MA4276 Theory of Algebraic Numbers

Thang Pang Ern

These notes are based off **Prof. Zhang Lei's** MA5202 Number Theory materials. Additional references are cited in the bibliography. Note that the old course code is MA5202 and it has been changed to MA4276. The new MA5202 Number Theory course will delve into class field theory.

This set of notes was last updated on July 3, 2026. If you would like to contribute a nice discussion to the notes or point out a typo, please send me an email at `thangpangern@u.nus.edu`.

Contents

Chapter 1

A Special Case of Fermat's Conjecture

1.1 Fermat's Conjecture

Algebraic number theory is the study of number fields. These refer to the finite extensions of the rational numbers $\mathbb{Q}$. Such fields are useful in solving problems which at first appear to involve only rational numbers. Consider the following problem (Example 1.1).

Example 1.1 (primitive Pythagorean triples). Find all primitive Pythagorean triples, i.e. integer solutions to $x^2+y^2=z^2$ having no common factor.

Assuming that we have such a triple and considering the equation modulo 4, it is clear that z is odd. Now comes the introduction of a number field into the problem. For example, consider $\mathbb{Q}[i]$, which can be regarded as the set containing all numbers of the form $a+bi$, where $a,b\in\mathbb{Q}$. We can now factorise the left side as $(x+yi)(x-yi)=z^2$. This becomes a multiplicative problem in the ring of Gaussian integers $\mathbb{Z}[i]$.

Recall from MA3201 Algebra II that $\mathbb{Z}[i]$ is a UFD. That is to say, every non-zero Gaussian integer can be expresed uniquely up to order and unit factors as a product of Gaussian primes. We will use this fact to show that $x+yi$ is of the form $u\alpha^2$ for some $\alpha\in\mathbb{Z}[i]$ and some Gaussian integer unit u. If we write $\alpha=m+ni$ and observe that the only units in $\mathbb{Z}[i]$ are ±1 and $\pm i$, we obtain

$$\{x,y\}=\left\{\pm\left(m^2-n^2\right),\pm2mn\right\}\quad\text{and}\quad z=\pm\left(m^2+n^2\right).$$

It is necessary for $\gcd(m,n)=1$ and not both odd, otherwise x,y,z would have a common factor. Moreover, it is easy to see that a primitive Pythagorean triple results in any such choice of m and n, and a choice of signs. The problem will be solved if we can show that for any primitive solution, $x+yi$ is of the form $u\alpha^2$. We omit the details but by working in the field $\mathbb{Q}[i]$, it is possible for one to determine all primitive Pythagorean triples.

Theorem 1.1 (Fermat's last theorem). There does not exist any positive integer solutions x, y, z to $x^n + y^n = z^n$ for $n > 2$.

We all know the history behind this problem. Using our result on primitive Pythagorean triples, we see that Fermat's *conjecture* (the first edition of [1] was published in 1977, before Fermat's last theorem was proven by Wiles in 1994) is true for $n = 4$ and hence true for any multiple of 4.[1] It is therefore sufficient to consider only the case in which n is an odd prime p, since if no solutions exist when $n = p$, then no solutions exist when n is a multiple of p.

We can reformulate the problem as follows:

if p is an odd prime then $x^p + y^p = z^p$ has no solution in non-zero integers x, y, z.

Suppose on the contrary that for some odd prime p, there exists a solution $x, y, z \in \mathbb{Z} \setminus \{0\}$. We may assume that x, y, z have no common factors (divide them out if there is one). To obtain a contradiction, we shall split into two cases as follows.

- **Case 1:** p divides none of x, y, z
- **Case 2:** p divides exactly one of x, y, z

For Case 2, note that it is impossible for p to divide more than one of x, y, z, otherwise it would divide all three, which is impossible. We will only consider Case 1. It is easy to show that $x^3 + y^3 = z^3$ has no Case 1 solutions. To see why, first consider the case when $p = 3$. Say x, y, z are not multiples of $p = 3$, then 9 does not divide $x^3 + y^3 - z^3$ since each of x^3, y^3, z^3 is ± 1 modulo 9.

Now, assume $p > 3$ and x, y, z are not multiples of p. We shall factorise the left side of $x^p + y^p = z^p$ to obtain

$$(x+y)(x+y\omega)\left(x+y\omega^2\right)\cdots\left(x+y\omega^{p-1}\right) = z^p, \tag{1.1}$$

where ω denotes the p^{th} root of unity. That is, $\omega = e^{\frac{2\pi i}{p}}$. To see why (1.1) holds, note that $1, \omega, \omega^2, \ldots, \omega^{p-1}$ are the p roots of the polynomial $t^p - 1$, so

$$t^p - 1 = (t-1)(t-\omega)\left(t-\omega^2\right)\cdots\left(t-\omega^{p-1}\right).$$

Setting $t = -x/y$, the result follows. We thus have a multiplicative problem in the number field $\mathbb{Q}[\omega]$, and in fact the subring $\mathbb{Z}[\omega]$. Kummer attempted to prove Fermat's conjecture by considering whether the unique factorisation property of $\mathbb{Z}$ or $\mathbb{Z}[i]$ generalises to the ring $\mathbb{Z}[\omega]$. Unforuntately, it does not (Example 1.2).

Example 1.2. If $p = 23$, then not all members of $\mathbb{Z}[\omega]$ factor uniquely into irreducible elements, i.e. elements $\alpha \in \mathbb{Z}[\omega]$ which are not units and such that whenever $\alpha = \beta\gamma$, then either β or γ is a unit. So, $\mathbb{Z}[\omega]$ is not a UFD for $p = 23$. However, it is a UFD for all primes strictly less than 23.

[1] For readers interested in the case when $n = 4$, please refer to p. 6 Question 15 of [**?**].

For primes strictly less than 23, it is not difficult to verify that $x^p + y^p = z^p$ has no Case 1 solutions.

Assuming that $\mathbb{Z}[\omega]$ is a UFD, it can be shown that $x + y\omega$ is of the form $u\alpha^p$ for some $\alpha \in \mathbb{Z}[\omega]$ and some unit $u \in \mathbb{Z}[\omega]$. Thereafter, for x and y not divisible by p, it can be shown that $x + y\omega = u\alpha^p$ implies $x \equiv y \pmod{p}$. Similarly, writing $x^p + (-z)^p = (-y)^p$, we obtain $x \equiv -z \pmod{p}$. As

$$2x^p \equiv x^p + y^p = z^p \equiv -x^p \pmod{p},$$

it follows that $p \mid 3x^p$. Earlier, we mentioned that p does not divide x and $p > 3$, so $p \neq 3$. This results in a contradiction. As such, Case 1 of Fermat's conjecture can be established for all primes p for which $\mathbb{Z}[\omega]$ is a UFD.

The question now is what can be done for other primes? This leads to Dedekind's amazing discovery of the correct generalisation of unique factorisation: although the elements of $\mathbb{Z}[\omega]$ may not factor uniquely into irreducible elements, the ideals in this ring always factor uniquely into prime ideals. So, the principal ideal $(x + y\omega)$ is the p^{th} power of some ideal I. For certain primes, known as *regular primes*, it follows that I must itself be a principal ideal, say (α), so that

$$(x + y\omega) = I^p = (\alpha)^p = (\alpha^p)$$

so $x + y\omega = u\alpha^p$ for some unit u.

> Definition 1.1 (regular prime). A prime p is regular if and only if p does not divide the class number of the ring $\mathbb{Z}[\omega]$. Here, the class number refers to an important arithmetic invariant that measures the extent to which unique factorisation fails in a given ring.

Given that $x + y\omega = u\alpha^p$, it implies $x \equiv y \pmod{p}$ and a contradiction follows. Hence, Case 1 of Fermat's conjecture can be established for all regular primes, which we now define.

We first note that there is an equivalence relation $\sim$ on the set of ideals of $\mathbb{Z}[\omega]$ defined as follows: for any ideals A and B, we have

$$A \sim B \quad \text{if and only if} \quad \alpha A = \beta B \text{ for some } \alpha, \beta \in \mathbb{Z}[\omega].$$

One can easily prove that the relation $\sim$ is indeed an equivalence relation. Here, we work under the assumption that $I_1 \sim I_2$ and $I_2 \sim I_3$. In due course, we will see that there are only finitely many equivalence classes of ideals under $\sim$. The number of classes is called the class number of $\mathbb{Z}[\omega]$, and is denoted by h, so h is a function of p. As mentioned in Definition 1.1, we see that p is regular if and only if p does not divide h.

To see why the ideal I in the equation $(x+y\omega) = I^p$ must be principal whenever p is a regular prime, we note that the ideal classes can be multiplied in the obvious way: the product of two ideal classes is obtained by selecting an ideal from each, multiplying them, and taking the ideal class which contains the product ideal. This is a well-defined operation, as the resulting ideal class does not depend on the particular ideals chosen but only on the two original ideal classes. Multiplied in this way, the ideal classes actually form a group. The identity element is the class consisting of all principal ideals, for which we denote this class by C_0. The existence of inverses will be established in due course. Thus, the ideal classes form a finite abelian group known as the *ideal class group*.

If p is regular, then this group contains no element of order p. Hence, if I^p is principal, then so is I. Let C be the ideal class containing I, then C^p is the class containing I^p, which is also C_0. Since C_0 is the identity in the ideal class group and C cannot have order p, so it follows that $C = C_0$, showing that I is principal.

As noted before, this leads to a contradiction, showing that $x^p + y^p = z^p$ has no Case 1 solutions. That is, there do not exist positive integer solutions to Fermat's equation for which p does not divide xyz, where p is a regular prime. Proving that no Case 2 solutions exist for regular primes is more difficult. Hence, Fermat's conjecture is proven for all regular primes p, hence for all positive integers $n \geq 3$ which have at least one regular prime factor. Unfortunately, irregular primes exist (such as $37, 59, 67$). For example, 37 divides the class number of the cyclotomic field $\mathbb{Q}(\zeta_{37})$, making it irregular.

Interestingly, it is a known fact that there are infinitely many irregular primes, but it is unknown whether there are infinitely many regular primes. In any case, our attempt to prove Fermat's conjecture leads us to consider various questions about the ring $\mathbb{Z}[\omega]$. What about the units in this ring? What are the irreducible elements? Do elements factor uniquely? If not, what can we say about the factorisation of ideals into prime ideals? How many ideal classes are there? The investigation of such problems forms a large portion of classical algebraic number theory.

Example 1.3 (Marcus p. 4 Question 1). Define the norm function $N : \mathbb{Z}[i] \to \mathbb{Z}$ by $N(a+bi) = a^2 + b^2$. Verify that for all $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$, either by direct computation or by using the fact that

$$N(a+bi) = (a+bi)(a-bi).$$

Conclude that if $\alpha \mid \gamma$ in $\mathbb{Z}[i]$, then $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.

Solution. Let $\alpha = a+bi$ and $\beta = c+di$, where $a, b, c, d \in \mathbb{Z}$. Then,

$$\alpha\beta = (a+bi)(c+di) = (ac-bd) + (ad+bc)i.$$

This implies that

$$\begin{aligned} N(\alpha\beta) &= N((ac-bd)+(ad+bc)i) \\ &= (ac-bd)^2+(ad+bc)^2 \\ &= \left(a^2+b^2\right)\left(c^2+d^2\right) \\ &= N(\alpha)N(\beta) \end{aligned}$$

It is interesting to note that the identity

$$(ac-bd)^2+(ad+bc)^2 = \left(a^2+b^2\right)\left(c^2+d^2\right)$$

is known as the Brahmagupta–Fibonacci identity.

Now suppose that $\alpha \mid \gamma$ in $\mathbb{Z}[i]$. Then, there exists $\delta \in \mathbb{Z}[i]$ such that $\gamma = \alpha\delta$. Applying the norm to both sides, we get

$$N(\gamma) = N(\alpha\delta) = N(\alpha)N(\delta).$$

Since $N(\delta) \in \mathbb{Z}$, then $N(\alpha) \mid N(\gamma)$. □

Example 1.4 (Marcus p. 5 Question 2). Let $\alpha \in \mathbb{Z}[i]$. Show that

$$\alpha \text{ is a unit} \quad \text{if and only if} \quad N(\alpha) = 1.$$

Conclude that the only units are ± 1 and $\pm i$.

Solution. We first prove that α is a unit if and only if $N(\alpha) = 1$. First, we show that if α is a unit, then $N(\alpha) = 1$. Since α is a unit, there exists some $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$. Applying the norm to both sides yields

$$N(\alpha)N(\beta) = 1$$

where we used the fact that the norm is multiplicative. However, $N(\alpha), N(\beta) \in \mathbb{Z}_{\geq 0}$. Hence, the only possibility is $N(\alpha) = 1$.

Next, suppose $N(\alpha) = 1$. Note that $\alpha\overline{\alpha} = N(\alpha) = 1$. Since $\alpha \in \mathbb{Z}[i]$, we also have $\overline{\alpha} \in \mathbb{Z}[i]$. Therefore $\overline{\alpha}$ is an inverse of α in $\mathbb{Z}[i]$, so α is a unit.

Next, we prove that the only units are ± 1 and $\pm i$. Write $\alpha = a + bi$, where $a, b \in \mathbb{Z}$. Since α is a unit implies $N(\alpha) = 1$, then $a^2 + b^2 = 1$. So, either $(a,b) = (\pm 1, 0)$ or $(0, \pm 1)$. □

Example 1.5 (Marcus p. 5 Question 3). Let $\alpha \in \mathbb{Z}[i]$. Show that if $N(\alpha)$ is a prime in $\mathbb{Z}$, then α is irreducible in $\mathbb{Z}[i]$. Show that the same conclusion holds if $N(\alpha) = p^2$, where $p \in \mathbb{Z}$ is prime and $p \equiv 3 \pmod 4$.

Solution. Suppose on the contrary that α is not an irreducible in $\mathbb{Z}[i]$. Then, there exists β, γ, neither of it is a unit, such that $\alpha = \beta\gamma$. Taking norms on each side yields $N(\alpha) = N(\beta)N(\gamma)$, where we used the fact that the norm function is multiplicative. Since $N(\alpha)$ is a prime in $\mathbb{Z}$, then we can write $p = N(\beta)N(\gamma)$, where $N(\beta), N(\gamma) > 1$. This contradicts the definition of a prime.

Next, we investigate the case where $N(\alpha) = p^2$, where $p \in \mathbb{Z}$ is prime and $p \equiv 3 \pmod 4$. In a similar vein, we can write $p^2 = N(\beta)N(\gamma)$. So, we consider two cases.

- **Case 1:** Suppose $N(\beta) = N(\gamma) = p$. Then, we previously showed that β and γ are irreducible in $\mathbb{Z}[i]$. Write $\beta = a + bi$, where $a, b \in \mathbb{Z}$. Then, $N(\beta) = a^2 + b^2 = p$. However, $p \equiv 3 \pmod 4$, while every square is congruent to either 0 or 1 $\pmod 4$. Hence $a^2 + b^2$ can only be congruent to $0, 1$, or 2 $\pmod 4$, and never 3 $\pmod 4$. This is a contradiction. Therefore α is irreducible in $\mathbb{Z}[i]$.
- **Case 2:** Suppose $N(\beta) = p^2$ and $N(\gamma) = 1$. However, this is a contradiction as we need $N(\gamma) > 1$. Also, one has the symmetric argument for $N(\beta) = 1$ and $N(\gamma) = p^2$.

Combining both cases, the result follows. □

Example 1.6 (Marcus p. 5 Question 4). Show that $1 - i$ is irreducible in $\mathbb{Z}[i]$ and $2 = u(1-i)^2$ for some unit u.

Solution. We first prove that $1 - i$ is irreducible in $\mathbb{Z}[i]$. Suppose on the contrary that $1 - i$ is not irreducible. Then, there exist $\alpha, \beta \in \mathbb{Z}[i]$ which are both not units such that $1 - i = \alpha\beta$. Taking the norm on both sides, $2 = N(\alpha)N(\beta)$. Without a loss of generality, suppose $N(\alpha) = 2$ and $N(\beta) = 1$ but this is a contradiction based on Example 1.4.

For the second part, observe that $(1-i)^2 = -2i$ so we can take the unit u to be i. □

Example 1.7 (Marcus p. 5 Question 8). We will use unique factorisation in $\mathbb{Z}[i]$ to prove that every prime $p \equiv 1 \pmod 4$ is a sum of two squares.

(a) Use the fact that the multiplicative group $\mathbb{Z}_p^\times$ of integers mod p is cyclic to show that if $p \equiv 1 \pmod 4$, then $n^2 \equiv -1 \pmod p$ for some $n \in \mathbb{Z}$.

(b) Prove that p cannot be irreducible in $\mathbb{Z}[i]$.[2]

(c) Prove that p is a sum of two squares[3].

Solution.

(a) Since p is prime, then $\mathbb{Z}_p^\times$ is cyclic so it is generated by some $g \in \mathbb{Z}_p^\times$. Hence, there exists some $m \in \mathbb{Z}$ such that $g^m \in \mathbb{Z}_p^\times$. By a corollary of Lagrange's theorem, since $\mathbb{Z}_p^\times$ is a finite group, then the order of any element divides the order of the group.

[2] A hint is to use the fact that $p \mid (n^2 + 1) = (n+i)(n-i)$.

[3] A hint is that **(b)** shows that $p = (a+bi)(c+di)$ with neither factor a unit. Take norms.

Since $\left|\mathbb{Z}_p^\times\right| = p-1$, then $(g^m)^{p-1}$ divides $p-1$. Also, given that $p-1$ is divisible by 4, then g^m is of order 2 in $\mathbb{Z}_p^\times$. Set $n = g^m$, then the result follows.

(b) Suppose on the contrary that p is not irreducible in $\mathbb{Z}[i]$. In **(a)**, we showed that p divides $n^2+1 = (n+i)(n-i)$. Since $\mathbb{Z}[i]$ is a UFD, then p is prime. So, $p \mid (n+i)$ or $p \mid (n-i)$. Without loss of generality, suppose $p \mid (n+i)$. Taking norms, $N(p) \mid N(n+i)$ so $p^2 \mid p$ which is a contradiction. Hence, p cannot divide either factor, which implies that p is irreducible in $\mathbb{Z}[i]$.

(c) By **(b)**, p is not irreducible in $\mathbb{Z}[i]$, so there exist $a,b,c,d \in \mathbb{Z}$ such that $p = (a+bi)(c+di)$, where neither factor is a unit. Taking norms,

$$\begin{aligned} N(p) &= N((a+bi)(c+di)) \\ p^2 &= \left(a^2+b^2\right)\left(c^2+d^2\right) \end{aligned}$$

As neither factor has norm 1, then $p = a^2+b^2 = c^2+d^2$, and the result follows. □

Example 1.8 (Marcus p. 5 Question 9). Describe all irreducible elements in $\mathbb{Z}[i]$.

Solution. Let $\alpha = a+bi \in \mathbb{Z}[i]$ be irreducible, where $a,b \in \mathbb{Z}$. Taking norms, $N(\alpha) = a^2+b^2$. We shall describe all irreducible elements of $\mathbb{Z}[i]$ up to multiplication by a unit. Recall from Example 1.4 that the units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

- **Case 1:** Suppose $N(\alpha) = p$, where $p \in \mathbb{Z}$ is a rational prime[4]. Suppose $\alpha = \beta\gamma$. Taking norms, we have
$$p = N(\beta)N(\gamma).$$
Since p is prime in $\mathbb{Z}$, we must have either $N(\beta) = 1$ or $N(\gamma) = 1$. Thus, either β or γ is a unit. Hence α is irreducible in $\mathbb{Z}[i]$. Therefore, every Gaussian integer whose norm is a rational prime is irreducible.
- **Case 2:** Suppose α is associated to a rational prime $p \equiv 3 \pmod 4$. We claim that p is irreducible in $\mathbb{Z}[i]$. Suppose $p = \beta\gamma$. Taking norms, we have
$$p^2 = N(\beta)N(\gamma),$$
which forces $N(\beta) = N(\gamma) = p$. So, we would need some Gaussian integer $\beta = x+yi$ such that $N(\beta) = x^2+y^2 = p$. However, this is impossible when $p \equiv 3 \pmod 4$ since squares modulo 4 are only 0 or 1, so $x^2+y^2 \equiv 0,1,2 \pmod 4$. As such, $N(\beta) = p$ is impossible so one of β and γ must have norm 1. Hence, one of them is a unit and p is irreducible in $\mathbb{Z}[i]$.

As such, every associate of such a prime is irreducible, namely up, where $u \in \{\pm 1, \pm i\}$, where $p \equiv 3 \pmod 4$.

[4] A rational prime just means an ordinary prime number in $\mathbb{Z}$. The word 'rational' is used to distinguish ordinary primes in $\mathbb{Z}$ from primes or irreducibles in other rings like $\mathbb{Z}[i]$. For example, even though $5 \in \mathbb{Z}$ is a prime, it is not a prime in $\mathbb{Z}[i]$ since $5 = (2+i)(2-i)$.

- **Case 3:** Suppose $p = 2$ or $p \equiv 1 \pmod 4$. First, note that $2 = (1+i)(1-i)$, where $1+i$ and $1-i$ are both of norm 2. Hence, $1+i$ and $1-i$ are irreducible by Case 1. Next, if $p \equiv 1 \pmod 4$, by Fermat's sum of two squares theorem, p is the sum of squares, so we can write $p = (a+bi)(a-bi)$, where each factor is irreducible.

Combining all cases, the irreducible elements of $\mathbb{Z}[i]$, up to multiplication by a unit, are precisely $1+i$, the rational primes $p \equiv 3 \pmod 4$, and the Gaussian integers $a+bi$ such that $a^2+b^2 = p$ for some rational prime $p \equiv 1 \pmod 4$. □

Example 1.9 (Marcus p. 5 Question 10). Let $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Define $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ by $N(a+b\omega) = a^2 - ab + b^2$. We say that $a+b\omega$ is an *Eisenstein integer*. Show that if $a+b\omega$ is written in the form $u+vi$, where u and v are real, then $N(a+b\omega) = u^2+v^2$.

