus the minimal polynomial for α divides R].

The totality of all algebraic numbers forms a field. Clear, since eg $\alpha+\beta$ is a zero of $\prod_{i=1}^{m}\prod_{j=1}^{n}(x-(\alpha_i+\beta_j))$, where $\alpha_1,..,\alpha_m$ and $\beta_1,..,\beta_n$ are the conjugates of α and β respectively.
Here the polynomial has rational coefficients in view of the symmetric function theorem.
Also, $\frac{1}{\beta}$, for $\beta \ne 0$, is a zero of $x^n p(\frac{1}{x})$, a polynomial with rational coefficients, where p is the minimal polynomial for β.

We shall denote the field of all algebraic numbers by Ω. Note that a zero of a polynomial P with algebraic coefficients is itself algebraic; for if $P(x) = \alpha_n x^n + \dots + \alpha_1 x + \alpha_0$ and $P(\alpha) = 0$, then $Q(\alpha) = 0$, with $Q(x) = \prod_{i_0,\dots,i_n} (\alpha_n^{(i_n)} x^n + \dots + \alpha_0^{(i_0)})$, where $\alpha_j^{(i_j)}$ runs through all the conjugates of α_j $(j = 1, \dots, n)$ and here $Q(x)$ has rational coefficients by the symmetric function theorem.

1.2. Algebraic Number Field.

Let α be an algebraic number, and let $\mathbb{Q}$ denote the rational number field. We define the field $K = \mathbb{Q}(\alpha)$, the algebraic number field generated by α over $\mathbb{Q}$, as the set of elements $P(\alpha)$, where P is any polynomial with coefficients in $\mathbb{Q}$. The set can be regarded as embedded in $\mathbb{C}$, whence we have the usual operations of addition and multiplication. With these, the set forms a field (a subfield of Ω). This is clear, eg, $P(\alpha) + Q(\alpha) = (P+Q)(\alpha)$, $P(\alpha)Q(\alpha) = (PQ)(\alpha)$. The only axiom that needs an element of proof is the division axiom. Accordingly, suppose that $P(\alpha) \neq 0$. Then, from the division algorithm, we have $P(x)R(x) + Q(x)S(x) = 1$, where $Q(x)$ is the minimal polynomial for α, and $R(x), S(x)$ have coefficients in $\mathbb{Q}$. Note here that $(P(x), Q(x)) = 1$, since $P(\alpha) \neq 0$. Now, putting $x = \alpha$ in the above equation, we obtain $P(\alpha)R(\alpha) = 1$, and so $\frac{1}{P(\alpha)} = R(\alpha)$ is in K, as required.

The degree of K is defined as the degree of α, say n. Then, by the division algorithm, K consists of all elements $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$, with $a_0, \dots, a_{n-1}$ in $\mathbb{Q}$. Now let $\alpha_1, \dots, \alpha_n$ be the conjugates of α. We define $\sigma_1, \dots, \sigma_n$ as the embeddings of K into $\mathbb{C}$ (monomorphisms) given by $\sigma_j(\alpha) = \alpha_j$. This gives conjugate fields $K_1, \dots, K_n$, where $K_j = \mathbb{Q}(\alpha_j)$

If $\theta = p(\alpha)$ is the typical element in K, we define the field conjugates of θ as $\theta_1, \dots, \theta_n$, where $\theta_j = p(\alpha_j) = \sigma_j(\theta)$. Further, we call the polynomial $(x - \theta_1)\dots(x - \theta_n)$ the field polynomial of θ.

The field polynomial is a power of the minimal polynomial.

Proof: Let q be the field polynomial for θ $(\in K)$ and p the minimal polynomial for θ. We write $q = p^m r$ for some polynomial r with $(r, p) = 1$. Now, if $r \neq 1$, then $r(\theta_j) = 0$ for some j. We have $\theta_j = P(\alpha_j)$, (assuming $\theta = p(\alpha)$). Hence, $r(p(\alpha_j)) = 0$. But $rp(x) \in \mathbb{Q}[x]$ and so note (iii) above gives $r(p(\alpha_j)) = 0$ $\forall j$. It follows that p divides r. Contradiction - $(r, p) = 1$. (See also: Stewart & Tall, p. 43).

Note that the degree of K is independent of the choice of generator, for we have K a vector space over $\mathbb{Q}$ with basis $1, \alpha, \dots, \alpha^{n-1}$. Hence the dimension $[K:\mathbb{Q}]$ of the vector space is the degree of K. Hence any other generator β will have the same degree. (Alternatively, observe that the minimal polynomial for β divides the field polynomial, whence degree $\beta \leq$ degree α; similarly, degree $\alpha \leq$ degree β. Hence the result).

Now let $k = \mathbb{Q}(\beta)$ be an algebraic number field. We define $K = k(\alpha)$ for an algebraic number α as the field consisting of all expressions $p(\alpha)$ where p is a polynomial ~~we~~ with coefficients in k.

Proposition: K is also an algebraic number field over $\mathbb{Q}$. Ie, we have $K = k(\alpha) = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(u\alpha+v\beta)$, for some integers u, v.

Proof: Let $\alpha_1,..,\alpha_n$ and $\beta_1,..,\beta_m$ be the conjugates of α, β. We choose u,v such that $u(\alpha_i - \alpha_{i'}) + v(\beta_j - \beta_{j'}) \neq 0$ $\forall$ i, i', j, j' except $i=i'$, $j=j'$. For brevity, let $w_{ij} = u\alpha_i + v\beta_j$, and assume $\alpha = \alpha_1$, $\beta = \beta_1$, so that $w := w_{11} = u\alpha + v\beta$.
We introduce the polynomial $Q(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - w_{ij})$ and put $R(x) = \sum_{i=1}^{n} \sum_{j=1}^{m} \beta_j \, Q(x)/(x - w_{ij})$.
Here, $R(x)$ is a polynomial, and by the symmetric function theorem, it has coefficients in $\mathbb{Q}$. Further, putting $x = w$, we get $\beta = \beta_1 = R(w)/Q'(w)$, where Q' is the derivative of Q. Hence $\beta \in \mathbb{Q}(w)$. Similarly $\alpha \in \mathbb{Q}(w)$, and so $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(u\alpha + v\beta)$, as required.

We define the degree of K over k as $[K : k]$, the degree of α over k (i.e. the degree of the minimal polynomial for α with coefficients in k). Then from the dimension theorem for vector spaces, we get $[K : \mathbb{Q}] = [K : k][k : \mathbb{Q}]$. (The dimension theorem states that if H, K, L are fields and $H \leq K \leq L$, then the dimensions satisfy $[L : H] = [L : K][K : H]$).

1.3. Algebraic Integers.

An algebraic number α is called an algebraic integer if the minimal polynomial for α has integer coefficients (still with a leading 1). [Note that for $\alpha \in \mathbb{Q}$, the minimal polynomial is $x - \alpha$ and so the definition gives the ordinary integers in this case].
The totality of algebraic integers forms a ring $\mathcal{O}$.
Note: conjugates of an algebraic integer are also algebraic integers.

Let $p(x)$ be the minimal polynomial for an algebraic number α. One calls the lowest common multiple of the denominators of the coefficients of $p(x)$ the denominator a of α. Thus, the denominator a is the least positive integer such that $ap(x)$ has relatively prime integer coefficients.

Corollary 1: $a\alpha$ is an algebraic integer.
Proof: We have $a^n p(x) = Q(ax)$ for some monic Q with ordinary integer coefficients. (If $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$, then $Q(x) = x^n + a \cdot a_{n-1} x^{n-1} + \dots + a^n a_0$).

Corollary 2: $a\alpha_1 \dots \alpha_m$ is an algebraic integer for any distinct conjugates $\alpha_1, .., \alpha_m$ of α
Proof: We shall prove that if $f(x) = \beta_k x^k + \dots + \beta_0 \in \mathcal{O}[x]$, and if $f(\gamma) = 0$, then $\frac{f(x)}{x-\gamma} \in \mathcal{O}[x]$. The corollary follows on taking $f(x) = ap(x)$, for then $\frac{f(x)}{\prod(x-\alpha_i)} \in \mathcal{O}[x]$, where α_i runs through all the conjugates of α other than $\alpha_1,..,\alpha_m$, whence $a(x-\alpha_1) \cdots (x-\alpha_m) \in \mathcal{O}[x]$, and so the constant coefficient $a\alpha_1 \dots \alpha_m$ (ignoring sign) is in $\mathcal{O}$ as required.
The assertion is proved by induction on k (assuming $\beta_k \neq 0$). It holds trivially for $k=1$.

Now consider $\varphi(x) = f(x) - \beta_k x^{k-1}(x-\gamma)$. This is a polynomial of degree $\leq k-1$, and we have $\varphi(\gamma)=0$. Further, we have $\varphi(x) \in \mathcal{O}[x]$, since $\beta_k \gamma \in \mathcal{O}$ as in corollary 1, ie, $\beta_k^{k-1} f(x) = g(\beta_k x)$ for some monic $g(x) \in \mathcal{O}[x]$. The required assertion follows by induction.

