6. Valuations and $p$-adic numbers

6.1. Let $F$ be a field. A map $\nu : F \to \mathbb{R} \cup \{\infty\}$ is called an order function of $F$ if it satisfies the following conditions:

(i) $\nu(x) = \infty \iff x = 0$;
(ii) $\nu(xy) = \nu(x) + \nu(y)$;
(iii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$;
(iv) There exists an element $z \in F, \neq 0$, such that $\nu(z) \neq 0$.

Here $\infty + a = a + \infty = \infty$ and $\infty \geq a$ for every $a \in \mathbb{R} \cup \{\infty\}$. Taking $z$ as in (iv), we have $\nu(z) = \nu(z \cdot 1) = \nu(z) + \nu(1)$, and so $\nu(1) = 0$. Then $0 = \nu((-1)(-1)) = \nu(-1) + \nu(-1)$, and so $\nu(-1) = 0$, and $\nu(-x) = \nu(-1) + \nu(x) = \nu(x)$. There is a noteworthy fact:

\begin{equation}
\nu(x + y) = \min\{\nu(x), \nu(y)\} \quad \text{if} \quad \nu(x) \neq \nu(y).
\end{equation}

Indeed, assuming that $\nu(x) < \nu(y)$, we have $\nu(x) = \nu(x + y + (-y)) \geq \min\{\nu(x + y), \nu(y)\}$, from which (6.1) follows.

An order function $\nu$ is called discrete if there exists a positive real number $t$ such that $\nu(F^\times) = t\mathbb{Z}$. A discrete order function is called normalized if $\nu(F^\times) = \mathbb{Z}$.

To find an example of an order function, take $F = \mathbb{Q}$ and fix a prime number $p$. Given $x \in \mathbb{Q}^\times$, considering the prime decomposition of $x$, we can put $x = p^ma/b$ with $m \in \mathbb{Z}$ and nonzero integers $a, b$ prime to $p$. We then put $\nu_p(x) = m$. We also put $\nu_p(0) = \infty$. It can easily be seen that this is a normalized order function.

6.2. Let $F$ be a field. A map $\varphi : F \to \{x \in \mathbb{R} \mid x \geq 0\}$ is called a valuation of $F$ if it satisfies the following conditions:

(i) $\varphi(x) = 0 \iff x = 0$;
(ii) $\varphi(xy) = \varphi(x)\varphi(y)$;
(iii) $\varphi(x + y) \leq \varphi(x) + \varphi(y)$;
(iv) There exists an element $z \in F, \neq 0$, such that $\varphi(z) \neq 1$.  

Such a \( \varphi \) is called nonarchimedean if
\[
(\mathrm{v}) \quad \varphi(x + y) \leq \text{Max}\{\varphi(x), \varphi(y)\}.
\]
Otherwise it is called archimedean. Notice that (v) implies (iii). We easily see that \( \varphi(\pm 1) = 1 \) and \( \varphi(-x) = \varphi(x) \). Since \( \varphi(x) = \varphi(x - y + y) \leq \varphi(x - y) + \varphi(y) \), we have \( \varphi(x) - \varphi(y) \leq \varphi(x - y) \). Exchanging \( x \) and \( y \), we obtain \( \varphi(y) - \varphi(x) \leq \varphi(y - x) = \varphi(x - y) \). Thus
\[
|\varphi(x) - \varphi(y)| \leq \varphi(x - y).
\]

If there is an isomorphism \( \sigma \) of \( F \) onto a subfield of \( C \), then we obtain an archimedean valuation \( \psi \) of \( F \) by putting \( \psi(x) = |x^\sigma| \) for \( x \in F \).

Given an order function \( \nu \) of \( F \), put \( \varphi(x) = \nu(x) \) with a fixed real number \( c \) such that \( 0 < c < 1 \). Then \( \varphi \) is a nonarchimedean valuation of \( F \). Conversely, given a nonarchimedean valuation \( \varphi \) of \( F \), put \( \nu(x) = -\log \varphi(x) \) for \( x \neq 0 \) and \( \nu(0) = \infty \). Then it can be shown that \( \nu \) is an order function of \( F \) and \( \varphi(x) = e^{-\nu(x)} \).

Take \( F = \mathbb{Q} \); fix a prime number \( p \). Define \( \nu_p \) as in §6.1 with this \( p \). Usually we define a nonarchimedean valuation \( \varphi_p \) by \( \varphi_p(x) = p^{-\nu_p(x)} \). For example, \( \varphi_p(\pm p^m) = p^{-m} \).

6.3. Given a valuation \( \varphi \) of \( F \), put \( \mu(x, y) = \varphi(x - y) \). We can easily verify that \( F \) is a metric space with respect to \( \mu \). Thus we can speak of open sets, closed sets, and continuity with respect to the topology defined by this metric. Then the maps \( (x, y) \mapsto x + y, x - y, xy, x/y \) are continuous. (Of course we assume \( y \neq 0 \) for \( x/y \).) The limit and convergence of an infinite sequence in \( F \) can be naturally defined. To be explicit, for an infinite sequence \( \{a_n\}_{n=1}^\infty \) in \( F \) and \( b \in F \) we write \( \lim_{n \to \infty} a_n = b \) if \( \lim_{n \to \infty} \varphi(a_n - b) = 0 \), which is so if and only if \( \lim_{n \to \infty} \nu(a_n - b) = \infty \) if \( \varphi \) is obtained from an order function \( \nu \). If \( \lim_{n \to \infty} \sum_{k=1}^n a_k = c \), then we write \( c = \sum_{k=1}^\infty a_k \).

For example, if \( \nu_p \) is the order function of \( \mathbb{Q} \) defined at the end of §6.1, then \( \lim_{n \to \infty} p_n = 0 \) and \( \sum_{k=0}^\infty b^k = (1 - p)^{-1} \).

6.4. An infinite sequence \( \{x_n\}_{n=1}^\infty \) in \( F \) is called a Cauchy sequence (with respect to \( \varphi \)) if for every \( \varepsilon > 0 \) there exists a positive integer \( N \) such that \( \varphi(x_m - x_n) < \varepsilon \) for every \( m, n > N \). If \( \varphi \) is obtained from an order function \( \nu \) as above, then \( \{x_n\}_{n=1}^\infty \) is a Cauchy sequence if for every \( C \in \mathbb{R}, \ v) > 0 \), there exists a positive integer \( N \) such that \( \nu(x_m - x_n) > C \) for every \( m, n > N \). We call \( F \) complete (with respect to \( \varphi \)) if every Cauchy sequence in \( F \) is convergent.

**Theorem 6.5.** Given a valuation \( \varphi \) of a field \( F \), we can find a field \( F^* \) and a valuation \( \varphi^* \) of \( F^* \) with the following properties:

1. \( F^* \) is complete with respect to \( \varphi^* \);
2. \( F \) is a subfield of \( F^* \) and \( \varphi^* = \varphi \) on \( F \);
6. VALUATIONS AND $p$-ADIC NUMBERS

(3) $F$ is dense in $F^*$.

(4) If $\varphi$ is obtained from an order function $\nu$ of $F$, then $\varphi^*$ is obtained from an order function $\nu^*$ of $F^*$ that coincides with $\nu$ on $F$. Moreover, $(F^*, \varphi^*)$ is unique for $(F, \varphi)$ up to isomorphism.

Since the whole proof is long and tedious, we merely give its idea. Let $X$ be the set of all Cauchy sequences in $F$. This is a commutative ring with respect to componentwise operations. Let $Y$ be the subset of $X$ consisting of all the sequences convergent to 0. Then $Y$ is a maximal ideal of $X$, and $F^*$ can be obtained as $X/Y$.

The field $F^*$ is called the $\varphi$-completion of $F$ and also the $\nu$-completion of $F$ if $\varphi$ is obtained from an order function $\nu$.

**Lemma 6.6.** Suppose that $F$ is complete with respect to a nonarchimedean valuation $\varphi$ obtained from an order function $\nu$. Then

$$\sum_{n=1}^{\infty} a_n \text{ is convergent} \iff \lim_{n \to \infty} a_n = 0 \iff \lim_{n \to \infty} \nu(a_n) = \infty \iff \lim_{n \to \infty} \varphi(a_n) = 0.$$ 

**Proof.** Suppose $\lim_{n \to \infty} \varphi(a_n) = 0$; put $b_n = \sum_{k=1}^{n} a_k$. Since $b_{n+p} - b_n = a_{n+1} + \cdots + a_{n+p}$, we have $\varphi(b_{n+p} - b_n) \leq \max\{\varphi(a_{n+1}), \ldots, \varphi(a_{n+p})\}$. Then we see that $\{b_n\}_{n=1}^{\infty}$ is a Cauchy sequence, and so it is convergent. The remaining part of our lemma is trivial.

**6.7.** Given an order function $\nu$ of a field $F$, put

$$(6.3) \quad R = \{x \in F \mid \nu(x) \geq 0\}, \quad M = \{x \in F \mid \nu(x) > 0\}.$$ 

Clearly

$$(6.4) \quad a \in R, \ a \notin M \iff \nu(a) = 0 \iff a \in R^\times.$$ 

We easily see that $R$ is a subring of $F$, $M$ is a maximal ideal of $R$, and $F$ is the field of quotients of $R$. Moreover, $M$ is the only maximal ideal of $R$. We call $R$ the valuation ring of $\nu$ and $M$ the maximal ideal of $R$.

Now suppose $\nu$ is discrete and normalized; then an element $\pi$ of $F$ is called a prime element of $F$ (with respect to $\nu$) if $\nu(\pi) = 1$. For any such element $\pi$ we have

$$\pi^m R = \{x \in F \mid \nu(x) \geq m\} = \{x \in F \mid \nu(x) > m - 1\}.$$ 

This is an open and closed subset of $F$, since $\nu$ is continuous. Every nonzero ideal of $R$ is of the form $\pi^m R$ with $m > 0$. Thus $R$ is a principal ideal domain. Every neighborhood of 0 contains $\pi^m R$ for some $m$, and so the sets $\pi^m R$ for all $m \in \mathbb{Z}, > 0$, form a base of neighborhoods of 0.

If $\nu$ is the order function $\nu_p$ of $\mathbb{Q}$, then
Let the notation be as in Theorem 6.5; suppose that \( \varphi \) is obtained from a discrete order function \( \nu \). Let \( R \) resp. \( R^* \) be the valuation ring of \( \nu \) resp. \( \nu^* \) and let \( M \) resp. \( M^* \) be the maximal ideal of \( R \) resp. \( R^* \).

Then the following assertions hold:

(i) \( \nu^*(F^*) = \nu(F) \); consequently \( \nu^* \) is discrete, and every prime element of \( F \) is a prime element of \( F^* \).

(ii) \( R^* \) resp. \( M^* \) is the closure of \( R \) resp. \( M \) in \( F^* \).

(iii) \( R^* \) is a prime element of \( M = pR \), \( R = R + \mathbb{Z} \), \( p\mathbb{Z} = M \cap \mathbb{Z} \), \( R/M \cong \mathbb{Z}/p\mathbb{Z} \).

Proof. We may assume that \( \nu \) is normalized. Since \( F \) is dense in \( F^* \), given \( a \in F^*, \neq 0 \), and any positive number \( t \), there exists an element \( b \in F \) such that \( \nu^*(b-a) = t \). Take \( t \) so that \( t > \nu^*(a) \). Then \( \nu(b) = \nu^*(b-a+a) = \nu^*(a) \) by (6.1), which proves (i). If \( a \in R^* \), then \( \nu(b) = \nu^*(a) \leq 0 \), and so \( b \in R \), which proves that \( R \) is dense in \( R^* \). Similarly \( M \) is dense in \( M^* \). This proves (ii). In the case \( a \in R^* \) we have \( a = a - b + b \). Since \( \nu^*(a-b) > 0 \), we have \( a-b \in M^* \), and so \( R^* = M^* + R \). That \( M = R \cap M^* \) is trivial. Then \( R^*/M^* = (R + M^*)/M^* \cong R/(R \cap M^*) = R/M \). This proves (iii). To prove (iv), given \( 0 \neq x \in F^* \), let \( m = \nu^*(x) \). Observe that

\[
S_{\nu^*} \text{ represents } M^n/M^{n+1}.
\]

Let us now prove by induction (on \( n \geq m \)) that \( x - \sum_{k=m}^{n} s_k \pi_k \in M^{n+1} \) with suitable \( s_k \in S \). If \( n = m \), this follows from (6.5). Assume that we have found \( s_k \) for \( m \leq k \leq n \). By (6.5) with \( n+1 \) in place of \( n \) we can find a desired \( s_{n+1} \). By Lemma 6.6, \( \sum_{k=m}^{n} s_k \pi_k \) is meaningful as an element of \( F^* \). Call it \( y \). Then \( x - y = \lim_{n \to \infty} \left( x - \sum_{k=m}^{n} s_k \pi_k \right) = 0 \), since the difference in the parentheses belongs to \( M^{n+1} \). Thus \( x = y = \sum_{k=m}^{\infty} s_k \pi_k \).

To prove the uniqueness of \( s_k \), suppose \( x = \sum_{k=\ell}^{\infty} t_k \pi_k \) with \( t_k \in S \). Clearly \( m = \nu^*(x) \geq \ell \). Putting \( s_k = 0 \) for \( \ell \leq k < m \), and \( u_k = s_k - t_k \), we have \( 0 = \sum_{k=\ell}^{\infty} u_k \pi_k \). Then we easily see that \( u_k = 0 \) by induction.

Lemma 6.9. The notation being as in Theorem 6.8, suppose that \( \nu \) is discrete and \( R/M \) is finite. Then both \( R^* \) and \( (R^*)^\times \) are open compact sets and \( F^* \) is locally compact.

Proof. As observed in §6.7, \( R^* \) and \( M^* \) are open and closed subsets of \( F^* \). Since \( (R^*)^\times \) is the complement of \( M^* \) in \( R^* \), it must be open and
closed. To prove that $R^\ast$ is compact, recall that a metric space is compact if every infinite sequence has a convergent subsequence. Let $X = \{x_n\}_{n=1}^\infty$ with $x_n \in R^\ast$. We are going to construct a chain of subsequences $X = X_0 \supset X_1 \supset \cdots \supset X_m \supset \cdots$ and a sequence $\{c_m\}_{m=0}^\infty$ with $c_m \in R^\ast$ such that $X_m$ is contained in $c_m + \pi^mR^\ast$, where we write $X \supset Y$ when $Y$ is a subsequence of $X$. We first take $c_0 = 0$. Suppose $X_m$ has been established. Observe that $c_m + \pi^mR^\ast = \bigsqcup_{i=1}^q (d_i + \pi^{m+1}R^\ast)$, where $q = [R:M]$. Therefore we can find an infinite subsequence $X_{m+1}$ of $X_m$ contained in $d_i + \pi^{m+1}R^\ast$ with some $i$. Putting $d_i = c_{m+1}$, we obtain the desired $\{X_m\}$ and $\{c_m\}$. Now pick $y_m$ from $X_m$ so that $\{y_m\}_{m=1}^\infty$ is a subsequence of $X$. Then we see that $y_k \in c_m + \pi^mR^\ast$ if $k \geq m$, and hence $y_k - y_m \in \pi^mR^\ast$ if $k \geq m$. Thus $\{y_m\}_{m=1}^\infty$ is a Cauchy sequence, and so is convergent. This proves that $R^\ast$ is compact, and consequently $F^\ast$ is locally compact. The group $(R^\ast)^\times$, being closed in $R^\ast$, must be compact. This completes the proof.

6.10. Fix a prime number $p$ and define an order function $\nu_p$ of $Q$ as in §6.2. The $\nu_p$-completion of $Q$ is called the $p$-adic field and denoted by $Q_p$. The closure of $Z$ in $Q_p$ is denoted by $Z_p$. An element of $Q_p$ (resp. $Z_p$) is called a $p$-adic number (resp. a $p$-adic integer). By Theorem 6.8(iv), $Q_p$ consists of all the infinite sums $\sum_{k=m}^\infty c_k p^k$ with $m \in Z$ and $c_k \in \{0, 1, 2, \ldots, p-1\}$. $Z_p$ consists of all such sums with $m = 0$. By Lemma 6.9, $Q_p$ is a locally compact topological additive group; both $Z_p$ and $Z_p^\times$ are open and compact subsets of $Q_p$.