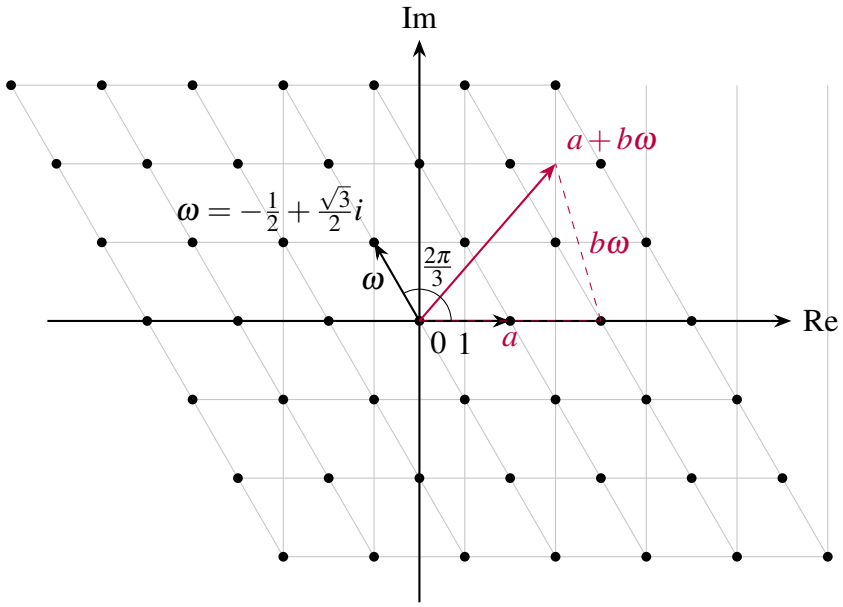


Figure 1.1: The Eisenstein integers $\mathbb{Z}[\omega] = \{a+b\omega : a,b \in \mathbb{Z}\}$

Solution. Note that $a,b \in \mathbb{Z}$. So,

$$a+b\omega = a+b\cos\left(\frac{2\pi}{3}\right) + ib\sin\left(\frac{2\pi}{3}\right).$$

Let $u = a+b\cos\left(\frac{2\pi}{3}\right)$ and $v = b\sin\left(\frac{2\pi}{3}\right)$. So,

$$a = u - v\cot\left(\frac{2\pi}{3}\right) \quad \text{and} \quad b = v\csc\left(\frac{2\pi}{3}\right).$$

As such,

$$N(a+b\omega) = a^2 - ab + b^2 = u^2 + v^2$$

via some tedious computation. □

Example 1.10 (Marcus p. 5 Question 11). Let $\omega = e^{2\pi i/3}$. For all $\alpha, \beta \in \mathbb{Z}[\omega]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$, either by direct computation or Example 1.9. So, we can conclude that

$$\alpha \mid \gamma \text{ in } \mathbb{Z}[\omega], \quad \text{then} \quad N(\alpha) \mid N(\gamma) \text{ in } \mathbb{Z}.$$

Example 1.11 (Marcus p. 5 Question 12). Let $\omega = e^{\frac{2\pi i}{3}}$ and $\alpha \in \mathbb{Z}[\omega]$. Then, α is a unit if and only if $N(\alpha) = 1$, and one can find all six units in $\mathbb{Z}[\omega]$.

Example 1.12 (Marcus p. 5 Question 13). Let $\omega = e^{\frac{2\pi i}{3}}$. Show that $1-\omega$ is irreducible in $\mathbb{Z}[\omega]$, and that $3 = u(1-\omega)^2$ for some unit u.

Solution. Suppose on the contrary that $1-\omega$ is not irreducible in $\mathbb{Z}[\omega]$. Then, we can write $1-\omega = \alpha\beta$, where neither α nor β is a unit. Taking norms yields $N(1-\omega) = N(\alpha)N(\beta)$. Since $N(1-\omega) = 3$, without loss of generality, this forces $N(\alpha) = 3$ and $N(\beta) = 1$. By Example 1.11, β is a unit, which is a contradiction. So, $1-\omega$ is irreducible.

The second part is trivial. □

Example 1.13 (Marcus p. 8 Question 29). Let $\omega = e^{\frac{2\pi i}{23}}$. Verify that the product

$$\left(1+\omega^2+\omega^4+\omega^5+\omega^6+\omega^{10}+\omega^{11}\right)\left(1+\omega+\omega^5+\omega^6+\omega^7+\omega^9+\omega^{11}\right)$$

is divisible by 2 in $\mathbb{Z}[\omega]$, although neither factor is.

Solution. Since $\omega^{23}-1 = 0$, then $1+\omega+\omega^2+\ldots+\omega^{22} = 0$. Expanding the polynomial yields

$$2\omega^5+2\omega^6+2\omega^7+2\omega^9+2\omega^{10}+6\omega^{11}+2\omega^{12}+2\omega^{13}+2\omega^{15}+2\omega^{16}+2\omega^{17}.$$

This is clearly divisible by 2 in $\mathbb{Z}[\omega]$. However, neither factor is divisible by 2. □

Chapter 2

Number Fields and Number Rings

2.1 Introduction

Let K be a number field. Then, as introduced in Chapter 1.1, $K \subseteq \mathbb{C}$ is a subfield such that the extension $[K : \mathbb{Q}]$ is finite. Note that every such field has the form $\mathbb{Q}[\alpha]$ for some $\alpha \in \mathbb{A} \subseteq \mathbb{C}$. Here, $\mathbb{A}$ denotes the set of algebraic numbers[1]. If α is a root of an irreducible polynomial of degree n over $\mathbb{Q}$, then

$$\mathbb{Q}[\alpha] = \left\{ a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q} \text{ for all } 0 \leq i \leq n-1 \right\}$$

and the representation in this form is unique, i.e. $\left\{1, \alpha, \ldots, \alpha^{n-1}\right\}$ is a basis for $\mathbb{Q}[\alpha]$ as a vector space over $\mathbb{Q}$.

Previously in Example 1.9, we discussed the Eisenstein integers $a + b\omega$, where ω is a 3rd root of unity. Note that 3 is prime. We shall now generalise this to arbitrary positive integers.

Definition 2.1 (cyclotomic field). Let $\omega = e^{\frac{2\pi i}{m}}$, where m is not necessarily prime. Then, the field $\mathbb{Q}[\omega]$ is called the m^{th} cyclotomic field. We will also use the notation $\mathbb{Q}[\zeta_m]$.

Example 2.1. The first two cyclotomic fields are just $\mathbb{Q}$.

Example 2.2. The third cyclotomic field is equal to the sixth. This is because if we set $\omega = e^{\frac{2\pi i}{6}}$, then $\omega = -\omega^4 = -\left(\omega^2\right)^2$, which shows that $\mathbb{Q}[\omega] = \mathbb{Q}\left[\omega^2\right]$.

Lemma 2.1. For odd m, the m^{th} cyclotomic field is the same as the $(2m)^{\text{th}}$.

Proof. Let $\omega = e^{\frac{2\pi i}{2m}}$. Then, $\omega = -\omega^{m+1} \in \mathbb{Q}\left[\omega^2\right]$. □

[1] In Definition 2.4, we will encounter the definition of an *algebraic integer*, which is not to be confused with algebraic numbers.

Lemma 2.2. For even m, where $m > 0$, the cyclotomic fields are all distinct.

Proof. Let $m, n > 0$ be even integers. Suppose $\mathbb{Q}[\zeta_m] = \mathbb{Q}[\zeta_n]$. For even m, the roots of unity contained in $\mathbb{Q}[\zeta_m]$ are precisely the m^{th} roots of unity. Thus,

$$\mu(\mathbb{Q}[\zeta_m]) = \langle \zeta_m \rangle$$

which has order m. Here, $\mu(K)$ denotes the group of roots of unity contained in the field K. Similarly,

$$\mu(\mathbb{Q}[\zeta_n]) = \langle \zeta_n \rangle$$

which has order n. Since the two fields are equal, they contain the same roots of unity. Hence, $m = n$. As such, the fields $\mathbb{Q}[\zeta_m]$, for even $m > 0$, are all distinct. □

Another infinite class of number fields is the quadratic fields (Definition 2.2).

Definition 2.2 (quadratic field). Let $m \in \mathbb{Z}$ be non-square. Then, $\mathbb{Q}[\sqrt{m}]$ is said to be a quadratic field.

Note that $[\mathbb{Q}\sqrt{m} : \mathbb{Q}] = 2$ with basis $\{1, \sqrt{m}\}$. Also, we only need to consider square-free m since for example $\mathbb{Q}\left[\sqrt{12}\right] = \mathbb{Q}\left[\sqrt{3}\right]$. The quadratic fields $\mathbb{Q}[\sqrt{m}]$, for m square-free, are all distinct.

Example 2.3 (Marcus p. 28 Question 1).

(a) Show that every number field of degree 2 over $\mathbb{Q}$ is one of the quadratic fields $\mathbb{Q}[\sqrt{m}]$, where $m \in \mathbb{Z}$.

(b) Show that the fields $\mathbb{Q}[\sqrt{m}]$, where m is squarefree, are pairwise distinct[2].

Solution.

(a) Let K be a number field such that $[K : \mathbb{Q}] = 2$. Since $K \supset \mathbb{Q}$ is a finite extension, then it is algebraic. So, there exists $\alpha \in K$ such that $K = \mathbb{Q}[\alpha]$. By considering the degree of the extension, the minimal polynomial of α over $\mathbb{Q}$ must be of degree 2. Let the polynomial be

$$f(x) = x^2 + bx + c \quad \text{where } f \text{ is irreducible over } \mathbb{Q}.$$

By computing the discriminant, we have $\Delta = b^2 - 4c = m$. Suppose it is non square. Then, either root of $f(\alpha) = 0$ can be expressed as the sum of $-\frac{b}{2} \in \mathbb{Q}$ and $\frac{\sqrt{m}}{2} \in \mathbb{Q}[\sqrt{m}]$. The result follows.

(b) Let $m \in \mathbb{Z}$ be squarefree. Suppose $a, b \in \mathbb{Q}$. Since $\sqrt{m} = a + b\sqrt{n}$, where $m \neq n$, by squaring both sides, we have $m - a^2 - b^2 n = 2ab\sqrt{n}$. Hence, either $a = 0$ or $b = 0$. If $a = 0$, then $m = b^2 n$, but this contradicts the definition of m being squarefree. On the other hand, if $b = 0$, then $m = a^2$, which also contradicts the definition of m being squarefree. We conclude that $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are pairwise distinct. □

[2] A hint is to consider the equation $\sqrt{m} = a + b\sqrt{n}$; use this to show that they are in fact pairwise non-isomorphic.

Definition 2.3 (real and imaginary quadratic fields). For $m > 0$, $\mathbb{Q}[\sqrt{m}]$ is a real quadratic field; for $m < 0$, $\mathbb{Q}[\sqrt{m}]$ is an imaginary quadratic field.

Example 2.4. $\mathbb{Q}[i]$ is an imaginary quadratic field, as well as a cyclotomic field.

Example 2.5. Not only is $\mathbb{Q}\left[\sqrt{-3}\right]$ is an imaginary quadratic field, but it is also a cyclotomic field, i.e. $\mathbb{Q}\left[\sqrt{-3}\right] = \mathbb{Q}[\omega]$, where ω is a 3rd root of unity.

The ring $\mathbb{Z}[\omega]$ has certain nice properties. For example, every ideal factors uniquely into prime ideals. This is true more generally for the ring $\mathbb{Z}[\omega]$ in any cyclotomic field. It is also true for $\mathbb{Z}[\sqrt{m}]$ for certain values of m. However, it fails, for example, for $\mathbb{Z}\left[\sqrt{-3}\right]$. Nevertheless, $\mathbb{Q}\left[\sqrt{-3}\right]$ has a subring in which ideals factor uniquely into primes, namely

$$\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right] = \mathbb{Z}[\omega] \quad \text{where } \omega = e^{2\pi i/3}.$$

The ring consists of all

$$\frac{a+b\sqrt{-3}}{2} \quad \text{where } a,b \in \mathbb{Z} \text{ and } a \equiv b \pmod 2.$$

Example 2.6 (Marcus p. 30 Example 15).

(a) Show that $\mathbb{Z}[\sqrt{-5}]$ contains no element whose norm is 2 or 3.

(b) Verify that $2 \cdot 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$ is an example of non-unique factorisation in the number ring $\mathbb{Z}\left[\sqrt{-5}\right]$. This shows that $\mathbb{Z}\left[\sqrt{-5}\right]$ is not a UFD.

Example 2.6 is a routine exercise from MA3201 Algebra II so we omit the details.

Definition 2.4 (algebraic integer). A complex number is an algebraic integer if and only if it is a root of some monic polynomial with coefficients in $\mathbb{Z}$.

Note that we have not required that the polynomial be irreducible over $\mathbb{Q}$. Thus, $\omega = e^{\frac{2\pi i}{m}}$ is an algebraic integer since it is a root of $x^m - 1$. It is true, however, that every α is a root of some monic irreducible polynomial with coefficients in $\mathbb{Z}$.

Lemma 2.3. Let f be a monic polynomial with coefficients in $\mathbb{Z}$ and suppose

$$f = gh \quad \text{where } g \text{ and } h \text{ are monic polynomials with coefficients in } \mathbb{Q}.$$

Then, g and h have coefficients in $\mathbb{Z}$.

Theorem 2.1. Suppose α is an algebraic integer and f is a monic polynomial over $\mathbb{Z}$ of least degree having α as a root. Then, f is irreducible over $\mathbb{Q}$.

Proof. Suppose on the contrary that f is not irreducible, then we can factorise f as gh, where g and h are non-constant polynomials in $\mathbb{Q}[x]$. Since f is monic, then g and h are monic and have coefficients in $\mathbb{Z}$ by Lemma 2.3. However, α is a root of either g or h, but $\deg f > \max\{\deg g, \deg h\}$, which is a contradiction. □

Corollary 2.1. The only algebraic integers in $\mathbb{Q}$ are the ordinary integers.

Corollary 2.2 shows that the algebraic integers in $\mathbb{Q}[\sqrt{m}]$ form a ring. The same is true in any number field. To prove this, it suffices to show that the sum and product of two algebraic integers are also algebraic integers.

Corollary 2.2. Let $m \in \mathbb{Z}$ be squarefree. The set of algebraic integers in the quadratic field $\mathbb{Q}[\sqrt{m}]$ is

$$\begin{aligned} &\left\{a+b\sqrt{m} : a,b \in \mathbb{Z}\right\} && \text{if } m \equiv 2 \text{ or } 3 \pmod 4 \quad \text{and} \\ &\left\{\frac{a+b\sqrt{m}}{2} : a,b \in \mathbb{Z}, a \equiv b \pmod 2\right\} && \text{if } m \equiv 1 \pmod 4 \end{aligned}$$

Proof. Let $\alpha = r+s\sqrt{m}$, where $r,s \in \mathbb{Q}$. If $s \neq 0$, then the monic irreducible polynomial over $\mathbb{Q}$ having α as a root is

$$x^2 - 2rx + r^2 - ms^2 \quad \text{by considering } \left(x-\left(r+s\sqrt{m}\right)\right)\left(x-\left(r-s\sqrt{m}\right)\right).$$

Thus, α is an algebraic integer if and only if $2r, r^2 - ms^2 \in \mathbb{Z}$. The result follows. □

We first state some alternative characterisations of algebraic integers.

Theorem 2.2. For any $\alpha \in \mathbb{C}$, the following are equivalent:

- **(i)** α is an algebraic integer
- **(ii)** the additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated
- **(iii)** α is a member of some subring of $\mathbb{C}$ having a finitely generated additive group
- **(iv)** $\alpha A \subseteq A$ for some finitely generated additive subgroup $A \subseteq \mathbb{C}$

Proof. Note that **(ii)** implies **(iii)** implies **(iv)** trivially. Hence, it suffics to prove **(i)** implies **(ii)** and **(iv)** implies **(i)**.

For our first assertion, say α is an algebraic integer, i.e. it is a root of a monic polynomial of degree n over $\mathbb{Z}$. Then, **(ii)** follows since the additive group of $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, \ldots, \alpha^{n-1}$.

We then prove that **(iv)** implies **(i)**. Suppose $a_1, \ldots, a_n$ generate A, i.e. any element of A can be written as an integer linear combination of $a_1, \ldots, a_n$. The condition $\alpha A \subseteq A$ implies that for each generator a_i, αa_i can be written as a linear combination of the generators $a_1, \ldots, a_n$ with integer coefficients. Hence,

$$\alpha a_i = \sum_{j=1}^{n} m_{ij} a_j \text{ for all } 1 \leq i \leq n \quad \text{or equivalently} \quad \alpha \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \mathbf{M} \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.$$

Here, $\mathbf{M} \in \mathcal{M}_{n\times n}(\mathbb{Z})$. So, α is an eigenvalue of $\mathbf{M}$ with corresponding eigenvector $(a_1,\ldots,a_n)$. Since $\mathbf{M} \in \mathcal{M}_{n\times n}(\mathbb{Z})$, we infer that the minimal polynomial of α is monic with integer coefficients. We conclude that α is an algebraic integer. □

Corollary 2.3. If α and β are algebraic integers, then so are $\alpha+\beta$ and $\alpha\beta$.

Proof. Since $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ have finitely generated additive groups, we can let their generators be $\alpha_1,\ldots,\alpha_m$ and $\beta_1,\ldots,\beta_n$ respectively. So, the mn products $\alpha_i\beta_j$ generate $\mathbb{Z}[\alpha,\beta]$, which implies that $\mathbb{Z}[\alpha,\beta]$ is also finitely generated. The result follows since $\alpha+\beta, \alpha\beta \in \mathbb{Z}[\alpha+\beta]$. □

So, we see that for any two algebraic integers, we can make use of eigenvalues and eigenvectors (or determinants) to obtain monic polynomials for their sum and product. This shows that the set of algebraic integers in $\mathbb{C}$ is a ring. We let $\mathbb{A}$ denote this set. In particular, for any number field K, $\mathbb{A}\cap K$ is a subring of K.

Definition 2.5. For any number field K, we let $\mathbb{A}\cap K$ denote the number ring corresponding to K.

We have determined the number rings corresponding to $\mathbb{Q}$ and the quadratic fields. For the cyclotomic fields, we have $\mathbb{A}\cap\mathbb{Q}[\omega] = \mathbb{Z}[\omega]$. However, as of now, only the inclusion $\mathbb{Z}[\omega] \subseteq \mathbb{A}\cap\mathbb{Q}[\omega]$ is clear since $\omega \in \mathbb{A}$ and $\mathbb{A}\cap\mathbb{Q}[\omega]$ is a ring. To prove the reverse inclusion, we would need to know more information about $\mathbb{Q}[\omega]$. In particular, we need to know $[\mathbb{Q}[\omega]:\mathbb{Q}]$ and its discriminant.

Example 2.7 (Marcus p. 29 Question 11).

(a) Suppose all roots of a monic polynomial $f \in \mathbb{Q}[x]$ have absolute value 1. Show that the coefficient of x^r has absolute value $\leq \binom{n}{r}$, where n is the degree of f and $\binom{n}{r}$ is the binomial coefficient.

(b) Show that there are only finitely many algebraic integers α of fixed degree n, all of whose conjugates (including α) have absolute value 1.[3]

(c) Show that α (as in **(b)**) must be a root of unity[4].

Solution.

(a) Suppose $\deg f = n$. Let the roots of f be $\beta_1,\ldots,\beta_n$, where $\beta_i \in \mathbb{Q}$ such that $|\beta_i| = 1$ for all $1 \leq i \leq n$. Then,

$$f(x) = (x-\beta_1)\ldots(x-\beta_n).$$

Observe that f is monic. So,

$$f(x) = x^n - x^{n-1}\sum_{i=1}^{n}\beta_i + x^{n-2}\sum_{i<j}\beta_i\beta_j - \sum_{i<j<k}\beta_i\beta_j\beta_k + \ldots + (-1)^n\beta_1\ldots\beta_n.$$

[3] A hint is that recall Theorem 2.1, which stated that if $\alpha \in \mathbb{A}$ and f is a monic polynomial over $\mathbb{Z}$ of least degree having α as a root, then f is irreducible over $\mathbb{Q}$.

[4] A hint is to show that its powers are restricted to a finite set.

The coefficient of x^r is

$$(-1)^{n-r} \sum_{a_1<\ldots<a_r} \beta_{a_1}\beta_{a_2}\ldots\beta_{a_r}$$

so taking absolute value of the coefficient yields

$$\left|(-1)^{n-r} \sum_{a_1<\ldots<a_r} \beta_{a_1}\beta_{a_2}\ldots\beta_{a_r}\right| \leq \sum_{a_1<\ldots<a_r} |\beta_{a_1}||\beta_{a_2}|\ldots|\beta_{a_r}|$$
$$= \sum_{a_1<\ldots<a_r} 1 \quad \text{since } |\beta_i| = 1 \text{ for all } 1 \leq i \leq n$$

Now, given an r-tuple $(a_1,\ldots,a_r)$, it suffices to show that the number of ways to construct them such that $1 \leq a_1 < \ldots < a_r \leq n$ is $\binom{n}{r}$. This is equivalent to choosing r objects out of n distinct ones, which guarantees to form an increasing sequence $a_1 < \ldots < a_r$, and the result follows.

(b) Suppose α is an algebraic integer of degree n, i.e. the degree of the minimal polynomial (over $\mathbb{Z}$) that α satisfies is n. Then, its irreducible polynomial of over $\mathbb{Q}$ of degree n has coefficients in $\mathbb{Z}$ by Theorem 2.1. The conjugates of α are precisely the root of this polynomial. By **(a)**, the coefficient of x^r has an absolute value at most $\binom{n}{r}$, so there are finitely many choices for this coefficient.

(c) We must show that there exists $m \in \mathbb{Z}^+$ such that $\alpha^m = 1$. From **(b)**, we see that there are finitely many algebraic integers of degree at most n, all of whose conjugates have absolute value 1. Taking α as mentioned in **(b)**, we see that $\mathbb{Q}[\alpha^m] \subseteq \mathbb{Q}[\alpha]$ so all α^m have degree at most m.