1.4. Units.

An algebraic integer ε is called a unit if $\frac{1}{\varepsilon}$ is an algebraic integer.
[Note: in $\mathbb{Q}$, the algebraic integers are called rational integers. Then, ε is a unit iff $\varepsilon = \pm 1$]
Alternatively, ε is a unit iff $\varepsilon_1 \cdots \varepsilon_n = \pm 1$, where $\varepsilon_1 \cdots \varepsilon_n$ are the conjugates of ε.
Proof: If $\varepsilon_1 \cdots \varepsilon_n = \pm 1$, then $\frac{1}{\varepsilon_1} = \pm \varepsilon_2 \cdots \varepsilon_n$, and so if $\varepsilon = \varepsilon_1 \in \mathcal{O}$, then $\varepsilon_2, \ldots, \varepsilon_n \in \mathcal{O}$ (by note at start of §1.3) and so, since $\mathcal{O}$ is a ring, we have $\frac{1}{\varepsilon_1} \in \mathcal{O}$.
Conversely, if $\frac{1}{\varepsilon} \in \mathcal{O}$, then $\frac{1}{\varepsilon_1}, \ldots, \frac{1}{\varepsilon_n}$, ie the conjugates of $\frac{1}{\varepsilon_1}$, must belong to $\mathcal{O}$, whence, by the ring property of $\mathcal{O}$, $\varepsilon_1, \ldots, \varepsilon_n$ are units. But then $\varepsilon_1 \cdots \varepsilon_n$ is a rational integer and a unit, so $\varepsilon_1 \cdots \varepsilon_n = \pm 1$.

Note: the product of units in $\mathcal{O}$ is again a unit, and the units form a multiplicative group, which we denote by $\mathcal{U}$.

Remark: if k is an algebraic number field then again the algebraic integers in k form a ring $\mathcal{O}_k$, and the units in k form a multiplicative group $\mathcal{U}_k$.

1.5. Norm and Trace.

Let α be any algebraic number, with conjugates $\alpha_1, \ldots, \alpha_n$. We define the (absolute) norm and trace of α as $N\alpha = \alpha_1 \cdots \alpha_n$ and $T_\alpha = \alpha_1 + \cdots + \alpha_n$. Thus, ε is a unit iff $N_\varepsilon = \pm 1$.
Now let k be an algebraic number field and let $\sigma_1, \ldots, \sigma_n$ be the monomorphisms from k to $\mathbb{C}$. If θ is any element of k, we define the relative norm and trace on k by $N_{k/\mathbb{Q}}(\theta) = \sigma_1(\theta) \cdots \sigma_n(\theta)$, $T_{k/\mathbb{Q}}(\theta) = \sigma_1(\theta) + \cdots + \sigma_n(\theta)$.

Then clearly, $N_{k/\mathbb{Q}}(\theta\varphi) = N_{k/\mathbb{Q}}(\theta)\, N_{k/\mathbb{Q}}(\varphi)$, $T_{k/\mathbb{Q}}(\theta + \varphi) = T_{k/\mathbb{Q}}(\theta) + T_{k/\mathbb{Q}}(\varphi)$.
Also, by the property of the field polynomial, we have $N_{k/\mathbb{Q}}\theta = (N\theta)^m$, $T_{k/\mathbb{Q}}\theta = m T\theta$, for some integer m. Note that when θ is an algebraic integer, $N\theta$, $T\theta$ are rational integers.

1.6 Basis and Determinant.

Let k be an algebraic number field. Then there is a basis $\psi_1, \ldots, \psi_n$ of k as a vector space over $\mathbb{Q}$. We define the discriminant of the basis as $\Delta(\psi_1, \ldots, \psi_n) = [\det(\sigma_i(\psi_j))]^2$
Then we have $\Delta(\psi_1, \ldots, \psi_n) = \det\begin{pmatrix} \sigma_1(\psi_1) & \cdots & \sigma_1(\psi_n) \\ \vdots & & \vdots \\ \sigma_n(\psi_1) & \cdots & \sigma_n(\psi_n) \end{pmatrix} \det\begin{pmatrix} \sigma_1(\psi_1) & \cdots & \sigma_n(\psi_1) \\ \vdots & & \vdots \\ \sigma_1(\psi_n) & \cdots & \sigma_n(\psi_n) \end{pmatrix} = \det\left(T_{k/\mathbb{Q}}(\psi_i \psi_j)\right)$.

Now suppose we have another basis for k over $\mathbb{Q}$, say $\psi_1', \ldots, \psi_n'$. Then $\psi_i' = \sum_{j=1}^{n} a_{ij} \psi_j$, rational a_{ij}. Let $A = \det(a_{ij}) \neq 0$ as change-of-basis matrix.
Clearly we have, $\Delta(\psi_1', \ldots, \psi_n') = A^2 \Delta(\psi_1, \ldots, \psi_n)$ ⊛

If $k = \mathbb{Q}(\alpha)$, then we can take $\psi_j = \alpha^{j-1}$, and $\Delta(1, \alpha, .., \alpha^{n-1})$ is the square of a Vandermonde determinant, whence $\Delta(1, \alpha, .., \alpha^{n-1}) = \prod_{1 \le i \le j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$.
Since α is a generator for k over $\mathbb{Q}$ we have $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ $(i \neq j)$, whence $\Delta(1, \alpha, .., \alpha^{n-1}) \neq 0$. It follows from ⊛ that $\Delta(\psi_1', .., \psi_n') \neq 0$ for all bases $\psi_1', .., \psi_n'$ of k over $\mathbb{Q}$.

Now consider the ring $\mathcal{O}_k$ of algebraic integers in k. A basis for $\mathcal{O}_k$ over $\mathbb{Z}$ is called an integral basis for k. Thus $\omega_1, .., \omega_n$ is an integral basis for k iff every element θ of $\mathcal{O}_k$ can be expressed in the form $\theta = u_1\omega_1 + \cdots + u_n\omega_n$ for some rational integers $u_1, .., u_n$.

Theorem: An integral basis always exists for k.
Proof: Note first that there certainly exists an $\mathcal{O}_k$-basis for k over $\mathbb{Q}$ with elements in $\mathcal{O}_k$; for instance, we could take $1, a\alpha, .., (a\alpha)^{n-1}$ where a is the denominator for α. Now, any $\mathcal{O}_k$-basis for k over $\mathbb{Q}$, say $\omega_1, .., \omega_n$, the discriminant $\Delta(\omega_1, .., \omega_n)$ is a rational integer by symmetry (since $\omega_j \in \mathcal{O}_k$, where $\Delta \in \mathcal{O}_k$). Thus there exist elements $\omega_1, .., \omega_n$ in $\mathcal{O}_k$ such that $|\Delta(\omega_1, .., \omega_n)|$ takes its smallest value. We proceed to prove that $\omega_1, .., \omega_n$ is an integral basis for k.
Accordingly, let θ ~~by~~ be any element of $\mathcal{O}_k$. Then certainly there exist rationals $u_1, .., u_n$ such that $\theta = u_1\omega_1 + \cdots + u_n\omega_n$. We have to show that, since $\theta \in \mathcal{O}_k$, these u's are in fact integers. But if, say, $u_1 = u + v$, with u an integer and $0 < v < 1$, then, on writing $\omega_1' = \theta - u\omega_1 = v\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n$, we would have an $\mathcal{O}_k$-basis for k over $\mathbb{Q}$, namely $\omega_1', \omega_2, .., \omega_n$, and from ⊛, we would have $\Delta(\omega_1', \omega_2, .., \omega_n) = V^2 \Delta(\omega_1, .., \omega_n)$, where $V = \det\begin{pmatrix} v & u_2 \cdots u_n \\ 0 & \ddots \\ & & 1\end{pmatrix} = v$. Since $0 < v < 1$, this contradicts the minimal property of $|\Delta(\omega_1, .., \omega_n)|$. The theorem follows.

It is clear from the proof above that $\Delta(\omega_1, .., \omega_n)$ takes the same value for any integral basis for k, for the determinant of the transformation from one integral basis to another is an integer and so ± 1. Now, by ⊛, the determinant is squared and so the value of $\Delta(\omega_1, .., \omega_n)$ is unchanged.
We define $\Delta(\omega_1, .., \omega_n)$ for an integral basis as the discriminant of k.

Exercise: prove that if $\theta_1, .., \theta_n$ are elements of $\mathcal{O}_k$ such that $\Delta(\theta_1, .., \theta_n)$ is square-free then $\theta_1, .., \theta_n$ is an integral basis for k.

1.7. The Quadratic Field.

Consider $k = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer (positive or negative). Then the elements of k have the form $x + y\sqrt{d}$, with $x, y \in \mathbb{Q}$. We determine an integral basis for k.
Accordingly, suppose $x + y\sqrt{d} \in \mathcal{O}_k$. Then $N_{k/\mathbb{Q}}(x + y\sqrt{d})$ and $T_{k/\mathbb{Q}}(x + y\sqrt{d}) \in \mathbb{Z}$. (Also clear from minimal polynomial). Hence, $x^2 - dy^2$ and $2x \in \mathbb{Z}$. Since d is square-free, it follows that $x = \frac{1}{2}u$, $y = \frac{1}{2}v$, where u, v are integers. Further, 4 divides $u^2 - dv^2$.