Suppose $p \neq 2$. For every $x \in Z_p$ we define $\left(\frac{x}{p}\right)$ by $\left(\frac{x}{p}\right) = \left(\frac{\xi}{p}\right)$ with any $\xi \in Z$ such that $x - \xi \in pZ_p$. Clearly this is well defined.

Lemma 6.11. Let $Z_p^{\times 2} = \{x^2 \mid x \in Z_p^\times\}$. Then

\begin{enumerate}[(i)]
  \item $Z_p^{\times 2} = \left\{x \in Z_p^\times \mid \left(\frac{x}{p}\right) = 1\right\}$ if $p \neq 2$,
  \item $Z_p^{\times 2} = \left\{x \in Z_p^\times \mid x - 1 \in 8Z_p\right\}$ if $p = 2$,
  \item $[Z_p^\times : Z_p^{\times 2}] = \begin{cases} 2 & \text{if } p \neq 2, \\ 4 & \text{if } p = 2, \end{cases}$
  \item $[Q_p^\times : Q_p^{\times 2}] = \begin{cases} 4 & \text{if } p \neq 2, \\ 8 & \text{if } p = 2. \end{cases}$
\end{enumerate}

Proof. Clearly the left-hand side of (i) is contained in the right-hand side. To prove the opposite inclusion, let $x \in Z_p^\times$. Now consider the natural homomorphism of $(Z_p/p^nZ_p)^\times$ onto $(Z/pZ)^\times$. In view of Theorem 2.3, we can find an element $r \in Z$ that generates $(Z_p/p^nZ_p)^\times$ and such that $x - r^k \in p^nZ_p$ with some $k$. If $\left(\frac{x}{p}\right) = 1$, then $k \in 2Z$, as $\left(\frac{r}{p}\right) = -1$. Thus we can find
an element \( y_n \in \mathbb{Z} \) such that \( y_n^2 - x \in p^n \mathbb{Z}_p \). The sequence \( \{y_n\}_{n=1}^{\infty} \) has a subsequence that converges to an element \( z \) of \( \mathbb{Z}_p \) and clearly \( z^2 = x \). This proves (i). We can prove (ii) in the same manner by means of Theorem 2.4. Then (iii) follows immediately from (i) and (ii). We have \( \mathbb{Q}_p^x = \mathbb{Z}_p^\times \cdot \{p^m \mid m \in \mathbb{Z}\} \), and so (iv) follows immediately from (iii).

Theorem 6.12. (i) If \( p \neq 2 \), then \( \mathbb{Q}_p \) has exactly three nonisomorphic quadratic extensions \( \mathbb{Q}_p(\sqrt{r}) \), \( \mathbb{Q}_p(\sqrt{p}) \), and \( \mathbb{Q}_p(\sqrt{pr}) \), where \( r \) is any quadratic nonresidue modulo \( p \).

(ii) If \( p = 2 \), then \( \mathbb{Q}_p \) has exactly seven nonisomorphic quadratic extensions, which are represented by \( \mathbb{Q}_2(\sqrt{s}) \), \( \mathbb{Q}_2(\sqrt{2s}) \), and \( \mathbb{Q}_2(\sqrt{2}) \), where \( s \in \{ -1, \pm 3 \} \).

Proof. Observe that every extension \( K \) of \( \mathbb{Q}_p \) of degree \( \leq 2 \) is of the form \( K = \mathbb{Q}_p(\sqrt{\alpha}) \) with \( \alpha \in \mathbb{Q}_p^x \). Assigning \( \mathbb{Q}_p(\sqrt{\alpha}) \) to \( \alpha \), we obtain a bijection of \( \mathbb{Q}_p^x / \mathbb{Q}_p^{x^2} \) onto the set of all such extensions of \( \mathbb{Q}_p \) (contained in a fixed algebraic closure of \( \mathbb{Q}_p \)). Suppose \( p = 2 \). By Lemma 6.11 (ii), \( \mathbb{Z}_2^x / \mathbb{Z}_2^{x^2} \) consists of \( \{ \pm 1, \pm 3 \pmod{8\mathbb{Z}_2} \} \), and so \( \mathbb{Q}_2^x / \mathbb{Q}_2^{x^2} \) can be represented by \( \{ \pm 1, \pm 3, \pm 2, \pm 6 \} \). The identity element corresponds to the trivial extension \( \mathbb{Q}_2 \) of \( \mathbb{Q}_2 \), and therefore we obtain (ii). If \( p \neq 2 \), \( \mathbb{Q}_p^x / \mathbb{Q}_p^{x^2} \) can be represented by \( \{1, r, p, pr\} \), and we obtain (i).

Theorem 6.13. Let \( \varphi \) and \( \psi \) be valuations of a field \( F \). Then the following conditions are equivalent to each other:

1. \( \varphi(x) > 1 \iff \psi(x) > 1 \).
2. \( \varphi(a) \geq \varphi(b) \iff \psi(a) \geq \psi(b) \).
3. \( \lim_{n \to \infty} \varphi(a^n) = 0 \iff \lim_{n \to \infty} \psi(a^n) = 0 \).
4. There exists a positive number \( \alpha \) such that \( \psi(x) = \varphi(x)^\alpha \) for every \( x \in F \).

Proof. It is easy to see that (1) \( \iff \) (2) and (4) \( \implies \) (3). Taking \( a_n \) of (3) to be \( (b/a)^n \), we can prove that (3) \( \implies \) (2). Let us now derive (4) from (1). Once we assume (1), then (2) holds. Also, taking \( a^{-1} \) in place of \( a \), we find that \( \varphi(a) < 1 \iff \psi(a) < 1 \). Consequently, \( \varphi(a) = 1 \iff \psi(a) = 1 \). Take \( z \in F \) so that \( \varphi(z) > 1 \). Given \( a \in F^\times \), we can find \( \lambda \in \mathbb{R} \) such that \( \varphi(a) = \varphi(z)^\lambda \). Take integers \( m > 0 \) and \( n \) so that \( n/m < \lambda \). Then \( \varphi(z)^n < \varphi(z)^{\lambda m} = \varphi(a)^m \), and so \( \psi(z)^n < \psi(a)^m \). Thus \( \psi(z)^{n/m} < \psi(a) \), which holds for all \( n/m \) smaller than \( \lambda \), and so \( \psi(z)^\lambda \leq \psi(a) \). Similarly taking \( n/m > \lambda \), we can show that \( \psi(z)^\lambda \geq \psi(a) \), and so \( \psi(z)^\lambda = \psi(a) \). Take \( \alpha \in \mathbb{R}, > 0 \), so that \( \psi(z) = \varphi(z)^\alpha \). Then \( \psi(a) = \varphi(z)^{\alpha \lambda} = \varphi(a)^\alpha \). This completes the proof.

We say that \( \varphi \) and \( \psi \) are equivalent if the conditions of the above theorem are satisfied. Clearly the topology of \( F \) depends only on the equivalence
class of valuations. Also, if \( \varphi \) and \( \psi \) correspond to order functions \( \nu \) and \( \mu \) as in §6.2, then \( \varphi \) and \( \psi \) are equivalent if and only if \( \nu = s\mu \) with \( 0 < s \in \mathbb{R} \), which is so if and only if \( \nu \) and \( \mu \) have the same valuation ring and maximal ideal.

**Theorem 6.14.** For \( x \in \mathbb{Q} \) put \( \varphi_\infty(x) = |x| \) and \( \varphi_p(x) = p^{-\nu_p(x)} \) with a prime number \( p \) as in §6.2. Then every nonarchimedean (resp. archimedean) valuation of \( \mathbb{Q} \) is equivalent to \( \varphi_p \) for some \( p \) (resp. \( \varphi_\infty \)). Moreover, these valuations are not equivalent to each other.

**Proof.** The last assertion can easily be seen by checking condition (1) of Theorem 6.13. To prove the main part, take a valuation \( \varphi \) of \( \mathbb{Q} \). Then for \( 0 < n \in \mathbb{Z} \) we have \( \varphi(n) \leq n\varphi(1) = n \). We first assume that there exists a positive integer \( z \) such that \( \varphi(z) > 1 \). We can put \( \varphi(z) = z^\alpha \) with \( 0 < \alpha \leq 1 \). Let \( 0 < n \in \mathbb{Z} \). Then we can put \( n = \sum_{i=0}^{k-1} c_iz^i \) with \( 0 \leq c_i < z \) and \( 1 \leq k \in \mathbb{Z} \), \( c_{k-1} \neq 0 \). Then \( z^{k-1} \leq n < z^k \) and

\[
\varphi(n) \leq \sum_{i=0}^{k-1} c_i\varphi(z)^i \leq z \sum_{i=0}^{k-1} \varphi(z)^i = \frac{z[\varphi(z)^k - 1]}{\varphi(z) - 1} \leq \frac{z\varphi(z)}{\varphi(z) - 1} \cdot \varphi(z)^{k-1}.
\]

Put \( A = z\varphi(z)/[\varphi(z) - 1] \). Then \( \varphi(n) \leq Az^{\alpha(k-1)} \leq An^\alpha \). Taking \( n^m \) in place of \( n \), we obtain \( \varphi(n^m) \leq An^{m\alpha} \), and so \( \varphi(n) \leq A^{1/m}n^\alpha \). Making \( m \) tend to \( \infty \), we obtain \( \varphi(n) \leq n^{\alpha} \). Since \( z^{k-1} \leq n < z^k \), we can put \( n = z^k - w \) with an integer \( w \) such that \( 0 < w \leq z^k - z^{k-1} \). Then \( \varphi(w) \leq w^{\alpha} \leq (z^k - z^{k-1})^{\alpha} \), and so

\[
\varphi(n) \geq \varphi(z^k) - \varphi(w) \geq z^{k\alpha} - (z^k - z^{k-1})^{\alpha} = z^{\alpha\{1 - (1 - z^{-1})^{\alpha}\}}.
\]

Put \( B = 1 - (1 - z^{-1})^{\alpha} \). Then \( \varphi(n) \geq Bz^{\alpha} > Bn^{\alpha} \). Taking \( n^m \) in place of \( n \) and making \( m \) tend to \( \infty \), we find that \( \varphi(n) \geq n^{\alpha} \). Thus we obtain \( \varphi(n) = n^{\alpha} \). For \( 0 < n' \in \mathbb{Z} \) we have \( \varphi(\pm n'/n) = \varphi(n')/\varphi(n) = (n'/n)^\alpha \). This means that \( \varphi \) is equivalent to \( \varphi_\infty \), and proves the case in which \( \varphi(z) > 1 \) for some positive integer \( z \).

Next suppose \( \varphi(z) \leq 1 \) for every \( z \in \mathbb{Z} \). We can find a prime number \( p \) such that \( \varphi(p) < 1 \). (Otherwise, the prime decomposition of a rational number shows that \( \varphi(a) = 1 \) for every \( a \in \mathbb{Q}^\times \).) Suppose there is a prime number \( q \neq p \) such that \( \varphi(q) < 1 \). For every positive integer \( m \), we can find integers \( r \) and \( s \) such that \( 1 = rp^m + sq^m \). Then \( 1 = \varphi(1) \leq \varphi(r)\varphi(p)^m + \varphi(s)\varphi(q)^m \leq \varphi(p)^m + \varphi(q)^m \), which tends to 0 as \( m \to \infty \), a contradiction. Thus there is only one prime number \( p \) such that \( \varphi(p) < 1 \). Put \( \varphi(p) = p^c \) with \( c \in \mathbb{R} \). Given \( x \in \mathbb{Q}^\times \), we have \( x = \pm p^{\nu_q(x)}a/b \) with integers \( a \) and \( b \) whose prime decompositions do not involve \( p \). Then \( \varphi(a) = \varphi(b) = 1 \), and so \( \varphi(x) = \varphi(p)^{\nu_p(x)} = p^{\nu_p(x)} \varphi_p(x)^c = \varphi_p(x)^c \). Thus \( \varphi \) is equivalent to \( \varphi_p \). This completes the proof.
Theorem 6.15: Product formula. For \( \varphi_\infty \) and \( \varphi_p \) as in Theorem 6.14 we have
\[
\varphi_\infty(x) \prod_p \varphi_p(x) = 1 \text{ for every } x \in \mathbb{Q}^\times.
\]

Proof. Given \( x \in \mathbb{Q}^\times \), we can put \( x = \pm \prod_p p^{a_p} \) with \( a_p \in \mathbb{Z} \), where \( \prod_p \) means the product over all prime numbers \( p \). Then \( \varphi_p(x) = p^{-a_p} \) and \( \varphi_\infty(x) = |x| \), and clearly our formula holds.

Exercises. 1. Let \( R = \bigcup_{n=0}^\infty p^{-n} \mathbb{Z} \) with a prime number \( p \). Prove: (i) \( R + \mathbb{Z}_p = \mathbb{Q}_p \) and \( R \cap \mathbb{Z}_p = \mathbb{Z} \); (ii) \( R/\mathbb{Z} \) as a module is isomorphic to \( \mathbb{Q}_p/\mathbb{Z}_p \).

2. Let \( p \) be a prime number, \( S_n \) the group of all \( p^n \)-th roots of unity in \( \mathbb{C} \), and \( S = \bigcup_{n=1}^\infty S_n \). Using the results of Exercise 1, show that the multiplicative group \( S \) is isomorphic to the additive group \( \mathbb{Q}_p/\mathbb{Z}_p \).

3. Show that \( \mathbb{Q}_p \), if \( p \neq 2 \), contains no \( p \)-th root of unity other than 1.

4. Let \( \nu \) be a normalized discrete order function of a field \( F \). Suppose that \( F \) is complete and the residue class field is a finite field with \( q \) elements. Let \( c \in F \) with \( \nu(c) = 0 \). Prove that the sequence \( \{ c^{q^n} \}_{n=0}^\infty \) converges to an element \( b \) of \( F \) such that \( b^{q-1} = 1 \) and \( \nu(b-c) > 0 \).

5. With \( F \) and \( \nu \) as in Exercise 4, let \( X \) be the cyclic group generated by a fixed prime element of \( F \), and \( Y \) the group of all roots of unity \( y \) such that \( y^{q-1} = 1 \); let \( 1 + M = \{ x \in F | \nu(x-1) > 0 \} \). Prove that \( F^\times \) is the direct product of \( X \), \( Y \), and \( 1 + M \).

6. Compute \( [\mathbb{Q}_p^\times : \mathbb{Q}_p^{\times 3}] \), where \( \mathbb{Q}_p^{\times 3} = \{ x^3 | x \in \mathbb{Q}_p^\times \} \).

7. Prove in the following steps that every automorphism \( f \) of the field \( \mathbb{Q}_p \) is the identity map.

(a) Show that \( f \) is the identity map on \( \mathbb{Q} \).

(b) Let \( x \in \mathbb{Z}_p^\times \). Write \( f(x) = p^m z \) with \( z \in \mathbb{Z}_p^\times \) and an integer \( m \). Derive a contradiction if \( m \neq 0 \), by showing that there exists a rational integer \( b \), prime to \( p \), such that \( bx = u^m \) with \( u \in \mathbb{Z}_p^\times \) and a positive integer \( n > |m| \).

(c) Complete the proof by showing the continuity of \( f \).

7. Hensel’s lemma and its applications

In this section \( F \) is a field with a discrete order function \( \nu \); \( R \) denotes the valuation ring, and \( M \) its maximal ideal.

Lemma 7.1. Let \( a, b, c \in k[x] \), where \( k \) is a field and \( x \) is an indeterminate. If \( a \) and \( b \) are relatively prime and \( b \neq 0 \), then there exist elements \( u, v \in k[x] \) such that \( c = au + bv \) and \( \deg(u) < \deg(b) \).