Letting $\alpha_1 = \alpha$, we see that if $\alpha_2, \alpha_2, \ldots, \alpha_n$ denote the conjugates of α, then the conjugates of α^m are α_i^m, where $2 \leq i \leq n$. So, the powers of α are restricted to a finite set. □

2.2 The Cyclotomic Fields

Let $\omega = e^{\frac{2\pi i}{m}}$. Recall that this is an m^{th} root of unity. We define a conjugate of ω to be another root of the same irreducible polynomial over $\mathbb{Q}$. It is clear that every conjugate of ω is also an m^{th} root of 1 and is not an n^{th} root of 1 for any $n < m$. To see why, note that the irreducible polynomial for ω over $\mathbb{Q}$ must divide $x^m - 1$, but it cannot divide $x^n - 1$, where $n < m$, since $\omega^n \neq 1$. So, the only conjugates of ω are ω^k, where $1 \leq k \leq m$ and $\gcd(k,m) = 1$. Again, this calls for the use of Euler's totient function since $[\mathbb{Q}[\omega] : \mathbb{Q}] = \varphi(m)$. This will enable us to determine the Galois group, and we would be able to determine which roots of 1 are in $\mathbb{Q}[\omega]$.

Theorem 2.3. All ω^k, where $1 \leq k \leq m$ and $\gcd(k,m) = 1$, are conjugates of ω.

Corollary 2.4. $[\mathbb{Q}[\omega] : \mathbb{Q}] = \varphi(m)$

Corollary 2.5. We have

$$\mathrm{Gal}\left(\mathbb{Q}\left[\omega\right]/\mathbb{Q}\right) \cong \mathbb{Z}_m^\times.$$

For each $k \in \mathbb{Z}_m^\times$, the corresponding automorphism in the Galois group sends ω to ω^k. So, for each $g \in \mathbb{Z}[x]$, we have $g\left(\omega\right) \mapsto g\left(\omega^k\right)$.

Proof. An automorphism of $\mathbb{Q}\left[\omega\right]$ is uniquely determined by the image of ω. This automorphism sends ω to any of the ω^k, where $\gcd\left(k,m\right) = 1$. This establishes a bijection between the Galois group and $\mathbb{Z}_m^\times$. □

As an application of Corollary 2.5, the subfields of $\mathbb{Q}\left[\omega\right]$ correspond to the subgroups of $\mathbb{Z}_m^\times$. In particular, for p prime, the p^{th} cyclotomic field contains a unique subfield of each degree dividing $p-1$ (since $\mathbb{Z}_p^\times$ is cyclic of order $p-1$). Hence, for any odd prime p, the p^{th} cyclotomic field contains a unique quadratic field. This turns out to be $\mathbb{Q}\left[\sqrt{\pm p}\right]$ with the sign depending on p. This fact is particularly useful as it is required in one of the proofs of the law of quadratic reciprocity.

Corollary 2.6. Let $\omega = e^{\frac{2\pi i}{m}}$. If m is even, the only roots of unity in $\mathbb{Q}\left[\omega\right]$ are the m^{th} roots of unity and if m is odd, the only roots of unity in $\mathbb{Q}\left[\omega\right]$ are the $(2m)^{\text{th}}$ roots of unity.

Proof. It suffices to prove the statement for even m. This is because if m is odd, the m^{th} cyclotomic field is the same as the $(2m)^{\text{th}}$ by Lemma 2.1. Say m is even and θ is a primitive k^{th} root of unity in $\mathbb{Q}\left[\omega\right]$. By this, we mean that θ is a k^{th} root of unity but not an n^{th} root of unity for any $n < k$. So, $\mathbb{Q}\left[\omega\right]$ contains a primitive r^{th} root of 1, where $r = \mathrm{lcm}\left(k,m\right)$. Since $\mathbb{Q}\left[\omega\right]$ contains the r^{th} cyclotomic field, then $\varphi\left(r\right) \leq \varphi\left(m\right)$, which is a contradiction unless $r = m$. Hence, $k \mid m$ and θ is an m^{th} root of unity. □

Corollary 2.7. For m even, $\mathbb{Q}\left[\zeta_m\right]$ are all distinct and pairwise non-isomorphic.

2.3 Embeddings in $\mathbb{C}$

Recall the definition of an embedding from MA4203 Galois Theory.

Definition 2.6 (embedding). Let $\sigma : K \to \mathbb{C}$ be a field homomorphism. We say that σ is an embedding of K into $\mathbb{C}$ if it preserves addition and multiplication, and satisfies the following properties for all $a,b \in K$:

(i) Additivity: $\sigma\left(a+b\right) = \sigma\left(a\right) + \sigma\left(b\right)$

(ii) Multiplicativity: $\sigma\left(ab\right) = \sigma\left(a\right)\sigma\left(b\right)$

(iii) Unitality: $\sigma\left(1_K\right) = 1_{\mathbb{C}}$

An embedding is a field monomorphism (an injective homomorphism), and we can write $\sigma : K \hookrightarrow \mathbb{C}$.

Let K be a number field such that $[K:\mathbb{Q}] = n$. We know that there are exactly n embeddings of K in $\mathbb{C}$. These are easily described by writing $K = \mathbb{Q}[\alpha]$ and observing that α can be sent to any one of its n conjugates over $\mathbb{Q}$. Each conjugate β determines a unique embedding of K in $\mathbb{Q}$, i.e. for all $g \in \mathbb{Q}[x]$, we have $g(\alpha) \mapsto g(\beta)$, and every embedding must arise in this way since α must be sent to one of its conjugates.

Example 2.8. The quadratic field $\mathbb{Q}[\sqrt{m}]$, where m is squarefree, has two embeddings in $\mathbb{C}$. They are namely, the identity mapping and also the one sending $a+b\sqrt{m}$ to $a-b\sqrt{m}$, where $a,b \in \mathbb{Q}$. This is because $\sqrt{m}$ and $-\sqrt{m}$ are the two conjugates of $\sqrt{m}$.

Example 2.9. $\mathbb{Q}[\zeta_m]$ has $\varphi(m)$ embeddings in $\mathbb{C}$, which are the $\varphi(m)$ automorphisms.

Example 2.10. $\mathbb{Q}\left[\sqrt[3]{2}\right]$ has three embeddings in $\mathbb{C}$, for which only the identity mapping is an automorphism (Figure 2.1). The other two embeddings correspond to the conjugates $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$ of $\sqrt[3]{2}$, where $\omega = e^{2\pi i/3}$. These are not real so they are not elements of $\mathbb{Q}\left[\sqrt[3]{2}\right]$.

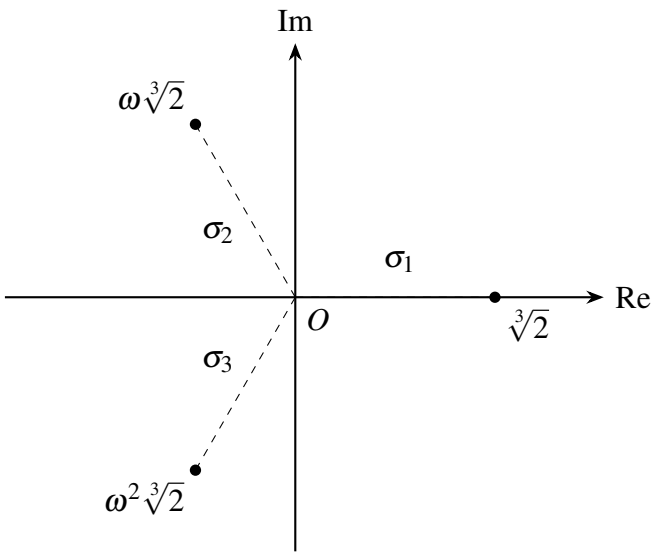


Figure 2.1: Only σ_1 is an automorphism

More generally, if K and L are number fields such that $K \subseteq L$, then every embedding of K in $\mathbb{C}$ extends to exactly $[L:K]$ embeddings of L in $\mathbb{C}$. In particular, L has $[L:K]$ embeddings in $\mathbb{C}$ which leave each point of K fixed.

It is often preferable to work with automorphisms of a field rather than embeddings in $\mathbb{C}$, particularly if we wish to compose them with each other. A useful trick for replacing embeddings of a number field K with automorphisms is to construct a normal extension $K \subseteq L$ of $\mathbb{Q}$. Each embedding of K extends to $[L:K]$ embeddings of L, all of which are automorphisms of L since L is normal.

Example 2.11. Let $K = \mathbb{Q}\left[\sqrt[3]{2}\right]$ and $L = \mathbb{Q}\left[\sqrt[3]{2}, \zeta_3\right]$ be fields. Then, L is normal over K. Each embedding of K extends to two automorphisms of L. One should know from MA4203 Galois Theory as to how to describe the six automorphisms $\sigma : L \to L$ in terms of where $\sqrt[3]{2}$ and ζ_3 are mapped to.

To see why the extension is normal, recall that we need to prove that the minimal polynomial of K over every element in L splits over L. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $f(x) = x^3 - 2$ with roots being $\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}$. Since L contains all these roots, then L is a normal extension of K.

2.4 The Trace and the Norm

Definition 2.7 (trace and norm). For any number field K, we define the trace T and the norm N as follows: let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$, where $n = [K : \mathbb{Q}]$. For each $\alpha \in K$, set

$$T(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha) \quad \text{and} \quad N(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha).$$

Example 2.12 (visualising trace and norm). For example, let $K = \mathbb{Q}\left[\sqrt{2}\right]$ and $\alpha = 3 + 2\sqrt{2}$. The two embeddings are $\sigma_1(\alpha) = 3 + 2\sqrt{2}$ and $\sigma_2(\alpha) = 3 - 2\sqrt{2}$. So, we send α to the point

$$\alpha \mapsto (\sigma_1(\alpha), \sigma_2(\alpha)) = \left(3 + 2\sqrt{2}, 3 - 2\sqrt{2}\right)$$

on the Cartesian plane. Clearly, $T(\alpha)$ is the sum of the coordinates, while $N(\alpha)$ is the product of the coordinates (Figure 2.2). The method to visualise this is known as Minkowski embedding, which is formally defined as a way to turn a number field into a lattice inside Euclidean space.

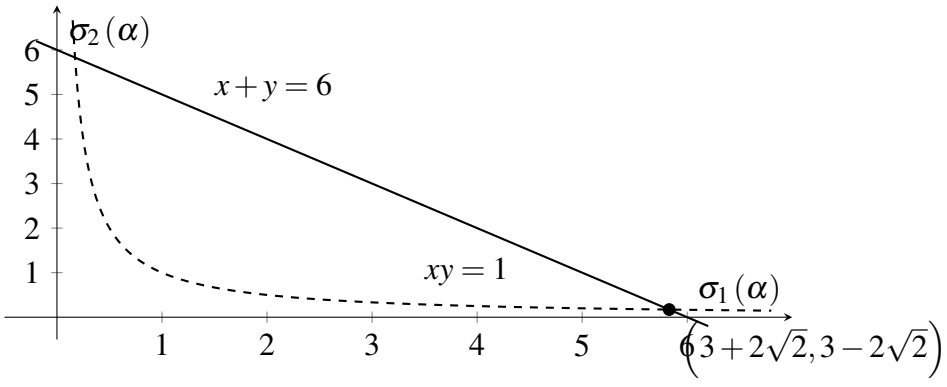


Figure 2.2: Visualising trace and norm

We see that $T(\alpha)$ and $N(\alpha)$ depend on K as well as α. When more than one field is involved, we will write $T^K(\alpha)$ and $N^K(\alpha)$ to avoid confusion.

Lemma 2.4. For all $\alpha, \beta \in K$, we have

$$T(\alpha+\beta) = T(\alpha) + T(\beta) \quad \text{and} \quad N(\alpha\beta) = N(\alpha)N(\beta). \tag{2.1}$$

Moreover, for $r \in \mathbb{Q}$, we have

$$T(r) = nr \quad \text{and} \quad N(r) = r^n. \tag{2.2}$$

If we further assume that $\alpha \in K$, then

$$T(r\alpha) = rT(\alpha) \quad \text{and} \quad N(r\alpha) = r^n N(\alpha). \tag{2.3}$$

Proof. Let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the $n = [K : \mathbb{Q}]$ embeddings of K into $\mathbb{C}$. Recall from Definition 2.7 that for every $\gamma \in K$, we define

$$T(\gamma) = \sum_{i=1}^{n} \sigma_i(\gamma) \quad \text{and} \quad N(\gamma) = \prod_{i=1}^{n} \sigma_i(\gamma).$$

Let $\alpha, \beta \in K$. Since each σ_i is a field homomorphism, we have

$$\sigma_i(\alpha+\beta) = \sigma_i(\alpha) + \sigma_i(\beta).$$

Hence,

$$T(\alpha+\beta) = \sum_{i=1}^{n} \sigma_i(\alpha+\beta) = \sum_{i=1}^{n} (\sigma_i(\alpha) + \sigma_i(\beta)) = \sum_{i=1}^{n} \sigma_i(\alpha) + \sum_{i=1}^{n} \sigma_i(\beta) = T(\alpha) + T(\beta).$$

Similarly, since each σ_i is multiplicative, we have

$$\sigma_i(\alpha\beta) = \sigma_i(\alpha)\sigma_i(\beta).$$

Therefore,

$$N(\alpha\beta) = \prod_{i=1}^{n} \sigma_i(\alpha\beta) = \prod_{i=1}^{n} (\sigma_i(\alpha)\sigma_i(\beta)) = \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right)\left(\prod_{i=1}^{n} \sigma_i(\beta)\right) = N(\alpha)N(\beta).$$

This proves (2.1). Next, let $r \in \mathbb{Q}$. Since every embedding $\sigma_i : K \hookrightarrow \mathbb{C}$ fixes $\mathbb{Q}$, we have $\sigma_i(r) = r$. Thus,

$$T(r) = \sum_{i=1}^{n} \sigma_i(r) = \sum_{i=1}^{n} r = nr \quad \text{and} \quad N(r) = \prod_{i=1}^{n} \sigma_i(r) = \prod_{i=1}^{n} r = r^n.$$

This proves (2.2). Finally, let $r \in \mathbb{Q}$ and $\alpha \in K$. Since each σ_i fixes r, we have

$$\sigma_i(r\alpha) = \sigma_i(r)\sigma_i(\alpha) = r\sigma_i(\alpha).$$

Therefore,

$$T(r\alpha) = \sum_{i=1}^{n} \sigma_i(r\alpha) = \sum_{i=1}^{n} r\sigma_i(\alpha) = r\sum_{i=1}^{n} \sigma_i(\alpha) = rT(\alpha).$$

Similarly,

$$N(r\alpha) = \prod_{i=1}^{n} \sigma_i(r\alpha) = \prod_{i=1}^{n} (r\sigma_i(\alpha)) = r^n \prod_{i=1}^{n} \sigma_i(\alpha) = r^n N(\alpha).$$

□

Suppose α has degree d over $\mathbb{Q}$. That is to say, the irreducible polynomial for α over $\mathbb{Q}$ has degree d, or equivalently, α has d conjugates over $\mathbb{Q}$. This can also be written as $[\mathbb{Q}[\alpha]:\mathbb{Q}]=d$.

Definition 2.8. Let K be a number field and $\alpha \in K$. Suppose $[\mathbb{Q}[\alpha]:\mathbb{Q}]=d$. Then, define $t(\alpha)$ and $n(\alpha)$ to be the sum and product, respectively, of the d conjugates of α over $\mathbb{Q}$.

Theorem 2.4. Let $n=[K:\mathbb{Q}]$. We have

$$T(\alpha)=\frac{n}{d}t(\alpha) \quad \text{and} \quad N(\alpha)=(n(\alpha))^{\frac{n}{d}}.$$

We first remark that n/d is an integer. To see why, recall that $[\mathbb{Q}[\alpha]:\mathbb{Q}]=d$ and $n=[K:\mathbb{Q}]$, so by the tower theorem, we have $n/d=[K:\mathbb{Q}[\alpha]]$.

Proof. $t(\alpha)$ refers to the trace $T^{\mathbb{Q}[\alpha]}$ of α. Each embedding of $\mathbb{Q}[\alpha]$ in $\mathbb{C}$ extends to exactly n/d embeddings of K in $\mathbb{C}$. The same can be said for the relationship between $N(\alpha)$ and $n(\alpha)$. □

Corollary 2.8. $T(\alpha)$ and $N(\alpha)$ are rational.

Proof. It suffices to prove that $t(\alpha)$ and $n(\alpha)$ are rational. This is obvious by considering the monic irreducible polynomial for α over $\mathbb{Q}$, for which we have $-t(\alpha)$ being the second coefficient and $\pm n(\alpha)$ being the constant term. □

Corollary 2.9. If α is an algebraic integer, then $T(\alpha)$ and $N(\alpha)$ are integers.

Proof. This follows from the fact that the monic polynomial for α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$. □

Example 2.13. Consider the quadratic field $K=\mathbb{Q}[\sqrt{m}]$. Then, for any $a,b\in\mathbb{Q}$, we have

$$T\left(a+b\sqrt{m}\right)=2a \quad \text{and} \quad N\left(a+b\sqrt{m}\right)=a^2-mb^2.$$

since the only embeddings are the identity automorphism or the one which sends $a+b\sqrt{m}$ to $a-b\sqrt{m}$. In this case, α is an algebraic integer if and only if its norm and trace are both in $\mathbb{Z}$.

Suppose we wish to determine the units in the ring $\mathbb{A}\cap K$ of algebraic integers in K. We claim that every unit has norm ± 1. This is because for any $\alpha,\beta\in\mathbb{A}\cap K$ such that $\alpha\beta=1$, we have $N(\alpha\beta)=N(\alpha)N(\beta)$ by the multiplicativity of the norm function. Hence, $N(\alpha\beta)=1$, which implies $N(\alpha)=1/N(\beta)$. Using the fact that $N(\alpha),N(\beta)\in\mathbb{Z}$, the result follows.

On the other hand, if α is an algebraic integer having norm ± 1, then $1/\alpha$ is also an

algebraic integer since all conjugates of α are algebraic integers. This shows that the units in $\mathbb{A} \cap K$ are the elements having norm ± 1.

Example 2.14. The only units in $\mathbb{Z}\left[\sqrt{-2}\right]$ are ± 1. On the other hand, the units in $\mathbb{Z}\left[\sqrt{2}\right]$ correspond to the integer solutions of the Pell-type equation $a^2 - 2b^2 = \pm 1$ and in fact, there are infinitely many of them.

Example 2.15 (Marcus p. 30 Question 13). Show that 1 and -1 are the only units in the ring $\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$, m squarefree, $m < 0$, $m \neq -1, -3$. What if $m = -1$ or $m = -3$?

Solution. Let $K = \mathbb{Q}[\sqrt{m}]$, where $m < 0$ and m is squarefree. Write $d = -m > 0$. Let $\alpha \in \mathcal{O}_K = \mathbb{A} \cap K$ be a unit. Then there exists $\beta \in \mathcal{O}_K$ such that $\alpha\beta = 1$. Taking norms, we get

$$N(\alpha)N(\beta) = 1.$$

Since α and β are algebraic integers, their norms are rational integers. Hence, $N(\alpha) = \pm 1$. But K is imaginary quadratic, so

$$N(\alpha) = \alpha\overline{\alpha} = |\alpha|^2 \geq 0.$$

Since $\alpha \neq 0$, we must have $N(\alpha) = 1$. We now determine all algebraic integers in K with norm 1.

First, suppose $m \not\equiv 1 \pmod 4$. Recall that we consider modulo 4 due to Corollary 2.2. Then, $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$. So, we may write

$$\alpha = a + b\sqrt{m} \quad \text{where } a, b \in \mathbb{Z}.$$

Then,

$$N(\alpha) = \left(a + b\sqrt{m}\right)\left(a - b\sqrt{m}\right) = a^2 - mb^2 = a^2 + db^2.$$

Since $N(\alpha) = 1$, we have $a^2 + db^2 = 1$. If $d \neq 1$, then $d \geq 2$, so the only integer solutions are $(a, b) = (\pm 1, 0)$ which implies $\alpha = \pm 1$. The excluded case $d = 1$ is exactly $m = -1$.

Next, suppose $m \equiv 1 \pmod 4$. Then,

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1 + \sqrt{m}}{2}\right].$$

Equivalently, every element of $\mathcal{O}_K$ can be written as

$$\alpha = \frac{a + b\sqrt{m}}{2} \quad \text{where } a, b \in \mathbb{Z} \text{ and } a \equiv b \pmod 2.$$

Then,

$$N(\alpha) = \frac{(a + b\sqrt{m})(a - b\sqrt{m})}{4} = \frac{a^2 - mb^2}{4} = \frac{a^2 + db^2}{4}.$$

Since $N(\alpha) = 1$, we get

$$a^2 + db^2 = 4.$$

Now $m \equiv 1 \pmod 4$, so $d = -m \equiv 3 \pmod 4$. If $d \neq 3$, then $d \geq 7$. Hence $b \neq 0$ would imply $a^2 + db^2 \geq 7 > 4$ which is impossible. As such, $b = 0$. Then, $a^2 = 4$ so $a = \pm 2$.

Thus, $\alpha = \pm 1$.

The excluded case $d = 3$ is exactly $m = -3$. Therefore, if $m < 0$, $m \neq -1, -3$, then the only units in $\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$ are ± 1.

On the other hand, if $m = -1$, then $K = \mathbb{Q}[i]$ so $\mathcal{O}_K = \mathbb{Z}[i]$. For $\alpha = a + bi \in \mathbb{Z}[i]$, we have $N(\alpha) = a^2 + b^2$. So, α is a unit if and only if $a^2 + b^2 = 1$. The solutions are $(a,b) = (\pm 1, 0), (0, \pm 1)$. Hence, the units are $\{\pm 1, \pm i\}$.

If $m = -3$, then

$$K = \mathbb{Q}\left[\sqrt{-3}\right] \quad \text{and} \quad \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right].$$

The units are the six roots of unity $\pm 1, \pm\zeta_3, \pm\zeta_3^2$. □

Example 2.16 (Marcus p. 30 Question 14). Show that $1 + \sqrt{2}$ is a unit in $\mathbb{Z}\left[\sqrt{2}\right]$, but not a root of unity. Use the powers of $1 + \sqrt{2}$ to generate infinitely many solutions to the Diophantine equation $a^2 - 2b^2 = \pm 1$. It will be shown in Chapter 5 that all units in $\mathbb{Z}\left[\sqrt{2}\right]$ are of the form $\pm\left(1 + \sqrt{2}\right)^k$, $k \in \mathbb{Z}$.

Solution. We use the formula $N\left(a + b\sqrt{2}\right) = a^2 - 2b^2$ to show that $N\left(1 + \sqrt{2}\right) = -1$. So, $1 + \sqrt{2}$ is a unit. However, it is not a root of unity since the complex number $1 + \sqrt{2}$ is of length $\sqrt{3}$, which is not equal to 1.