Now, if $d \equiv 2$ or $3 \pmod 4$, then since a square $\equiv 0$ or $1 \pmod 4$, it follows that $u^2 = v^2 = 0 \pmod 4$, ie. u, v are even, whence x and y are integers, and $1, \sqrt{d}$ is an integral basis for k.
If $d \equiv 1 \pmod 4$, the only other possibility, then u, v have the same parity (ie, $u \equiv v \bmod 2$), and so, on writing $x + y\sqrt{d} = \frac{1}{2}(u-v) + \frac{1}{2}v(1+\sqrt{d})$, and noting that $\frac{1}{2}(u-v)$ and v are integers, we see that $1, \frac{1}{2}(1+\sqrt{d})$ is an integral basis for k.

The discriminant of k is thus $4d$ when $d \equiv 2$ or $3 \pmod 4$, and d when $d \equiv 1 \pmod 4$, since $\begin{vmatrix} 1 & \frac{1}{2}(1+\sqrt{d}) \\ 1 & \frac{1}{2}(1-\sqrt{d}) \end{vmatrix} = \sqrt{d}$.

2. Ideals.

2.1. Origins.

Not every algebraic number field has a unique factorisation. Consider, for example, $k = \mathbb{Q}(\sqrt{-5})$. An integral basis is $1, \sqrt{-5}$. Then, $21 = 3.7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$.
Now, disregarding units, $3, 7, 1 \pm 2\sqrt{-5}$ cannot be further factorised in $\mathcal{O}_k$.
Suppose, for instance, $3 = \alpha\beta$, where $\alpha, \beta \in \mathcal{O}_k$. Then $N\alpha N\beta = 9$, so if neither α nor β were a unit we would have $N\alpha = 3$. But this is impossible since it implies $x^2 + 5y^2 = 3$ for integers x, y, and there is no such solution.
Note that the units in $\mathbb{Q}(\sqrt{-5})$ are given by $x^2 + 5y^2 = \pm 1$ (since $N(x+y\sqrt{-5}) = x^2+5y^2$), where $x = \pm 1$, $y = 0$. So, the only units in k are ± 1.
Similarly, $7, 1 \pm 2\sqrt{-5}$ cannot factorise further. Hence $\mathbb{Q}(\sqrt{-5})$ does not have a unique factorisation.

Ideals were introduced by Kummer, Dedekind, etc. to restore the property.

2.2. Definitions.

Let k be an algebraic number field and let $\mathcal{O}_k$ be the ring of integers of k.
An ideal in k is a non-empty subset of $\mathcal{O}_k$, denoted by $\underline{a}$, say, such that
(i) if $\alpha_1, \alpha_2 \in \underline{a}$, then $\alpha_1 - \alpha_2 \in \underline{a}$.
(ii) if $\alpha \in \underline{a}$, $\beta \in \mathcal{O}_k$, then $\alpha\beta \in \underline{a}$.

Theorem: every ideal $\underline{a}$ in k is finitely generated. That is, there exist elements $\alpha_1, \ldots, \alpha_m$ in $\underline{a}$ such that $\underline{a}$ is the set of all elements $\alpha_1\beta_1 + \cdots + \alpha_m\beta_m$ with $\beta_1, \ldots, \beta_m$ in $\mathcal{O}_k$. We write $\underline{a} = [\alpha_1, \ldots, \alpha_m]$

Proof: Clearly given $\alpha_1, \ldots, \alpha_m$ as above, the set of all $\alpha_1\beta_1 + \cdots + \alpha_m\beta_m$ with $\beta_1, \ldots, \beta_m$ in $\mathcal{O}_k$ satisfies (i) and (ii), whence it is an ideal.
Conversely, if $\underline{a}$ is an ideal, then there is an integral basis for $\underline{a}$, ie a set $\gamma_1, \ldots, \gamma_n$ of elements of $\underline{a}$ such that every element α in $\underline{a}$ can be expressed in the form $u_1\gamma_1 + \cdots + u_n\gamma_n$ with rational integers $u_1, \ldots, u_n$. The

verification follows as in section 1.6, for if $\omega_1, \dots, \omega_n$ is an integral basis for $\mathcal{O}_k$ and α is any element of $\underline{\underline{a}}$, then $\alpha\omega_1, \dots, \alpha\omega_n$ are in $\underline{\underline{a}}$ (and play the same rôle as $1, a\theta, \dots, (a\theta)^{n-1}$ in 1.6), and then we deduce that we can take for $\gamma_1, \dots, \gamma_n$ any set of elements of $\underline{\underline{a}}$ such that $|\Delta(\gamma_1, \dots, \gamma_n)|$ takes its smallest value. Now, if $\gamma_1, \dots, \gamma_n$ is an integral basis for $\underline{\underline{a}}$ then we have $\underline{\underline{a}} = [\gamma_1, \dots, \gamma_n]$.

We define the product $\underline{\underline{a}}\,\underline{\underline{b}}$ of ideals $\underline{\underline{a}}, \underline{\underline{b}}$ in k as the set of all elements $a_1b_1 + \dots + a_tb_t$ with $a_1, \dots, a_t$ in $\underline{\underline{a}}$ and $b_1, \dots, b_t$ in $\underline{\underline{b}}$. Plainly, if $\underline{\underline{a}} = [\alpha_1, \dots, \alpha_n]$, $\underline{\underline{b}} = [\beta_1, \dots, \beta_l]$, then $\underline{\underline{a}}\,\underline{\underline{b}} = [\alpha_1\beta_1, \dots, \alpha_1\beta_l, \dots, \alpha_n\beta_l]$. Further, we have $\underline{\underline{a}}\,\underline{\underline{b}} = \underline{\underline{b}}\,\underline{\underline{a}}$ (commutativity) and $(\underline{\underline{a}}\,\underline{\underline{b}})\underline{\underline{c}} = \underline{\underline{a}}(\underline{\underline{b}}\,\underline{\underline{c}})$ (associativity).
We say that $\underline{\underline{a}}$ divides $\underline{\underline{b}}$ if there is an ideal $\underline{\underline{c}}$ such that $\underline{\underline{b}} = \underline{\underline{a}}\,\underline{\underline{c}}$.
We define $\underline{\underline{a}}^k$ as $\underline{\underline{a}} \dots \underline{\underline{a}}$ (k times) and $\underline{\underline{a}}^0 = \underline{\underline{e}} = [1] = \mathcal{O}_k$.

2.3. Principal Ideals.

An ideal $\underline{\underline{a}}$ is said to be principal if $\underline{\underline{a}} = [\alpha]$ for some $\alpha \in \mathcal{O}_k$. If $[\alpha] = [\beta]$, then α/β and $\beta/\alpha \in \mathcal{O}_k$, ie α/β is a unit in $\mathcal{O}_k$, and we say that α and β are associated in k.

Theorem: For any ideal $\underline{\underline{a}}$ in k there is $\underline{\underline{b}}$ in k such that $\underline{\underline{a}}\,\underline{\underline{b}}$ is principal. In fact, there is an ideal $\underline{\underline{b}}$ such that $\underline{\underline{a}}\,\underline{\underline{b}} = [c]$ with $c \in \mathbb{Z}$.

[We can define $\underline{\underline{a}}^{-1}$ as $\underline{\underline{b}}/[c]$, ie if $\underline{\underline{b}} = [\beta_1, \dots, \beta_l]$, then $\underline{\underline{a}}$ can be defined as $[\frac{\beta_1}{c}, \dots, \frac{\beta_l}{c}]$, termed a fractional ~~i~~ ideal, by extending the original definition to allow generators in k of the form β/c with $\beta \in \mathcal{O}_k$, $c \in \mathbb{Z}$. The original ideals are then called integral ideals. Then obviously $\underline{\underline{a}}\,\underline{\underline{a}}^{-1} = \underline{\underline{e}}$]