Proof. Take \( u, v \) without the condition \( \deg(u) < \deg(b) \). We can put \( u = bq + u_1 \) with \( q, u_1 \in k[x] \) such that \( \deg(u_1) < \deg(b) \). Then \( c = au_1 + b(aq + v) \), and we have only to replace \( (u, v) \) by \( (u_1, aq + v) \).
Theorem 7.2 (Hensel’s lemma). Suppose $F$ is complete; put $k = R/M$. For $a \in R$ (resp. $a \in R[x]$) denote by $\bar{a}$ the residue class of $a$ modulo $M$ (resp. $M[x]$). Given $f \in R[x], \not\in M[x]$, suppose that $\bar{f} = g^* h^*$ with $g^*, h^* \in k[x]$ such that $(g^*, h^*) = 1$. Then there exist elements $g, h \in R[x]$ such that $f = gh, \bar{f} = g^*, \bar{h} = h^*$, and $\deg(g) = \deg(g^*)$.

Proof. Let $r = \deg(g^*), s = \deg(h^*), \text{ and } m = \deg(f)$. Clearly $r + s \leq m$. We construct inductively two sequences $\{g_i\}_{i=1}^{\infty} \text{ and } \{h_i\}_{i=1}^{\infty}$ in $R[x]$ so that

$$f \equiv g_nh_n, \quad g_{n+1} \equiv g_n, \quad h_{n+1} \equiv h_n \pmod{M^n[x]},$$

$$\deg(g_n) = r, \quad \deg(h_n) \leq m - r.$$  

First take $g_1, h_1$ so that $\bar{g}_1 = g^*, \bar{h}_1 = h^*, \deg(g_1) = r, \text{ and } \deg(h_1) = s$. Suppose $g_n, h_n$ are already defined; take any $c \in R$ so that $\nu(c) = n$. We can then put $f - g_nh_n = ct$ with $t \in R[x]$. Let $g_{n+1} = g_n + cu \text{ and } h_{n+1} = h_n + cv \text{ with } u, v \in R[x]$. Since $f - g_{n+1}h_{n+1} = c(t - uh_n - v g_n - cuv)$, we have to take $u, v \text{ so that } \bar{u}h^* + \bar{v}g^* = \bar{f}$. Since $(g^*, h^*) = 1,$ we can find such $u, v$. By Lemma 7.1 we can take them so that $\deg(u) < \deg(\bar{u}) < \deg(g) = r$ and $\deg(v) = \deg(\bar{v})$. Also $\deg(g_{n+1}) = r, \text{ and } \deg(v) + r = \deg(\bar{v}g^*) = \deg(\bar{f} - \bar{u}h^*) \leq m$. Thus $\deg(v) \leq m - r, \text{ and hence } \deg(h_{n+1}) \leq m - r$. We can therefore establish the desired sequences. Let $g = \lim_{n \to \infty} g_n \text{ and } h = \lim_{n \to \infty} h_n$. (These are meaningful, since the degrees of $g_n \text{ and } h_n$ are bounded.) Then we obtain the desired conclusion.

Lemma 7.3. If $F$ is complete and $R/M$ is a finite field with $q$ elements, then $R$ has a primitive $(q - 1)st$ root of unity. Moreover, its powers, together with 0, form a complete set of representatives for $R/M$.

Proof. Apply Hensel’s lemma to $f(x) = x^{q-1} - 1$.

Theorem 7.4. Suppose $F$ is complete; let $g(x) = a_0 + a_1x + \cdots + a_nx^n$ be an irreducible element of $F[x]$. Then

$$\text{Min}\{\nu(a_i) \mid 0 \leq i \leq n\} = \text{Min}\{\nu(a_0), \nu(a_n)\}.$$  

Proof. Assuming $\text{Min}\{\nu(a_i) \mid 0 \leq i \leq n\} < \text{Min}\{\nu(a_0), \nu(a_n)\}$, take the smallest $j$ such that $\nu(a_j) = \text{Min}\{\nu(a_i) \mid 0 \leq i \leq n\}$. Then $0 < j < n$ and $a_j^{-1}a_k \in M$ for $k < j$, and so $a_j^{-1}g \equiv x^j(1 + \cdots + c_nx^{n-j}) \pmod{M[x]}$ with $c_n \in R$. Applying Hensel’s lemma to $a_j^{-1}g$, we find that $g$ is reducible, a contradiction.

Corollary 7.5. Let $g(x) = x^n + b_1x^{n-1} + \cdots + b_n \in F[x]$; suppose $F$ is complete, $g$ is irreducible, and $b_n \in R$. Then $g \in R[x]$.

This is merely a special case of Theorem 7.4.
Before proceeding further, let us recall the notion of the trace and norm maps of a finite algebraic extension $K$ of a field $F$. To simplify our exposition, we consider only the case where $K$ is separable over $F$. Given such a $K$, we can find a Galois extension $M$ of $F$ containing $K$. Put $G = \text{Gal}(M/F)$ and $H = \text{Gal}(M/K)$. For $\alpha \in M$ and $\sigma \in G$ we denote by $\alpha^\sigma$ the image of $\alpha$ under $\sigma$. Thus $H = \{ \sigma \in G \mid \alpha^\sigma = \alpha \text{ for every } \alpha \in K \}$. Take a subset $R$ of $G$ so that $G = \bigsqcup_{\sigma \in R} H\sigma$. Then for $\alpha \in K$ we put

$$N_K/F(\alpha) = \prod_{\sigma \in R} \alpha^\sigma, \quad \text{Tr}_{K/F}(\alpha) = \sum_{\sigma \in R} \alpha^\sigma.$$  

We easily see that these are elements of $F$ determined independently of the choice of $M$ and also of $R$.

Clearly

$$N_K/F(\alpha \beta) = N_K/F(\alpha)N_K/F(\beta),$$

$$\text{Tr}_{K/F}(c \alpha + d \beta) = c\text{Tr}_{K/F}(\alpha) + d\text{Tr}_{K/F}(\beta)$$

for $\alpha, \beta \in K$ and $c, d \in F$.

7.7. The notation being as in §7.6, let $[K : F] = n$ and $R = \{ \sigma_1, \ldots, \sigma_n \}$. Thus $G = \bigsqcup_{i=1}^n H\sigma_i$. Given $n$ elements $\alpha_1, \ldots, \alpha_n$ of $K$, we put

$$D(\alpha_1, \ldots, \alpha_n) = \det \left[ \text{Tr}_{K/F}(\alpha_i \alpha_j) \right]_{i,j=1}^n,$$

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(A), \quad A = \begin{bmatrix}
\alpha_1^{\sigma_1} & \alpha_1^{\sigma_2} & \cdots & \alpha_1^{\sigma_n} \\
\alpha_2^{\sigma_1} & \cdots & \cdots & \cdots \\
\alpha_n^{\sigma_1} & \alpha_n^{\sigma_2} & \cdots & \alpha_n^{\sigma_n}
\end{bmatrix}.$$  

Then we have

$$\Delta(\alpha_1, \ldots, \alpha_n)^2 = D(\alpha_1, \ldots, \alpha_n),$$

$$\Delta(1, \xi, \ldots, \xi^{n-1}) = \prod_{i > j} (\xi^{\sigma_i} - \xi^{\sigma_j}) \quad (\xi \in K).$$

The last formula is well known. To prove (7.6), observe that the $(i, k)$-entry of $A^i A$ is $\sum_{j=1}^n \alpha_j^{\sigma_i} \alpha_k^{\sigma_j} = \text{Tr}_{K/F}(\alpha_i \alpha_k)$. Therefore $\det(A^i A) = D(\alpha_1, \ldots, \alpha_n)$, which gives (7.6). Take $\xi \in K$ such that $K = F(\xi)$, and take $\sigma_1 = 1$, so that $\xi^{\sigma_1} = \xi$. Put $f(x) = \prod_{i=1}^n (x - \xi^{\sigma_i})$. Then $f$ is the minimal polynomial of $\xi$ over $F$, and we easily see the

$$\Delta(1, \xi, \ldots, \xi^{n-1}) = (-1)^{n(n-1)/2} \prod_{i=1}^n f'(\xi)^{\sigma_i}$$

$$= (-1)^{n(n-1)/2} N_{K/F}[f'(\xi)].$$

Theorem 7.8. For a finite separable extension $K$ of $F$, the following assertions hold:
(i) We have $D(\alpha_1, \ldots, \alpha_n) \neq 0$ if $\{\alpha_i\}_{i=1}^n$ is an $F$-basis of $K$, and consequently the $F$-bilinear map $(\alpha, \beta) \mapsto \text{Tr}_{K/F}(\alpha \beta)$ of $K \times K$ into $F$ is nondegenerate.

(ii) Let $L$ be a finite algebraic extension of $K$. Then, for every $\alpha \in L$,
$$N_{L/F}(\alpha) = N_{K/F}(N_{L/K}(\alpha)) \quad \text{and} \quad \text{Tr}_{L/F}(\alpha) = \text{Tr}_{K/F}(\text{Tr}_{L/K}(\alpha)).$$

(iii) Let the notation be as in (7.1), and for a fixed $\alpha \in K$ let $g(x)$ be the minimal polynomial of $\alpha$ over $F$. Then $\prod_{\sigma \in R}(x - \alpha^\sigma) = g(x)^k$, where $k = [K : F(\alpha)]$.

(iv) For $\alpha \in K$ let $\rho(\alpha)$ denote the $F$-linear endomorphism $\xi \mapsto \alpha \xi$ of $K$ as a vector space over $F$. Then $N_{K/F}(\alpha) = \det[\rho(\alpha)]$ and $\text{Tr}_{K/F}(\alpha) = \text{tr}[\rho(\alpha)]$.

**Proof.** We prove here only (i), (iii), and (iv), as (ii) is an easy exercise. Our first task is to show that $\det[\text{Tr}_{K/F}(\alpha_i \alpha_j)]_{i,j=1}^n \neq 0$ for an $F$-basis $\{\alpha_i\}_{i=1}^n$ of $K$. Take an element $\xi$ of $K$ so that $K = F(\xi)$. Then $\{\xi^\nu\}_{\nu=0}^{n-1}$ is an $F$-basis of $K$, and the desired fact follows from (7.6) and (7.7). Assertion (i) follows also from a well known fact that any finite number of distinct homomorphisms of a group into $F^\times$ are linearly independent over $F$. To prove (iii), take $M$ and $G$ as in §7.6; let $J = \text{Gal}(M/F(\alpha))$. If $\sigma$ runs over $R$, then we see that $\alpha^\sigma$ runs over the conjugates of $\alpha$ over $F$ exactly $[J : H]$ times. Assertion (iii) follows from this fact immediately. The notation being as in (iv), we easily see that $g(x)$ is the minimal polynomial of $\rho(\alpha)$, since $\alpha \mapsto \rho(\alpha)$ is injective. Let $f(x)$ be the characteristic polynomial of $\rho(\alpha)$. It is well known that $f$ divides the power of $g$. Since $g$ is irreducible and $f$ is of degree $[K : F]$, we see that $f = g^k$. Thus $f(x) = \prod_{\sigma \in R}(x - \alpha^\sigma)$, from which we obtain (iv).

8. Integral elements in algebraic extensions

In this section $F$ is the field of quotients of an integral domain $R$.

8.1. Let $\alpha$ be an element of an algebraic extension $L$ of $F$. We call $\alpha$ integral over $R$ if

$$(8.1) \quad \alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0$$

with $c_i \in R$ and $n > 0$. Let $\xi \in L$. Then $\xi^m + b_1\xi^{m-1} + \cdots + b_m = 0$ with some $b_i \in F$ and $m > 0$. We can find a nonzero element $a$ of $R$ such that $ab_i \in R$ for all $i$. Then $(a\xi)^m + a\xi(b_1\xi^{m-1} + \cdots + a^mb_m = 0$, and so $a\xi$ is integral over $R$. Thus any element of $L$ times a suitable nonzero element of $R$ is integral over $R$. The set of all the elements of $L$ integral over $R$ is called the integral closure of $R$ in $L$. We call $R$ integrally closed if every element of $F$ integral over $R$ is contained in $R$. 
Lemma 8.2. Let $R$ be a unique factorization domain. Then $R$ is integrally closed, and more generally the polynomial ring $R[x_1, \ldots, x_n]$ with independent indeterminates $x_1, \ldots, x_n$ is integrally closed. In particular, a principal ideal domain is integrally closed.

Proof. Let $\alpha = a/b$ with relatively prime elements $a$ and $b$ of $R$; suppose (8.1) holds with $c_i \in R$. Then $a^n = -b(c_1a^{n-1} + \cdots + c_nb^{n-1})$. This is a contradiction if $b \notin R^\times$, and so $b \in R^\times$. Thus $\alpha \in R$, which means that $R$ is integrally closed. By Theorem 1.2, any principal ideal domain and $R[x_1, \ldots, x_n]$ are unique factorization domains. Thus we obtain our lemma.

Lemma 8.3. Let $\alpha$ be an element of an algebraic extension $L$ of $F$. Then $\alpha$ is integral over $R$ if and only if $\alpha$ is contained in a subring of $L$ that is a finitely generated $R$-module.

Proof. If (8.1) is satisfied with $c_i \in R$, then $\alpha^m = -\sum_{i=1}^{n} c_i \alpha^{m-i}$ for $m \geq n$, and so we can show inductively that every power of $\alpha$ belongs to $\sum_{i=0}^{n-1} R\alpha^i$, and so $R[\alpha] = \sum_{i=0}^{n-1} R\alpha^i$. Conversely, suppose $\alpha \in B$ with a subring $B$ of the form $B = \sum_{i=1}^{k} R\beta_i$ of $L$. Then $\alpha \beta_i = \sum_{j=1}^{k} c_{ij} \beta_j$ with $c_{ij} \in R$, and so the matrix $\alpha 1_k - (c_{ij})$ annihilates the vector $(\beta_i)$. If $\alpha \neq 0$, then $(\beta_i) \neq 0$, so that $\text{det}[\alpha 1_k - (c_{ij})] = 0$, which is an equation of the form (8.1), and so $\alpha$ is integral over $R$.

Lemma 8.4. Let $\alpha, \beta$ be elements of an algebraic extension $L$ of $F$, integral over $R$. Then $\alpha \pm \beta$ and $\alpha \beta$ are integral over $R$. Consequently the integral closure of $R$ in $L$ is a subring of $L$. Moreover, $L$ is its field of quotients.

Proof. We have $R[\alpha] = R + R\alpha + \cdots + R\alpha^{n-1}$ and $R[\beta] = R + R\beta + \cdots + R\beta^{m-1}$ with some $n$ and $m$. Then $R[\alpha, \beta] = \sum_{i<n} \sum_{j<n} R\alpha^i \beta^j$, and this ring contains $\alpha \pm \beta$ and $\alpha \beta$. Therefore by Lemma 8.3, those elements are integral over $R$. Also every element of $L$ times a suitable nonzero element of $R$ is integral over $R$. Thus we obtain our proposition.

Lemma 8.5. Let $L$ be as above, and $B$ a subring of $L$ containing $R$; let $\alpha \in L$. If $\alpha$ is integral over $B$ and every element of $B$ is integral over $R$, then $\alpha$ is integral over $R$. Consequently the integral closure of $R$ in $L$ is integrally closed.

Proof. Take (8.1) with $c_i \in B$. Since the $c_i$ are integral over $R$, the same technique as in the proof of Lemma 8.4 shows that $R[c_1, \ldots, c_n] = \sum_{j=1}^{m} Rd_j$ with some $d_j$. Then $R[c_1, \ldots, c_n, \alpha] = \sum_{k=1}^{n} \sum_{j=1}^{m} R\alpha^k d_j$, and so by Lemma 8.3, $\alpha$ is integral over $R$. Thus we obtain our lemma.