We then consider some powers of $1 + \sqrt{2}$. Note that

$$a^2 - 2b^2 = \pm 1 \quad \text{is equivalent to} \quad \left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right) = \pm 1.$$

So, $\left(1 + \sqrt{2}\right)^n$ is of norm $(-1)^n$. As such, we can generate infinitely many solutions to the Diophantine equation $a^2 - 2b^2 = \pm 1$.[5] □

The norm can also be used to show that certain elements are irreducible in $\mathbb{A} \cap K$. Clearly, $\alpha \in \mathbb{A} \cap K$ is irreducible in $\mathbb{A} \cap K$ whenever its norm is a prime in $\mathbb{Z}$. However, the converse may not be true.

Example 2.17. In $\mathbb{Z}\left[\sqrt{10}\right]$, we have $N\left(9 + \sqrt{10}\right) = 71$ which is prime[6] so $9 + \sqrt{10}$ is irreducible in $\mathbb{Z}\left[\sqrt{10}\right]$.

As an application of the trace, we can show that certain fields cannot contain certain elements.

Example 2.18 (Marcus p. 30 Question 16). Set $\alpha = \sqrt[4]{2}$. Use the trace $T^{\mathbb{Q}[\alpha]}$ to show that $\sqrt{3} \notin \mathbb{Q}[\alpha]$. To do this, you can write

$$\sqrt{3} = a + b\alpha + c\alpha^2 + d\alpha^3$$

[5] For example, when $n = 2$, we have $\left(1 + \sqrt{2}\right)^2 = 3 + 2\sqrt{2}$ which is of norm 1. Then, a solution to $a^2 - 2b^2 = 1$ is $(a,b) = (3,2)$.

[6] To see why, $N\left(a + b\sqrt{10}\right) = a^2 - 10b^2$.

and successively show that $a=0, b=0, c=0$, and finally, obtain a contradiction. Determine what $T\left(\frac{\sqrt{3}}{\alpha}\right)$ is in the meantime.

Solution. Note that α is a solution to $x^4-2=0$. This is the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$. In fact, the four solutions are $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$. Each of these roots defines an embedding $\sigma_i : \mathbb{Q}[\alpha] \hookrightarrow \mathbb{C}$, where

$$\sigma_1 : \sqrt[4]{2} \mapsto \sqrt[4]{2} \quad \sigma_2 : \sqrt[4]{2} \mapsto -\sqrt[4]{2} \quad \sigma_3 : \sqrt[4]{2} \mapsto i\sqrt[4]{2} \quad \sigma_4 : \sqrt[4]{2} \mapsto -i\sqrt[4]{2}.$$

Consider writing $\sqrt{3}$ as

$$\sqrt{3} = a + b\alpha + c\alpha^2 + d\alpha^3 \quad \text{where } a,b,c,d \in \mathbb{Q}. \tag{2.4}$$

Applying the trace to both sides, $0 = T\left(\sqrt{3}\right) = 4a$ so $a=0$. Hence,

$$\sqrt{3} = b\alpha + c\alpha^2 + d\alpha^3.$$

Dividing both sides by α,

$$\frac{\sqrt{3}}{\alpha} = b + c\alpha + d\alpha^2.$$

Applying the trace to both sides, $0 = T\left(\frac{\sqrt{3}}{\alpha}\right) = 4b$ so $b=0$. Consequently, one can prove that $c=0$.

By re-looking at (2.4), $\sqrt{3} = d\alpha^3$, where $d \in \mathbb{Q}$. Raising both sides by a power of 4, $9 = 8d^6$, but this implies d is irrational, which leads to a contradiction. □

The trace is also closely connected with the discriminant, which we will define in Chapter 2.5. First, we shall generalise the trace and the norm by replacing $\mathbb{Q}$ with an arbitrary number field.

Definition 2.9 (relative trace and relative norm). Let K and L be number fields such that $K \subseteq L$. Suppose $\sigma_1, \ldots, \sigma_n$ are the embeddings of L in $\mathbb{C}$ which fix K pointwise, where $n = [L:K]$. For $\alpha \in L$, define the relative trace and relative norm by

$$T_K^L(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha) \quad \text{and} \quad N_K^L(\alpha) = \sigma_1(\alpha)\cdots\sigma_n(\alpha).$$

Using this notation, we have $T^K = T_{\mathbb{Q}}^K$ and $N^K = N_{\mathbb{Q}}^K$.

As such, by considering Definitions 2.7 and 2.9, the relative trace T_K^L sums only embeddings fixing K, whereas the absolute trace $T_{\mathbb{Q}}^L$ sums all embeddings fixing $\mathbb{Q}$.

Lemma 2.5. For all $\alpha, \beta \in L$, we have

$$T_K^L(\alpha+\beta) = T_K^L(\alpha) = T_K^L(\beta) \quad \text{and} \quad N_K^L(\alpha\beta) = N_K^L(\alpha)N_K^L(\beta).$$

For all $\delta \in K$, we have

$$T_K^L(\delta) = n\delta \quad \text{and} \quad N_K^L(\delta) = \delta^n.$$

Furthermore, if $\alpha \in L$, we have

$$T_K^L(\delta\alpha) = \delta T_K^L(\alpha) \quad \text{and} \quad N_K^L(\delta\alpha) = \delta^n N_K^L(\alpha).$$

Similar to Theorem 2.4, we have the following result:

Theorem 2.5. Let $\alpha \in L$ and let d be the degree of α over K. Let $t(\alpha)$ and $n(\alpha)$ be the sum and product of the d conjugates of α over K. Then,

$$T_K^L(\alpha) = \frac{n}{d} t(\alpha) \quad \text{and} \quad N_K^L(\alpha) = (n(\alpha))^{n/d}.$$

Corollary 2.10. $T_K^L(\alpha), N_K^L(\alpha) \in K$. If $\alpha \in \mathbb{A} \cap L$, then they are in $\mathbb{A} \cap K$.

When there are three different fields, the relative traces and norms are related in the following way (Theorem 2.6).

Theorem 2.6 (tower formula for trace and norm). Let K, L, M be number fields such that $K \subseteq L \subseteq M$. Then, for all $\alpha \in M$, we have

$$T_K^L\left(T_L^M(\alpha)\right) = T_K^M(\alpha) \quad \text{and} \quad N_K^L\left(N_L^M(\alpha)\right) = N_K^M(\alpha).$$

2.5 The Discriminant of an n-tuple

Definition 2.10 (discriminant). Let K be a number field such that $[K : \mathbb{Q}] = n$. Let $\sigma_1, \ldots, \sigma_n$ denote the n embeddings of K in $\mathbb{C}$. For any n-tuple of elements $\alpha_1, \ldots, \alpha_n \in K$, define the discriminant of $\alpha_1, \ldots, \alpha_n$ to be

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \left|\sigma_i\left(\alpha_j\right)\right|^2. \tag{2.5}$$

In Definition 2.10, the right side of (2.5) refers to the square of the determinant of the matrix whose (i, j)-entry is $\sigma_i\left(\alpha_j\right)$. Note that the square makes the discriminant independent of the ordering of the σ_i's and α_j's.

We can express the discriminant in terms of the trace $T = T^K$.

Example 2.19 (Marcus p. 30 Question 19). Let R be a commutative ring and fix elements

$a_1, a_2, \ldots \in R$. Then, one can prove by induction that the Vandermonde determinant

$$\det \begin{bmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{bmatrix} \quad \text{is equal to the product} \quad \prod_{1 \le r < s \le n} (a_s - a_r).$$

In particular, if we assume that the result holds for some n, consider the determinant

$$\det \begin{bmatrix} 1 & a_1 & \cdots & a_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^n \\ 1 & a_{n+1} & \cdots & a_{n+1}^n \end{bmatrix} = \det \begin{bmatrix} 1 & a_1 & \cdots & f(a_1) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & f(a_n) \\ 1 & a_{n+1} & \cdots & f(a_{n+1}) \end{bmatrix}$$

for any monic polynomial f over R of degree n. In fact, f can be cleverly chosen so that the determinant is easily calculated. In particular, we can set $f(x) = (x - a_1) \cdots (x - a_n)$.

Theorem 2.7. We have $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \left| T\left(\alpha_i \alpha_j\right) \right|$.

Proof. This follows from the matrix equation

$$\left[\sigma_j(\alpha_i)\right]\left[\sigma_i\left(\alpha_j\right)\right] = \left[\sigma_1\left(\alpha_i\alpha_j\right) + \cdots + \sigma_n\left(\alpha_i\alpha_j\right)\right] = \left[T\left(\alpha_i\alpha_j\right)\right]$$

and familiar properties of the determinant, which are namely $\left|a_{ij}\right| = \left|a_{ji}\right|$[7] and $\det(\mathbf{AB}) = \det(\mathbf{A})\det(\mathbf{B})$. □

Corollary 2.11. We have $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$. Furthermore, if $\alpha_i \in \mathbb{A}$, then $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.

Theorem 2.8. We have

$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0$ if and only if $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$.

The proof of this theorem requires some basic knowledge of linear algebra. It also shows that every basis for K over $\mathbb{Q}$ has a non-zero discriminant. We can obtain a relatively simple formula for the discriminant for the case of a basis consisting of the powers of a single element.

Theorem 2.9. Suppose $K = \mathbb{Q}[\alpha]$ and let $\alpha_1, \ldots, \alpha_n$ denote the conjugates of α over $\mathbb{Q}$. Then,

$$\operatorname{disc}\left(1, \alpha, \ldots, \alpha^{n-1}\right) = \prod_{1 \le r < s \le n} (\alpha_r - \alpha_s)^2 = \pm N^K\left(f'(\alpha)\right).$$

Here, f is the monic irreducible polynomial for α over $\mathbb{Q}$. Also, the $+$ sign holds if and only if $n \equiv 0, 1 \pmod 4$.

[7] This merely involves the determinant of the transpose of a matrix

Example 2.20. We shall compute $\operatorname{disc}\left(1,\omega,\ldots,\omega^{p-2}\right)$, where $\omega = e^{\frac{2\pi i}{p}}$ and p is an odd prime. Also, the field K is $\mathbb{Q}[\omega]$. By the definition of the p^{th} cyclotomic polynomial, we know that

$$f(x) = 1 + x + x^2 + \ldots + x^{p-1}.$$

The easiest way to compute $f'(\omega)$ is to consider f as a geometric series, and then write $x^p - 1 = (x-1) f(x)$. Differentiating both sides yields

$$px^{p-1} = f(x) + (x-1) f'(x) \quad \text{so} \quad f'(\omega) = \frac{p}{\omega(\omega-1)}.$$

Taking norms, we obtain

$$N\left(f'(\omega)\right) = \frac{N(p)}{N(\omega)N(\omega-1)}.$$

Since $K = \mathbb{Q}[\omega]$ has degree $p-1$, we have $N(p) = p^{p-1}$ by (2.2). Also, since ω is a root of unity, then $N(\omega) = 1$. Next,

$$N(1-\omega) = \prod_{1 \le a \le p-1} (1 - \omega^a)$$

but we note that

$$f(x) = \prod_{1 \le a \le p-1} (x - \omega^a).$$

Substituting $x = 1$, we see that

$$f(1) = \prod_{1 \le a \le p-1} (1 - \omega^a) = p.$$

So, $N(1-\omega) = p$. Since $p-1$ is even, we also have

$$N(\omega - 1) = N(-(1-\omega)) = (-1)^{p-1} N(1-\omega) = p.$$

As such,

$$N\left(f'(\omega)\right) = \frac{N(p)}{N(\omega)N(\omega-1)} = \frac{p^{p-1}}{1 \cdot p} = p^{p-2}.$$

Now, since ω has minimal polynomial $f(x)$ over $\mathbb{Q}$, the discriminant of the power basis $1, \omega, \ldots, \omega^{p-2}$ is given by

$$\operatorname{disc}\left(1,\omega,\ldots,\omega^{p-2}\right) = (-1)^{\frac{(p-1)(p-2)}{2}} N\left(f'(\omega)\right).$$

Since p is odd, this sign is equivalently $(-1)^{\frac{p-1}{2}}$. Hence,

$$\operatorname{disc}\left(1,\omega,\ldots,\omega^{p-2}\right) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Example 2.21 (Marcus p. 31 Question 21). Let α be an algebraic integer and let f be a monic polynomial over $\mathbb{Z}$ (not necessarily irreducible) such that $f(\alpha) = 0$. Show that $\operatorname{disc}(\alpha)$ divides $N^{\mathbb{Q}[\alpha]} f'(\alpha)$.

Solution. Let $g(x)$ denote the minimal polynomial of α. Since α satisfies $f(\alpha)=0$, then α also satisfies $g(\alpha)=0$. As f and g are monic polynomials in $\mathbb{Z}[x]$, Gauss' lemma implies there exists $h(x)\in\mathbb{Z}[x]$ such that

$$f(x)=g(x)h(x).$$

Differentiating both sides yields

$$f'(x)=g(x)h'(x)+g'(x)h(x).$$

Substituting $x=\alpha$ yields

$$f'(\alpha)=g(\alpha)h'(\alpha)+g'(\alpha)h(\alpha)=g'(\alpha)h(\alpha).$$

Taking norms (and using the fat that it is multiplicative),

$$N\left(f'(\alpha)\right)=N\left(g'(\alpha)\right)N\left(h(\alpha)\right).$$

Since g is the minimal polynomial of α, then g is irreducible. By Theorem 2.9,

$$N\left(g'(\alpha)\right)=\pm\operatorname{disc}(\alpha)\quad\text{so}\quad N\left(f'(\alpha)\right)=\pm\operatorname{disc}(\alpha)N\left(h(\alpha)\right).$$

The result follows. □

Example 2.22 (Marcus p. 29 Question 8).

(a) Let $\omega=e^{\frac{2\pi i}{p}}$, where p is an odd prime. Show that[8]

$$\mathbb{Q}[\omega]\text{ contains }\begin{cases}\sqrt{p} & \text{if } p\equiv 1 \pmod 4;\\ \sqrt{-p} & \text{if } p\equiv -1 \pmod 4\end{cases}. \tag{2.6}$$

Express $\sqrt{-3}$ and $\sqrt{5}$ as polynomials in the appropriate ω.

(b) Show that the 8th cyclotomic field contains $\sqrt{2}$.

(c) Show that every quadratic field is contained in a cyclotomic field.

Solution.

(a) Let $\omega=e^{\frac{2\pi i}{p}}$, where p is an odd prime. Recall that the embeddings of $\mathbb{Q}[\omega]$ into $\mathbb{C}$ are given by

$$\sigma_a(\omega)=\omega^a\quad\text{where } a=1,2,\ldots,p-1.$$

Hence, the discriminant of the basis $1,\omega,\omega^2,\ldots,\omega^{-2}$ is

$$\operatorname{disc}\left(1,\omega,\omega^2,\ldots,\omega^{p-2}\right)=\left|\sigma_a\left(\omega^{b-1}\right)\right|^2.$$

Set $\Delta=\left|\sigma_a\left(\omega^{b-1}\right)\right|$. Then, $\Delta\in\mathbb{Q}[\omega]$. Since $\det(\omega)=(-1)^{\frac{p-1}{2}}p^{p-2}$ by Example 2.20, we have

$$\Delta^2=(-1)^{\frac{p-1}{2}}p^{p-2}.$$

[8] A hint is to recall that $\operatorname{disc}(\omega)=\pm p^{p-2}$ with $+$ holding if and only if $p\equiv 1 \pmod 4$.

Define

$$\eta = \frac{\Delta}{p^{\frac{p-3}{2}}},$$

which is an element of $\mathbb{Q}[\omega]$, and

$$\eta^2 = \frac{\Delta^2}{p^{p-3}} = (-1)^{\frac{p-1}{2}} p.$$

Hence,

$$\eta^2 = \begin{cases} p & \text{if } p \equiv 1 \pmod 4; \\ -p & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

Thus, (2.6) holds.

Next, for $p = 3$, let $\omega = e^{\frac{2\pi i}{3}}$. Since $\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$, we obtain $\sqrt{-3} = 1 + 2\omega$. For $p = 5$, let $\omega = e^{\frac{2\pi i}{5}}$. Then,

$$\omega + \omega^{-1} = 2\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{2}.$$

Since $\omega^{-1} = \omega^4$, we have

$$\sqrt{5} = 1 + 2\left(\omega + \omega^4\right).$$

(b) The 8th root of unity is $\zeta_8 = e^{\frac{2\pi i}{8}}$. Note that $\zeta_8 + \zeta_8^{-1} = 2\cos\left(\frac{\pi}{4}\right) = \sqrt{2}$ and because $\zeta_8^{-1} = \zeta_8^7$, we have

$$\sqrt{2} = \zeta_8 + \zeta_8^7.$$

The result follows.

(c) We show that every quadratic field is contained in a cyclotomic field. Let $K = \mathbb{Q}\left[\sqrt{d}\right]$, where $d \neq 1$ is a squarefree integer. Write

$$d = \pm 2^{\varepsilon} q_1 q_2 \cdots q_r,$$

where $\varepsilon \in \{0, 1\}$ and $q_1, \ldots, q_r$ are distinct odd primes. Choose

$$N = 8 q_1 q_2 \cdots q_r.$$

Then, $\mathbb{Q}[\zeta_N]$ contains $\mathbb{Q}[\zeta_8]$, and hence contains $\sqrt{2}$ and i. Also, for each odd prime q_j, it contains $\mathbb{Q}\left[\zeta_{q_j}\right]$. By **(a)**,

$$\mathbb{Q}\left[\zeta_{q_j}\right] \text{ contains } \begin{cases} \sqrt{q_j} & \text{if } q_j \equiv 1 \pmod 4; \\ \sqrt{-q_j} & \text{if } q_j \equiv -1 \pmod 4. \end{cases}$$

If $q_j \equiv -1 \pmod 4$, then since $i \in \mathbb{Q}[\zeta_N]$, we also have $i\sqrt{-q_j} \in \mathbb{Q}[\zeta_N]$ and $\left(i\sqrt{-q_j}\right)^2 = q_j$. Thus, $\mathbb{Q}[\zeta_N]$ contains $\sqrt{q_j}$ for every odd prime q_j. Since it also contains $\sqrt{2}$, it contains

$$\sqrt{|d|} = \left(\sqrt{2}\right)^{\varepsilon} \sqrt{q_1}\sqrt{q_2}\cdots\sqrt{q_r}.$$

If $d > 0$, then

$$\sqrt{d} = \sqrt{|d|} \in \mathbb{Q}[\zeta_N].$$

If $d < 0$, then

$$\sqrt{d} = i\sqrt{|d|} \in \mathbb{Q}[\zeta_N].$$

Therefore, $\mathbb{Q}\left[\sqrt{d}\right] \subseteq \mathbb{Q}[\zeta_N]$. Hence every quadratic field is contained in a cyclotomic field. □

In fact, there is a precise way to state **(c)** of Example 2.22. That is, $\mathbb{Q}[\sqrt{m}]$ is contained in the d^{th} cyclotomic field, where $d = \operatorname{disc}(\mathbb{A} \cap \mathbb{Q}[\sqrt{m}])$ denotes discriminant.

Example 2.23 (Stickelberger's criterion; Marcus p. 31 Question 22). Let K be a number field of degree n over $\mathbb{Q}$ and fix algebraic integers $\alpha_1, \ldots, \alpha_n \in K$. We know that $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ is in $\mathbb{Z}$; we will show that $d \equiv 0$ or $1 \pmod 4$. Letting $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K in $\mathbb{C}$, we know that d is the square of the determinant $\left|\sigma_i(\alpha_j)\right|$. This determinant is a sum of $n!$ terms, one for each permutation of $\{1, \ldots, n\}$. Let P denote the sum of the terms corresponding to even permutations, and let N denote the sum of the terms (without negative signs) corresponding to odd permutations. Thus

$$d = (P-N)^2 = (P+N)^2 - 4PN.$$

Complete the proof by showing that $P+N$ and PN are in $\mathbb{Z}$.[9] In particular we have $\operatorname{disc}(\mathbb{A} \cap K) \equiv 0$ or $1 \pmod 4$. This is known as Stickelberger's criterion.

Solution. Let $\sigma_1, \ldots, \sigma_n$ be embeddings of K into $\mathbb{C}$. Set $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$. By Definition 2.10, $d = \left|\sigma_i(\alpha_j)\right|^2$. Expanding the determinant using Leibniz's formula,

$$\det\left(\sigma_i(\alpha_j)\right) = \sum_{\tau \in S_n} \operatorname{sgn}(\tau) \prod_{i=1}^{n} \sigma_i\left(\alpha_{\tau(i)}\right).$$

Let P denote the sum of the terms corresponding to even permutations, so

$$P = \sum_{\substack{\tau \in S_n \\ \tau \text{ even}}} \prod_{i=1}^{n} \sigma_i\left(\alpha_{\tau(i)}\right).$$

Next, let N denote the sum of the terms corresponding to odd permutations without negative signs, so

$$N = \sum_{\substack{\tau \in S_n \\ \tau \text{ odd}}} \prod_{i=1}^{n} \sigma_i\left(\alpha_{\tau(i)}\right).$$

It is easy to see that $\det = P - N$. Thus, to prove that $\operatorname{disc}(\mathbb{A} \cap K) \equiv 0$ or $1 \pmod 4$, it suffices to prove that $P+N \in \mathbb{Z}$ and $PN \in \mathbb{Z}$.

[9] A suggestion is to show that they are algebraic integers and that they are in $\mathbb{Q}$; for the latter, extend all σ_i to some normal extension L of $\mathbb{Q}$ so that they become automorphisms of L.

We first show that $P+N$ and PN are algebraic integers. Since each α_j is an algebraic integer, each conjugate $\sigma_i(\alpha_j)$ is also an algebraic integer. Hence, each product

$$\prod_{i=1}^{n} \sigma_i(\alpha_{\tau(i)}) \quad \text{is an algebraic integer.}$$

Since P and N are finite sums of algebraic integers, then P and N are algebraic integers. Consequently, $P+N$ and PN are algebraic numbers.