Proof (constructive): Let $\underline{\underline{a}} = [\alpha_0, \dots, \alpha_m]$ with $\alpha_0, \dots, \alpha_m \in \mathcal{O}_k$. Put $f(x) = a_m x^m + \dots + \alpha_0$. Consider the polynomial $F(x) = N_{k/\mathbb{Q}}(f(x))$, that is, $F(x) = \prod_{j=1}^{n} \{\alpha_m^{(j)} x^m + \dots + \alpha_0^{(j)}\}$, where $\alpha_0^{(j)}, \dots, \alpha_m^{(j)}$ are $\sigma_j(\alpha_0), \dots, \sigma_j(\alpha_m)$ respectively, the field conjugates. Then $F(x) = f(x)g(x)$, and $g(x) \in \mathcal{O}_k[x]$, since $F(x) \in \mathbb{Z}[x]$. (Note that certainly $\alpha_0^{(j)}, \dots, \alpha_m^{(j)} \in \mathcal{O}_k$, whence $g(x) \in \mathcal{O}_k[x]$).
Now let $g(x) = \beta_l x^l + \dots + \beta_0$ and put $\underline{\underline{b}} = [\beta_l, \dots, \beta_0]$.
Further, let c be the highest common factor of the coeffecients of $F(x)$. We have to show that $\underline{\underline{a}}.\underline{\underline{b}} = [c]$. First, we verify that $\underline{\underline{a}}\,\underline{\underline{b}}$ is contained in $[c]$. In fact, it suffices to show that $\alpha_r\beta_s \in [c]$ for all r, s. But α_r/α_m is an elementary symmetric polynomial in the zeroes of f, and similarly for β_s/β_l in terms of $g(x)$.
Hence, $\alpha_r\beta_s = \alpha_m\beta_l\gamma_{rs}$, where γ_{rs} is a product of elementary symmetric functions in the zeroes of f and g and these are precisely the zeroes of F. Since $c^{-1}\alpha_m\beta_l$ is the leading coefficient in $c^{-1}F$ and the latter $\in \mathbb{Z}[x]$, it follows from Corollary 2 in section 1.3 that $c^{-1}\alpha_r\beta_s \in \mathcal{O}$ for all r, s and thus $\underline{\underline{a}}\,\underline{\underline{b}}$ is contained in $[c]$.
Secondly, we show that $[c]$ is contained in $\underline{\underline{a}}\,\underline{\underline{b}}$. Now c is the hcf of the coefficients of $F(x)$, whence it is a linear combination of these coefficients with multipliers in $\mathbb{Z}$, (Note - if $c = hcf(a_0, \dots, a_t)$, then $c = a_0b_0 + \dots + a_tb_t$ with $b_1, \dots, b_t \in \mathbb{Z}$), and the coefficients of F are themselves linear combinations of the $\alpha_r\beta_s$ ($0 \le r \le m$, $0 \le s \le l$), since $F = fg$. Hence c is in $\underline{\underline{a}}\,\underline{\underline{b}}$ and the theorem follows.

Corollary 1: If $\underline{\underline{a}}\,\underline{\underline{c}} = \underline{\underline{b}}\,\underline{\underline{c}}$ then $\underline{\underline{a}} = \underline{\underline{b}}$.

Proof: Obvious on multiplying by $\underline{\underline{c}}^{-1}$ (fractional ideals), or considering ideal $\underline{\underline{d}}$, which exists from the theorem, such that $\underline{\underline{c}}\,\underline{\underline{d}} = [d]$. Then $\underline{\underline{a}}\,\underline{\underline{c}}\,\underline{\underline{d}} = \underline{\underline{b}}\,\underline{\underline{c}}\,\underline{\underline{d}}$, ie. $\underline{\underline{a}}[d] = \underline{\underline{b}}[d]$ and it is now clear that $\underline{\underline{a}} = \underline{\underline{b}}$ (consider generators).

Corollary 2: $\underline{\underline{a}} \mid \underline{\underline{b}} \iff$ every element of $\underline{\underline{b}}$ is in $\underline{\underline{a}}$.

Proof: ($\Rightarrow$) if $\underline{\underline{a}} \mid \underline{\underline{b}}$ then $\underline{\underline{b}} = \underline{\underline{a}}\,\underline{\underline{c}}$ for some ideal $\underline{\underline{c}}$. From the definition of $\underline{\underline{a}}\,\underline{\underline{c}}$ in terms of generators, we get $\underline{\underline{b}} \subset \underline{\underline{a}}$, trivially.

($\Leftarrow$) if every element of $\underline{\underline{b}}$ is in $\underline{\underline{a}}$ then $\underline{\underline{b}}\,\underline{\underline{a}}^{-1}$ is contained in $\mathcal{O}_k$, ie $\underline{\underline{b}} = \underline{\underline{a}}\,\underline{\underline{c}}$ for some $\underline{\underline{c}}$ as required. Alternatively, avoiding fractional ideals, we observe that $\exists\, \underline{\underline{c}}$ such that $\underline{\underline{a}}\,\underline{\underline{c}} = [c]$, whence every element of $\underline{\underline{b}}\,\underline{\underline{c}}$ is in $[c]$. Hence $[c]$ divides $\underline{\underline{b}}\,\underline{\underline{c}}$, ie $\underline{\underline{a}}\,\underline{\underline{c}}$ divides $\underline{\underline{b}}\,\underline{\underline{c}}$, and the result now follows from corollary 1.

2.4. Prime Ideals

An ideal $\underline{\underline{p}}$ in k is said to be prime if it is divisible only by itself and $\underline{\underline{e}}$. Our object is to establish the analogue of the fundamental theorem of arithmetic, ie, every ideal $\underline{\underline{a}}$ in k can be expressed essentially uniquely as $\underline{\underline{p}}_1^{j_1} \cdots \underline{\underline{p}}_k^{j_k}$ for some prime ideals $\underline{\underline{p}}_1, \ldots, \underline{\underline{p}}_k$ and some nonnegative integers $j_1, \ldots, j_k$.

Proof: (i) To get $\underline{\underline{a}} = \underline{\underline{p}}_1^{j_1} \cdots \underline{\underline{p}}_k^{j_k}$, it suffices to show that every ideal has only finitely many divisors.

(ii) To get uniqueness, it suffices to show that if $\underline{\underline{p}} \mid \underline{\underline{a}}\,\underline{\underline{b}}$ then $\underline{\underline{p}} \mid \underline{\underline{a}}$ or $\underline{\underline{p}} \mid \underline{\underline{b}}$.

Verification: (i) By the theorem above, $\exists\, \underline{\underline{b}}$ such that $\underline{\underline{a}}\,\underline{\underline{b}} = [c]$, $c \in \mathbb{Z}$, whence every divisor $\underline{\underline{d}}$ of $\underline{\underline{a}}$ must divide $[c]$. Now, by corollary 2, c is in $\underline{\underline{d}}$. Further, every element $\alpha \in \mathcal{O}_k$ can be written as $c\beta + \gamma$, where $\gamma, \beta \in \mathcal{O}_k$ and γ can take at most c^n values, for we have $\alpha = u_1 w_1 + \cdots + u_n w_n$ in terms of a basis for k, and the observation follows on writing $u_j = c q_j + r_j$ with $0 \le r_j < c$ so that $\beta = q_1 w_1 + \cdots + q_n w_n$, $\gamma = r_1 w_1 + \cdots + r_n w_n$.
Applying this to each of the generators $\alpha_1, \ldots, \alpha_m$, say, of $\underline{\underline{d}}$, so that $\alpha_j = c\beta_j + \gamma_j$, we obtain $\underline{\underline{d}} = [\gamma_1, \ldots, \gamma_m, c]$, whence there are only finitely many possibilities for $\underline{\underline{d}}$.

(ii) For this we need the definition of $\underline{\underline{a}} + \underline{\underline{b}}$. Namely, if $\underline{\underline{a}} = [\alpha_1, \ldots, \alpha_m]$ and $\underline{\underline{b}} = [\beta_1, \ldots, \beta_l]$, then $\underline{\underline{a}} + \underline{\underline{b}} = [\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_l]$. Note that it is the same as the set of $a+b$ with a in $\underline{\underline{a}}$ and b in $\underline{\underline{b}}$, and so is independent of choice of generators. Also, $\underline{\underline{d}} = \underline{\underline{a}} + \underline{\underline{b}}$ is the greatest common divisor of $\underline{\underline{a}}, \underline{\underline{b}}$, ie $\underline{\underline{d}} \mid \underline{\underline{a}}$, $\underline{\underline{d}} \mid \underline{\underline{b}}$, and every divisor of $\underline{\underline{a}}$ and $\underline{\underline{b}}$ also divides $\underline{\underline{d}}$. Now if $\underline{\underline{p}} \mid \underline{\underline{a}}\,\underline{\underline{b}}$ and $\underline{\underline{p}} \nmid \underline{\underline{a}}$, then $\underline{\underline{a}} + \underline{\underline{p}} = \underline{\underline{e}}$. This gives $\underline{\underline{a}}\,\underline{\underline{b}} + \underline{\underline{p}}\,\underline{\underline{b}} = \underline{\underline{b}}$ and hence $\underline{\underline{p}} \mid \underline{\underline{b}}$. This establishes unique factorisation for ideals.

2.5. Norms of Ideals.

An element α of $\mathcal{O}_k$ is said to be divisible by an ideal $\underline{\underline{a}}$ in k if $\underline{\underline{a}} \mid [\alpha]$. If now $\alpha, \beta \in \mathcal{O}_k$ and $\underline{\underline{a}}$ divides $\alpha - \beta$, we write $\alpha \equiv \beta \pmod{\underline{\underline{a}}}$. This is an equivalence relation, and the number of equivalence classes is finite, for we have $\underline{\underline{a}}\,\underline{\underline{b}} = [c]$, $c \in \mathbb{Z}$, for some $\underline{\underline{b}}$, and by 2.4., there are only finitely many classes (mod $[c]$). Note that if $\alpha \not\equiv \beta \pmod{\underline{\underline{a}}}$ then $\alpha \not\equiv \beta \pmod{[c]}$. The number of equivalence classes mod $\underline{\underline{a}}$ is defined as the norm, $N\underline{\underline{a}}$, of $\underline{\underline{a}}$.