Theorem 8.6. Suppose $R$ is integrally closed; let $f(x) \in R[x]$ and $f = gh$ with monic $g$ and $h$ in $F[x]$. Then both $g$ and $h$ belong to $R[x]$.
Let $g(x) = \prod_i (x - \alpha_i)$ in an extension of $F$. Then the $\alpha_i$ are integral over $R$ and so the coefficients of $g$, being the elementary symmetric functions of the $\alpha_i$, are integral over $R$. Since they belong to $F$ and $R$ is integrally closed, they belong to $R$.

As an immediate consequence of this theorem we obtain

**Corollary 8.7.** Suppose $R$ is integrally closed; let $\alpha$ be an element of an extension of $F$ integral over $R$. Then the minimal polynomial of $\alpha$ over $F$ has coefficients in $R$.

**Lemma 8.8.** Suppose $R$ is integrally closed; let $K$ be a separable extension of $F$ of degree $n$, and $B$ the integral closure of $R$ in $K$. Then $\text{Tr}_{K/F}$ and $N_{K/F}$ maps $B$ into $R$. Moreover, if $R$ is a principal ideal domain, then $B$ is a free $R$-module of rank $n$.

**Proof.** If $\alpha \in B$, then $\alpha^\sigma$ of (7.1) also belongs to $B$, and so $\text{Tr}_{K/F}(\alpha)$ and $N_{K/F}(\alpha)$ are integral over $R$. This proves the first assertion, since $R$ is integrally closed. Let $\{\xi_i\}_{i=1}^n$ be an $F$-basis of $K$. Changing this for $\{c\xi_i\}_{i=1}^n$ with a suitable $c \in R$, we may assume that $\xi_i \in B$. Let $\alpha \in B$. Put $\alpha = \sum_i b_i \xi_i$ with $b_i \in F$. Then $\sum_{i=1}^n b_i \text{Tr}_{K/F}(\xi_i \xi_j) = \text{Tr}_{K/F}(\alpha \xi_j) \in R$ for every $j$. Put $d = \det (\text{Tr}_{K/F}(\xi_i \xi_j))$. Since $\text{Tr}_{K/F}(\xi_i \xi_j) \in R$, we see that $b_j \in d^{-1} R$. Therefore $B \subset d^{-1} \sum_{i=1}^n R \xi_i$. By Theorem 5.1, $B$ is a free $R$-module of finite rank; the rank must be $n$, since $\xi_i \in B$.

8.9. Let $\overline{Q}$ denote the algebraic closure of $Q$ in $C$. An element of $\overline{Q}$ integral over $Z$ is called an algebraic integer. A subfield $K$ of $\overline{Q}$ is called an algebraic number field. In general $[K : Q]$ may be infinite. In this book, however, whenever we speak of an algebraic number field, we always assume that it is of finite degree over $Q$.

If $K$ is an algebraic number field, the ring of all algebraic integers in $K$ (that is, the integral closure of $Z$ in $K$) is traditionally called the maximal order of $K$. We denote it by $J_K$. By Lemma 8.8, $J_K$ is a free $Z$-module of rank $[K : Q]$. We have

$$J_K^\times = \{\alpha \in J_K \mid N_{K/Q}(\alpha) = \pm 1\}.$$  

To prove this, take the Galois closure $L$ of $K$ over $Q$. Let $\alpha \in J_K$. Then $\alpha^\sigma \in J_L$ for every $\sigma \in \text{Gal}(L/Q)$, and so by (7.1), $N_{K/Q}(\alpha) = \alpha \beta$ with $\beta \in J_L$. If $N_{K/Q}(\alpha) = \pm 1$, then $\alpha^{-1} = \pm \beta \in J_L \cap K = J_K$, and so $\alpha \in J_K^\times$. Conversely, if $\alpha \in J_K^\times$, then $\beta \in J_L^\times$, and so $N_{K/Q}(\alpha) \in J_L^\times \cap Q = J_L^\times \cap Z = \{\pm 1\}$. Thus $N_{K/Q}(\alpha) = \pm 1$, and we obtain (8.2).

9. Order functions in algebraic extensions

In this section $F$ is a field with a discrete order function $\nu$; $R$ denotes the valuation ring, and $M$ its maximal ideal; we put $k = R/M$.
9.1. Let $K$ be a finite algebraic extension of $F$, and $\mu$ an order function of $K$ that coincides with $cv$ on $F$ with a positive real constant $c$. Let $R'$ be the valuation ring of $\mu$ and $M'$ its maximal ideal. Clearly $R = R' \cap F$ and $M = M' \cap F$. Put $k' = R'/M'$. then $k$ can be viewed as a subfield of $k'$. We put

$$f(\mu/\nu) = [k' : k], \quad e(\mu/\nu) = [\mu(K^\times) : cv(F^\times)].$$

These are called the residue class degree of $\mu$ over $\nu$ and the ramification index of $\mu$ over $\nu$. We are going to show that they are finite. The finiteness implies that $\mu$ is discrete if $\nu$ is discrete.

We say that $\nu$ is ramified (resp. unramified) in $K$ if $e(\mu/\nu) > 1$ for some $\mu$ that extends $\nu$ to $K$ (resp. if $e(\mu/\nu) = 1$ for every $\mu$ that extends $\nu$ to $K$).

If $L$ is a finite algebraic extension of $K$ and $\lambda$ is an order function of $L$ that coincides with a constant multiple of $\mu$ on $K$, then clearly

$$e(\lambda/\nu) = e(\lambda/\mu)e(\mu/\nu), \quad f(\lambda/\nu) = f(\lambda/\mu)f(\mu/\nu).$$

**Lemma 9.2.** For $\alpha \in R'$ let $\overline{\alpha}$ denote its residue class modulo $M'$. Let $\alpha_1, \ldots, \alpha_m \in R'$. If $\overline{\alpha}_1, \ldots, \overline{\alpha}_m$ are linearly independent over $k$, then $\alpha_1, \ldots, \alpha_m$ are linearly independent over $F$, and

$$\mu(c_1\alpha_1 + \cdots + c_m\alpha_m) = \text{Min}(\nu(c_1), \ldots, \nu(c_m))$$

for $c_i \in F$.

**Proof.** Take $m$ elements $c_i$ of $F$; suppose at least one of them is nonzero.
Let $\nu(c_j) = \text{Min}(\nu(c_1), \ldots, \nu(c_m))$. Then $c_j \neq 0$. Put $b_i = c_j^{-1}c_i$. Then $b_i \in R$ and $\sum_i b_i\overline{\alpha}_i \neq 0$, since $b_j = 1$. Thus $\mu(\sum_i b_i\alpha_i) = 0$, and so $\mu(\sum_i c_i\alpha_i) = \nu(c_j) < \infty$, which gives $(\ast)$. Therefore $\sum_i c_i\alpha_i \neq 0$, which proves the linear independence of the $\alpha_i$.

**Theorem 9.3.** $[K : F] \geq e(\mu/\nu)f(\mu/\nu)$.

**Proof.** For simplicity we assume that $\mu = \nu$ on $F$. Take $\alpha_1, \ldots, \alpha_m \in R'$ so that $\overline{\alpha}_1, \ldots, \overline{\alpha}_m$ are linearly independent over $k$; take $y_1, \ldots, y_t \in K^\times$ so that the cosets $\nu(F^\times) + \mu(y_t)$ for $1 \leq i \leq t$ form a disjoint union in $\mu(K^\times)$. Suppose $\sum_{i,j} c_{ij}\alpha_i y_j = 0$ with some $c_{ij} \in F$. Put $b_j = \sum_i c_{ij}\alpha_i$. Then $\sum_j b_jy_j = 0$. If $b_j \neq 0$, then by Lemma 9.2, $\mu(b_j) = \text{Min}(\nu(c_{1j}), \ldots, \nu(c_{mj})) \in \nu(F^\times)$, so that $\mu(b_j y_j) \in \nu(F^\times) + \mu(y_j)$. Thus the $\mu(b_j y_j)$ for all $j$ such that $b_j \neq 0$ are all different, and so $\sum_j b_jy_j \neq 0$, a contradiction. Therefore $b_j = 0$ for all $j$, that is, $\sum_i c_{ij}\alpha_i = 0$ for all $j$. Since the $\alpha_i$ are linearly independent over $F$, we obtain $c_{ij} = 0$ for all $i$ and $j$, which means that the $\alpha_i y_j$ are linearly independent over $F$, and hence $mt \leq [K : F]$.

From this proof we immediately obtain
Corollary 9.4. Suppose $\mu = \nu$ on $F$ and $[K : F] = e(\mu/\nu)f(\mu/\nu)$; take $\alpha_1, \ldots, \alpha_f \in R'$ so that $\bar{\alpha}_1, \ldots, \bar{\alpha}_f$ form a $k$-basis of $k'$ and take $y_1, \ldots, y_e \in K^\times$ so that $\mu(K^\times) = \bigcup_{j=1}^e (\nu(F^\times) + \mu(y_j))$. Then the $\alpha_iy_j$ for $1 \leq i \leq f$ and $1 \leq j \leq e$ form an $F$-basis of $K$.

Theorem 9.5. Suppose $F$ is complete; let $K$ be a finite (separable or inseparable) algebraic extension of $F$. Then

1. $\nu$ can be uniquely extended to an order function $\mu$ of $K$.
2. $\mu$ is discrete.
3. $K$ is complete with respect to $\mu$.
4. $[K : F] = e(\mu/\nu)f(\mu/\nu)$.
5. Let $R'$ be the valuation ring of $\mu$. Then $R'$ is the integral closure of $R$ in $K$ and $R'$ is a free $R$-module of rank $[K : F]$.
6. Let $b$ be an element of $K$ such that $\mu(b) > 0$ and let $h_b(x) = x^m + \sum_{i=0}^{m-1} c_i x^i$ be the minimal polynomial for $b$ over $F$. Then $\nu(c_i) > 0$ for every $i$.

Proof. Put $n = [K : F]$ and $\mu(a) = n^{-1}\nu(N_{K/F}(a))$ for every $a \in K^\times$; put $\mu(0) = \infty$. Clearly $\mu = \nu$ on $F$ and $\mu(ab) = \mu(a) + \mu(b)$. For a fixed $a \in K^\times$ let $g$ be the minimal polynomial of $a$ over $F$, $d = \deg(g)$, and $c$ the constant term of $g$. Then by Theorem 7.8(iii), $N_{K/F}(a) = \pm c^n/d$, and so $\mu(a) = d^{-1}\nu(c)$. Let us now prove

$$\mu(a) \geq 0 \implies \mu(1 + a) \geq 0.$$  

If $\mu(a) \geq 0$, then $\nu(c) \geq 0$, and so $g \in R[x]$ by Corollary 7.5. Thus $a$ is integral over $R$. In addition, $1 + a$ is a root of the polynomial $h(x) = g(x - 1)$, whose constant term, say $c'$, belongs to $R$. Therefore $\mu(1 + a) = d^{-1}\nu(c') \geq 0$, which proves (*). If $x, y \in K$ and $\mu(x) \geq \mu(y), y \neq 0$, then $\mu(x/y) \geq 0$; hence $\mu(x + y) = \mu(y) + \mu(1 + (x/y)) \geq \mu(y)$ by (*). Therefore $\mu$ is an order function of $K$. (It satisfies condition (iv) of §6.1, since $\mu = \nu$ on $F$.) Clearly it is discrete.

To prove the uniqueness of $\mu$ and (5), let $\lambda$ be an extension of $\nu$ to $K$ and let $R^*$ be the integral closure of $R$ in $K$; let $R'$ resp. $R''$ be the valuation ring of $\mu$ resp. $\lambda$, and $M'$ resp. $M''$ the maximal ideal of $R'$ resp. $R''$. We have seen that $R' \subset R^*$. Now, if $\alpha \in R^*$, then $\alpha^m + c_1 \alpha^{m-1} + \cdots + c_m = 0$ with some $c_i \in R$. If $\lambda(\alpha) < 0$, then $\alpha \neq 0$ and $1 = -c_1 \alpha^{m-1} - \cdots - c_m \alpha^{-m}$, and hence $\lambda(1) > 0$, a contradiction. Thus $\lambda(\alpha) \geq 0$. This shows that $R^* \subset R''$. Taking $\mu$ as $\lambda$, we find that $R^* = R'$. Suppose $R' \neq R''$; then $R''$ has an element $y$ such that $\mu(y) < 0$. We easily see that $K = \bigcup_{k=0}^{\infty} y^k R' \subset R''$, which is impossible. Therefore $R' = R''$, and $M' = M''$, since the valuation ring has a unique maximal ideal. Take $\pi \in R'$ so that $M' = \pi R'$. Clearly $\lambda(a) = \mu(a) = 0$ if $a \in (R')^\times$. If $a \in \pi^r(R')^\times$ and $r \neq 0$, then $\lambda(a)/\mu(a) =$
\[ r\lambda(\pi)/[r\mu(\pi)] = \lambda(\pi)/\mu(\pi). \]  
Thus \( \lambda/\mu \) is a constant on the set of all such \( a \)'s, which must be 1, since \( \lambda = \mu \) on \( F \).

Put \( e = e(\mu/\nu) \) and \( f = f(\mu/\nu) \). Then \( ef \leq n \) by Theorem 9.3. To prove the remaining part of our theorem, we may assume that \( \mu(K^\times) = \mathbb{Z} \); then \( \nu(F^\times) = e\mathbb{Z} \).

Take a complete set of representatives \( S \) for \( k = R/M \) including 0; take also \( \alpha_1, \ldots, \alpha_f \in R' \) so that \( \overline{\alpha}_1, \ldots, \overline{\alpha}_f \) form a \( k \)-basis of \( R'/M' \). Let \( T \) be the set of all linear combinations \( \sum_{i=1}^f s_i \alpha_i \) with \( s_i \in S \). We easily see that \( T \) gives a complete set of representatives for \( R'/M' \). Let \( \pi \) resp. \( \tau \) be a prime element of \( R' \) resp. \( R \) for \( 0 < m \in \mathbb{Z} \) we put \( \pi_m = \pi^i \tau^j \) with nonnegative integers \( i \) and \( j \) such that \( i < e \) and \( m = ej+i \). Then, \( \mu(\pi_m) = m \), and given \( a \in R' \), by the same argument as in the proof of Theorem 6.8(iv), we can find \( \{t_m\}_{m=0}^{\infty} \subset T \) such that \( a - \sum_{m=0}^N t_m \pi_m \in (M')^{N+1} \) for every \( N \in \mathbb{Z}, > 0 \). This can be written in the form \( a - \sum_{i=0}^{e-1} \sum_{j=0}^{N-1} t_{ij} \pi_i \tau^j \in (M')^r \) with \( t_{ij} \in T \) for \( 0 < r \in \mathbb{Z} \). We have \( t_{ij} = \sum_{h=1}^f s_{hij} \alpha_h \) with \( s_{hij} \in S \). Put \( b_{hi} = \sum_{j=0}^f s_{hij} \tau^j \). This is meaningful as an element of \( F \), since \( F \) is complete. Then \( a - \sum_{i=0}^{e-1} \sum_{h=1}^f b_{hi} \pi^i \alpha_h \in (M')^r \) for every \( r \in \mathbb{Z}, > 0 \), and so \( a = \sum_{i=0}^{e-1} \sum_{h=1}^f b_{hi} \pi^i \alpha_h \). This shows that \( R' = \sum_{i=0}^{e-1} \sum_{h=1}^f R \pi^i \alpha_h \) and consequently \( K = \sum_{i=0}^{e-1} \sum_{h=1}^f F \pi^i \alpha_h \). Since \( ef \leq n = [K:F] \), we see that the elements \( \pi^i \alpha_h \) form an \( F \)-basis of \( K \) and \( ef = n \); also \( R' \) is a free \( R \)-module of rank \( n \).