It remains to prove that $P+N$ and PN are rational numbers. Let $L/\mathbb{Q}$ be a normal extension containing K. Take for example, the Galois closure of K over $\mathbb{Q}$. Extend each embedding $\sigma_i : K \hookrightarrow \mathbb{C}$ to an automorphism of L. We will still denote these extensions by σ_i. Let $\rho \in \mathrm{Gal}(L/\mathbb{Q})$. Since ρ is an automorphism of L, the embeddings $\rho\sigma_1, \ldots, \rho\sigma_n$ are again precisely the n embeddings of K into $\mathbb{C}$. Thus ρ permutes the embeddings $\sigma_1, \ldots, \sigma_n$. Hence, there exists some permutation $\pi \in S_n$ such that

$$\rho\sigma_i = \sigma_{\pi(i)} \quad \text{where } i = 1, \ldots, n.$$

Now, apply ρ to $P+N$. We have

$$P+N = \sum_{\tau \in S_n} \prod_{i=1}^{n} \sigma_i(\alpha_{\tau(i)})$$

because $P+N$ is the sum of all determinant terms without signs. Therefore,

$$\rho(P+N) = \sum_{\tau \in S_n} \prod_{i=1}^{n} \rho\sigma_i(\alpha_{\tau(i)}).$$

Since $\rho\sigma_i = \sigma_{\pi(i)}$, this becomes

$$\rho(P+N) = \sum_{\tau \in S_n} \prod_{i=1}^{n} \sigma_{\pi(i)}(\alpha_{\tau(i)}).$$

Let $j = \pi(i)$. Then,

$$\rho(P+N) = \sum_{\tau \in S_n} \prod_{j=1}^{n} \sigma_j\left(\alpha_{\tau(\pi^{-1}(j))}\right).$$

As τ runs through S_n, the permutation $\tau \circ \pi^{-1}$ also runs through S_n. Hence, $\rho(P+N) = P+N$. Therefore, $P+N$ is fixed by every element of $\mathrm{Gal}(L/\mathbb{Q})$. Since $L/\mathbb{Q}$ is Galois, it follows that $P+N \in \mathbb{Q}$.

The proof that $PN \in \mathbb{Q}$ is similar. □

Definition 2.11 (abelian extension). An abelian extension is normal with an abelian Galois group.

More generally, Kronecker and Weber proved that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field. Hilbert and others investigated the abelian extensions of an arbitrary number field; their results are known in *class field theory*.

2.6 The Additive Structure of a Number Ring

Let K be a number field such that $[K:\mathbb{Q}] = n$ and let $R = \mathbb{A} \cap K$ be the ring of algebraic integers in K. We will use the discriminant to determine the additive structure of R. Specifically, we will show that R is a free abelian group of rank n.

> Definition 2.12 (free abelian group). A free abelian group of finite rank n is any group that is the direct sum of n subgroups, each of which is isomorphic to $\mathbb{Z}$.
>
> Equivalently, we can think of a free abelian group of rank n as one which is isomorphic to the additive group $\mathbb{Z}^n$ of lattice points in Euclidean n-space. The rank of such a group is well-defined as the $\mathbb{Z}^n$ are pairwise non-isomorphic.

Example 2.24 (Marcus p. 57 Question 3). Let G be a free abelian group of rank n with additive notation. Show that for any $m \in \mathbb{Z}$, G/mG is the direct sum of n cyclic groups of order m.

Solution. Up to isomorphism, there is only one free abelian group of rank n, which is $\mathbb{Z}^n$. Hence, it suffices to show that there exist n cyclic groups C_i, where $|C_i| = m$, such that

$$\mathbb{Z}^n/m\mathbb{Z}^n = \bigoplus_{i=1}^{n} C_i.$$

Note that every element of $\mathbb{Z}^n/m\mathbb{Z}^n$ is of the form $(a_1,\ldots,a_n)$, where $0 \le a_i \le m-1$ for all $1 \le i \le n$. Hence, $\mathbb{Z}^n/m\mathbb{Z}^n \cong (\mathbb{Z}/m\mathbb{Z})^n$ since each coordinate acts independently modulo m. Since $\mathbb{Z}/m\mathbb{Z}$ is a cyclic group of order n, we can choose each C_i to be as mentioned. □

The only thing we need to know about free abelian groups is the fact that every subgroup of a free abelian group of rank n is also a free abelian group of rank $\le n$. From this, it immediately follows that if a group is *sandwiched* between two free abelian groups of equal rank, then it too must be such a group, i.e. if $A \subseteq B \subseteq C$ and if A and C are both free abelian groups of rank n, then so is B. We will use this to establish the result for $R = \mathbb{A} \cap K$.

First, we claim that there exist bases for K over $\mathbb{Q}$ consisting entirely of algebraic integers. Such a basis can be obtained from any given basis by multiplying all members by a fixed integer. This follows immediately from the observation that for any $\alpha \in K$, there exists $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer. Fixing such a basis $\{\alpha_1,\ldots,\alpha_n\} \subseteq R$ for K over $\mathbb{Q}$, we have a free abelian group A of rank n inside R, i.e.

$$A = \left\{ \sum_{i=1}^{n} m_i\alpha_i : m_i \in \mathbb{Z} \right\} \quad \text{which is the additive group generated by the } \alpha_i\text{'s.}$$

We can express this as the direct sum

$$\mathbb{Z}\alpha_1 \oplus \ldots \oplus \mathbb{Z}\alpha_n \quad \text{which is free abelian of rank } n$$

since $\mathbb{Z}\alpha_i \cong \mathbb{Z}$ for all $1 \leq i \leq n$.

We have $A \subseteq R$. In order to prove that $R \subseteq A$, we need to use the discriminant.

Theorem 2.10. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for K over $\mathbb{Q}$ consisting entirely of algebraic integers. Set $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$. Then, every $\alpha \in R$ can be expressed as

$$\frac{1}{d}\sum_{i=1}^{n} m_i \alpha_i \quad \text{with } m_i \in \mathbb{Z} \text{ and } d \mid m_i^2.$$

Note that the formula is valid since $\{\alpha_1, \ldots, \alpha_n\}$ forms a basis for K over $\mathbb{Q}$ and d is a non-zero integer since the α_i's are algebraic integers.

Proof. Write α as a linear combination of the α_j's, i.e.

$$\alpha = \sum_{j=1}^{n} x_j \alpha_j \quad \text{where } x_j \in \mathbb{Q}.$$

Let $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K in $\mathbb{C}$ and we apply each σ_i to the above equation, for which we obtain

$$\sigma_i(\alpha) = \sum_{j=1}^{n} x_j \sigma_i(\alpha_j).$$

By Cramer's rule,

$$x_j = \frac{y_j}{\delta}, \quad \text{where } \delta \text{ is the determinant } \left|\sigma_i(\alpha_j)\right|$$

and y_j is obtained from δ by replacing the j^{th} column by the $\sigma_i(\alpha)$'s. It is clear that y_j and δ are algebraic integers. Moreover, $\delta^2 = d$. Hence, $dx_j = \delta y_j$, so dx_j is also an algebraic integer, i.e. $\mathbb{Z} \ni dx_j = m_j$.

It remains to show that $m_j^2/d \in \mathbb{Z}$. Note that this quantity is rational, so it suffices to prove that it is an algebraic integer. This is easy to see because

$$\frac{m_j^2}{d} = dx_j^2 = \frac{\delta^2 y_j^2}{d} = y_j^2.$$

□

Theorem 2.10 shows that

$$R \subseteq \frac{1}{d}A = \mathbb{Z}\frac{\alpha_1}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha_n}{d}.$$

Thus, R contains, and is contained in, free abelian groups of rank n. As such, we have the following corollary.

Corollary 2.12. R is a free Abelian group of rank n.

Corollary 2.12 is also equivalent to saying that R has a basis over $\mathbb{Z}$, i.e. for any $\alpha \in R$, there exist unique $\beta_1, \ldots, \beta_n \in R$ such that

$$\alpha = \sum_{i=1}^{n} m_i \beta_i \quad \text{where } m_i \in \mathbb{Z}.$$

We say that $\{\beta_1, \ldots, \beta_n\}$ is an integral basis for R, or a basis for R over $\mathbb{Z}$. Hence, $\{\beta_1, \ldots, \beta_n\}$ is also a basis for K over $\mathbb{Q}$.

Definition 2.13 (integral basis). Let K be a number field with $[K : \mathbb{Q}] = n$, and let R be the ring of integers of K. An integral basis for R is a set $\{\beta_1, \ldots, \beta_n\} \subseteq R$ such that every $\alpha \in R$ can be written uniquely in the form

$$\alpha = \sum_{i=1}^{n} m_i \beta_i,$$

where $m_i \in \mathbb{Z}$ for all i. Equivalently, R is a free abelian group with basis $\{\beta_1, \ldots, \beta_n\}$. In this case, $\{\beta_1, \ldots, \beta_n\}$ is also a basis for K over $\mathbb{Q}$.

Example 2.25. In the quadratic field $\mathbb{Q}[\sqrt{m}]$, where m squarefree,

$$\text{an integral basis for } R = \mathbb{A} \cap \mathbb{Q}\left[\sqrt{m}\right] \quad \text{consists of} \begin{cases} 1, \sqrt{m} & \text{if } m \equiv 2,3 \pmod 4; \\ 1, \frac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

In fact, this is not surprising.

As we have indicated, the ring of algebraic integers in the m^{th} cyclotomic field is $\mathbb{Z}[\omega]$, and hence an integral basis consists of $1, \omega, \ldots, \omega^{\varphi(m)-1}$. At this point, we can prove it for the case in which m is a power of a prime.

Theorem 2.11. Let $\omega = e^{\frac{2\pi i}{m}}$, where $m = p^r$ and p is prime. Then, $\mathbb{A} \cap \mathbb{Q}[\omega] = \mathbb{Z}[\omega]$.

To prove this theorem, we would need two lemmas. We will not prove the theorem.

Lemma 2.6. For all $m \geq 3$, we have

$$\mathbb{Z}[1-\omega] = \mathbb{Z}[\omega] \quad \text{and} \quad \operatorname{disc}(1-\omega) = \operatorname{disc}(\omega).$$

Proof. We have $\omega = 1 - (1-\omega)$, which implies $\mathbb{Z}[1-\omega] = \mathbb{Z}[\omega]$. Since α_i runs through the conjugates of ω, then $1 - \alpha_i$ runs through the conjugates of $1 - \omega$, which implies

$$\operatorname{disc}(\omega) = \prod_{r<s} (\alpha_r - \alpha_s)^2 = \prod_{r<s} ((1-\alpha_r) - (1-\alpha_s))^2 = \operatorname{disc}(1-\omega)$$

which concludes the proof. □

Lemma 2.7. Let p be a prime. If $m = p^r$, then

$$\prod_k \left(1 - \omega^k\right) = p$$

where the product is taken over all k such that $1 \leq k \leq m$ and p does not divide k.

A number ring has more than one integral basis, and there is not always an obvious choice. However, all of them have the same discriminant (Theorem 2.12).

Theorem 2.12 (integral bases of number ring have same discriminant). Let

$$\{\beta_1, \ldots, \beta_n\} \text{ and } \{\gamma_1, \ldots, \gamma_n\} \quad \text{be two integral bases for } R = \mathbb{A} \cap K.$$

Then, $\operatorname{disc}(\beta_1, \ldots, \beta_n) = \operatorname{disc}(\gamma_1, \ldots, \gamma_n)$.

Proof. Since each β_i can be written as an integer linear combination of γ_i, then we can write

$$\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \mathbf{M} \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix} \quad \text{where } \mathbf{M} \in \mathcal{M}_{n\times n}(\mathbb{Z}).$$

Applying each σ_j to each of the n equations yields the matrix equation $\left[\sigma_j(\beta_i)\right] = \mathbf{M}\left[\sigma_j(\gamma_i)\right]$. Taking determinants and squaring both sides, we obtain

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = (\det(\mathbf{M}))^2 \operatorname{disc}(\gamma_1, \ldots, \gamma_n).$$

Since $\mathbf{M} \in \mathcal{M}_{n\times n}(\mathbb{Z})$, then $\det(\mathbf{M}) \in \mathbb{Z}$, which shows that $\operatorname{disc}(\gamma_1, \ldots, \gamma_n)$ is a divisor of $\operatorname{disc}(\beta_1, \ldots, \beta_n)$, and both have the same sign. Also, recall that both of these discriminants are integers since β_i and γ_i are algebraic integers. By a symmetric argument, one can also prove that $\operatorname{disc}(\beta_1, \ldots, \beta_n)$ is a divisor of $\operatorname{disc}(\gamma_1, \ldots, \gamma_n)$, so the discriminants are equal. □

Definition 2.14 (discriminant of integral basis). The discriminant of an integral basis can be regarded as an invariant of the ring R. We shall denote it by $\operatorname{disc}(R)$. If $R = \mathbb{A} \cap K$, we write $\operatorname{disc}(K)$.

Example 2.26. Suppose the number field K denotes the quadratic field $\mathbb{Q}[\sqrt{m}]$, where m is squarefree. We have

$$\operatorname{disc}\left(\mathbb{A} \cap \mathbb{Q}\left[\sqrt{m}\right]\right) = \begin{cases} \operatorname{disc}(\sqrt{m}) = 4m & \text{if } m \equiv 2, 3 \pmod 4; \\ \operatorname{disc}\left(\frac{1+\sqrt{m}}{2}\right) = m & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

Example 2.27. One application of the discriminant is in identifying integral bases: assuming that $\alpha_1, \ldots, \alpha_n \in R$, they form an integral basis for R if and only if $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \operatorname{disc}(R)$.

As another application, recall that if ω is an m^{th} root of unity, where m is the power of a prime, then $\mathbb{A} \cap \mathbb{Q}[\omega] = \mathbb{Z}[\omega]$. We can generalise this to arbitrary cyclotomic fields. This will follow from a more general result relating the algebraic integers in a composite field KL to those in K and L. We know that if K and L are two number fields, then the composite KL, which is defined to be the smallest subfield of $\mathbb{C}$ containing K and L, consists of all finite sums

$$\alpha_1\beta_1 + \ldots + \alpha_r\beta_r \quad \text{where } \alpha_i \in K \text{ and } \beta_i \in L.$$

If we let R, S, T denote the rings of algebraic integers in K, L, KL respectively, then it is obvious that T contains the ring

$$RS = \{\alpha_1\beta_1 + \ldots + \alpha_r\beta_r : \alpha_i \in R, \beta_i \in S\}.$$

It is natural to ask whether equality holds, i.e. is it true whether $T \subseteq RS$? In general, it does not. However, we can show that $T = RS$ under certain conditions which are conveniently satisfied by cyclotomic fields.

Theorem 2.13 (integral basis for composition). Let $[K : \mathbb{Q}] = m$ and $[L : \mathbb{Q}] = n$, and $d = \gcd(\operatorname{disc}(R), \operatorname{disc}(S))$. Assume that $[KL : \mathbb{Q}] = mn$. Then, $T \subseteq \frac{1}{d}RS$.

In particular, we have the following corollary:

Corollary 2.13. If $[KL : \mathbb{Q}] = mn$ and $d = 1$, then $T = RS$.

To prove Theorem 2.13, one needs to use the following result from field theory: if $[KL : \mathbb{Q}] = mn$ and $\sigma : K \hookrightarrow \mathbb{C}$ and $\tau : L \hookrightarrow \mathbb{C}$ are embeddings, then there exists an embedding of KL in $\mathbb{C}$ which restricts to σ on K and to τ on L.

Corollary 2.14. Let $K = \mathbb{Q}[\omega]$, with $\omega = e^{\frac{2\pi i}{m}}$. Suppose $R = \mathbb{A} \cap K$. Then, $R = \mathbb{Z}[\omega]$.

It would be nice if every number ring had the form $\mathbb{Z}[\alpha]$ for some α. Unfortunately, this is not always the case. Equivalently, there may not exist an integral basis of the form $1, \alpha, \ldots, \alpha^{n-1}$. This suggests the following vague question: does there always exist an integral basis whose members are expressed in terms of a single element? Of course, the answer is yes since $K = \mathbb{Q}[\alpha]$ for some α so every member of K is a polynomial expression in α with coefficients in $\mathbb{Q}$. This is not particularly illuminating. However, what if we require that these polynomials have some special form? An answer is provided by the following result (Theorem 2.14).

Theorem 2.14. Let $\alpha \in R$ and suppose α has degree n over $\mathbb{Q}$. Then, there exists an integral basis

$$1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{n-1}(\alpha)}{d_{n-1}}$$

where the $d_i \in \mathbb{Z}$ satisfy $d_1 \mid d_2 \mid \ldots \mid d_{n-1}$; the f_i are monic polynomials over $\mathbb{Z}$ and

$\deg f_i = i$. The d_i are uniquely determined.

We have already seen Theorem 2.14 for quadratic fields: taking $\alpha = \sqrt{m}$, where m squarefree, we have the integral basis $\{1, \alpha\}$ if $m \equiv 2,3 \pmod 4$ and $\left\{1, \frac{\alpha+1}{2}\right\}$ if $m \equiv 1 \pmod 4$. Another good class of examples is provided by the pure cubic fields $\mathbb{Q}[\sqrt[3]{m}]$, where m is cubefree. Setting $\alpha = \sqrt[3]{m}$, we deduce the following result (Theorem 2.15).

Theorem 2.15 (integral basis for pure cubic fields). Let $\alpha = \sqrt[3]{m}$. If m is squarefree, then a basis for $R = \mathbb{A} \cap \mathbb{Q}[\alpha]$ consists of

$$\begin{aligned} 1, \alpha, \alpha^2 \quad &\text{if } m \not\equiv \pm 1 \pmod 9; \\ 1, \alpha, \frac{\alpha^2 \pm \alpha + 1}{3} \quad &\text{if } m \equiv \pm 1 \pmod 9 \end{aligned}$$

If m is not squarefree, define k to be the product of all primes which divide m twice, i.e. $m = hk^2$, with h and k squarefree and $\gcd(h,k) = 1$. Then, an integral basis for R consists of

$$\begin{aligned} 1, \alpha, \frac{\alpha^2}{k} \quad &\text{if } m \not\equiv \pm 1 \pmod 9; \\ 1, \alpha, \frac{\alpha^2 \pm k^2\alpha + k^2}{3k} \quad &\text{if } m \equiv \pm 1 \pmod 9 \end{aligned}$$

Example 2.28. Let $\alpha = \sqrt[3]{2}$. Since $m = 2$ is squarefree and $2 \not\equiv \pm 1 \pmod 9$, an integral basis for $R = \mathbb{A} \cap \mathbb{Q}\left[\sqrt[3]{2}\right]$ is $\{1, \alpha, \alpha^2\}$. Thus,

$$R = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2.$$

Example 2.29 (Marcus p. 33 Question 28). Let $f(x) = x^3 + ax + b$, a and $b \in \mathbb{Z}$, and assume f is irreducible over $\mathbb{Q}$. Let α be a root of f.

(a) Show that

$$f'(\alpha) = -\frac{2a\alpha + 3b}{\alpha}.$$

(b) Show that $2a\alpha + 3b$ is a root of

$$\left(\frac{x - 3b}{2a}\right)^3 + a\left(\frac{x - 3b}{2a}\right) + b.$$

Use this to find $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha + 3b)$.

(c) Show that $\operatorname{disc}(\alpha) = -\left(4a^3 + 27b^2\right)$.

(d) Suppose $\alpha^3 = \alpha + 1$. Prove that $\left\{1, \alpha, \alpha^2\right\}$ is an integral basis for $\mathbb{A} \cap \mathbb{Q}[\alpha]$. Do the same if $\alpha^3 + \alpha = 1$.

Solution.

(a) We have $f'(x) = 3x^2 + a$. As $f(\alpha) = 0$, then $\alpha^3 + a\alpha + b = 0$, so

$$f'(\alpha) = 3\alpha^2 + a = -\frac{2a\alpha + 3b}{\alpha}.$$

(b) The first part is left as an exercise. For the second part, suppose f is irreducible over $\mathbb{Q}$. Let $\alpha_1, \alpha_2, \alpha_3$ denote the conjugates of α and that the embeddings are $\sigma_i(\alpha) = \alpha_i$. Let $\beta = 2a\alpha + 3b$. Then,

$$\sigma_i(\beta) = 2a\sigma_i(\alpha) + 3b = 2a\alpha_i + 3b.$$

As such,

$$N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\beta) = \prod_{i=1}^{3} \sigma_i(\beta) = \prod_{i=1}^{3} (2a\alpha_i + 3b).$$

Since $\alpha_1, \alpha_2, \alpha_3$ are the roots of the equation $f(x) = 0$, then

$$f(x) = \prod_{i=1}^{3} (x - \alpha_i) = -\prod_{i=1}^{3} (\alpha_i - x).$$

Factoring $2a$ from the norm,

$$N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]} = (2a)^3 \prod_{i=1}^{3} \left(\alpha_i + \frac{3b}{2a} \right).$$

Set $x = -\frac{3b}{2a}$ so that

$$N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]} = -(2a)^3 f\left(-\frac{3b}{2a} \right) = b\left(4a^3 + 27b^2\right).$$

(c) Use Theorem 2.9.

(d) If $\alpha^3 = \alpha + 1$, then α is a root of the cubic equation $x^3 - x - 1 = 0$. This polynomial is irreducible over $\mathbb{Q}$ since it has no rational roots. By **(c)**, $\operatorname{disc}(\alpha) = -23$, which is squarefree. The result follows by p. 32 Question 27**(e)** of [1]. The second part has a similar argument. □

Chapter 3

Prime Decomposition in Number Rings

3.1 Introduction

We have seen that number rings are not always UFDs — elements may not factor uniquely into irreducibles. However, we will prove that the non-zero ideals in a number ring always factor uniquely into prime ideals. This can be regarded as a generalisation of unique factorisation in $\mathbb{Z}$, where the ideals are just the principal ideals (n) and the prime ideals are the ideals (p), where p is a prime integer.

We will show that number rings have three special properties and that any integral domain with these properties also has the unique factorisation property for ideals. Accordingly, we have the following definition on Dedekind domains (Definition 3.1).

Definition 3.1 (Dedekind domain). A Dedekind domain is an integral domain R such that the following conditions are satisfied:

(i) Every ideal is finitely generated

(ii) Every non-zero prime ideal is a maximal ideal

(iii) R is integrally closed in its field of fractions

$$K = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in R, \beta \neq 0 \right\}.$$

This means that if $\frac{\alpha}{\beta} \in K$ is a root of some monic polynomial over R, then in fact $\frac{\alpha}{\beta} \in R$.

Example 3.1 (examples of Dedekind domains).