Main Property: $N\mathfrak{a} N\mathfrak{b} = N(\mathfrak{a}\mathfrak{b})$ for all ideals $\mathfrak{a}, \mathfrak{b}$ in k.

Proof: In view of the fundamental theorem on representation by prime ideals (ie, $\mathfrak{a} = \mathfrak{p}_1^{j_1} \cdots \mathfrak{p}_i^{j_i}$), it suffices to prove the result when $\mathfrak{a}, \mathfrak{b}$ are prime ideals. In fact, we shall assume only that $\mathfrak{b} = \mathfrak{p}$, a prime ideal. Thus we have to show that $N\mathfrak{a} N\mathfrak{p} = N(\mathfrak{a}\mathfrak{p})$.

Now, let α be an element in $\mathfrak{a}$ but not in $\mathfrak{a}\mathfrak{p}$ (such an α exists, else $\mathfrak{a}\mathfrak{p}$ divides $\mathfrak{a}$, whence $\mathfrak{p} | \mathfrak{e}$). We shall show that $\sigma + \alpha\rho$ runs through all representatives in the congruence classes mod $\mathfrak{a}\mathfrak{p}$ as σ, ρ run through the representatives mod $\mathfrak{a}$, mod $\mathfrak{p}$. Then $N(\mathfrak{a}\mathfrak{p}) = N\mathfrak{a} N\mathfrak{p}$.

We need two facts: (i) the $\sigma + \alpha\rho$ are incongruent mod $\mathfrak{a}\mathfrak{p}$,
(ii) if $\beta \in \mathcal{O}_k$ then $\beta \equiv \sigma + \alpha\rho \pmod{\mathfrak{a}\mathfrak{p}}$ for some σ, ρ. The result then follows.

Now, (i) is obvious, for if $\sigma + \alpha\rho \equiv \sigma' + \alpha\rho' \pmod{\mathfrak{a}\mathfrak{p}}$, then $\sigma \equiv \sigma' \pmod{\mathfrak{a}}$, as $\alpha \in \mathfrak{a}$. This gives $\sigma = \sigma'$ and then we obtain $\rho \equiv \rho' \pmod{\mathfrak{p}}$, so that $\rho = \rho'$.

To establish (ii), we note first that $\beta \equiv \sigma \pmod{\mathfrak{a}}$ for some σ. But $\mathfrak{a} = [\alpha] + \mathfrak{a}\mathfrak{p}$, since $\mathfrak{p}$ is a prime ideal. Hence $\beta - \sigma$ is given by $\alpha\beta' + \gamma$, where $\beta' \in \mathcal{O}_k$ and $\gamma \in \mathfrak{a}\mathfrak{p}$. This gives $\beta \equiv \sigma + \alpha\beta' \pmod{\mathfrak{a}\mathfrak{p}}$. Further, $\beta' \equiv \rho \pmod{\mathfrak{p}}$, whence $\alpha\beta' \equiv \alpha\rho \pmod{\mathfrak{a}\mathfrak{p}}$. Thus, $\beta \equiv \sigma + \alpha\rho \pmod{\mathfrak{a}\mathfrak{p}}$, which is (ii).

Formula for $N\mathfrak{a}$: If $\gamma_1, \dots, \gamma_n$ is a basis for $\mathfrak{a}$ (ie. $u_1\gamma_1 + \dots + u_n\gamma_n$ gives all elements of $\mathfrak{a}$ for integers $u_1, \dots, u_n$) and $\omega_1, \dots, \omega_n$ is an integral basis for k, then $N\mathfrak{a} = \left[\frac{\Delta(\gamma_1 \dots \gamma_n)}{\Delta(\omega_1, \dots, \omega_n)}\right]^{1/2}$. (Note: $\Delta(\omega_1, \dots, \omega_n)$ is the discriminant of k).

Proof: We shall show that $\exists$ a basis $\gamma_1', \dots, \gamma_n'$ for $\mathfrak{a}$ of the form: $\gamma_1' = a_{11}\omega_1$, $\gamma_2' = a_{21}\omega_1 + a_{22}\omega_2, \dots, \gamma_n' = a_{n1}\omega_1 + \dots + a_{nn}\omega_n$, where a_{ij} are integers, $a_{jj} > 0$. Since $\Delta(\gamma_1', \dots, \gamma_n') = \Delta(\gamma_1, \dots, \gamma_n)$, we have to verify $N\mathfrak{a} = \left(\frac{\Delta(\gamma_1', \dots, \gamma_n')}{\Delta(\omega_1, \dots, \omega_n)}\right)^{1/2}$. But, $\Delta(\gamma_1', \dots, \gamma_n') = (a_{11} \cdots a_{nn})^2 \Delta(\omega_1, \dots, \omega_n)$, thus we have to verify that $N\mathfrak{a} = a_{11} \cdots a_{nn}$. But it will be clear from the construction of $\gamma_1', \dots, \gamma_n'$ that the numbers $u_1\omega_1 + \dots + u_n\omega_n$ with $0 \le u_i < a_{ii}$ $(1 \le i \le n)$ are incongruent mod $\mathfrak{a}$, and they represent all congruence classes mod $\mathfrak{a}$. Hence $N\mathfrak{a} = a_{11} \cdots a_{nn}$ as required.

To construct $\gamma_1', \dots, \gamma_n'$, consider the element $a_{n1}\omega_1 + \dots + a_{nn}\omega_n$ in $\mathfrak{a}$, and choose it so that $a_{nn} > 0$ and minimal. (We cannot have $a_{nn} = 0$ for all elements in $\mathfrak{a}$, since there is a basis $\gamma_1, \dots, \gamma_n$). Call this γ_n'. Now if $\alpha = u_1\omega_1 + \dots + u_n\omega_n$ is any element in $\mathfrak{a}$, then $u_n = r a_{nn} + s$ with $0 \le s < a_{nn}$, and then $\alpha - r\gamma_n' = a_{n-1,1}\omega_1 + \dots + a_{n-1,n-1}\omega_{n-1} + s\omega_n$, and here $s = 0$ by the minimal choice of a_{nn}. Now, proceeding similarly with $a_{n-1,1}\omega_1 + \dots + a_{n-1,n-1}\omega_{n-1}$, taking $a_{n-1,n-1}$ positive and minimal and defining this as γ_{n-1}' we get the required basis.

Corollary 1: $N[\alpha] = |N_{k/\mathbb{Q}}(\alpha)|$

Proof: Apply the formula with $\gamma_j = \alpha\omega_j$ $(1 \le j \le n)$. Clearly $\gamma_1, \dots, \gamma_n$ is a basis for $[\alpha]$ and $\Delta(\gamma_1, \dots, \gamma_n) = (\sigma_1(\alpha) \cdots \sigma_n(\alpha))^2 \Delta(\omega_1, \dots, \omega_n)$. Further, by definition, $N_{k/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha)$.

Corollary 2: There is a unique prime p such that if $\mathfrak{p}$ is a prime ideal in k, then $\mathfrak{p} | p$.

Proof: First we observe that $\mathfrak{a} | N\mathfrak{a}$ for any ideal $\mathfrak{a}$ in k, for if $\vartheta_1, \dots, \vartheta_N$ represent all the congruence classes mod $\mathfrak{a}$ so that $N = N\mathfrak{a}$, then also $\vartheta_1 + 1, \dots, \vartheta_N + 1$ represent all the congruence classes.

Hence, $\vartheta_1 + \cdots + \vartheta_N \equiv (\vartheta_1+1) + \cdots + (\vartheta_N+1) \pmod{\underline{a}}$, so $N \equiv 0 \pmod{\underline{a}}$, so $\underline{a} \mid N\underline{a}$.
Now let $\mathfrak{p}$ be a prime ideal. Then $\mathfrak{p} \mid N\mathfrak{p}$. Plainly, the least integer p such that $\mathfrak{p} \mid p$ is a prime, since $\mathfrak{p} \mid nm \Rightarrow \mathfrak{p} \mid n$ or $\mathfrak{p} \mid m$. Further, p is unique, for if $\mathfrak{p} \mid p'$ for some $p' \neq p$, then $\exists\, a, a'$ such that $ap + a'p' = 1$, whence $\mathfrak{p} \mid [e]$, which is impossible.

<u>Corollary 3</u>: We have $N\mathfrak{p} = p^f$ for some rational integer f, which is called the <u>degree</u> of $\mathfrak{p}$.
<u>Proof</u>: we have $[p] = \mathfrak{p}\underline{a}$ for some ideal $\underline{a}$. By the main property for norms, this gives $p^n = N\mathfrak{p}\, N\underline{a}$, since by Corollary 1, $N[p] = |N_{K/\mathbb{Q}}\, p| = p^n$. Hence $N\mathfrak{p} = p^f$.

<u>Definition</u>: If $p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_l^{e_l}$ (we omit the square brackets around p) as a canonical product of prime ideals, then we call $e_1, \ldots, e_l$ the <u>ramification indices</u> of $\mathfrak{p}_1, \ldots \mathfrak{p}_l$.