To prove that \( K \) is complete, we first note that if \( a = \sum_{h,i} b_{hi} \pi^i \alpha_h \) with \( b_{hi} \in F \), then

\[ \mu(a) \geq re \implies \nu(b_{hi}) \geq r. \]

Indeed, if \( \mu(a) \geq re \), then \( \sum_{h,i} \tau^{-r} b_{hi} \pi^i \alpha_h = \tau^{-r}a \in R' \), and so \( \tau^{-r}b_{hi} \in R \), which proves (**). Now let \( \{a_m\}_{m=1}^{\infty} \) be a Cauchy sequence in \( K \). Put \( a_m = \sum_{h,i} b_{mhi} \pi^i \alpha_h \) with \( b_{mhi} \in F \). By (** \( \forall \)) we easily see that \( \{b_{mhi}\}_{m=1}^{\infty} \) is a Cauchy sequence in \( F \) for every \( (h,i), \) and therefore convergent. Thus we obtain the desired convergence of \( \{a_m\} \), which proves (3). Let \( b \) and \( h_b \) be as in (6). Take the smallest normal extension \( L \) of \( F \) containing \( K \) and \( h \). Then \( h_b(x) = \prod_{i=1}^m (x - \beta_i) \) with \( \beta_i \in L \). For each fixed \( i \) there exists an isomorphism \( \sigma \) of \( F(b) \) onto \( F(\beta_i) \) over \( F \) such that \( b^\sigma = \beta_i \). This \( \sigma \) can be extended to an automorphism of \( L \) over \( F \). Applying (1) to \( L \), we can extend \( \mu \) uniquely to an order function \( \lambda \) of \( L \). The uniqueness shows that \( \lambda(a^\sigma) = \lambda(a) \) for every \( a \in L \), and so \( \lambda(\beta_i) = \lambda(b) = \mu(b) > 0 \). This is so for every \( i \), and the conclusion of (6) follows from this fact. This completes the proof of our theorem.

Since \( \mu \) is unique, we often write \( e(K/F) \) and \( f(K/F) \) for \( e(\mu/\nu) \) and \( f(\mu/\nu) \). We say that \( K \) is ramified, totally ramified, or unramified over \( F \) according as \( e(K/F) > 1, e(K/F) = [K:F], \) or \( e(K/F) = 1 \).
Corollary 9.6. If $K$ is a finite algebraic extension of $F$, then $\nu$ can be extended to an order function of $K$ (even if $F$ is not complete).

**Proof.** We have $K = F(\alpha_1, \ldots, \alpha_m)$ with some $\alpha_i$, and so it is sufficient to prove the case $K = F(\alpha)$ with a single element $\alpha$. Take an irreducible polynomial $g(x)$ in $F[x]$ such that $g(\alpha) = 0$. Let $F^*$ be the $\nu$-completion of $F$. Take an extension $F^*(\beta)$ with a root of $g$ considered over $F^*$. The above theorem guarantees an extension of $\nu$ to $F^*(\beta)$. Since $F(\alpha)$ is isomorphic to the subfield $F(\beta)$ of $F^*(\beta)$, we obtain our assertion for such a $K$.

**Theorem 9.7.** Suppose $F$ is complete and $k$ is a finite field with $q$ elements; let $L$ be a finite algebraic extension of $F$, and let $f = f(L/F)$. Then the following assertions hold:

(i) There is an extension $K$ of $F$ contained in $L$ such that $e(K/F) = 1$ and $[K : F] = f(K/F) = f$. (Consequently $f(L/K) = 1$ and $e(L/K) = e(L/F)$.)

(ii) Every unramified extension of $F$ contained in $L$ is contained in $K$. Consequently $K$ is uniquely determined by property (i).

(iii) $K = F(\gamma)$ with a root of unity $\gamma$ of order $q^f - 1$, where $q$ is the number of elements of $k$.

**Proof.** We first recall that for every positive integer $n$, $k$ has a unique extension of degree $n$, which is generated by a root of unity of order $q^n - 1$; see §1.9. Now put $m = q^f - 1$. By Lemma 7.3, $L$ contains a root of unity $\gamma$ of order $m$. Let $K = F(\gamma)$ and let $k_0$ (resp. $k_1$) be the valuation ring of $K$ (resp. $L$) modulo its maximal ideal. Since $\mathfrak{m}$, the residue class of $\gamma$, is contained in $k_0$, the last part of Theorem 7.2 shows that $\mathfrak{m}$ is of order $m$, and $k_0 = k_1$. This shows that $f(K/F) = f$. Let $g(x)$ be the minimal polynomial of $\gamma$ over $F$. Then $\overline{g}$ divides $x^m - 1$, and so has no multiple root. Therefore Hensel’s lemma shows that $\overline{g}$ is irreducible over $k$. Thus $[K : F] = \deg(g) = \deg(\overline{g}) = f$, as $\overline{\gamma}$ is of order $m$. This proves (i). Since $e(K/F)f(K/F) = [K : F]$, we obtain $e(K/F) = 1$. Notice that $L = K$ if $L$ is unramified over $F$. Now let $H$ be an unramified extension of $F$ contained in $L$; let $h = f(H/F)$. Take $H$ in place of $L$. Then $H$ is generated over $F$ by a root of unity of order $q^h - 1$. Since $h|f$, that root of unity is a power of $\gamma$, and so $H \subset K$. This proves (ii). Once we know the uniqueness of $K$, then (iii) is included in the first part of our proof.

**Theorem 9.8.** Suppose $F$ is complete; let $\overline{F}$ be an algebraic closure of $F$; let $q$ be the number of elements in $k$. Then the following assertions hold:

(i) For every positive integer $n$, $\overline{F}$ contains a unique unramified extension of $F$ of degree $n$.

(ii) Such an extension is cyclic over $F$ and generated by a primitive $m$-th root of unity, where $m = q^n - 1$. 
Proof. Let $K$ be the splitting field of $x^m - 1$ over $F$ contained in $\tilde{F}$ with $m$ as above. Observe that the characteristic of $F$ is either $0$ or the prime number that divides $q$. Since $x^m - 1$ has no multiple root, we have $K = F(\alpha)$ with a primitive $m$-th root of unity $\alpha$. Then $x^m - 1 = \prod_{i=0}^{m-1} (x - \alpha^i)$. Let $g$ be the minimal polynomial of $\alpha$ over $F$. Repeating the last part of the proof of Theorem 9.7, we see that $\overline{g}$ is irreducible. Now $x^m - 1 = \prod_{i=0}^{m-1} (x - \overline{\alpha}^i)$ in the residue field, and since $x^m - 1$ is a separable polynomial over $k$, we see that $\overline{\alpha}$ is of order $m$. Therefore the first statement of the proof of Theorem 9.7 shows that $n = \deg(\overline{g}) = \deg(g) = [K : F]$. Then clearly $n = f(K/F)$, and so $e(K/F) = 1$. To prove the uniqueness, take an unramified extension $L$ of $F$ of degree $n$. By Theorem 9.7(i, iii), $L$ is generated by a root of unity of order $m$, and so must coincide with the above $K$.

In the setting of the above proof let $G = \text{Gal}(K/F)$. Then $g(x) = \prod_{\sigma \in G} (x - \alpha^\sigma)$. Since the extension of the order function of $F$ to $K$ is unique by Theorem 9.5, we see that every $\sigma \in G$ sends $R_K$ and $M_K$ onto themselves, and so $\sigma$ induces an automorphism of $R_K/M_K$, which we denote by $\overline{\sigma}$. We have then $\overline{g}(x) = \prod_{\sigma \in G} (x - (\overline{\alpha})^\sigma)$. Since $\overline{g}$ is irreducible, this means that $\text{Gal}(\kappa/\phi) = \{ \overline{\sigma} \mid \sigma \in G \}$, where $\kappa = R_K/M_K$ and $\phi = R_F/M_F$. Therefore $\sigma \mapsto \overline{\sigma}$ gives an isomorphism of $\text{Gal}(K/F)$ onto $\text{Gal}(\kappa/\phi)$, and we easily see that

\begin{equation}
N_{\kappa/\phi}(\overline{a}) = \overline{N_{K/F}(a)} \quad \text{and} \quad \text{Tr}_{\kappa/\phi}(\overline{a}) = \overline{\text{Tr}_{K/F}(a)} \quad (a \in R_K).
\end{equation}

**Theorem 9.9.** Suppose $F$ is complete; let $K$ be a finite algebraic extension of $F$.

(i) If $K$ is unramified over $F$, then $R_K = R_F[\gamma]$ with a root of unity $\gamma$ as in Theorem 9.7(iii).

(ii) If $K$ is totally ramified over $F$, then $R_K = R_F[\pi]$ with any prime element $\pi$ of $K$.

Proof. Our assertions are special cases of the formula $R_K = \sum_{i,j} R_F \alpha_i \pi^j$ shown in the proof of Theorem 9.5.

**Theorem 9.10.** Let $F$ be a finite algebraic extension of $\mathbb{Q}_p$. Then the following assertions hold:

(i) If $K$ is an abelian extension of $F$ of degree $n$, then $[F^\times : N_{K/F}(K^\times)] = n$.

(ii) In particular, if $K$ is unramified over $F$, then $N_{K/F}(R_K^\times) = R_F^\times$, and $F^\times/N_{K/F}(K^\times)$ is generated by the coset represented by a prime element of $F$.

(iii) Let $\tilde{F}$ be an algebraic closure of $F$. Then, assigning $N_{K/F}(K^\times)$ to every finite abelian extension $K$ of $F$ contained in $\tilde{F}$, we obtain a bijection of the set of such $K$ onto the set of all subgroups of $F^\times$ of finite index.
Proof. These are basic facts in local class field theory, which was first presented by Chevalley in [C]. Here we prove (ii) as stated; we prove (i) only in the following two cases: (a) \( K \) is unramified over \( F \); (b) \([K : F] = 2\). The latter case will be proven in Theorem 21.15. As for (iii), we will prove it only when \( F = \mathbb{Q}_p \) and \( n = 2 \). We first discuss (ii) by considering an unramified extension \( K \) of \( F \). Take any prime element \( \pi \) of \( F \) and let \( G = \text{Gal}(K/F) \). Then for every \( b \in R_K \) and \( 0 < a \in \mathbb{Z} \) we have \( N_{K/F}(1 + \pi^a b) = 1 + \pi^a \text{Tr}_{K/F}(b) + \pi^{a+1} c \) with \( c \in R_K \). Clearly \( c \in R_F \), and so \( N_{K/F}(1 + \pi^a b) \equiv 1 + \pi^a \text{Tr}_{K/F}(b) \pmod{M_F^{a+1}} \). Given \( 1 + \pi^a \beta \) with \( \beta \in R_F \), we can find, in view of (9.1), an element \( b \in R_K \) such that \( \text{Tr}_{K/F}(b) - \beta \in M_F \), as \( \text{Tr}_{K/F}(\kappa) = \varphi \), where \( \kappa = R_K/M_K \) and \( \varphi = R_F/M_F \). Then \( N_{K/F}(1 + a + \pi^a b) \equiv 1 + \pi^a \beta \pmod{M_F^{a+1}} \). Applying the same procedure to \( (1 + \pi^a \beta)^{-1} N_{K/F}(1 + \pi^a b) \) with \( a + 1 \) in place of \( a \), we eventually find that \( N_{K/F}(1 + M_K) = 1 + M_F \). Since \( N_{K/F}(\kappa^R) = \varphi^R \), given \( \gamma \in R_K^R \), we can find an element \( \varepsilon \in R_K^R \) such that \( N_{K/F}(\varepsilon) = \gamma \), that is, \( \gamma N_{K/F}(\varepsilon)^{-1} \in 1 + M_F \). Thus \( \gamma \in (1 + M_F) N_{K/F}(R_K) \subseteq N_{K/F}(R_K^R) \), and so \( R_K^R = N_{K/F}(R_K^R) \). Since \( K^R = \bigcup_{h \in \mathbb{Z}} \pi^n h R_K^R \), we have \( N_{K/F}(K^R) = \bigcup_{h \in \mathbb{Z}} \pi^n h R_F^R \), which shows that \( [F^R : N_{K/F}(K^R)] = n \).

Next suppose \( F = \mathbb{Q}_p \) and \( n = 2 \). In Theorem 6.12 we enumerated all quadratic extensions \( K \) of \( F \). For each \( p \) there exists a unique unramified quadratic extension by Theorem 9.8. We have to consider only the case in which \( K \) is ramified over \( F \), as the unramified case has been proved in general. We first treat the case \( p \neq 2 \). By Theorem 6.12(ii) we see that \( K = \mathbb{Q}_p(\sqrt{p}) \) or \( K = \mathbb{Q}_p(\sqrt{\rho p}) \), where \( r \) is a quadratic nonresidue, and \( R_K = \mathbb{Z}_p[\sqrt{p}] \) or \( R_K = \mathbb{Z}_p[\sqrt{\rho p}] \) accordingly by Theorem 9.9(ii). For simplicity let us write \( R \) and \( N \) for \( R_K \) and \( N_{K/F} \). If \( a + b \sqrt{p} \in R^R \) with \( a, b \in \mathbb{Z}_p \), then \( a \in \mathbb{Z}_p^R \), and \( N(a + b \sqrt{p}) = a^2 - b^2 p \equiv a^2 \pmod{p \mathbb{Z}_p} \). This combined with Lemma 6.11(i) shows that \( N(R^R) = \mathbb{Z}_p^{x^2} \). Since \( -p = N(\sqrt{p}) \), we obtain the first of the following two formulas:

\[
N(K^R) = \{ (-p)^m \mid m \in \mathbb{Z} \} \cdot \mathbb{Z}_p^{x^2} \quad \text{if } K = \mathbb{Q}_p(\sqrt{p}), \quad p \neq 2,
\]

\[
N(K^R) = \{ (-rp)^m \mid m \in \mathbb{Z} \} \cdot \mathbb{Z}_p^{x^2} \quad \text{if } K = \mathbb{Q}_p(\sqrt{\rho p}), \quad p \neq 2.
\]

Here \( r \) is a quadratic nonresidue modulo \( p \). The latter formula can be shown by the same argument. We thus obtain \([\mathbb{Q}_p^R : N(K^R)] = 2 \) in both cases. In the unramified case we have \( N(K^R) = \bigcup_{m \in \mathbb{Z}} p^{2m} \mathbb{Z}_p^R \). Therefore \( N(K^R) \) determines \( K \) when \( p \neq 2 \).

Next suppose \( p = 2 \). There are seven quadratic extensions of \( \mathbb{Q}_2 \) as listed in Theorem 6.12(ii). Let \( \zeta = (-1 + \sqrt{-3})/2 \). Then \( \mathbb{Q}_2(\zeta) = \mathbb{Q}_2(\sqrt{-3}) \), which is unramified over \( \mathbb{Q}_2 \) by Theorem 9.8(ii). In this case the general results we proved show that \( N(R_K) = \mathbb{Z}_2^x \) and \([\mathbb{Q}_2^R : N(K^R)] = 2 \). We now present the table of \( N(K^R) \) for the seven quadratic extensions \( K \) of \( \mathbb{Q}_2 \).
II. ARITHMETIC IN AN ALGEBRAIC NUMBER FIELD

$K \quad N_{K/Q_2}(K^\times)$

$Q_2(\sqrt{-3}) \quad 4^2 \mathbb{Z}_2^\times$
$Q_2(\sqrt{-1}) \quad 2^2 \cdot \{x \in \mathbb{Z}_2 \mid x \equiv 1 \pmod{4 \mathbb{Z}_2}\}$
$Q_2(\sqrt{3}) \quad (-2)^2 \cdot \{x \in \mathbb{Z}_2 \mid x \equiv 1 \pmod{4 \mathbb{Z}_2}\}$
$Q_2(\sqrt{2}) \quad 2^2 \cdot \{x \in \mathbb{Z}_2 \mid x \equiv 1 \pmod{8 \mathbb{Z}_2}\}$
$Q_2(\sqrt{-2}) \quad 2^2 \cdot \{x \in \mathbb{Z}_2 \mid x \equiv 1 \pmod{8 \mathbb{Z}_2} \text{ or } x \equiv 3 \pmod{8 \mathbb{Z}_2}\}$
$Q_2(\sqrt{6}) \quad (-2)^2 \cdot \{x \in \mathbb{Z}_2 \mid x \equiv 1 \pmod{8 \mathbb{Z}_2} \text{ or } x \equiv 3 \pmod{8 \mathbb{Z}_2}\}$
$Q_2(\sqrt{-6}) \quad 6^2 \cdot \{x \in \mathbb{Z}_2 \mid x \equiv 1 \pmod{8 \mathbb{Z}_2}\}$

Here $a^Z = \{a^m \mid m \in \mathbb{Z}\}$. To prove these, we note that

$\{x \in \mathbb{Z}_2 \mid x \equiv 1 \pmod{8 \mathbb{Z}_2}\} = \mathbb{Z}_2^{\times 2} \subset N(R^\times)$.