(i) The ring $\mathbb{Z}$ is a Dedekind domain. Indeed, $\mathbb{Z}$ is an integral domain. Every ideal of $\mathbb{Z}$ is principal, hence finitely generated. Also, every non-zero prime ideal of $\mathbb{Z}$ is of

the form $p\mathbb{Z}$, where p is a prime number, and $p\mathbb{Z}$ is maximal since $\mathbb{Z}/p\mathbb{Z}$ is a field. Finally, $\mathbb{Z}$ is integrally closed in its field of fractions $\mathbb{Q}$.

(ii) Every PID is a Dedekind domain. Let R be a PID. Since every ideal of R is principal, every ideal is finitely generated. Also, in a PID, every non-zero prime ideal is maximal. Finally, every PID is integrally closed in its field of fractions. Hence, R is a Dedekind domain.

(iii) Here is a more relevant example. Let K be a number field and let $R = \mathbb{A} \cap K$ denote the ring of algebraic integers in K. Then R is a Dedekind domain. In particular, if $K = \mathbb{Q}\left[\sqrt{d}\right]$, then its ring of integers $\mathcal{O}_K$ is a Dedekind domain.

Definition 3.2 (Noetherian ring). Note that condition **(i)** of a Dedekind domain is equivalent to each of the following conditions:

(i) Every increasing sequence of ideals is eventually constant, i.e.

$$\text{if } I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \quad \text{then} \quad \text{all } I_n \text{ are equal for sufficiently large } n \tag{3.1}$$

(ii) Every non-empty set S of ideals has a maximal element, i.e.

$$\text{there exists } M \in S \quad \text{such that} \quad M \subseteq I \in S \text{ implies } M = I$$

Recall from MA3201 Algebra II any ring satisfying the either of the aforementioned two conditions in Definition 3.2 is said to be Noetherian.

Lemma 3.1 (Marcus p. 57 Question 1). **(i)** of Definition 3.1 and **(i)** and **(ii)** of Definition 3.2 are equivalent.

To be explicit, saying that an integral domain R is finitely generated is equivalent to saying that every increasing sequence of ideals in R is eventually constant, which is also equivalent to saying that every non-empty set S of ideals has a maximal element. We now prove this result.

Proof. We first prove that if an integral domain R is finitely generated, then every increasing sequence of ideals is eventually constant. Say every ideal in an integral domain R is finitely generated and let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be an ascending chain of ideals. Define

$$I = \bigcup_{n=1}^{\infty} I_n.$$

Since I is also an ideal of R, then it is finitely generated by a set of elements, say $\{a_1, \ldots, a_k\}$. Each generator a_i belongs to I, so for each a_i, there exists a positive integer N_i such that $a_i \in I_{N_i}$. Let $N = \max\{N_1, \ldots, N_k\}$ so for all $n \geq N$, we have $I = I_n$ and the result follows.

We then prove that if every increasing sequence of ideals in R is eventually constant,

then every non-empty set S of ideals has a maximal element. We shall argue it by contradiction. Suppose on the contrary that there exists a non-empty set S of ideals with no maximal element. We shall choose an ideal $I_1 \in S$. By assumption, I_1 is not a maximal ideal in S. By the ascending chain condition (3.1), we have $I_1 \subseteq I_2$. Again, we can assume that I_2 is not maximal in S. So, we can construct an infinite strictly increasing chain of ideals in S which never stabilises, which is a contradiction.

Lastly, we shall prove that if every non-empty set S of ideals has a maximal element, then the integral domain R is finitely generated. Let I be an arbitrary ideal in R. It suffices to prove that I is finitely generated. Let S be the set of finitely generated ideals contained in I, i.e.

$$S = \{J \subseteq I : J \text{ is a finitely generated ideal of } R\}.$$

Note that $S \neq \emptyset$ since the zero ideal (0) is finitely generated, so $(0) \in S$. Since S is a non-empty set of ideals, by the premise, it has a maximal element $M \in S$. Let this ideal be J, i.e.

$$J \in S \quad \text{and for all } K \in S \quad J \subseteq K \subseteq I \text{ implies } J = K.$$

Suppose on the contrary that $J \neq I$. Then there exists $a \in I$ such that $a \notin J$. Consider the ideal K generated by J and (a), i.e.

$$K = J + (a) = \{j + ra : kj \in J, r \in R\}.$$

Since J and (a) are ideals of R, then K is also an ideal of R. One can prove that K is finitely generated, which contradicts the maximality of J in S, which is a contradiction. Hence, $J = I$. Since this applies to any ideal I of R, the result follows. □

Theorem 3.1. Every number ring is a Dedekind domain.

We will prove the unique factorisation result in an arbitrary Dedekind domain. Also, throughout the discussion, the term 'ideal' will always mean 'non-zero ideal'.

Theorem 3.2. Let I be an ideal in a Dedekind domain R. Then, there exists an ideal J such that IJ is principal.

Corollary 3.1. The ideal classes in a Dedekind domain form a group.

Corollary 3.2 (cancellation law). If A, B, C are ideals in a Dedekind domain and $AB = AC$, then $B = C$.

Corollary 3.3. If A and B are ideals in a Dedekind domain R, then $A \mid B$ if and only if $A \supset B$.

Theorem 3.3. Every ideal in a Dedekind domain R is uniquely representable as a product of prime ideals.

Corollary 3.4. The ideals in a number ring factor uniquely into prime ideals.

Example 3.2. Consider the principal ideals (2) and (3) in the number ring $R = \mathbb{Z}\left[\sqrt{-5}\right]$. It is easily shown that

$$(2) = \left(2, 1+\sqrt{-5}\right)^2 \quad \text{and} \quad (3) = \left(3, 1+\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right). \tag{3.2}$$

One can verify this. Note that the product $(\alpha,\beta)(\gamma,\delta)$ is generated by $\alpha\gamma, \beta\gamma, \alpha\delta, \beta\delta$. Moreover, each of the ideals on the right is a prime ideal.

In view of Theorem 3.3, we can define the greatest common divisor $\gcd(I,J)$ and the least common multiple $\operatorname{lcm}(I,J)$ for any two ideals, in an obvious way via their prime decompositions. The terms 'greatest' and 'least' actually have opposite meanings here. That is to say, $\gcd(I,J)$ is actually the smallest ideal containing both I and J, and $\operatorname{lcm}(I,J)$ is the largest ideal contained in both (Definition 3.3).

Definition 3.3. We have $\gcd(I,J) = I+J$ and $\operatorname{lcm}(I,J) = I \cap J$.

Using this observation, it is clear that every ideal in a Dedekind domain is generated as an ideal by at most two elements; in fact one of them can be chosen arbitrarily (Theorem 3.4).

Theorem 3.4. Let I be an ideal in a Dedekind domain R, and let α be any non-zero element of I. Then, there exists $\beta \in I$ such that $I = (\alpha, \beta)$.

Proof. Let R be a Dedekind domain and let I be an ideal of R. Let $\alpha \in I$, where $\alpha \neq 0$. Since $\alpha \in I$, then $(\alpha) \subseteq I$. As R is a Dedekind domain, by Theorem 3.3, every non-zero ideal factors uniquely as a product of non-zero prime ideals. Hence, $(\alpha) = IJ$ for some integral ideal $J \subseteq R$. Indeed, since $(\alpha) \subseteq I$, the ideal $J = (\alpha) I^{-1}$ is an integral ideal.

Now factor J into prime ideals:

$$J = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

We shall choose $\beta \in I$ such that $\beta \notin I\mathfrak{p}_i$ for every $i = 1, \ldots, r$. For every i, the ideal $I\mathfrak{p}_i$ is a proper subideal of I. Hence, we can choose $x_i \in I \setminus I\mathfrak{p}_i$. Since distinct prime ideals in a Dedekind domain are comaximal, we have

$$\mathfrak{p}_i + \mathfrak{p}_j = R \quad \text{for every } i \neq j.$$

Multiplying by I, we get $I\mathfrak{p}_i + I\mathfrak{p}_j = I$. Therefore, by the Chinese remainder theorem applied to the R-module I, there exists $\beta \in I$ such that $\beta \equiv x_i \pmod{I\mathfrak{p}_i}$ for every $i = 1, \ldots, r$. In particular, $\beta \notin I\mathfrak{p}_i$ for every $i = 1, \ldots, r$.

We now claim that $I = (\alpha, \beta)$. It is clear that $(\alpha, \beta) \subseteq I$. It remains to prove the reverse inclusion. Suppose, for contradiction, that $(\alpha, \beta) \subsetneq I$. Since R is Dedekind, we can write $(\alpha, \beta) = IL$ for some proper integral ideal $L \subsetneq R$. Since L is proper, it is contained in some maximal ideal, say $L \subseteq \mathfrak{p}$. In a Dedekind domain, every non-zero maximal ideal is a prime ideal (see **(ii)** of Definition 3.1), so $\mathfrak{p}$ is prime. Then

$$(\alpha, \beta) = IL \subseteq I\mathfrak{p}.$$

Thus $\alpha \in I\mathfrak{p}$ and $\beta \in I\mathfrak{p}$. However, $\alpha \in I\mathfrak{p}$ implies $(\alpha) \subseteq I\mathfrak{p}$. Since $(\alpha) = IJ$, then $IJ \subseteq I\mathfrak{p}$. Multiplying by I^{-1}, $J \subseteq \mathfrak{p}$. Hence $\mathfrak{p}$ is one of the prime ideals appearing in the factorisation of J, say $\mathfrak{p} = \mathfrak{p}_i$. But then, $\beta \in I\mathfrak{p} = I\mathfrak{p}_i$, contradicting our choice of β. The result follows. □

Recall from MA3201 Algebra II that every PID is a UFD, but in general, the converse is false. Take for example, the UFD $\mathbb{Z}[x]$, but it is not a PID (one can show that the ideal $(2, x)$ is non-principal). On the other hand, the converse is valid for Dedekind domains (Theorem 3.5).

Theorem 3.5. A Dedekind domain is a UFD if and only if it is a PID.

3.2 Splitting of Primes in Extensions

So far, we have seen examples of primes in $\mathbb{Z}$ which are not irreducible in a larger number ring. For example, $5 = (2+i)(2-i)$ in $\mathbb{Z}[i]$. Also, although 2 and 3 are irreducible in $\mathbb{Z}[\sqrt{-5}]$, the corresponding principal ideals (2) and (3) are not prime ideals as seen in Example 3.2. In fact, the phenomenon mentioned in (3.2) is known as splitting. We say that 3 splits into the product of two primes in $\mathbb{Z}[\sqrt{-5}]$.

Now, we will consider the problem of determining how a given prime splits in a given number ring. More generally, if P is any prime ideal in any number ring $R = \mathbb{A} \cap K$, where K is a number field, and if L is a number field containing K, we consider the prime decomposition of the ideal generated by P in the number ring $S = \mathbb{A} \cap L$.

Throughout, let K and L be number fields with $K \subset L$, and let $R = \mathbb{A} \cap K$ and $S = \mathbb{A} \cap L$. In [1], the 'prime' is used to represent a non-zero prime ideal, but throughout this set of notes, we will *try* to explicitly mention non-zero prime ideals.

Theorem 3.6. Suppose $R \subset S$ are rings of integers for $K \subset L$, so S is integral over R and both are Dedekind domains. Let P be a non-zero prime ideal of R and Q be a non-zero prime ideal of S. Then, the following conditions are equivalent:

(i) $Q \mid PS$

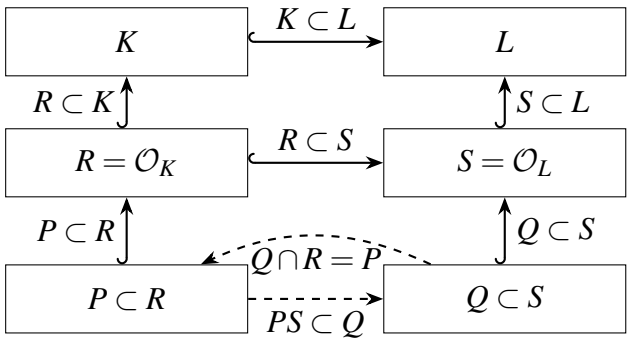
(ii) $Q \supset PS$

(iii) $Q \supset P$

(iv) $Q \cap R = P$

(v) $Q \cap K = P$

When either condition holds, we will say that Q lies over P, or P lies under Q.



Q lies over P

We first give an example for Theorem 3.6 before proving it.

Example 3.3. Take $K = \mathbb{Q}$ and $R = \mathbb{Z}$, and $L = \mathbb{Q}[i]$ and $S = \mathbb{Z}[i]$. One checks that $R \subset S$ are rings of integers for $K \subset L$. Let $P = (5) \subseteq \mathbb{Z}$ and $Q = (2+i)$. It is easy to check that each of the *equivalent* conditions[1] is satisfied.

Proof. First, **(i)** and **(ii)** are equivalent by Corollary 3.3 and Theorem 3.2. Next, **(ii)** and **(iii)** are equivalent since Q is an ideal in S.

Suppose **(iv)** holds. Then clearly **(iii)** holds. Also, **(iv)** and **(v)** are equivalent since $Q \subset \mathbb{A}$. Finally, we shall prove hat **(iii)** implies **(iv)**. Observe that $Q \cap R$ contains P and is easily seen to be an ideal in R. Since P is a maximal ideal (Definition 3.1), then $Q \cap R$ is either P or R. If the intersection is R, then $1 \in Q$, implying that $Q = S$ which is a contradiction. □

Theorem 3.7. Every non-zero prime ideal Q of S lies over a unique non-zero prime ideal P of R; every non-zero prime ideal P of R lies under at least one non-zero prime ideal Q of S.

As we have noted, the primes lying over a given P are the ones which occur in the prime decomposition of PS. The exponents with which they occur are called the *ramification indices*.

[1] For instance, to see why **(i)** holds, i.e. $Q \mid PS$, we see that $PS = 5\mathbb{Z}[i]$. By definition,

$$PS = \left\{ \sum_{k=1}^{m} p_k s_k : p_k \in P, s_k \in S \right\}.$$

Since $P = (5)$, then every element in P is of the form $5a_k$, where $a_k \in \mathbb{Z}$. As $a_k \in \mathbb{Z} \subseteq \mathbb{Z}[i]$, then $p_k s_k \in \mathbb{Z}[i]$ so $PS \subseteq \mathbb{Z}[i]$. Conversely, every element of $(5) \subseteq \mathbb{Z}[i]$ has the form $5s$, where $s \in S$. Since $5 \in P$, then $5s \in PS$. As such, $5\mathbb{Z}[i] = (5)$ in $\mathbb{Z}[i]$.

Definition 3.4 (ramification index). Let Q be a non-zero prime ideal. Then, if Q^e is the exact power of Q dividing PS, we say that e is the ramification index of Q over P, denoted by $e(Q \mid P)$.

Example 3.4. Let $R = \mathbb{Z}$ and $S = \mathbb{Z}[i]$. Then the principal ideal $(1-i)$ in S lies over 2, where by 2 we really mean the ideal $2\mathbb{Z}$. In fact, $(1-i)$ is a prime ideal of S. This can be seen by considering the order of the quotient ring $S/(1-i)$. Moreover, we have $2S = (1-i)^2$, and hence

$$e((1-i) \mid 2) = 2.$$

On the other hand,

$$e(Q \mid p) = 1$$

whenever $p \neq 2$ and Q lies over p.

Example 3.5. More generally, if $R = \mathbb{Z}$ and $S = \mathbb{Z}[\omega]$, where $\omega = e^{\frac{2\pi i}{m}}$ and $m = p^r$ for some prime $p \in \mathbb{Z}$, then the principal ideal $(1-\omega)$ in S is a prime ideal lying over p. Moreover,

$$e((1-\omega) \mid p) = \varphi(m) = p^{r-1}(p-1).$$

On the other hand,

$$e(Q \mid q) = 1$$

whenever $q \neq p$ and Q lies over q.

There is another important number associated with a pair of prime ideals P and Q, where Q lies over P. Since P and Q are non-zero prime ideals in number rings, they are maximal ideals by Definition 3.1. Therefore, the quotient rings R/P and S/Q are fields. Moreover, there is a natural way to view R/P as a subfield of S/Q. Indeed, the containment $R \subseteq S$ induces a ring homomorphism

$$R \to S/Q.$$

The kernel of this homomorphism is $R \cap Q$. Since Q lies over P, we have $R \cap Q = P$. Thus, we obtain an embedding

$$R/P \hookrightarrow S/Q.$$

Definition 3.5 (residue field and inertial degree). The fields R/P and S/Q are called the residue fields associated with P and Q.

Since these residue fields are finite fields, S/Q is a finite extension of R/P. The degree of this extension is called the inertial degree of Q over P, and is denoted by $f(Q \mid P)$. Thus,

$$f(Q \mid P) = [S/Q : R/P].$$

Example 3.6. Let $R = \mathbb{Z}$ and $S = \mathbb{Z}[i]$. We have seen hat the prime 2 in $\mathbb{Z}$ lies under the prime ideal $(1-i)$ in $\mathbb{Z}[i]$. Also, $S/2S$ has order 4, and $(1-i)$ properly contains $2S$. As

such, $|S/(1-i)|$ must be a proper divisor of 4. The only possibility is 2. Hence,

$$R/2\mathbb{Z} \text{ and } S/(1-i) \quad \text{are finite fields of order 2.}$$

As such,

$$f((1-i) \mid 2) = 1.$$

On the other hand, $3S$ is a prime ideal of S, and $|S/3S| = 9$. Since $|\mathbb{Z}/3\mathbb{Z}| = 3$, then $[S/3S : \mathbb{Z}/3\mathbb{Z}] = 2$ so

$$f(3S \mid 3) = 2.$$

The ramification index e and the inertial degree f are multiplicative in towers. More precisely, suppose $P \subset Q \subset U$ are prime ideals in three number rings $R \subset S \subset T$, then

$$e(U \mid P) = e(U \mid Q)\, e(Q \mid P) \quad \text{and} \quad f(U \mid P) = f(U \mid Q)\, f(Q \mid P).$$

In general, if Q is any prime ideal in S, then Q lies over a unique prime $p \in \mathbb{Z}$. Then S/Q is a finite field of order p^f, where $f = f(Q \mid p)$. Since Q contains pS, the number p^f is at most $|S/pS|$. If S is the ring of integers of a number field L of degree n over $\mathbb{Q}$, then

$$|S/pS| = p^n.$$

Hence, $f \leq n$.

Theorem 3.8 (fundamental identity). Let n be the degree of L over K. Let R and S be the rings of integers of K and L, respectively. Let $Q_1, \ldots, Q_r$ be the prime ideals of S lying over a prime ideal P of R. Denote by $e_1, \ldots, e_r$ and $f_1, \ldots, f_r$ the corresponding ramification indices and inertial degrees. Then,

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

For an R-ideal I, write $\|I\|$ to denote the index $|R/I|$.

Theorem 3.9. Let R, S, K, L be as in our above discussion (Theorem 3.8), and let $n = [L : K]$. Then, the following hold.

(a) For ideals I and J in R,

$$\|IJ\| = \|I\|\,\|J\|.$$

(b) If I is an ideal in R, then for the S-ideal IS,

$$\|IS\| = \|I\|^n.$$

(c) If $\alpha \in R$ and $\alpha \neq 0$, then for the principal ideal (α),

$$\|(\alpha)\| = \left|N_{\mathbb{Q}}^{K}(\alpha)\right|.$$

As an application of these results, we have two ways to see that the principal ideal $(1-\omega)$ in $\mathbb{Z}[\omega]$, where $\omega = e^{\frac{2\pi i}{m}}$ and $m = p^r$, is a prime ideal. We know that

$$(1-\omega)^n = p\mathbb{Z}[\omega] \quad \text{where } n = p^{r-1}(p-1) = \varphi(m).$$

Since n is the degree of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$, any further splitting of $(1-\omega)$ into prime ideals would violate the fundamental identity (Theorem 3.8). Thus, $(1-\omega)$ must be a prime ideal.

Also, from Theorem 3.9, we have

$$\|(1-\omega)\|^n = \|(1-\omega)^n\| = \|p\mathbb{Z}[\omega]\| = p^n \quad \text{so} \quad \|(1-\omega)\| = p.$$

Moreover, the theorem shows that whenever $\|I\|$ is a prime, I must be a prime ideal.

Example 3.7 (splitting in cubic fields). We give some examples of splitting in cubic fields.

(i) Let $K = \mathbb{Q}$, $L = \mathbb{Q}\left[\sqrt[3]{2}\right]$ and $S = \mathbb{A} \cap L$. We know that $S = \mathbb{Z}[\alpha]$, where $\alpha = \sqrt[3]{2}$. Obviously, $2S = (\alpha)^3$. Hence, (α) must be a prime ideal since any further splitting would violate the fundamental identity (Theorem 3.8). Moreover, we must have

$$f((\alpha) \mid 2) = 1.$$

A similar result holds if we replace $2S$ by $3S$ and α by $\alpha+1$.

In the same field, one can show that

$$5S = (5, \alpha+2)\left(5, \alpha^2+3\alpha-1\right),$$

and that the ideals on the right are relatively prime. Thus the only question is whether one of these ideals splits further. The ring

$$S/\left(5, \alpha^2+3\alpha-1\right)$$

can be shown to be a field of order 25. Thus, $\left(5, \alpha^2+3\alpha-1\right)$ is a prime ideal and the corresponding inertial degree is 2. Applying the fundamental identity (Theorem 3.8) again, we find that $(5, \alpha+2)$ must be a prime ideal, with inertial degree 1.

(ii) Now, let α satisfy $\alpha^3 = \alpha+1$ and set $L = \mathbb{Q}[\alpha]$. Then, $S = \mathbb{A} \cap L = \mathbb{Z}[\alpha]$. One can show that we have the factorisation

$$23S = (23, \alpha-10)^2(23, \alpha-3),$$

and that the ideals on the right are relatively prime. It follows that the factors on the right are prime ideals and that the corresponding inertial degrees are 1.

In **(ii)**, the prime ideals lying over 23 do not have the same ramification index. In the previous example, the prime ideals lying over 5 did not have the same inertial degree. We will see that this sort of phenomenon can only happen when the field extension is not normal.