<u>Corollary 4</u>: The degrees and ramification indices f_j and e_j of $\mathfrak{p}_j$, $(1 \le j \le l)$ satisfy $e_1 f_1 + \cdots + e_l f_l = n$, where $n = [K : \mathbb{Q}]$.
<u>Proof</u>: We have $N[p] = (N\mathfrak{p}_1)^{e_1} \cdots (N\mathfrak{p}_l)^{e_l}$, whence $p^n = p^{e_1 f_1} \cdots p^{e_l f_l}$, and the assertion follows.

3. Units.

3.1. Minkowski's Theorem.

By a <u>convex body</u> we mean a bounded open set of points in Euclidean n-space, ie, set contains $\lambda \underline{x} + (1-\lambda)\underline{y}$ $(0<\lambda<1)$ whenever it contains $\underline{x}$ and $\underline{y}$. A set of points is said to be <u>symmetrical about the origin</u> if it contains $-\underline{x}$ whenever it contains $\underline{x}$. By a <u>lattice</u> Λ, we mean a set of points $\underline{x} = (x_1, \ldots, x_n)$, ~~and~~ with $x_i = \sum_{j=1}^{n} a_{ij} u_j$ where the matrix (a_{ij}) has real entries and $u_1, \ldots, u_n$ run through all the integers. The <u>determinant</u> $d(\Lambda)$ of Λ is defined as $|\det(a_{ij})|$.

<u>Minkowski's Theorem</u>: If S is a convex body symmetrical about the origin and if the volume V of S satisfies $V > 2^n d(\Lambda)$, then S contains a point of Λ other than the origin.
<u>Proof</u> *: It suffices to establish that if R is a bounded set with volume $V = d(\Lambda)$ then $\exists$ points $\underline{x}, \underline{y}$ in R such that $\underline{x} - \underline{y} \in \Lambda$. (This is Blichfeldt's Theorem). To get Minkowski's Theorem, we apply Blichfeldt with $R = \frac{1}{2}S$, then $\underline{x} - \underline{y} = \frac{1}{2}(2\underline{x} - 2\underline{y})$ and since $2\underline{x}$, $2\underline{y}$ are in S and S is convex and symmetric, we have $\underline{x} - \underline{y} \in S$.
To establish Blichfeldt, we consider the part $R_{\underline{u}}$ of R in the cell of Λ with lower vertex $\underline{u}$. If $R'_{\underline{u}}$ is the translation of $R_{\underline{u}}$ to the unit cell with lower vertex the origin and if V_u is the volume of $R_{\underline{u}}$, then since $V = \sum_u V_u = \sum_u V'_u$ and $V > d(\Lambda)$ by hypothesis, we have $\underline{v}, \underline{w}$ in Λ $(\underline{v} \neq \underline{w})$, such that $R'_{\underline{v}}, R'_{\underline{w}}$ overlap. Hence $\exists\, \underline{x}, \underline{y}$ in R such that $\underline{v} - \underline{x} = \underline{w} - \underline{y}$. Then $\underline{x} - \underline{y} = \underline{v} - \underline{w}$, $\in \Lambda$, as required.
The main application of Minkowski's Theorem is <u>Minkowski's Linear Forms Theorem</u>. This states that if $L_i = \sum_{j=1}^{n} c_{ij} x_j$ $(1 \le i \le n)$ are real linear forms with $\Delta = \det(c_{ij}) \neq 0$, and if $\lambda_1 > 0, \ldots, \lambda_n > 0$, $\lambda_1 \cdots \lambda_n > |\Delta|$, then $\exists$ integers $x_1, \ldots, x_n$, not all zero, with $|L_i| < \lambda_i$ $(1 \le i \le n)$
<u>Proof</u>: Apply Minkowski's Theorem with S as the hypercube $|x_i| < \lambda_i$, with volume $V = 2^n \lambda_1 \cdots \lambda_n$. The lattice is defined by the L_i.

There is a refined version of the linear forms theorem to the effect that if $\lambda_1 \ldots \lambda_n = |\Delta|$ then the same assertion holds with $|L_1| < \lambda_1$ replaced by $|L_1| \le \lambda_1$.

Proof: From the crude version we have, for any integer $m > 0$, integers $x_1^{(m)}, \ldots, x_2^{(m)}$ such that $|L_1| < \lambda_1 + \frac{1}{m}$, $|L_i| < \lambda_i$ $(2 \le i \le n)$. Then, by compactness, a subsequence converges to a point $x_1, \ldots, x_n$ as required.

3.2. Dirichlet's Unit Theorem.

This asserts that $\exists\, r = s+t-1$ fundamental units $\varepsilon_1, \ldots, \varepsilon_r$ in $K = \mathbb{Q}(\alpha)$ such that every unit in K can be expressed uniquely in the form $\rho \varepsilon_1^{m_1} \ldots \varepsilon_r^{m_r}$, where $m_1, \ldots, m_r$ are rational integers and ρ is a root of unity. Here, s is the number of real numbers in $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ and t is the number of complex conjugate pairs in this set. Thus $n = s + 2t$. The theorem shows that U_K is a finitely generated multiplicative group. Proof involves an application of the linear forms theorem.

3.3. Quadratic Fields.

Let $K = \mathbb{Q}(\sqrt{d})$, d a square-free integer. If $d < 0$ we say K is an imaginary quadratic field, and we have $s = 0$, $t = 1$, $r = s+t-1$, whence, by Dirichlet, every unit in K is a root of unity.
If $d > 0$, say K is real quadratic, and we have $s = 2$, $t = 0$, $r = s+t-1$, whence, by Dirichlet, every unit in K is given by $\pm\varepsilon^m$ for some ε, where $m = 0, \pm 1, \pm 2, \ldots$
Here we are using the fact that the only real roots of unity are ± 1. (For a direct proof, see, for example, "Concise Introduction to the Theory of Numbers" by Baker).

Determination of units in imaginary quadratic fields is easy. Recall $\mathbb{Q}(\sqrt{d})$ has integral basis $1, \sqrt{d}$ $(d \equiv 2,3 \bmod 4)$ and $1, \frac{1}{2}(1+\sqrt{d})$ $(d \equiv 1 \bmod 4)$, and discriminant D, which is $4d$ $(d \equiv 2,3 \bmod 4)$ or d $(d \equiv 1 \bmod 4)$. Now if $\alpha = x + y\sqrt{d}$, then $N\alpha = x^2 - dy^2$, and if $\alpha = x + \frac{1}{2}y(1+\sqrt{d})$, then $N\alpha = (x + \frac{1}{2}y)^2 - \frac{1}{4}dy^2$. Thus the units are given by $x^2 - dy^2 = \pm 1$ $(d \equiv 2,3 \bmod 4)$ and $x^2 + xy + \frac{1}{4}(1-d)y^2 = \pm 1$ $(d \equiv 1 \bmod 4)$.

If $D < -4$ then these equations have only the solutions (in integers x, y) given by $x = \pm 1$, $y = 0$. Hence units are ± 1.
If $d = -1$, that is if $\mathbb{Q}(\sqrt{d})$ is the Gaussian field, then the units are given by $x^2 + y^2 = \pm 1$, and the solutions are $x = \pm 1, y = 0$; $x = 0, y = \pm 1$. Hence the units are $\pm 1, \pm i$.
If $d = -3$, (the only other possibility if $D < 0$), then the units are given by $x^2 + xy + y^2 = \pm 1$, and the solutions are $x = \pm 1$, $y = 0$; $x = 0$, $y = \pm 1$; $x = 1$, $y = -1$; $x = -1$, $y = 1$. Hence the units are ± 1, $\frac{1}{2}(\pm 1 \pm i\sqrt{3})$.
Note that these agree with Dirichlet's Theorem, since the units are roots of unity, namely zeroes of $x^2 - 1$ $(D < -4)$, $x^4 - 1$ $(d = -1)$, $x^6 - 1$ $(d = -3)$

The theory of units in real quadratic fields is closely related to the solutions of the Pell equation, that is $x^2 - dy^2 = 1$. Consider more generally $x^2 - dy^2 = m$. This can be written as $N(x + y\sqrt{d}) = m$, and we shall assume $m > 0$. Then, $N[x + y\sqrt{d}] = m$, where $[x + y\sqrt{d}]$ is the principal ideal in $\mathbb{Q}(\sqrt{d})$. Now, since $\underline{a} \mid N\underline{a}$, and we have unique factorisation of ideals, there are only finitely many $\theta \in \mathcal{O}_K$ such that $N[\theta] = m$. Further, $[\theta] = [\theta']$ iff θ and θ' are associated. Hence

$x + y\sqrt{d}$ is associated to one of a finite set $s_1, .., s_l$ of elements of $\mathcal{O}_k$ (determinable from the factorisation of $[m]$ into prime ideals). This gives $x + y\sqrt{d} = \pm \varepsilon^j s_q$ for some integer j and some $q \in \{1, .., l\}$. Hence, $x = \pm \frac{1}{2}(\varepsilon^j s_q + \bar{\varepsilon}^j \bar{s}_q)$, $y = \pm \frac{1}{2\sqrt{d}}(\varepsilon^j s_q - \bar{\varepsilon}^j \bar{s}_q)$, where the bar signifies complex conjugation.