Let $K = Q_2(\sqrt{-1})$ and $\pi = 1 + \sqrt{-1}$. Then $N(\pi) = 2$ and $R = \mathbb{Z}_2[\pi]$. If $a + b\pi \in R^\times$ with $a, b \in \mathbb{Z}_2$, then $a \in \mathbb{Z}_2^{\times}$ and $N(a + b\pi) = a^2 + 2b(a + b) \equiv a^2 \equiv 1 \pmod{4 \mathbb{Z}_2}$ and $5 = N(1 + 2\sqrt{-1})$. Since $\{x \in \mathbb{Z}_2 \mid x \equiv 1 \pmod{4 \mathbb{Z}_2}\}$ is generated by $\mathbb{Z}_2^{\times 2}$ and 5, we obtain $N(K^\times)$ for $K = Q_2(\sqrt{-1})$. If $K = Q_2(\sqrt{3})$, we can use the same technique with $\pi = 1 + \sqrt{3}$, and observe that $N(\pi) = -2$ and $N(3 + 2\sqrt{3}) = -3$. In the remaining four cases we have $R = \mathbb{Z}_2 + \mathbb{Z}_2 \sqrt{m}$ with a multiple $m$ of 2, and for $a, b \in \mathbb{Z}_2$ we have $a + b\sqrt{m} \in R^\times$ if and only if $a \in \mathbb{Z}_2^{\times}$. Thus $N(R^\times) = \mathbb{Z}_2^{\times 2} \cdot N(1 + \mathbb{Z}_2 \sqrt{m}) = \mathbb{Z}_2^{\times 2} \cdot \{1 - b^2m \mid b \in \mathbb{Z}_2\}$. Now $1 - b^2m \equiv 1 \pmod{8 \mathbb{Z}_2}$ if $b \equiv 2 \mathbb{Z}_2$ and $1 - b^2m \equiv 1 - m \pmod{8 \mathbb{Z}_2}$ if $b \not\equiv 2 \mathbb{Z}_2$. Also, $N(2 + \sqrt{2}) = 2, N(\sqrt{-2}) = 2$, and $N(\sqrt{-6}) = 6$. Thus we obtain $N(K^\times)$ as given in the above table. Clearly $[Q_2^\times : N(K^\times)] = 2$ in all cases. If $H$ is a subgroup of $Q_2^\times$ of index 2, then $Q_2^{\times 2} \subset H$. Since $Q_2^\times / Q_2^{\times 2}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$, we see that there are exactly seven such $H$, and clearly the above $N(K^\times)$ exhaust them.

**Exercises.**

1. Let $F$ be a field with a normalized discrete order function $\nu$, and let $f(x) = x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n$ with $c_i \in F$; suppose that $\nu(c_1) > 0, \ldots, \nu(c_{n-1}) > 0, \nu(c_n) = 1$. (Such an $f$ is called an Eisenstein polynomial, $f = 0$ an Eisenstein equation.)
   (a) Let $\mu$ be an extension of $\nu$ to $F(s)$ with any root $s$ of $f$. Prove that $\mu(s) = 1/n$.
   (b) Using (a), prove that $f$ is irreducible over $F$.
   (c) Prove that every totally ramified extension of $F$ is generated by such an $s$.

2. Let $F$ be a field complete with respect to a discrete order function $\nu$, and $K$ a finite algebraic extension of $F$ of degree $n$. Suppose that $K$ is totally ramified over $F$ (that is, $\epsilon(K/F) = n$), and the characteristic of the residue class field $k$ of $\nu$ does not divide $n$. Prove that $K = F(\alpha)$ with an $n$-th root $\alpha$ of a prime element of $F$. (Hint: Take a prime element $\beta$ of $K$
and find a prime element $\gamma$ of $F$ such that $\nu(\gamma^{-1}\beta^n - 1) > 0$. Use Hensel’s lemma to find an $n$-th root of $\gamma^{-1}\beta^n$.

3. Let $F$, $k$, and $\nu$ be as in Exercise 2; suppose that $k$ is a finite field with $q$ elements. Let $K$ be a finite separable algebraic extension of $F$; let $R_K$ resp. $R_F$ denote the valuation ring of $K$ resp. $F$. Prove that $R_K = R_F[\alpha]$ for some $\alpha \in J_K$. (Hint: Let $M = F(\gamma) (\gamma^m = 1, m = q^f - 1)$ be the maximal unramified extension of $F$ contained in $K$, and $\pi$ a prime element of $K$. If $K \neq M$, put $\beta = \gamma + \pi$ and show that $\beta^m - 1$ is a prime element. Recall the formula $R_K = \sum_{i,j} R_F \alpha_i \pi^j$.)

4. Let $F$ be a finite algebraic extension of $Q_p$ and $K$ a finite abelian extension of $F$. Employing Theorem 9.10, prove that $K$ is unramified over $F$ if every unit of $F$ is contained in $N_{K/F}(K^\times)$, where $n = [K : F]$.

10. Ideal theory in an algebraic number field

In this section $Q$ denotes the algebraic closure of $Q$ in $C$, $F$ an algebraic number field of finite degree contained in $Q$, and $J = J_F$ its maximal order.

10.1. By a fractional ideal in $F$ we mean a $J$-submodule $X$ of $F$ such that $\{0\} \neq \alpha X \subset J$ for some $\alpha \in F^\times$. Let $Y$ be an ideal of $J$ different from $\{0\}$, and let $c$ be a nonzero element of $Y$. Then $cJ \subset Y \subset J$. By Lemma 8.8, $J$ is a free $Z$-module of rank $n$, where $n = [F : Q]$, and so $Y$ is a free $Z$-module of rank $n$ by Theorem 5.1. Thus, every fractional ideal in $F$ is a free $Z$-module of rank $n$, and consequently contains a $Q$-basis of $F$. Thus every fractional ideal is a $Z$-lattice in $F$, and every $Z$-lattice in $F$ that is a $J$-submodule is a fractional ideal.

We call a fractional ideal $Y$ integral if $Y \subset J$. A fractional ideal that is integral is called an integral ideal. An integral ideal is an ideal of $J$ different from $\{0\}$, and vice versa. Thus $[J : Y]$ is finite if $Y$ is an integral ideal, in which case we put

$$N(Y) = [J : Y],$$

and call $N(Y)$ the norm of $Y$. Clearly $N(Y) < N(X)$ if $X \subsetneq Y$. For every $\alpha \in F^\times$, the set $\alpha J$ is a fractional ideal. Such an ideal is called a principal ideal (even if it may not be contained in $J$).

**Lemma 10.2.** Let $P$ be a prime ideal of $J$ different from $\{0\}$. Then $P$ is a maximal ideal of $J$ and $J/P$ is a finite field.

**Proof.** This is because $J/P$ is a finite integral domain, and so must be a field.

Let $p$ be the characteristic of the field $J/P$. Then $N(P) = p^f$ with $0 < f \in Z$ and $pZ = Z \cap P = Q \cap P$. By a prime ideal in $F$ we always mean $P$
Theorem 10.3. (i) All the fractional ideals of $F$ form an abelian group with respect to the multiplication law $(X,Y) \mapsto XY$, where $XY$ is the submodule of $F$ consisting of all the finite sums $\sum x_iy_i$ with $x_i \in X$ and $y_i \in Y$. (This group is called the ideal group of $F$.)

(ii) $J$ is the identity element of this group, and $X^{-1} = \{ x \in F \mid aX \subset J \}$. 

(iii) Every fractional ideal $X$ different from $J$ can be uniquely written as a product $X = P_1^{m_1} \cdots P_r^{m_r}$ with different prime ideals $P_i$ and $m_i \in \mathbb{Z}$, $m_i > 0$ for every $i$.

That $XY$ as in (i) is a fractional ideal is clear. It is also easy to see that it defines an associative and commutative law of multiplication. We settle the remaining points after proving several facts (A, B, C, D, E, F) below.

(A) Let $P$ be a prime ideal. If $AB \subset P$ for two integral ideals $A$ and $B$, then $A \subset P$ or $B \subset P$.

Proof. Suppose $A \not\subset P$ and $B \not\subset P$; then $A$ has an element $a$ not contained in $P$, and $B$ has an element $b$ not contained in $P$. Since $P$ is a prime ideal, $ab \not\subset P$, which contradicts the assumption $AB \subset P$.

(B) Every integral ideal $M$ other than $J$ contains a product of prime ideals.

Proof. We prove this by induction on $N(M)$. There is no problem if $M$ is a prime ideal, and so we assume that $M$ is not a prime ideal. Then $J$ has elements $a$ and $b$ not contained in $M$ such that $ab \in M$. Put $A = M + Ja$ and $B = M + Jb$. Then $AB \subset M$ and $N(A) < N(M)$, since $M \nsubseteq A$. Similarly $N(B) < N(M)$. Applying our induction to $A$ and $B$, we obtain our assertion.

(C) For a fractional ideal $M$ put $M^{-1} = \{ x \in F \mid xM \subset J \}$. If $M \nsubseteq J$, then $J \nsubseteq M^{-1}$.

Proof. Suppose $M \nsubseteq J$; then clearly $J \subset M^{-1}$. Take a maximal ideal $P$ containing $M$. Then $P$ is a prime ideal and $J \subset P^{-1} \subset M^{-1}$. Suppose $J = M^{-1}$. Then $P^{-1} = J$. Take any nonzero element $a$ not contained in $M$ such that $ab \in M$. Put $A = M + Ja$ and $B = M + Jb$. Then $AB \subset M$ and $N(A) < N(M)$, since $M \nsubseteq A$. Similarly $N(B) < N(M)$. Applying our induction to $A$ and $B$, we obtain our assertion.

(D) If $\alpha \in F$ and $\alpha X \subset X$ with a $\mathbb{Z}$-lattice $X$ in $F$, then $\alpha \in J$. 

36 II. ARITHMETIC IN AN ALGEBRAIC NUMBER FIELD
Proof. Take a \( \mathbb{Z} \)-basis \( \{e_i\}_{i=1}^n \) of \( X \). Then \( \alpha e_i = \sum_{j=1}^n c_{ij}e_j \) with \( c_{ij} \in \mathbb{Z} \), and so the matrix \( \alpha 1_n - (c_{ij}) \) annihilates the nonzero vector \( (e_i) \), and so \( \det(\alpha 1_n - (c_{ij})) = 0 \), which is an equation of type (8.1). Thus \( \alpha \) is integral over \( \mathbb{Z} \), and so \( \alpha \in J \).

(E) \( MM^{-1} = J \) for every fractional ideal \( M \).

Proof. Clearly \( MM^{-1} \subset J \). Suppose \( MM^{-1} \neq J \). Then \( MM^{-1} \subset P \subset J \) for some maximal ideal \( P \). Then \( J \subsetneq P^{-1} \) by (C), and \( P^{-1} \subset (M M^{-1})^{-1} \). Clearly \( (M M^{-1})^{-1} M M^{-1} \subset J \), and so \( (M M^{-1})^{-1} M^{-1} \subset M^{-1} \). Taking \( M^{-1} \) as \( X \) in (D), we obtain \( (M M^{-1})^{-1} \subset J \), a contradiction. Thus \( MM^{-1} = J \).

(F) Let \( X \) and \( Y \) be fractional ideals of \( F \). Then \( X \subset Y \iff XY^{-1} \subset J \iff X = YA \) with an integral ideal \( A \).

The proof may be left to the reader, as it is straightforward. If \( X \) and \( Y \) as in (F) we say that \( Y \) divides \( X \).

Once (E) is established it is easy to see that (i) and (ii) of Theorem 10.3 hold. We prove that every integral \( M \) is a product of prime ideals by induction on \( N(M) \). We may assume that \( M \neq J \) and \( M \) is not a prime ideal. Given such an \( M \), define \( A \) and \( B \) as in the proof of (B). We have seen that \( N(B) \neq N(M) \) and \( AB \subset M \subsetneq A \), and so \( B \neq J \). Put \( C = B^{-1}M \). Then \( M = BC \subset C \) and \( M \neq C \), since \( B \neq J \). Thus \( N(C) \neq N(M) \). By induction, \( B \) and \( C \) are products of prime ideals, and so \( M \) is a product of prime ideals. The uniqueness of such a product expression for \( M \) follows from (A). We have to extend the result from integral ideals to fractional ideals, which is easy, and so may be left to the reader.

Lemma 10.4. Let \( A \), \( B \), and \( C \) be integral ideals of \( F \). Then \( A + B = J \) if and only if there is no prime ideal that divides both \( A \) and \( B \). For such \( A \) and \( B \) we have \( AB = A \cap B \) and \( J/AB \) is ring-isomorphic to \( (J/A) \oplus (J/B) \); moreover, if \( A \) divides \( BC \), then \( A \) divides \( C \).

Proof. Suppose \( A + B = J \). If an integral ideal \( D \) divides both \( A \) and \( B \), then \( J = A + B \subset D \), and so \( D = J \). If \( A + B \neq J \), then taking a maximal ideal containing \( A + B \), we find a prime ideal \( P \) that divides both \( A \) and \( B \). This proves the first assertion. If \( A + B = J \), then \( A \cap B = (A \cap B)J = (A \cap B)A + (A \cap B)B \subset BA + AB = AB \). Clearly \( AB \subset A \cap B \), and so \( AB = A \cap B \). By Theorem 1.3, \( J/AB \cong (J/A) \oplus (J/B) \). Finally suppose \( BC \subset A \). Since \( AC \subset A \), we have \( C = JC = AC + BC \subset A \), which proves the last assertion.

For integral ideals \( A \) and \( B \) we say that \( A \) is prime to \( B \) if \( A + B = J \).
Lemma 10.5. Let $X$ be a fractional ideal and $C$ an integral ideal. Then the following assertions hold:

(i) There exist an integral ideal $B$ and an element $\alpha$ of $F$ such that $B+C = J$ and $B = \alpha X$.

(ii) $X/CX$ and $J/C$ are isomorphic as $J$-modules.

(iii) Suppose $C$ is prime to $mJ$ with $0 \neq m \in \mathbb{Z}$; then $N(C)$ is prime to $m$.

Proof. Assuming that $C \neq J$, let $P_1, \ldots, P_r$ be the prime ideals dividing $C$; put $Y = X^{-1}P_1 \cdots P_r$. Then $Y \subseteq YP_i^{-1} \subseteq X^{-1}$. Take $\alpha_i \in YP_i^{-1} \not\in Y$, and put $\alpha = \alpha_1 + \cdots + \alpha_r$. Then $\alpha_i \in X^{-1}P_j$ if $i \neq j$. Suppose $\alpha_1 \in X^{-1}P_1$. Then $\alpha_1P_1 \subseteq P_1 \cap P_2 \cap \cdots \cap P_r = P_1 \cdots P_r$, so that $\alpha_1 \in Y$, a contradiction. Thus $\alpha \not\in X^{-1}P_1$. Since $\alpha_1 \not\in X^{-1}P_i$ for $i \neq 1$, we see that $\alpha \not\in X^{-1}P_1$. Similarly $\alpha \not\in X^{-1}P_i$ for every $i$. Thus $\alpha X \not\subseteq P_i$ for every $i$. Put $B = \alpha X$. Then $B$ is integral and prime to every $P_i$, so that $B$ is prime to $C$, which proves (i). To prove (ii), take $\alpha$ and $B$ as in (i). By Lemma 10.4, $BC = B \cap C$, and the map $x \mapsto \alpha x$ sends $X/CX$ onto $B/BC$ which is isomorphic to $J/C$ as expected. To prove (iii), take a prime ideal $P$ dividing $C$. Then $P + mJ = J$, and so $m$ is invertible in $J/P$. Thus $m$ is prime to $N(P)$. Since $N(C)$ is the product of powers of $N(P)$ for all prime factors $P$ of $C$, we obtain (iii).