If L is a normal extension of K, and P is a prime ideal of $R = \mathbb{A} \cap K$, then it is easy to see that the Galois group $G = \mathrm{Gal}(L/K)$ permutes the prime ideals lying over P. Indeed, if Q is one such prime ideal and $\sigma \in G$, then $\sigma(Q)$ is a prime ideal in $\sigma(S) = S$ lying over $\sigma(P) = P$ Furthermore, G permutes them transitively.

Theorem 3.10. With notation as above, assume that L is normal over K. Let Q and Q' be two prime ideals of S lying over the same prime ideal P of R. Then

$$\sigma(Q) = Q' \quad \text{for some } \sigma \in G.$$

Proof. Suppose on the contrary that $\sigma(Q) \neq Q'$ for every $\sigma \in G$. By the Chinese remainder theorem, there is a solution to the system of congruences

$$x \equiv 0 \pmod{Q'} \quad \text{and} \quad x \equiv 1 \pmod{\sigma(Q)}$$

for all $\sigma \in G$.

Let $\alpha \in S$ be such a solution. Then,

$$N_K^L(\alpha) \in R \cap Q' = P$$

since one of the factors of $N_K^L(\alpha)$ is $\alpha \in Q'$. On the other hand, we have $\alpha \notin \sigma(Q)$ for every $\sigma \in G$. Hence, $\sigma^{-1}(\alpha) \notin Q$. We can express $N_K^L(\alpha)$ as the product of all $\sigma^{-1}(\alpha)$. Since none of these elements are in the prime ideal Q, it follows that $N_K^L(\alpha) \notin Q$. However, we have already seen that

$$N_K^L(\alpha) \in P \subset Q$$

which is a contradiction. □

Corollary 3.5. If L is normal over K, and Q and Q' are two prime ideals lying over P, then

$$e(Q \mid P) = e(Q' \mid P) \quad \text{and} \quad f(Q \mid P) = f(Q' \mid P).$$

Proof. First, $e(Q \mid P) = e(Q' \mid P)$ follows from the unique factorisation of ideals. Next, $f(Q \mid P) = f(Q' \mid P)$ is obtained by establishing an isomorphism $S/Q \cong S/Q'$. □

Corollary 3.5 shows that in the normal extension case, a prime ideal P of R splits into $(Q_1 Q_2 \cdots Q_r)^e$ in S, where the Q_i are distinct prime ideals. All the Q_i have the same ramification index e over P. Moreover, $ref = [L : K]$ by Theorem 3.8.

Definition 3.6 (ramified prime ideal). Let K, L, R, S be as usual. A prime ideal P of R is said to be ramified in S, or ramified in L, if

$$e(Q \mid P) > 1$$

for some prime ideal Q of S lying over P. Equivalently, PS is not squarefree.

We have seen that p is ramified in $\mathbb{Z}[\omega]$, where $\omega = e^{\frac{2\pi i}{m}}$ and $m = p^r$, and we claimed that no other primes of $\mathbb{Z}$ are ramified in $\mathbb{Z}[\omega]$. We saw that 2 and 3 are ramified in $\mathbb{Z}\left[\sqrt[3]{2}\right]$, but 5 is not, and that 23 is ramified in $\mathbb{Z}[\alpha]$, where $\alpha^3 = \alpha + 1$. Recall from Definition 2.10 that the discriminants of these rings are, respectively, a power of p, $-3^3 \cdot 2^2$ and -23.

In general, a prime $p \in \mathbb{Z}$ is ramified in a number ring R if and only if $p \mid \operatorname{disc}(R)$.

Theorem 3.11. Let p be a prime in $\mathbb{Z}$, and suppose p is ramified in a number ring R. Then, $p \mid \operatorname{disc}(R)$.

Proof. Let P be a prime ideal of R lying over p such that $e(P \mid p) > 1$. Then, $pR = PI$, where I is divisible by all prime ideals of R lying over p.

Let $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K in $\mathbb{C}$, where K is the number field corresponding to R. As usual, extend all σ_i to automorphisms of some extension L of K which is normal over $\mathbb{Q}$.

Let $\alpha_1, \ldots, \alpha_n$ be any integral basis for R. We will replace one of the α_i by a suitable element which will enable us to see that p divides $\operatorname{disc}(R)$.

In particular, take any $\alpha \in I - pR$. We know that I properly contains pR. Then α is in every prime ideal of R lying over p, but $\alpha \notin pR$. If we write

$$\alpha = m_1\alpha_1 + \cdots + m_n\alpha_n, \quad \text{where } m_i \in \mathbb{Z},$$

then the fact that $\alpha \notin pR$ implies that not all m_i are divisible by p. Rearranging the α_i if necessary, we can assume that $p \nmid m_1$. Set

$$d = \operatorname{disc}(R) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n).$$

Then it is easy to see that

$$\operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n) = m_1^2 d.$$

Since $p \nmid m_1$, it will be sufficient to show that

$$p \mid \operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n).$$

Recall that α is in every prime ideal of R lying over p. It follows that α is in every prime ideal of $S = \mathbb{A} \cap L$ lying over p. Indeed, each such prime ideal contains p and intersects R in some prime ideal. This prime ideal of R contains p, hence lies over p, and hence contains α.

Fix any prime ideal Q of S lying over p. We claim that $\sigma(\alpha) \in Q$ for every automorphism σ of L. To see this, notice that $\sigma^{-1}(Q)$ is a prime ideal of $\sigma^{-1}(S) = S$ lying over p, and hence contains α. Therefore, $\sigma_i(\alpha) \in Q$ for all i. It follows that Q contains

$\operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n)$. Since this discriminant is necessarily in $\mathbb{Z}$, it lies in $Q \cap \mathbb{Z} = p\mathbb{Z}$. Hence,

$$p \mid \operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n).$$

This completes the proof. □

If we work a little harder, we can obtain a stronger statement about the power of p dividing $\operatorname{disc}(R)$.

Corollary 3.6. Let $\alpha \in R$, let

$$K = \mathbb{Q}[\alpha],$$

and let f be any monic polynomial over $\mathbb{Z}$ such that

$$f(\alpha) = 0.$$

If p is a prime such that

$$p \nmid N_{\mathbb{Q}}^{K}\left(f'(\alpha)\right),$$

then p is unramified in K.

Corollary 3.7. Only finitely many primes of $\mathbb{Z}$ are ramified in a number ring R.

Corollary 3.8. Let R and S be number rings such that

$$R \subset S.$$

Then only finitely many primes of R are ramified in S.

Proof. If P is a prime ideal of R which is ramified in S, then $P \cap \mathbb{Z} = p\mathbb{Z}$ is ramified in S, since e is multiplicative in towers. There are only finitely many possibilities for p, and each one lies under only finitely many prime ideals of R. Hence there are only finitely many possibilities for P. □

Of course, p can be ramified in S without P being ramified in S. There is a finer tool for showing prime ideals of R are unramified in S. Better yet, there is a criterion for determining whether a particular prime ideal Q of S is ramified over R, meaning that

$$e(Q \mid P) > 1 \quad \text{and} \quad P = Q \cap R.$$

There is a special ideal in S, called the different of S with respect to R, which is divisible by exactly those prime ideals Q which are ramified over R.

We now consider in detail the way primes $p \in \mathbb{Z}$ split in quadratic fields. Let $R = \mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$, where m is squarefree. Recall that R has integral basis $\{1, \sqrt{m}\}$ and discriminant $4m$ when $m \equiv 2, 3 \pmod 4$. It has integral basis $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$ and discriminant m when $m \equiv 1 \pmod 4$.

Let p be a prime in $\mathbb{Z}$. The fundamental identity (Theorem 3.8) shows that there are just three possibilities:

$$pR = \begin{cases} P^2 & \text{if } f(P \mid p) = 1; \\ P & \text{if } f(P \mid p) = 2; \\ P_1 P_2 & \text{if } f(P_1 \mid p) = f(P_2 \mid p) = 1 \end{cases} \tag{3.3}$$

Theorem 3.12. With notation as in (3.3), we have the following.

(i) If $p \mid m$, then $pR = (p, \sqrt{m})^2$.

(ii) If m is odd, then

$$\begin{cases} 2R = (2, 1+\sqrt{m})^2 & \text{if } m \equiv 3 \pmod 4; \\ 2R = \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right) & \text{if } m \equiv 1 \pmod 8; \\ 2R \text{ is prime} & \text{if } m \equiv 5 \pmod 8. \end{cases}$$

(iii) If p is odd and $p \nmid m$, then

$$\begin{cases} pR = (p, n+\sqrt{m}) & \text{if } m \equiv n^2 \pmod p; \\ pR \text{ is prime} & \text{if } m \text{ is not a square modulo } p. \end{cases}$$

Theorem 3.13. Write $m = p^k n$, where $p \nmid n$. Then, $e = \varphi\left(p^k\right)$ and f is the multiplicative order of p modulo n. In other words,

$$p^f \equiv 1 \pmod n$$

and f is the smallest positive integer with this property.

We restate Theorem 3.13 for the special case in which $p \nmid m$.

Corollary 3.9. If $p \nmid m$, then p splits into $\frac{\varphi(m)}{f}$ distinct prime ideals in $\mathbb{Z}[\omega]$, where f is the order of p modulo m.

We have not yet given a general procedure for determining how a given prime splits in a given number ring. Such a procedure exists, and it works almost all the time.

Now, let R, S, K, L be as always, and let $n = [L : K]$. Fix an element $\alpha \in S$ of degree n over K, so that $L = K[\alpha]$. In general, $R[\alpha]$ is an additive subgroup of S, possibly proper. However, the factor group $S/R[\alpha]$ is necessarily finite. One way to see this is to observe that S and $R[\alpha]$ are both free abelian groups of rank mn, where $m = [K : \mathbb{Q}]$. Another way is to show that $S/R[\alpha]$ is a finitely generated torsion group.

We will show that for all but finitely many prime ideals P of R, the splitting of P in S can be determined by factoring a certain polynomial modulo P. Specifically, it will work whenever P lies over a prime $p \in \mathbb{Z}$ which does not divide the order of $S/R[\alpha]$. Thus, if $S = R[\alpha]$, it will work for all P.

Fixing a prime ideal P of R, we establish the following notation. For a polynomial $h \in R[x]$, let $\overline{h}$ denote the corresponding polynomial in $(R/P)[x]$ obtained by reducing the coefficients of h modulo P.

Now let g be the monic irreducible polynomial for α over K. The coefficients of g are algebraic integers, since they can be expressed in terms of the conjugates of the algebraic integer α. Hence they are in $\mathbb{A} \cap K = R$. Thus, $g \in R[x]$ and we can consider $\overline{g} \in (R/P)[x]$. The polynomial $\overline{g}$ factors uniquely into monic irreducible factors in $(R/P)[x]$, and we can write this factorisation in the form

$$\overline{g} = \overline{g}_1^{e_1} \overline{g}_2^{e_2} \cdots \overline{g}_r^{e_r} \quad \text{where the } g_i \text{ are monic polynomials over } R.$$

It is assumed that the $\overline{g}_i$ are distinct.

Theorem 3.14 (Dedekind-Kummer theorem). Let everything be as above, and assume also that p does not divide $|S/R[\alpha]|$, where p is the prime of $\mathbb{Z}$ lying under P. Then the prime decomposition of PS is given by

$$Q_1^{e_1} Q_2^{e_2} \cdots Q_r^{e_r},$$

where Q_i is the ideal $(P, g_i(\alpha))$ in S generated by P and $g_i(\alpha)$. In other words,

$$Q_i = PS + (g_i(\alpha)).$$

Also, $f(Q_i \mid P)$ is equal to the degree of g_i.

We note that the condition on p is satisfied, in particular, whenever $L = \mathbb{Q}[\alpha]$ and $p^2 \nmid \operatorname{disc}(\alpha)$. This is because $|S/R[\alpha]|^2$ divides $|S/\mathbb{Z}[\alpha]|^2$, which is finite in this case, and the latter number is a divisor of $\operatorname{disc}(\alpha)$.

We give some applications of Theorem 3.14. Taking $\alpha = \sqrt{m}$, we can re-obtain the results of Theorem 3.3, except when $p = 2$ and $m \equiv 1 \pmod 4$. In this exceptional case, the result can be obtained by taking

$$\alpha = \frac{1 + \sqrt{m}}{2}.$$

As another example, we can determine how any prime splits in $\mathbb{Z}[\alpha]$, where $\alpha^3 = \alpha + 1$, by factoring the polynomial $x^3 - x - 1$ modulo p.

Chapter 4

Galois Theory applied to Prime Decomposition

4.1 Introduction

Up to now, the Galois-theoretic aspects of number fields have not figured prominently in our theory. Essentially, all we did was to determine the Galois group of the m^{th} cyclotomic field, which as the multiplicative group of integers mod m and to show that in the case of a normal extension, the Galois group permutes the primes over a given prime transitively. In this chapter, we apply Galois theory to the general problem of determining how a prime ideal of a number ring splits in an extension field.

We recap a bit of Galois theory. Let L and K be number fields such that L is a normal extension of K. Thus, the Galois group $G = \mathrm{Gal}(L/K)$, consisting of all automorphisms of L which fix K pointwise, has order $n = [L:K]$. As usual, let R and S denote the corresponding number rings. Fix a non-zero prime ideal P of Q. Recall that all non-zero prime ideals Q of S lying over P have the same ramification index and inertial degree. Hence, if there are r such non-zero prime ideals Q, then the sum of $e_i f_i$ is n, where e_i and f_i denote the corresponding ramification indices and inertial degrees respectively. For each prime Q lying over P, we shall define the decomposition group D and inertia group E, where $D, E \leq G$.

Definition 4.1 (decomposition group and inertia group). Let Q be a non-zero prime ideal lying over P. Then, define the decomposition group D and the inertia group E as follows:

$$D = D(Q \mid P) = \{\sigma \in G : \sigma Q = Q\}$$
$$E = E(Q \mid P) = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{Q} \text{ for all } \alpha \in S\}$$

It is clear that these are actually subgroups of G, and that $E \subset D$. The condition $\sigma Q = Q$ can be expressed as $\sigma(\alpha) \equiv 0 \pmod{Q}$ if and only if $\alpha \equiv 0 \pmod{Q}$. Obvi-

ously, the condition for E implies this.

The members of D induce automorphisms of the field S/Q in a natural way: Every $\sigma \in G$ restricts to an automorphism of S, and if $\sigma \in D$ then the induced mapping $S \to S/Q$ has kernel Q; thus each $\sigma \in D$ induces an automorphism $\overline{\sigma}$ of S/Q, in such a way that this diagram commutes:

$$\begin{array}{ccc} S & \xrightarrow{\sigma} & S \\ \downarrow & & \downarrow \\ S/Q & \xrightarrow{\overline{\sigma}} & S/Q \end{array}$$

Moreover it is clear that $\overline{\sigma}$ fixes the subfield R/P pointwise since σ fixes K, hence R, pointwise. Thus $\overline{\sigma}$ is a member of the Galois group $\overline{G}$ of S/Q over R/P. All of this can be summed up by saying that we have a mapping $D \to \overline{G}$, and it is easy to see that is a group homomorphism: composition of automorphisms in D corresponds to composition in $\overline{G}$. The kernel of the homomorphism $D \to \overline{G}$ is easily seen to be E; this shows that E is a normal subgroup of D and that the factor group D/E is embedded in $\overline{G}$. We will see that $D \to \overline{G}$ is actually onto, hence $D/E \to \overline{G}$ is actually a group isomorphism. We know the structure of $\overline{G}$: It is cyclic of order f, hence the same is true for D/E.

Now look at the fixed fields of D and E; denote them by L_D and L_E, respectively. L_D is called the decomposition field and L_E the inertia field. In general, we adopt the following system of notation: For any subgroup H of G, L_H denotes the fixed field of H; thus $L_{\{1\}} = L$ and $L_G = K$. More generally, for any subset $X \subset L$, let X_H denote $X \cap L_H$. Thus S_H is the number ring in L_H, and Q_H is the unique prime of S_H lying under Q. Obviously Q_H lies over P, and it follows easily from the way we have defined things that S_H/Q_H is an intermediate field between S/Q and R/P. (Verify all of this.)

We can now state the main result:

Theorem 4.1. Let $K, L, R, S, P, Q, G, D, E, r, e$ and f be as above. Then we have the

following:

Degrees			Ramification indices	Inertial degrees
	L	Q		
e	|	|	e	1
	L_E	Q_E		
f	|	|	1	f
	L_D	Q_D		
r	|	|	1	1
	K	P		

Corollary 4.1. D is mapped onto $\overline{G}$ by the natural mapping $\sigma \mapsto \overline{\sigma}$; the kernel is E, hence D/E is cyclic of order f.

Proof. We have already seen that D/E is embedded in $\overline{G}$. Moreover both groups have order f, since $|D/E| = [L_E : L_D]$. □

The following special case indicates a reason for the terms 'decomposition field' and 'inertia field'.

Corollary 4.2. Suppose $D \trianglelefteq G$. Then P splits into r distinct primes in L_D. If E is also normal in G, then each of them remains prime (is 'inert') in L_E. Finally, each one becomes an e^{th} power in L.

Proof. If $D \trianglelefteq G$, then by Galois theory, L_D is a normal extension of K. We know that Q_D has ramification index and inertial degree 1 over P, hence so does every prime P' in L_D lying over P. Then there must be exactly r such primes. It follows that there are exactly r primes in L_E lying over P since this is true in both L_D and L. This implies that each P' lies under a unique prime P'' in L_E; however it seems conceivable that P'' might be ramified over P'. If E is normal in G, so that L_E is normal over K, then

$$e\left(P'' \mid P\right) = e\left(Q_E \mid P\right) = 1 \quad \text{so} \quad e\left(P'' \mid P'\right) = 1.$$

This proves that P' is inert in L_E: $P'' = P'S_E$. One can show that P'' becomes an e^{th} power in L. □

We have already seen an example of this phenomenon: The prime 2 in $\mathbb{Z}$ splits into two distinct primes in $\mathbb{Q}\left[\sqrt{-23}\right]$, and each remains prime in $\mathbb{Q}[\omega]$, where $\omega = e^{\frac{2\pi i}{23}}$. This could have been predicted by Corollary 4.2. We know that 2 splits into two primes in $\mathbb{Q}[\omega]$, hence the decomposition field has degree 2 over $\mathbb{Q}$; moreover there is only one

quadratic subfield of $\mathbb{Q}[\omega]$ since the Galois group is cyclic of order 22. So the decomposition field must be $\mathbb{Q}\left[\sqrt{-23}\right]$. Finally, 2 is unramified in $\mathbb{Q}[\omega]$, so the inertia field is all of $\mathbb{Q}[\omega]$.

Slightly more generally, whenever L is normal over K with cyclic Galois group and P (a prime in K) splits into r primes in L, then the decomposition field is the unique intermediate field of degree r over K, and P splits into r primes in every intermediate field containing the decomposition field.

Example 4.1. As another example, consider the field $L = \mathbb{Q}\left[i, \sqrt{2}, \sqrt{5}\right]$; this is normal of degree 8 over $\mathbb{Q}$, and the Galois group is the direct sum of three cyclic groups of order 2. The prime 5 splits into two primes in $\mathbb{Q}[i]$, is inert in $\mathbb{Q}\left[\sqrt{2}\right]$, and becomes a square in $\mathbb{Q}\left[\sqrt{5}\right]$. Consequently L must contain at least two primes lying over 5, and each must have ramification index and inertial degree at least 2; it follows that each of these numbers is exactly 2. The inertia field must be a field of degree 4 over $\mathbb{Q}$ in which 5 is unramified. The only choice is $\mathbb{Q}\left[i, \sqrt{2}\right]$. Thus, $(2+i)$ and $(2-i)$ remain prime in $\mathbb{Q}\left[i, \sqrt{2}\right]$ and become squares of primes in L.

Example 4.2. Here is a non-abelian example. Let

$$L = \mathbb{Q}\left[\sqrt[3]{19}, \omega\right] \quad \text{where } \omega = e^{\frac{2\pi i}{3}}.$$

Then L is normal of degree 6 over $\mathbb{Q}$ with Galois group S_3, the permutation group on three objects. Consider how the prime 3 splits: It becomes a square in $\mathbb{Q}[\omega]$, and has the form P^2Q in $\mathbb{Q}\left[\sqrt[3]{19}\right]$. Consequently L must contain at least two primes lying over 3, and each must have ramification index divisible by 2. The only possibility is for L to contain three primes over 3, each with $e = 2$ and $f = 1$. For each of these primes, the decomposition field has degree 3 over $\mathbb{Q}$.

There are three such fields: $\mathbb{Q}\left[\sqrt[3]{19}\right]$, $\mathbb{Q}\left[\omega\sqrt[3]{19}\right]$, $\mathbb{Q}\left[\omega^2\sqrt[3]{19}\right]$. Any one of them can be the decomposition field, depending on which prime over 3 is being considered. The fact that they all can occur is easily seen by the fact that each of them can be sent to any other one by an automorphism of L. The inertia field is the same since $f = 1$. Notice that 3 does not split into three distinct primes in any of these decomposition fields since in fact it is ramified in each (it splits into P^2Q in one of them, hence in all since they are all isomorphic extensions of $\mathbb{Q}$). This shows that the normality condition on D was actually necessary in Corollary 4.2.

We now consider a variation on the situation. What happens if K is replaced by a larger subfield K' of L? We know that K' is the fixed field of some subgroup $H \subset G$; in our previous notation, $K' = L_H$. Moreover the ring

$$R' = \mathbb{A} \cap K'$$

is S_H, and $P' = Q \cap R'$ is the unique prime of R' lying under Q. P' also lies over P, but it need not be unique in that respect. We know that L is a normal extension of K', so the

decomposition and inertia groups

$$D\left(Q \mid P'\right) \quad \text{and} \quad E\left(Q \mid P'\right)$$

can be considered. From the definition, we immediately find that

$$D\left(Q \mid P'\right) = D \cap H \quad \text{and} \quad E\left(Q \mid P'\right) = E \cap H,$$

where D and E are as before (for Q over P). Then by Galois theory, the fields $L_D K'$ and $L_E K'$ are the decomposition and inertia fields, respectively, for Q over P'. We use this observation to establish certain maximal and minimal conditions for decomposition and inertia fields.