The question remains as to the determination of ε. This involves continued fractions. In fact, if $x^2 - dy^2 = 1$, then $x - \sqrt{d}\,y = \frac{1}{x + \sqrt{d}y}$, where $|\sqrt{d} - \frac{x}{y}| < \frac{1}{2y^2}$, and so $\frac{x}{y}$ is convergent to $\sqrt{d}$. ($\sqrt{d} = [a_0, \overline{a_1, a_2, \dots, a_2, a_1, 2a_0}]$)

4. Factorisation

4.1. Elements in ideals.

We need a result of the form: if $\underline{\underline{a}}$ is an ideal in k and d is the discriminant of k, then $\exists$ an element θ in $\underline{\underline{a}}$ such that $|N\theta| \le c\, N\underline{\underline{a}}\sqrt{|d|}$, where c is a constant depending only on the degree of k, or, more precisely, on s, t where $n = s + 2t$ as in the last chapter. We shall prove this here with $c = 1$ and remark on other values later.

Theorem: In every ideal $\underline{\underline{a}}$ of $k = \mathbb{Q}(\alpha)$ there is an element θ such that $|N_{k/\mathbb{Q}}\theta| \le N\underline{\underline{a}}\sqrt{|d|}$, where d is the discriminant of k.

Proof: (i) Totally real case. This means that $\sigma_1(\alpha), .., \sigma_n(\alpha)$ are all real $(n = [k:\mathbb{Q}])$. Let $\gamma_1, .., \gamma_n$ be a basis for $\underline{\underline{a}}$ and let $\lambda_1, .., \lambda_n$ be positive real numbers with $\lambda_1 \cdots \lambda_n = N\underline{\underline{a}}\sqrt{|d|}$. Then, by the refined form of Minkowski's Linear forms theorem, there exist integers $x_1, .., x_n$ such that $\theta = x_1\gamma_1 + \cdots + x_n\gamma_n$ satisfies $|\sigma_j(\theta)| \le \lambda_j$ $(1 \le j \le n)$. Note that the hypotheses of Minkowski's Theorem are satisfied since the determinant of the $\sigma_j(\theta)$ is $\sqrt{|\Delta(\gamma_1, .., \gamma_n)|}$ and by chapter 2 we have $N\underline{\underline{a}} = \sqrt{|\Delta(\gamma_1, .., \gamma_n)|}/\sqrt{|d|}$, ie the determinant is $\lambda_1 \cdots \lambda_n$ by definition of the λ's. Now we have $N_{k/\mathbb{Q}}\theta = \sigma_1(\theta) \cdots \sigma_n(\theta)$, and so $|N_{k/\mathbb{Q}}(\theta)| \le \lambda_1 \cdots \lambda_n$, whence the result.

(ii) The general case. We suppose that $\sigma_1(\alpha), .., \sigma_s(\alpha)$ are real, $\sigma_{s+1}(\alpha), .., \sigma_{s+t}(\alpha)$ are complex, with complex conjugates $\sigma_{s+t+1}(\alpha), .., \sigma_{s+2t}(\alpha)$, respectively. $(n = s + 2t)$.
Proof, as above, that we solve the inequalities $|\sigma_j(\theta)| \le \lambda_j$ $(1 \le j \le s)$, $|\mathrm{re}\,\sigma_j(\theta)| \le \frac{\lambda_j}{\sqrt{2}}$ (for $s+1 \le j \le s+t$), $|\mathrm{im}\,\sigma_j(\theta)| \le \frac{\lambda_j}{\sqrt{2}}$ $(s+t+1 \le j \le s+2t)$. Then the hypotheses of Minkowski's Linear forms theorem are again satisfied, since the determinant of the linear system is $2^{-t}\sqrt{|\Delta(\gamma_1, .., \gamma_n)|} = \lambda_1 \cdots \lambda_s(\lambda_{s+1}/\sqrt{2})^2 \cdots (\lambda_{s+t}/\sqrt{2})^2$. To verify the calculation of the determinant, first add $\mathrm{re}\,\sigma_j(\theta)$ $(s+1 \le j \le s+t)$ to $\mathrm{im}\,\sigma_j(\theta)$ $(s+1 \le j \le s+t)$ to get $\sigma_j(\theta)$ (rows $s+1$ to $s+t$), then multiply rows $s+t+1$ to n by 2, take out a factor 2^{-t} to compensate, and then subtract rows $s+1$ to $s+t$ (ie, $\sigma_j(\theta)$) from rows $s+t+1$ to n. This gives, except for sign, the conjugates of $\sigma_{s+1}(\theta), .., \sigma_{s+t}(\theta)$, ie, $\sigma_{s+t+1}(\theta), .., \sigma_n(\theta)$. Finally, note that we have $|\sigma_j(\theta)| \le \lambda_j$ for all j. [Using $|\sigma_j(\theta)| = \sqrt{(\mathrm{re}\,\sigma_j(\theta))^2 + (\mathrm{im}\,\sigma_j(\theta))^2}$.

4.2. Ideal Classes.

We say ideals $\mathfrak{a}, \mathfrak{b}$ in k are equivalent if $\exists$ principal ideals $[\vartheta], [\varphi]$ such that $[\vartheta]\mathfrak{a} = [\varphi]\mathfrak{b}$. This is an equivalence relation, and the number of equivalence classes is finite.

Lemma: Every ideal $\mathfrak{a}$ is equivalent to an ideal $\mathfrak{b}$ with $N\mathfrak{b} \leq \sqrt{|d|}$

Proof: There is an ideal $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{c}$ is principal. Further, by the theorem above, $\exists\, \vartheta$ in $\mathfrak{c}$ such that $|N_{k/\mathbb{Q}}(\vartheta)| \leq N\mathfrak{c}\sqrt{|d|}$. Now $\mathfrak{c} \mid [\vartheta]$, so $[\vartheta] = \mathfrak{b}\mathfrak{c}$, and $|N_{k/\mathbb{Q}}(\vartheta)| = N\mathfrak{b}\, N\mathfrak{c}$. So we get $N\mathfrak{b} \leq \sqrt{|d|}$. Further, $\mathfrak{a}$ is equivalent to $\mathfrak{b}$ since $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = \mathfrak{b}(\mathfrak{a}\mathfrak{c})$ and $\mathfrak{b}\mathfrak{c} = [\vartheta]$, $\mathfrak{a}\mathfrak{c} = [\varphi]$ are principal.

The number of ideal classes is denoted by h; it is called the class number of k. The classes form a group under multiplication [ie $(\mathrm{cl}\,\mathfrak{a}) \cdot (\mathrm{cl}\,\mathfrak{b}) = \mathrm{cl}(\mathfrak{a}\mathfrak{b})$]. The group is abelian, and the identity element is the class of principal ideals.
The order of the class group is h, and hence $\mathfrak{a}^h$ is principal for all ideals $\mathfrak{a}$ in k.
In the case $h=1$ we have $\mathfrak{a}$ principal for every $\mathfrak{a}$ in k and thus k has unique factorisation.

Note: In every ideal class there is an ideal $\mathfrak{b}$ such that $N\mathfrak{b} \leq c\sqrt{|d|}$, where $c = \frac{(4/\pi)^t\, n!}{n^n}$:
Here, c is called Minkowski's constant. The result follows from a more refined application of the Geometry of Numbers; it depends on the inequality of the arithmetic and geometric means, ie, $(a_1 \cdots a_n)^{1/n} \leq \frac{1}{n}(a_1 + \cdots + a_n)$. [See Stewart and Tall].

Example: Let $k = \mathbb{Q}(\sqrt{-5})$. Here $n=2$, $s=0$, $t=1$, and $d=-20$. Hence, by the note above, there is an ideal $\mathfrak{b}$ in k such that $N\mathfrak{b} \leq (\frac{4}{\pi})(\frac{1}{2})\sqrt{20} < 3$. This gives $N\mathfrak{b} = 1$ or 2.
Now, if $N\mathfrak{b} = 1$ then $\mathfrak{b} = \mathfrak{e}$. If $N\mathfrak{b} = 2$ then $\mathfrak{b} \mid 2$. But $2 = [2, 1+\sqrt{-5}]^2$ as a product of prime ideals (either direct or by next section), whence $\mathfrak{b} = [2, 1+\sqrt{-5}]$. Further, $\mathfrak{b}$ is not principal since $N\mathfrak{b} = 2$, and $x^2 + 5y^2 = 2$ is not soluble in integers x and y.
We conclude that $h = 2$.

4.3. Dedekind's Theorem

This applies when $\mathcal{O}_k$ (ring of integers of k) has a power integral basis, ie when $\mathcal{O}_k = \mathbb{Z}(\alpha)$, or $1, \alpha, \ldots, \alpha^{n-1}$ is an integral basis for k for some α in $\mathcal{O}_k$. We take f as the minimal polynomial for α. Suppose that p is any prime. Let $\bar{f}$ be the polynomial obtained by replacing each coefficient in f by its residue mod p, ie $\bar{f} \equiv f \bmod p$, in $\mathbb{Z}/p\mathbb{Z}$ (mod p-field).