Lemma 10.6. Every fractional ideal is generated over $J$ by two elements.

Proof. Given a fractional ideal $Y$, take a nonzero element $\beta \in Y$ and put $X = Y^{-1}$ and $C = \beta X$. Then $C$ is an integral ideal. Applying Lemma 10.5(i) to this $X$ and $C$, we obtain an element $\alpha$ such that $\alpha X + C = J$. Multiplying by $Y$, we obtain $\alpha J + \beta J = Y$, which proves our lemma.

Lemma 10.7. $N(XY) = N(X)N(Y)$ if $X$ and $Y$ are integral ideals.

Proof. By Lemma 10.5(ii) we have $X/YX \cong J/Y$, and so $[X : YX] = [J : Y]$. Thus $N(XY) = [J : YX] = [J : X][X : YX] = [J : X][J : Y] = N(X)N(Y)$.

10.8. Given a fractional ideal $X$, take integral ideals $S$ and $T$ so that $X = S^{-1}T$, and put $N(X) = N(S)^{-1}N(T)$. From Lemma 10.7 we easily see that this is well defined, and $X \mapsto N(X)$ is a homomorphism of the ideal group of $F$ into $\mathbb{Q}^\times$; $N(X)$ is called the norm of $X$. In particular,

$$(10.2) \quad N(\alpha J) = |N_{F/Q}(\alpha)| \quad \text{for every } \alpha \in F^\times.$$ 

It is sufficient to prove this when $\alpha \in J$. For $0 \neq \alpha \in J$ let $\rho(\alpha)$ denote the matrix representing the $\mathbb{Q}$-linear automorphism $\xi \mapsto \alpha \xi$ of the vector space $F$ with respect to a $\mathbb{Z}$-basis of $J$. By Theorem 7.8(iv) we have $N_{F/Q}(\alpha) = \det[\rho(\alpha)]$. By Lemma 5.8, $[J : \alpha J] = |\det[\rho(\alpha)]|$, which gives (10.2).
Hereafter we put $[F : \mathbb{Q}] = n$. Let $X$ be a $\mathbb{Z}$-lattice in $F$ and $\{\xi_i\}_{i=1}^n$ a $\mathbb{Z}$-basis of $X$. Then we put
\begin{equation}
D(X) = D(\xi_1, \ldots, \xi_n) = \det (\Tr_{F/\mathbb{Q}}(\xi_i \xi_j)).
\end{equation}
This is a special case of (7.4), and is called the discriminant of $X$. In the present situation $\Tr_{F/\mathbb{Q}}(\xi_i \xi_j) \in \mathbb{Q}$ and $D(X) \neq 0$ by Theorem 7.8(i), and so $D(X) \in \mathbb{Q}^\times$. We easily see that it is determined independently of the choice of $\{\xi_i\}_{i=1}^n$. In particular, if $X = J$, then $\Tr_{F/\mathbb{Q}}(\xi_i \xi_j) \in \mathbb{Z}$ by Lemma 8.8. Thus $D(J)$ is a nonzero positive or negative integer. We put $D_F = D(J)$ and call $D_F$ the discriminant of $F$. Let $\sigma_1, \ldots, \sigma_n$ be all the different isomorphic embeddings of $F$ into $\overline{\mathbb{Q}}$. Then by (7.6),
\begin{equation}
D(X) = \det (\xi_j^{\sigma_i})^2.
\end{equation}

Lemma 10.10. (i) If $X$ and $Y$ are $\mathbb{Z}$-lattices in $F$ and $X \subset Y$, then $[Y : X]^2 = D(X)/D(Y)$.
(ii) If $X$ is a fractional ideal of $F$, then $N(X)^2 = D(X)/D_F$.

The proof of these statements is left to the reader, as it is an easy exercise.

10.11. Let $p$ be a prime number and let $P_1, \ldots, P_g$ be the prime ideals dividing $pJ$. Then $N(P_i) = p^{f_i}$ and
\begin{equation}
pJ = P_1^{e_1} \cdots P_g^{e_g},
\end{equation}
with positive integers $e_i$ and $f_i$. Taking the norm of both sides, we obtain $p^n = N(pJ) = \prod_{i=1}^g p^{e_i f_i}$, and so
\begin{equation}
n = \sum_{i=1}^g e_i f_i.
\end{equation}

10.12. Fix a prime ideal $P$ of $F$. Given $a \in F$, put $aJ = P^mX$ with $m \in \mathbb{Z}$ and a fractional ideal $X$ that does not involve $P$. Put then $m = \nu_P(a)$; put also $\nu_P(0) = \infty$. Then we can easily verify that $\nu_P$ is a normalized discrete order function. We call the $\nu_P$-completion of $F$ the $P$-completion of $F$. Every order function of $F$ is equivalent to $\nu_P$ with a unique $P$.

Let $R_P$ be the valuation ring of $\nu_P$, and $M_P$ the maximal ideal of $R_P$ (see §6.7). Then
\begin{equation}
R_P = \{ u/v \mid u, v \in J, v \notin P \},
\end{equation}
\begin{equation}
R_P = J + M_P, \quad P = J \cap M_P, \quad R_P/M_P \cong J/P.
\end{equation}
To prove these, denote by $R'$ the right-hand side of (10.7). Clearly $R' \subset R_P$. To prove the opposite inclusion, let $a \in R_P$ and $aJ = P^mX$ as above. Then $m \geq 0$. We can put $X = YZ^{-1}$ with relatively prime integral ideals $Y$ and $Z$. By Lemma 10.5(i) there exist an integral ideal $B$ and an element $\gamma$ of $F$ such that $B + P = J$ and $B = \gamma Z^{-1}$. Then $\gamma aJ = P^m YB \subset J$, and so $\gamma a \in J$. 

10. IDEAL THEORY IN AN ALGEBRAIC NUMBER FIELD 39
II. ARITHMETIC IN AN ALGEBRAIC NUMBER FIELD

Since both $B$ and $Z$ are prime to $P$ and $\gamma J = BZ$, we see that $\gamma \notin P$. Thus $a = \gamma a/\gamma \in R'$, which proves (10.7).

To prove (10.8), let $u, v \in J$ and $v \notin P$. Since $J/P$ is a field, $J$ has an element $w$ such that $wv - 1 \in P$. Then $u/v - wu = u(1 - wv)/v$, which clearly belongs to $MP$. Thus $RP = J + MP$. That $J \cap MP = P$ is clear from the definition of $\nu P$. Then $RP/MP = (J + MP)/MP \cong J/(J \cap MP) = J/P$. Thus we obtain (10.8).

For $p, P_i, e_i$, and $f_i$ as in (10.5) and (10.6), put $\nu_i = e_i^{-1}\nu P_i$. Then $\nu_i$ coincides with $\nu P_i$ on $Q$, and

$$(10.9) \quad e_i = e(\nu_i/\nu_P), \quad f_i = f(\nu_i/\nu_P).$$

Indeed, (10.5) shows that $\nu_i(p) = 1$, and so $\nu_i(Q^\times) = Z$, whereas $\nu_i(F^\times) = e_i^{-1}Z$. Thus $e_i = e(\nu_i/\nu_P)$. Next, $Z/pZ \cong Z_p/pZ_p$, which is contained in $RP_i/MP_i \cong J/P_i$. Since $[J : P_i] = N(P_i) = p^{f_i}$, we have $[J/P_i : Z/pZ] = f_i$, and so $f_i = f(\nu_i/\nu_P)$.

We say that $p$ is **ramified in** $F$ if $e_i > 1$ for some $i$, and $p$ is **unramified in** $F$ if $e_i = 1$ for every $i$.

**Theorem 10.13.** A prime number $p$ is ramified in $F$ if and only if $p|DF$.

**Theorem 10.14.** Let $\theta$ be an element of $J$ such that $F = Q(\theta)$, and $h(x)$ the minimal polynomial of $\theta$ over $F$. Let $p$ be a prime number that does not divide $[J : Z[\theta]]$. Denote by $\overline{h}$ the class of $h$ modulo $pZ[x]$. Let $\overline{h}(x) = \prod_{i=1}^g k_i(x)^{e_i}$ be the decomposition of $\overline{h}$ in $(Z/pZ)[x]$ with different irreducible polynomials $k_i$. Then we have $pJ = P_1^{e_1} \cdots P_g^{e_g}$ with exactly $g$ different prime ideals $P_i$ such that $N(P_i) = p^{f_i}$ with $f_i = \deg(k_i)$.

We do not give the proof of these two theorems here, since we will later prove generalizations of these as Theorems 14.10 and 14.11.

**10.15.** An algebraic extension of $Q$ of degree 2 is traditionally called a **quadratic field**. Such a field is given as $F = Q(\sqrt{\alpha})$ with an element $\alpha$ of $Q^\times$ that is not a square in $Q$. We call $F$ a **real** or **imaginary quadratic field** according as $\alpha > 0$ or $\alpha < 0$. Replacing $\alpha$ by its suitable integer multiple, we may assume that $F = Q(\sqrt{m})$ with a square-free positive or negative integer $m \neq 1$. Let $J = J_F$ as before. Then

$$(10.10a) \quad J = Z[\mu], \quad \mu = (1 + \sqrt{m})/2 \quad \text{if} \quad m - 1 \in 4Z.
$$

$$(10.10b) \quad J = Z[\sqrt{m}] \quad \text{if} \quad m - 1 \notin 4Z.
$$

To prove these, take $\xi = \alpha + \beta \sqrt{m} \in J$ with $\alpha, \beta \in Q$. Then $2\alpha = \text{Tr}_{F/Q}(\xi) \in Z$ and $\alpha^2 - \beta^2 m = N_{F/Q}(\xi) \in Z$. Put $a = 2\alpha$ and $b = 2\beta$. Then $a \in Z$ and $b^2 m \in Z$. Since $m$ is square-free, we easily see that $b \in Z$. Now $a^2 - b^2 m = 4(a^2 - \beta^2 m) \in 4Z$. We easily see that $a \in 2Z$ if and only if $b \in 2Z$, in which
case \( \alpha, \beta \in \mathbb{Z} \), and so \( \xi \in \mathbb{Z} + \mathbb{Z}\sqrt{m} = \mathbb{Z}[\sqrt{m}] \). Therefore \( a \notin 2\mathbb{Z} \) if and only if \( b \notin 2\mathbb{Z} \), in which case \( m - 1 \in 4\mathbb{Z} \), since \( a^2 \equiv b^2 \equiv 1 \) (mod 4).

Case I: \( m - 1 \notin 4\mathbb{Z} \). In this case we always have \( a, b \in 2\mathbb{Z} \), and so \( \xi \in \mathbb{Z}[\sqrt{m}] \). Thus \( J = \mathbb{Z}[\sqrt{m}] \), which proves (10.10b).

Case II: \( m - 1 \in 4\mathbb{Z} \). Put \( \mu = (1 + \sqrt{m})/2 \). Then \( \mu^2 - \mu = (m - 1)/4 \), and so \( \mu \) is integral over \( \mathbb{Z} \); thus \( \mu \in J, \sqrt{m} = 2\mu - 1 \in \mathbb{Z}[\mu] \). We have to consider the case in which \( a \notin 2\mathbb{Z} \) and \( b \notin 2\mathbb{Z} \). Then \( \xi - \mu = (a - 1)/2 + \sqrt{m}(b - 1)/2 \in \mathbb{Z}[\sqrt{m}] \subset \mathbb{Z}[\mu] \). Thus \( J = \mathbb{Z}[\mu] \), which proves (10.10a).

An easy calculation shows that

\[
(10.11) \quad D_F = m \text{ if } m - 1 \notin 4\mathbb{Z}, \quad D_F = 4m \text{ if } m - 1 \notin 4\mathbb{Z}.
\]

10.16. Still in the setting of §10.15, let us now study the decomposition of a prime number \( p \) in \( F \). Since \( n = 2 \), (10.5) can take only the following three forms:

\[
(10.12a) \quad pJ = P_1P_2, \quad P_1 \neq P_2, \quad N(P_1) = N(P_2) = p,
\]

\[
(10.12b) \quad pJ = P, \quad N(P) = p^2,
\]

\[
(10.12c) \quad pJ = P^2, \quad N(P) = p.
\]

Here \( P \) and \( P_i \) are prime ideals in \( F \); \( p \) is unramified in \( F \) in Cases (10.12a) and (10.12b); \( p \) is ramified in \( F \) in Case (10.12c). By Theorem 10.13, \( p \) is ramified in \( F \) exactly when \( p|m \) or \( p|4m \) according as \( m - 1 \in 4\mathbb{Z} \) or \( m - 1 \notin 4\mathbb{Z} \). For instance, take \( m = -1 \) and \( F = \mathbb{Q}(\sqrt{-1}) \); put \( P = (1 + \sqrt{-1})J \). Then \( p^2 = 2\sqrt{-1}J = 2J \), which is a special case of (10.12c).

Next, take \( \sqrt{m} \) to be \( \theta \) of Theorem 10.14. Then \( [J : \mathbb{Z}[\sqrt{m}]] = 1 \) if \( m - 1 \notin 4\mathbb{Z} \) and \( [J : \mathbb{Z}[\sqrt{m}]] = 2 \) if \( m - 1 \in 4\mathbb{Z} \), which can be seen from Lemma 10.10(i), for example. Therefore Theorem 10.14 is applicable to every odd prime number \( p \). We have \( h(x) = x^2 - m \), and so \( pJ = P_1P_2 \) as in (10.12a) if and only if \( x^2 - m \) has two roots in \( \mathbb{Z}/p\mathbb{Z} \), and \( pJ = P \) as in (10.12b) if and only if \( x^2 - m \) has no root in \( \mathbb{Z}/p\mathbb{Z} \). Recalling the definition of the quadratic residue symbol in §3.1, we see that for every odd prime number \( p \) that does not divide \( m \),

\[
(10.13) \quad \frac{m}{p} = 1, \quad pJ = P \quad \frac{m}{p} = -1.
\]

Now Theorem 3.7 can be reformulated as follows. To each quadratic field \( F = \mathbb{Q}(\sqrt{m}) \) as above we can assign a real primitive character \( \chi \) of conductor \( |D_F| \) such that \( \chi(p) = \left( \frac{m}{p} \right) \) for every odd prime number \( p \) prime to \( m \), and the correspondence \( F \leftrightarrow \chi \) is one-to-one. Moreover, \( \chi(-1)D_F > 0 \). Here \( D_F \) is determined by (10.11). This combined with (10.13) determines the decomposition of \( pJ \) in \( F \). For example, the result given in §3.8 determines the prime numbers \( p \) such that \( pJ \) decomposes into the product of two prime ideals in \( \mathbb{Q}(\sqrt{15}) \).
10.17. We cannot say anything about $2J$ by (10.13). By Theorem 10.13, 2 is ramified in $F$ if $D_F$ is even, which is so if and only if $m - 1 \notin 4\mathbb{Z}$. Assuming that $m - 1 \in 4\mathbb{Z}$, put $\mu = (1 + \sqrt{m})/2$ as we did in (10.10a). Then the minimal polynomial of $\mu$ over $\mathbb{Q}$ is $x^2 - x - (m - 1)/4$. By Theorem 10.14, $2J$ is a prime ideal in $F$ if and only if this polynomial is irreducible over $\mathbb{Z}/2\mathbb{Z}$, which is so if and only if $m - 5 \in 8\mathbb{Z}$. Thus

$$2J = P_1P_2 \iff m - 1 \in 8\mathbb{Z}, \quad 2J = P \iff m - 5 \in 8\mathbb{Z}. \tag{10.14}$$

Let us now show that if $\chi$ is the real character of conductor $|D_F|$ corresponding to $F$, then

$$2J = P_1P_2 \iff \chi(2) = 1, \quad 2J = P \iff \chi(2) = -1. \tag{10.15}$$

Indeed, as shown in §3.5, we have $\left(\frac{2}{p}\right) = \chi_1(p)$, and so by (1') in the proof of Theorem 3.7 we have $\chi(2) = \chi_1(p_1 \cdots p_r g_1 \cdots g_s) = \chi(p^e) = \chi_1(m)$, and $\chi(2) = 1$ if $m - 1 \in 8\mathbb{Z}$ and $\chi(2) = -1$ if $m - 5 \in 8\mathbb{Z}$, and so we obtain (10.15) from (10.14). We will give a conceptual meaning of (10.15) in §17.7.