Dedekind's Theorem: If $\bar{f} = \bar{p}_1^{e_1} \cdots \bar{p}_l^{e_l}$ as a product of irreducible monic polynomials $\bar{p}_1, \ldots, \bar{p}_l$ in $\mathbb{Z}/p\mathbb{Z}$, then $[p] = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_l^{e_l}$ as a product of prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$, where $\mathfrak{p}_j = [p, \bar{p}_j(\alpha)]$

Proof: We have $\mathfrak{p}_j = [p, \bar{p}_j(\alpha)]$ as the kernel of the mapping $\mathbb{Z}(\alpha) \to (\mathbb{Z}/p\mathbb{Z})(\bar{\alpha}_j)$, where $\bar{\alpha}_j$ is any zero of $\bar{p}_j$. Obviously, $\mathfrak{p}_j$ is contained in the kernel (since $p \to 0$ and $\bar{p}_j(\alpha) \to \bar{p}_j(\bar{\alpha}_j) = 0$), and if $q(x) \in \mathbb{Z}(x)$ and $q(\alpha) \to 0$, then $\bar{q}(\bar{\alpha}_j) = 0$ ($\bar{q} \equiv q \bmod p$), but $\bar{p}_j$ is irreducible, whence $\bar{q} = \bar{p}_j \bar{s}$, with $\bar{s}(x) \in (\mathbb{Z}/p\mathbb{Z})(x)$ and so $q(\alpha)$ is in $\mathfrak{p}_j$, that is the kernel is in $\mathfrak{p}_j$. It

follows from properties of kernels that $\mathfrak{p}_j$ is a prime ideal.
[Or directly: consider $\mathfrak{p} = \underline{\underline{a}}\,\underline{\underline{b}}$ and choose $\sigma \in \underline{\underline{a}}$, $\rho \in \underline{\underline{b}}$ so that $\sigma = a(\alpha)$, $\rho = b(\alpha)$ for some $a, b \in \mathbb{Z}(x)$, and from $\bar{a}(\bar{\alpha}_j)\bar{b}(\bar{\alpha}_j) = 0$ we have either $\bar{a}(\bar{\alpha}_j) = 0$ or $\bar{b}(\bar{\alpha}_j) = 0$, so $\mathfrak{p} | \underline{\underline{a}}$ or $\mathfrak{p} | \underline{\underline{b}}$].
Now, we have $\mathfrak{p}_j^{e_j} \subset [p, (\bar{p}_j(\alpha))^{e_j}]$ and so $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_l^{e_l} \in [p, (\bar{p}_1(\alpha))^{e_1} \cdots (\bar{p}_l(\alpha))^{e_l}] = [p, \bar{f}(\alpha)] = [p]$, since $\bar{f} \equiv f \bmod p$ and $f(\alpha) = 0$.
It remains to show that $[p] \subset \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_l^{e_l}$. But $N\mathfrak{p}_j = p^{f_j}$, where f_j is the degree of $\mathfrak{p}_j$, and this is the same as the degree of $\bar{p}_j(x)$. [since every element of $\mathfrak{p}_j$ is congruent mod $\mathfrak{p}_j$ to an element of the form $a_0 + a_1\alpha + \cdots + a_{f_j-1}\alpha^{f_j-1}$ $(0 \le a_r < p)$.
Finally, $N[p] = p^n$ and $N(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_l^{e_l}) = p^{e_1 f_1 + \cdots + e_l f_l}$, and since $\bar{f}$ is monic we have degree $\bar{f} = n = e_1 f_1 + \cdots + e_l f_l$. This gives $[p] = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_l^{e_l}$, as required.

4.4. The Quadratic Field.

Let $K = \mathbb{Q}(\sqrt{d})$. Suppose first that $d \equiv 2, 3 \bmod 4$. Then $\mathcal{O}_K = \mathbb{Z}(\sqrt{d})$. Thus by Dedekind's Theorem, we have three possibilities:
(i) $x^2 - d$ reduces mod p into two distinct factors. Then $\left(\frac{d}{p}\right) = 1$ and $p = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}' \ne \mathfrak{p}$ and $N\mathfrak{p} = N\mathfrak{p}' = p$.
(ii) $x^2 - d$ reduces mod p to a square. Then $x^2 - d = (x - a)^2 \bmod p$, whence $p | D = 4d$, so that $\left(\frac{D}{p}\right) = 0$, $p = \mathfrak{p}^2$, $N\mathfrak{p} = p$.
(iii) $x^2 - d$ is irreducible mod p, then $\left(\frac{d}{p}\right) = -1$, $N\mathfrak{p} = p^2$, $p = \mathfrak{p}$.

Now suppose that $d \equiv 1 \bmod 4$. Then $\mathcal{O}_K = \mathbb{Z}\left(\frac{1}{2}(1 + \sqrt{d})\right)$. The minimal polynomial for $\frac{1}{2}(1 + \sqrt{d})$ is $x^2 + x + \frac{1}{4}(1 - d)$, say $f(x)$, and $4f(x) = (2x + 1)^2 - d$. Hence if p is odd, then we have the possibilities (i), (ii), (iii) as above.

If $p = 2$, then we have to consider the cases $d \equiv 1$ or $5 \bmod 8$.
When $d \equiv 1 \bmod 8$, then $f(x) = x(x+1) \bmod 2$ and so $p = \mathfrak{p}\mathfrak{p}'$ as in (i).
When $d \equiv 5 \bmod 8$, then $f(x)$ is irreducible mod 2 and so $p = \mathfrak{p}$ as in (iii)

On defining the character $\chi(p) = \left(\frac{D}{p}\right)$ we see that for $d \equiv 2, 3 \bmod 4$ and $s > 1$ we have $\prod_{\mathfrak{p}, p} (1 - (N\mathfrak{p})^{-s}) = (1 - p^{-s})(1 - \chi(p)p^{-s})$.
The same holds for $d \equiv 1 \bmod 4$ if we define the character χ so that $\chi(2) = \left(\frac{2}{|D|}\right)$.
This gives: $\zeta_K(s) = \zeta(s) L(s, \chi)$, where ζ_K is the Dedekind Zeta Function: $\zeta_K(s) = \sum_{\underline{\underline{a}}} (N\underline{\underline{a}})^{-s} = \prod_{\mathfrak{p}} (1 - (N\mathfrak{p})^{-s})^{-1}$, ζ is the Riemann Zeta Function: $\sum_n n^{-s} = \prod_p (1 - p^{-s})^{-1}$, and L is the L-function: $L(s, \chi) = \sum_n \frac{\chi(n)}{n^s} = \prod_p (1 - \chi(p)p^{-s})^{-1}$.
Here, the sums and products all converge for $s > 1$, and in fact for any complex $s = \sigma + it$ with $\sigma > 1$.

Note on ramification indices: If $p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_l^{e_l}$ in canonical factorisation then $e_1, \ldots, e_l$ are called the ramification indices of $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$. They satisfy $\sum e_j f_j = n$. If $e_j = n$ we say $\mathfrak{p}_j$ is totally ramified (since $p = \mathfrak{p}_j^n$). If $e_j = 1$ we say $\mathfrak{p}_j$ is unramified.

4.5. The Cyclotomic Field.

Let q be an integer >2. The qth cyclotomic field is defined as $\mathbb{Q}(\zeta)$, where ζ is the qth root of unity $e^{2\pi i/q}$. We shall discuss only the case q prime.

(i) minimal polynomial. We have $\zeta^q = 1$ and so ζ is a zero of the qth cyclotomic polynomial $\Phi_q(x) = x^{q-1} + x^{q-2} + \dots + 1$. This is irreducible and thus the minimal polynomial for ζ, for by Eisenstein's theorem, the polynomial $\Phi_q(x+1) = \frac{(x+1)^q - 1}{x} = x^{q-1} + \binom{q}{1} x^{q-2} + \dots + \binom{q}{q-1}$ is irreducible. Hence we conclude that $\mathbb{Q}(\zeta)$ has degree $q-1$, and the conjugates of ζ are $\zeta, \zeta^2, \dots, \zeta^{q-1}$.

(ii) integral basis. This is given by $1, \zeta, \dots, \zeta^{q-2}$ (Proof - see, e.g., Borevich/Shafarevich). This gives as discriminant $(-1)^{\frac{1}{2}(q-1)} \cdot q^{q-2}$ (exercise!)

(iii) Factorisation of primes. We have $\mathcal{O}_k = \mathbb{Z}(\zeta)$ and so Dedekind's Theorem is applicable. Further, $x^q - 1$ and its derivative are relativity prime in the mod p field, whence $\Phi_q(x)$ has no repeated factors mod p. We conclude that $p = \mathfrak{p}_1 \cdots \mathfrak{p}_l$ for distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_l$, i.e, all the prime ideals in $\mathbb{Q}(\zeta)$ are unramified.

There is an equation $\zeta_k(s) = \zeta(s) \prod_{\chi \neq \chi_0} L(s, \chi)$ analogous to that for the quadratic field.