10.18. Let $\mathcal{I}$ (or $\mathcal{I}_F$) denote the ideal group of $F$ and $\mathcal{P}$ the subgroup of $\mathcal{I}$ consisting of all the principal ideals of $F$. Then $\mathcal{I}/\mathcal{P}$ is called the ideal class group of $F$, which is a finite group as will be shown in Theorem 12.7 below. We call $[\mathcal{I} : \mathcal{P}]$ the class number of $F$. Each coset of $\mathcal{I}/\mathcal{P}$ is called an ideal class of $F$; in particular, the coset $X\mathcal{P}$ for $X \in \mathcal{I}$ is called the ideal class of $X$.

Theorem 10.19. Let $L$ be a $J$-lattice in a vector space $V$ over $F$ of dimension $n$, and $\{e_i\}_{i=1}^n$ an $F$-basis of $V$. Then the following assertions hold:

(i) There exist an $F$-basis $\{g_i\}_{i=1}^n$ of $V$ and $n$ fractional ideals $A_1, \ldots, A_n$ in $F$ such that $L = \sum_{i=1}^n A_i g_i$. Moreover, $\{g_i\}$ can be chosen so that $g_i \in \sum_{k=1}^n F e_k$.

(ii) Let $L = \sum_{i=1}^n A_i g_i$ with an $F$-basis $\{g_i\}_{i=1}^n$ of $V$ and $n$ fractional ideals $A_i$ in $F$. Then the isomorphism class of $L$ as a $J$-module is determined by the ideal class of $A_1 \cdots A_n$.

Proof. Assertion (i) is obvious if $n = 1$. Therefore we prove (i) by induction on $n$. Given $L$ and an $F$-basis $\{e_i\}_{i=1}^n$ of $V$ with $n > 1$, put $A = \{a_1 \mid \sum_{i=1}^n a_i e_i \in L\}$, where $a_i \in F$. Clearly $A$ is a fractional ideal in $F$. If $\sum_{i=1}^n b_i e_i \in A^{-1} L$, then $\alpha b_1 \in A$ for every $\alpha \in A$, and so $b_1 \in J$. Also, $1 = \sum_{\nu=1}^k \beta_\nu \alpha_\nu$ with $\beta_\nu \in A^{-1}$ and $\alpha_\nu \in A$. We can find elements $x_\nu = \sum_{i=1}^n \alpha_\nu e_i$ of $L$ such that $\alpha_\nu = \alpha_\nu$. Put $g_1 = \sum_{\nu=1}^k \beta_\nu x_\nu$ and $\gamma_i = \sum_{\nu=1}^k \beta_\nu \alpha_\nu e_i$. Then $g_1 \in A^{-1} L$, $g_1 = \sum_{i=1}^n \gamma_i e_i$, and $\gamma_1 = 1$. This proves that $J = \{b_1 \mid \sum_{i=1}^n b_i e_i \in A^{-1} L\}$. Let $x = \sum_{i=1}^n c_i e_i \in A^{-1} L$
and \( M = A^{-1}L \cap (\sum_{i=2}^n Fe_i) \). Then \( c_1 \in J \) and \( x - c_1g_1 \in M \), and so \( A^{-1}L = Jg_1 + M \). Now \( M \) is a \( J \)-lattice in \( \sum_{i=2}^n Fe_i \) by Lemma 4.3(ii). Applying our induction to \( M \) and multiplying by \( A \), we obtain (i). To prove (ii), we need the following facts:

(10.16) Two fractional ideals \( X \) and \( Y \) in \( F \) are isomorphic as \( J \)-modules if and only if \( X = \beta Y \) with \( \beta \in F^\times \).

(10.17) For two fractional ideals \( A \) and \( B \) in \( F \), \( A \oplus B \) and \( J \oplus AB \) are isomorphic as \( J \)-modules.

We leave the proof of (10.16) to the reader as an easy exercise. (Hint: Assume \( X \subset J \); for \( x, y \in X \) and a \( J \)-isomorphism \( g \) of \( X \) onto \( Y \) we have \( xg(y) = g(xy) = yg(x) \).) To prove (10.17), we may assume that both \( A \) and \( B \) are integral. Also, by Lemma 10.5(i), replacing \( B \) by \( \gamma B \) with a suitable \( \gamma \in F^\times \), we may assume that \( A + B = J \). Then we can find elements \( a \in A \) and \( b \in B \) such that \( a + b = 1 \). We view \( A \oplus B \) as a subset of \( F \oplus F = F_2 \), and we let \( GL_2(F) \) act on the right of \( F_2 \). Put \( \sigma = \begin{bmatrix} 1 & -b \\ 1 & a \end{bmatrix} \); then \( \sigma^{-1} = \begin{bmatrix} a & b \\ -1 & 1 \end{bmatrix} \).

The right action of \( \sigma \) sends \( A \oplus B \) into \( J \oplus AB \), and that of \( \sigma^{-1} \) sends \( J \oplus AB \) into \( A \oplus B \). This proves (10.17). To prove (ii), take an \( F \)-basis \( \{x_i\}_{i=1}^n \) of \( V \). Given a \( J \)-lattice \( L \) in \( V \), take an \( F \)-basis \( \{y_i\}_{i=1}^n \) contained in \( L \), put \( y_i = \sum_{j=1}^n c_{ij}x_j \), and denote by \( \lambda(L) \) the fractional ideal generated by \( \det [(c_{ij})] \) for all possible choices of \( \{y_i\}_{i=1}^n \). (Alternatively, \( \lambda(L) \) is defined by \( \bigwedge^n L = \lambda(L)x_1 \wedge \cdots \wedge x_n \).) Clearly the ideal class of \( \lambda(L) \) does not depend on the choice of \( \{x_i\}_{i=1}^n \). If \( L = \sum_{i=1}^n A_i g_i \) as in (ii), then \( \lambda(L) = \varepsilon A_1 \cdots A_n \) with \( \varepsilon \in F^\times \). Also, (10.17) shows that \( L \cong J_{n-1}^1 \oplus A_1 \cdots A_n \). This combined with (10.16) proves (ii).

**Lemma 10.20.** (i) Given \( a, b, c \in J \), \( a \neq 0 \), there exists an element \( k \in J \) such that \( aJ + bJ + cJ = aJ + (b + kc)J \).

(ii) Suppose \( n > 1 \) and \( \sum_{i=1}^n a_iJ + X = J \) with \( a_i \in J \) and an integral ideal \( X \). Then there exist \( n \) elements \( b_i \in J \) such that \( \sum_{i=1}^n b_iJ = J \) and \( b_i - a_i \in X \) for every \( i \).

**Proof.** To prove (i), we may assume that \( c \neq 0 \); replacing \( b \) by a suitable element of \( b + cJ \), we may also assume that \( b \neq 0 \). Put \( aJ + bJ + cJ = Y \), \( aJ = AY \), \( bJ = BY \), and \( cJ = CY \) with ideals \( Y \), \( A \), \( B \), \( C \). Then \( A + B + C = J \). If \( A = J \), then \( Y = aJ \), and so \( aJ + bJ = Y \). Thus we may assume that \( A \neq J \). Let \( S \) be the set of all prime ideals that divide \( A \). For each \( P \in S \) put \( m_P = 1 \) if \( B \subset P \) and \( m_P = 0 \) otherwise. We see that \( C \nsubseteq P \) if \( m_P = 1 \). By Theorem 1.3 we can take \( k \in J \) so that \( k - m_P \in P \) for every \( P \in S \). Then \( b + kc \notin PY \) for every \( P \in S \). (Indeed, if \( B \subset P \), then \( b \in PY \), \( kc - c \in cP \subset PY \), and \( c \notin PY \), and so \( b + kc \notin PY \); if \( B \nsubseteq P \), then \( b \notin PY \) and \( kc \in PY \), and
so \( b + kc \notin PY \). Thus we can put \((b + kc)J = DY\) with an integral ideal \(D\) prime to \(A\), and consequently \(aJ + (b + kc)J = Y\), which proves (i).

If the \(a_i\) and \(X\) are given as in (ii), then \(\sum_{i=1}^{n} a_i g_i + h = 1\) with some \(g_i \in J\) and \(h \in X\). Then \(\sum_{i=1}^{n} a_i J + hJ = J\). There is no problem if \(h = 0\), and so we assume that \(h \neq 0\). Replacing \(a_1\) by a suitable element of \(a_1 + hJ\), we may assume that \(a_1 \neq 0\). By (i), we have \(a_1 J + a_2 J + hJ = a_1 J + (a_2 + kh)J\) for some \(k \in J\). Then \(a_1 J + (a_2 + kh)J + \sum_{i=3}^{n} a_i J = \sum_{i=1}^{n} a_i J + hJ = J\), which proves (ii).

**Theorem 10.21.** Given \(\alpha \in M_n(J)\) such that \(\det(\alpha) - d \in X\) with an integral ideal \(X\) and an element \(d\) of \(J\) prime to \(X\), there exists an element \(\xi\) of \(M_n(J)\) such that \(\det(\xi) = d\) and \(\xi - \alpha \in X_n\). In particular, the natural map of \(M_n(J)\) onto \(M_n(J/X)\) gives a surjection of \(SL_n(J)\) onto \(SL_n(J/X)\).

**Proof.** We first prove this for \(d = 1\) by induction on \(n\). The case \(n = 1\) is obvious and so we assume \(n > 1\). Let \(\alpha_i\) denote the \(i\)-th row of \(\alpha\) and let \(\alpha_n = [a_1 \ldots a_n]\) with \(a_i \in J\). Since \(\det(\alpha) - 1 \in X\), we see that \(\sum_{i=1}^{n} a_i c_i - 1 \in X\) with some \(c_i \in J\), and so \(\sum_{i=1}^{n} a_i J + X = J\). By Lemma 10.20(ii) we can find elements \(b_i \in J\) such that \(\sum_{i=1}^{n} b_i J = J\) and \(b_i - a_i \in X\) for every \(i\). Replacing \(a_i\) by \(b_i\), we may assume that \(\sum_{i=1}^{n} a_i J = J\). Let \(L = J_n\). Then \(J = \{b \in F \mid b_\alpha \in L\}\). By Theorem 10.19(i) we can put \(L = \sum_{i=1}^{n} A_i \xi_i\) with fractional ideals \(A_i\) and an \(F\)-basis \(\{\xi_i\}_{i=1}^{n}\) of \(F_n^\prime\) such that \(\xi_i \in \sum_{k=i}^{n} F \alpha_k\). Then \(\xi_n \in F \alpha_n\). Put \(N = \sum_{i=1}^{n-1} A_i \xi_i\). Then we easily see that \(A_n \xi_n = J \alpha_n\) and \(L = N \oplus J \alpha_n\). By Theorem 10.19(ii), \(A_2 \cdots A_n\) is a principal ideal, and so by the same theorem we can put \(N = \sum_{i=1}^{n-1} J \varepsilon_i\) with \(n - 1\) elements \(\{\varepsilon_i\}_{i=1}^{n-1}\), which together with \(\alpha_n\) form a \(J\)-basis of \(L\). Changing the coordinate system of \(L\) (which means the replacement of \(\alpha\) by \(\sigma \alpha \sigma^{-1}\) with an element \(\sigma\) of \(GL_n(J)\)), we may assume that \(\{\varepsilon_i\}_{i=1}^{n}\) is the standard \(J\)-basis of \(L\), where we put \(\varepsilon_n = \alpha_n\). For each \(i < n\) we have \(\alpha_i = \beta_i + c_i \varepsilon_n\) with \(\beta_i \in N\) and \(c_i \in J\). Then

\[
\begin{bmatrix}
1 & \cdots & 0 & -c_1 \\
\cdots & \cdots & \cdots & \cdots \\
0 & \cdots & 1 & -c_{n-1} \\
0 & \cdots & 0 & 1
\end{bmatrix}
\alpha = 
\begin{bmatrix}
\beta_1 & 0 \\
0 & 1
\end{bmatrix}
\beta
\]

We see that \(\det(\beta) - 1 \in X\). Applying our induction to \(\beta\), we can find \(\gamma \in SL_{n-1}(J)\) such that \(\gamma - \beta \in X_{n-1}^{n-1}\). Putting

\[
\xi = 
\begin{bmatrix}
1 & \cdots & 0 & c_1 \\
\cdots & \cdots & \cdots & \cdots \\
0 & \cdots & 1 & c_{n-1} \\
0 & \cdots & 0 & 1
\end{bmatrix}
\begin{bmatrix}
\gamma & 0 \\
0 & 1
\end{bmatrix},
\]

we have \(\det(\xi) = 1\) and \(\xi - \alpha \in X_n\). This proves the case \(d = 1\). Given \(\alpha\) and \(d\) as in our theorem, take \(e \in J\) so that \(de - 1 \in X\) and put \(\alpha' = \alpha + de\). Then

\[
\alpha' = \alpha + de \in M_n(J) + X_n
\]

and by induction \(\alpha' = c \xi + \epsilon\) with \(c \in J\) and \(\epsilon \in X_n\). Hence, \(\alpha + de = c \xi + \epsilon\), which proves the case \(d \neq 0\). Therefore, \(\alpha + de \in M_n(J) + X_n\). By induction \(\alpha + de = c \xi + \epsilon\) with \(c \in J\) and \(\epsilon \in X_n\). Hence, \(\alpha + de = c \xi + \epsilon\), which proves the case \(d = 0\). Therefore, \(\alpha \in M_n(J) + X_n\).
\[ \alpha \cdot \text{diag}[1_{n-1}, e]. \] Then \( \det(\alpha') - 1 \in X \) and so we can find \( \xi' \in SL_n(J) \) such that \( \xi' - \alpha' \in X_n^n. \) Put \( \eta = \xi' \cdot \text{diag}[1_{n-1}, d]. \) Then \( \det(\eta) = d \) and \( \eta - \alpha \in X_n^n. \) This completes the proof.

**Exercises.**

1. Let \( A \) be either a principal ideal domain or the maximal order of an algebraic number field. Let \( P \) be a prime ideal of \( A \) and let \( 0 < e \in \mathbb{Z} \). Prove that \( A/P^e \) cannot be decomposed into the direct sum of two nontrivial subrings. (Hint: Every subring (or ideal) of \( A/P^e \) is of the form \( X/P^e \) with some \( X. \))

2. Let \( F \) be an algebraic number field, \( J \) the maximal order of \( F \), \( P \) a prime ideal in \( F \), and \( p \) the rational prime divisible by \( P \). Under what condition on \( P \) can \( J/P^m \) be isomorphic to \( \mathbb{Z}/p^m\mathbb{Z} \) as a \( \mathbb{Z} \)-module?

3. Prove the following classical theorem: A square-free positive rational integer \( c \) can be written in the form \( c = a^2 + b^2 \) with rational integers \( a \) and \( b \) if and only if \( c \) has no prime factor \( p \) of the form \( p \equiv 3 \pmod{4} \). (Hint: If \( c \) is divisible by such a \( p \), \( a + b\sqrt{-1} \) or \( a - b\sqrt{-1} \) is divisible by \( p \).)

4. Prove that if \( A + B = C \) for fractional ideals \( A, B, \) and \( C \) in \( F \), then \( A^m + B^m = C^m \) for every \( m \in \mathbb{Z}, > 0. \)
Arithmetic of Quadratic Forms
Shimura, G.
2010, XII, 238 p., Hardcover
ISBN: 978-1-4419-1731-7