Theorem 4.2. With all notation as above,

(i) L_D is the largest intermediate field K' such that

$$e\left(P' \mid P\right) = f\left(P' \mid P\right) = 1$$

(ii) L_D is the smallest K' such that Q is the only prime of S lying over P'

(iii) L_E is the largest K' such that

$$e\left(P' \mid P\right) = 1$$

(iv) L_E is the smallest K' such that Q is totally ramified over P', i.e.

$$e\left(Q \mid P'\right) = \left[L : K'\right]$$

This theorem has some interesting consequences. We will use it to prove the quadratic reciprocity law. It will be helpful to introduce the following concept: A prime P in a number field K splits completely in an extension field F if and only if P splits into $[F : K]$ distinct primes, in which case all must have e and $f = 1$. Conversely, if all primes of F lying over P have e and $f = 1$, then P splits completely in F. It follows that if a prime splits completely in an extension F of K then it also splits completely in every sub-extension. As such, we obtain the following corollary:

Corollary 4.3. If $D \trianglelefteq G$ for some Q lying over P, then P splits completely in K' if and only if $K' \subset L_D$.

Proof. If P splits completely in K', then in particular,

$$e\left(P' \mid P\right) = f\left(P' \mid P\right) = 1 \quad \text{where } P' = Q \cap R'.$$

Then $K' \subset L_D$ by (1). Conversely, P splits completely in L_D and hence also in any K', $K \subset K' \subset L_D$. □

This will be applied in a situation in which G is abelian, so that all subgroups of G are normal.

Definition 4.2 (Legendre symbol). Let p be an odd prime in $\mathbb{Z}$. For $n \in \mathbb{Z}$, $p \nmid n$, define the Legendre symbol

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a square mod } p; \\ -1 & \text{otherwise.} \end{cases}$$

Theorem 4.3 (quadratic reciprocity law). We have

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8; \\ -1 & \text{if } p \equiv \pm 3 \pmod 8, \end{cases}$$

and for odd primes $q \neq p$, we have

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \text{ or } q \equiv 1 \pmod 4; \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

We will establish a criterion for a prime to be a d^{th} power mod p, for any divisor d of $p-1$. All of the action takes place inside the cyclotomic field $\mathbb{Q}[\omega]$, where $\omega = e^{\frac{2\pi i}{p}}$. We know that the Galois group G of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$ is cyclic of order $p-1$, hence there is a unique subfield $F_d \subset \mathbb{Q}[\omega]$ having degree d over $\mathbb{Q}$, for each divisor d of $p-1$. Here, F_d is the fixed field of the unique subgroup of G having order $\frac{p-1}{d}$. Moreover,

$$F_{d_1} \subset F_{d_2} \quad \text{iff} \quad d_1 \mid d_2.$$

Theorem 4.4. Let p be an odd prime, and let q be any prime $\neq p$. Fix a divisor d of $p-1$. Then q is a d^{th} power mod p iff q splits completely in F_d.

Theorem 4.5. Let K be a number field, and let L and M be two extensions of K. Fix a prime P of K. If P is unramified in both L and M, then P is unramified in the composite field LM. If P splits completely in both L and M, then P splits completely in LM.

Corollary 4.4. Let K and L be number fields, $K \subset L$, and let P be a prime in K. If P is unramified or splits completely in L, then the same is true in the normal closure M of L over K. M is the smallest normal extension of K containing L; it is the composite of all the fields $\sigma(L)$ for all embeddings $\sigma : L \to \mathbb{C}$ fixing K pointwise.

We return to the situation in which L is a normal extension of K. G, R, S, P, and Q are as above. We are interested in knowing what happens to the groups

$$D(Q \mid P) \quad \text{and} \quad E(Q \mid P)$$

when Q is replaced by another prime Q' of S lying over the same P. We know that $Q' = \sigma Q$ for some $\sigma \in G$; it is then easy to see that

$$D(\sigma Q \mid P) = \sigma D(Q \mid P)\sigma^{-1}$$

and

$$E(\sigma Q \mid P) = \sigma E(Q \mid P)\sigma^{-1}.$$

Thus D and E are just replaced by conjugate subgroups of G. In particular we see that when G is abelian, the groups $D(Q \mid P)$ and $E(Q \mid P)$ depend only on P, not on Q.

4.2 The Frobenius Automorphism

Assume now that P is unramified in L, so that $E(Q \mid P)$ is trivial. Then we have an isomorphism from $D(Q \mid P)$ to the Galois group of S/Q over R/P. This Galois group has a special generator, the mapping which sends every $x \in S/Q$ to $x^{\|P\|}$ (see Appendix C). The corresponding automorphism $\phi \in D$ has the property

$$\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{Q}$$

for every $\alpha \in S$. Assuming that P is unramified in L, ϕ is the only element in D with this property, and in fact the only element in G since this property clearly implies $\phi \in D$. We denote this automorphism by $\phi(Q \mid P)$ to indicate its dependence on Q and P. It is called the Frobenius automorphism of Q over P. It is easy to see that

$$\phi(\sigma Q \mid P) = \sigma\phi(Q \mid P)\sigma^{-1}$$

for each $\sigma \in G$, and since all primes lying over P are of this form, we conclude that the conjugacy class of the element $\phi(Q \mid P)$ is uniquely determined by P. In particular, when G is abelian $\phi(Q \mid P)$ itself is uniquely determined by the unramified prime P. This ϕ satisfies the same congruence for all Q, hence it satisfies

$$\phi(\alpha) = \alpha^{\|P\|} \pmod{PS}$$

because PS is the product of the primes Q lying over P. We summarise all of this:

> Theorem 4.6. Let L be a normal extension of K and let P be a prime of K which is unramified in L. For each prime Q of L lying over P there is a unique $\phi \in G$ such that
>
> $$\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{Q} \quad \text{for all } \alpha \in S;$$
>
> when G is abelian ϕ depends only on P, and
>
> $$\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{PS} \quad \text{for all } \alpha \in S.$$

Part of the significance of the Frobenius automorphism can be seen in the fact that its order is $f(Q \mid P)$, and thus $\phi(Q \mid P)$ indicates how P splits in L. We know this because

$\overline{G}$ is cyclic of order $f(Q \mid P)$ and $\phi(Q \mid P)$ corresponds to a generator of $\overline{G}$ under the isomorphism $D \to \overline{G}$. Thus, for example, an unramified prime P splits completely in the normal extension L if and only if $\phi = 1$.

The cyclotomic fields provide a good example. Let $L = \mathbb{Q}[\omega]$, $\omega = e^{2\pi i/m}$, and let $K = \mathbb{Q}$. We know that G is isomorphic to $\mathbb{Z}_m^*$, the multiplicative group of integers mod m, with $\sigma \in G$ corresponding to $k \in \mathbb{Z}_m^*$ iff $\sigma(\omega) = \omega^k$. The Frobenius automorphism is defined for all unramified primes p, which are the primes not dividing m, and also when $m \equiv 2 \pmod 4$. The Galois group is abelian, so ϕ depends only on p. We must have $\phi(z) \equiv z^p \pmod{p\mathbb{Z}[\omega]}$ $\forall z \in \mathbb{Z}[\omega]$. It is easy to guess which member of G satisfies this; surely it must be the automorphism σ which sends ω to ω^p. In general we have

$$\left(\sum a_i \omega^i\right)^p = \sum a_i \omega^{pi} \qquad (a_i \in \mathbb{Z});$$

thus we must show that

$$\sum a_i \omega^{pi} \equiv \left(\sum a_i \omega^i\right)^p \pmod{p\mathbb{Z}[\omega]}$$

for integers a_i. We leave it to the reader to verify this. Note that this provides another way of seeing that f is the order of p mod m when $p \nmid m$. The proof there was essentially the same, establishing an isomorphism between $\overline{G}$ and the group generated by σ; however, we had not yet developed the necessary properties of the decomposition and inertia groups and therefore required a slightly different argument.

Although the Frobenius automorphism is defined only in the case of a normal extension, it can be used to determine how a prime splits in an arbitrary extension, provided that the prime is unramified there. Suppose $K \subset L \subset M$ are number fields with M normal over K. Let G denote the Galois group of M over K, and let R, S, and T denote the number rings in K, L, and M respectively. We fix a prime P of K which is known to be unramified in M. Thus, if P is unramified in L, then M can be taken to be the normal closure of L over K. Fix any prime U of M lying over P, and let $\phi = \phi(U \mid P)$, $D = D(U \mid P)$. Finally let H denote the subgroup of G fixing L pointwise, so that H is the Galois group of M over L. We will show that the way P splits in L can be determined by considering how ϕ permutes the right cosets of H.

The cosets $H\sigma$, $\sigma \in G$, are permuted by right-multiplication by ϕ: $H\sigma$ goes to $H\sigma\phi$. The set of right cosets is then partitioned into disjoint sets orbits, each one having the form

$$\left\{H\sigma, H\sigma\phi, H\sigma\phi^2, \ldots, H\sigma\phi^{m-1}\right\}$$

for some $\sigma \in G$, with $H\sigma\phi^m = H\sigma$. Equivalently, this is one of the cycles of the permutation.

Theorem 4.7. With all notation as above, suppose that the set of right cosets of H in G is partitioned into sets

$$\left\{H\sigma_1, H\sigma_1\phi, H\sigma_1\phi^2, \ldots, H\sigma_1\phi^{m_1-1}\right\}$$

$$\vdots$$

$$\left\{H\sigma_r, H\sigma_r\phi, H\sigma_r\phi^2, \ldots, H\sigma_r\phi^{m_r-1}\right\}.$$

Then the splitting of P in L is given by

$$PS = Q_1Q_2\cdots Q_r \quad \text{where } Q_i = (\sigma_i U)\cap S.$$

Moreover, $f(Q_i \mid P) = m_i$.

Theorem 4.8. Let K be a number field, $R = \mathbb{A}\cap K$, p a prime in $\mathbb{Z}$ which divides $\operatorname{disc}(R)$. Then p is ramified in K.

Chapter 5

The Ideal Class Group and the Unit Group

5.1 The Ideal Class Group

Recall from Chapter 1.1 that the ideal class group of a number ring R consists of equivalence classes of non-zero ideals under the relation $I \sim J$ if and only if $\alpha I = \beta J$ for some non-zero $\alpha, \beta \in R$, where the group operation is multiplication defined in the obvious way.

In this chapter, we will prove that the ideal class group of a number ring is finite and establish some quantitative results that will help us to determine the ideal class group in specific cases. We will also determine the structure of the group of units of a number ring.

Finiteness of the ideal class group, as we would see in Corollary 5.2, is surprisingly easy to establish.

Theorem 5.1 (Minkowski bound for ideals). Let K be a number field and $R = \mathbb{A} \cap K$. Then, there exists a positive real number $\wedge > 0$ depending on K such that every non-zero ideal I of R contains a non-zero element α with

$$\left|N_{\mathbb{Q}}^{K}(\alpha)\right| \leq \wedge \|I\|.$$

Here, $\wedge$ is independent of I.

Proof. Fix an integral basis $\alpha_1, \ldots, \alpha_n$ of R and let $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K in $\mathbb{C}$. We claim that

$$\wedge = \prod_{i=1}^{n} \sum_{j=1}^{n} \left|\sigma_i \alpha_j\right|.$$

For any ideal I, let m denote the unique positive integer satisfying

$$m^n \leq \|I\| < (m+1)^n$$

and consider the $(m+1)^n$ members of R, which are

$$\sum_{j=1}^{n} m_j \alpha_j \quad \text{where } m_j \in \mathbb{Z} \text{ and } 0 \leq m_j \leq m.$$

By the pigeonhole principle, since there are more the $\|I\|$ these members, two of these must be congruent modulo I. Taking their difference, we obtain a non-zero member of I of the form

$$\alpha = \sum_{j=1}^{n} m_j \alpha_j \quad \text{where } m_j \in \mathbb{Z} \text{ and } \left|m_j\right| \leq m.$$

Finally, we have

$$\left|N_{\mathbb{Q}}^{K}(\alpha)\right| = \prod_{i=1}^{n} |\sigma_i \alpha| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} m_j \left|\sigma_i \alpha_j\right| \leq m^n \wedge \leq \|I\| \wedge .$$

□

Corollary 5.1. Every ideal class of R contains an ideal J with $\|J\| \leq \wedge$.

Corollary 5.2. There are only finitely many ideal classes in R.

Theorem 5.2. Let K be a number field and $R = \mathbb{A} \cap K$. The map $K \to \mathbb{R}^n$ sends R onto an n-dimensional lattice $\wedge_R$. A fundamental parallelotope for this lattice has volume

$$\frac{1}{2^s}\sqrt{|\text{disc}\,(R)|}.$$

By a fundamental parallelotope for an n-dimensional lattice $\wedge$ in $\mathbb{R}^n$, we mean a set of the form

$$\left\{ \sum_{i=1}^{n} a_i v_i : a_i \in \mathbb{R}, 0 \leq a_i < 1 \right\},$$

where $\{v_1, \ldots, v_n\}$ is any $\mathbb{Z}$-basis for $\wedge$. It is well-known that the n-dimensional volume of such a parallelotope is the absolute value of the determinant formed by taking the rows $v_1, \ldots, v_n$ (for example, see Figure 5.1). It is easy to show that any basis for $\wedge$ results in the same volume (Example 5.1), hence, this volume is an invariant of $\wedge$. We will denote it by $\text{vol}\,(\mathbb{R}^n/\wedge)$. Thus,

$$\text{vol}\,(\mathbb{R}^n/\wedge_R) = \frac{1}{2^s}\sqrt{|\text{disc}\,(R)|}.$$

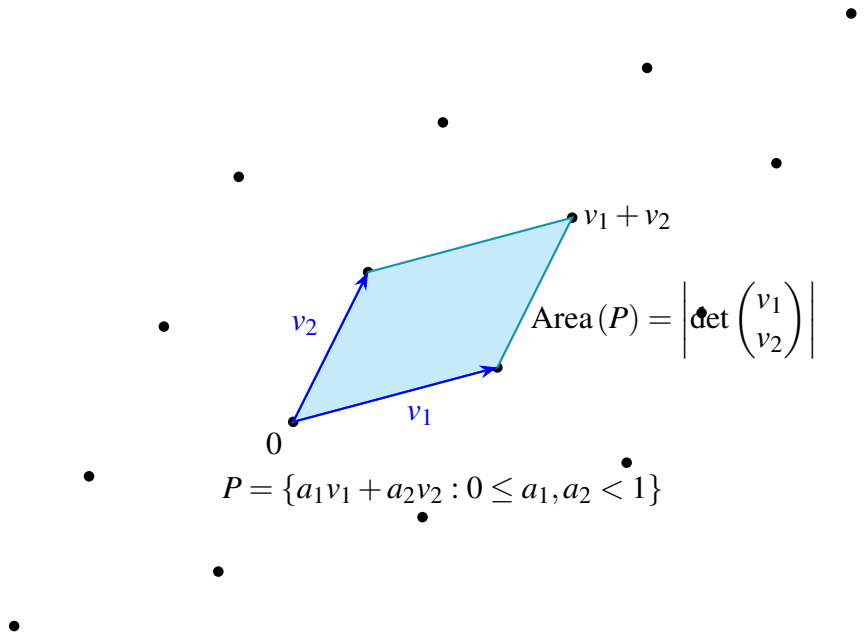


Figure 5.1: A fundamental parallelepiped in $\mathbb{R}^2$

Replacing integer coefficients by rational ones, we see that the image of K is dense in $\mathbb{R}^n$.

Example 5.1 (Marcus p. 103 Question 2). Let $\wedge$ be an n-dimensional lattice in $\mathbb{R}^n$ and let $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, w_n\}$ be any two bases for $\wedge$ over $\mathbb{Z}$. Prove that the absolute value of the determinant formed by taking the v_i as the rows is equal to the one formed from the w_i. This shows that $\text{vol}(\mathbb{R}^n/\wedge)$ can be defined unambiguously.

Solution. Since both sets are bases for $\wedge$ over $\mathbb{Z}$, then each w_i can be uniquely written as an integral linear combination of the v_j. Thus, there exist integers $a_{ij} \in \mathbb{Z}$ such that

$$w_i = \sum_{j=1}^{n} a_{ij} v_j.$$

Let $\mathbf{A} = (a_{ij}) \in \mathcal{M}_{n\times n}(\mathbb{Z})$. Then, in matrix form, we have $\mathbf{W} = \mathbf{AV}$.

Similarly, since the w_i also form a $\mathbb{Z}$-basis for $\wedge$, then each v_i can be uniquely written as an integral linear combination of the w_j. Hence, there exists a matrix $\mathbf{B} \in \mathcal{M}_{n\times n}(\mathbb{Z})$ such that $\mathbf{V} = \mathbf{BW}$.

As such, $\mathbf{V} = \mathbf{BAV}$. Since $\wedge$ is an n-dimensional lattice in $\mathbb{R}^n$, the vectors $v_1, \ldots, v_n$ are linearly independent over $\mathbb{R}$. So, $\mathbf{V}$ is invertible, which implies $\mathbf{BA} = \mathbf{I}$. A similar argument yields $\mathbf{AB} = \mathbf{I}$, so $\mathbf{A} \in \text{GL}(\mathbb{Z})$. This implies $\det(\mathbf{A})\det(\mathbf{B}) = 1$. Since the determinant of each matrix is an integer, then $\det(\mathbf{A}) = \pm 1$. The result follows. □

Example 5.2 (Marcus p. 103 Question 3). Let $\wedge$ be an n-dimensional lattice in $\mathbb{R}^n$ and let M be any n-dimensional sublattice of $\wedge$. Prove that

$$\text{vol}(\mathbb{R}^n/M) = |\wedge/M| \,\text{vol}(\mathbb{R}^n/\wedge). \tag{5.1}$$

Solution. Let $v_1,\dots,v_n$ be a $\mathbb{Z}$-basis for $\wedge$. Since $M \subseteq \wedge$ is an n-dimensional sublattice, M also has a $\mathbb{Z}$-basis $w_1,\dots,w_n$. Because each $w_i \in M \subseteq \wedge$, we can write each w_i as an integral linear combination of the v_j. Hence there exists an integer matrix $\mathbf{A}$ such that

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \mathbf{A} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

Since $w_1,\dots,w_n$ are linearly independent over $\mathbb{R}$, we have $\det(\mathbf{A}) \neq 0$.

Let $\mathbf{V}$ be the matrix whose rows are $v_1,\dots,v_n$, and let $\mathbf{W}$ be the matrix whose rows are $w_1,\dots,w_n$. Then, $\mathbf{W} = \mathbf{A}\mathbf{V}$. Taking determinants,

$$\det(\mathbf{W}) = \det(\mathbf{A})\det(\mathbf{V}).$$

But the volume of a fundamental parallelotope of a lattice is the absolute value of the determinant of a basis matrix. Hence

$$\operatorname{vol}(\mathbb{R}^n/M) = |\det(\mathbf{W})| \quad \text{and} \quad \operatorname{vol}(\mathbb{R}^n/\wedge) = |\det(\mathbf{V})|.$$

Thus,

$$\operatorname{vol}(\mathbb{R}^n/M) = |\det(\mathbf{A})| \operatorname{vol}(\mathbb{R}^n/\wedge).$$

It remains to show that $|\det(\mathbf{A})| = |\wedge/M|$. Using the basis $v_1,\dots,v_n$, we may identify $\wedge$ with $\mathbb{Z}^n$. Under this identification, the sublattice M corresponds to $\mathbf{A}\mathbb{Z}^n \subseteq \mathbb{Z}^n$. Therefore,

$$\wedge/M \cong \mathbb{Z}^n/\mathbf{A}\mathbb{Z}^n.$$

It is a standard fact that if $\mathbf{A} \in \mathcal{M}_{n\times n}(\mathbb{Z})$ and $\det(\mathbf{A}) \neq 0$, then

$$|\mathbb{Z}^n/\mathbf{A}\mathbb{Z}^n| = |\det(\mathbf{A})|.$$

Hence,

$$|\wedge/M| = |\det(\mathbf{A})|.$$

Substituting this into the previous equation gives

$$\operatorname{vol}(\mathbb{R}^n/M) = |\wedge/M| \operatorname{vol}(\mathbb{R}^n/\wedge).$$

□

Returning to the case of a general n-dimensional lattice $\wedge$, suppose M is an n-dimensional sublattice of $\wedge$. Then, $\wedge/M$ is a finite group, and it is easy to show that (5.1) holds, as seen in Example 5.2. Applying this to the image $\wedge_I$ of a non-zero ideal I in R, we obtain

$$\operatorname{vol}(\mathbb{R}^n/\wedge_I) = \operatorname{vol}(\mathbb{R}^n/\wedge_R)\,|\wedge_R/\wedge_I| = \frac{1}{2^s}\sqrt{|\operatorname{disc}(R)|}\,\|I\|.$$

Next, define a special *norm* on $\mathbb{R}^n$, depending on r and s, in the following way: for each point $x = (x_1,\dots,x_n) \in \mathbb{R}^n$, set

$$N(x) = x_1 \cdots x_r \left(x_{r+1}^2 + x_{r+2}^2\right) \cdots \left(x_{n-1}^2 + x_n^2\right). \tag{5.2}$$

This is contrived to agree with the field norm. That is to say, if $\alpha \in R$ maps to $x \in \wedge_R$, then $N(x) = N_{\mathbb{Q}}^K(\alpha)$.

Theorem 5.3. With N defined as in (5.2), every n-dimensional lattice $\wedge$ in $\mathbb{R}^n$ contains a non-zero point x with

$$|N(x)| \leq \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^s \operatorname{vol}(\mathbb{R}^n/\wedge).$$

Corollary 5.3. Every non-zero ideal I in R contains a non-zero element α with

$$\left|N_{\mathbb{Q}}^K(\alpha)\right| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(R)|}\cdot\|I\|.$$

Corollary 5.4 (Minkowski's bound for ideal classes). Every ideal class of R contains an ideal J with

$$\|J\| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(R)|}.$$

Corollaries 5.3 and 5.4 are good results as the factor $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s$, known as Minkowski's constant, gets small quickly as n increases. As such, we have an improvement over the value of $\wedge$ in Theorem 5.1. For example, when $R = \mathbb{Z}\left[\sqrt{-5}\right]$, we have

$$\|J\| \leq \frac{4\sqrt{5}}{\pi} < 3$$

so every ideal class contains some J with $\|J\| \leq 2$. Another example deals with the fifth cyclotomic field $\mathbb{Q}[\omega]$, where $\omega = e^{\frac{2\pi i}{5}}$. Every ideal class contains some J with $\|J\| \leq \frac{15\sqrt{5}}{2\pi^2}$. This quantity is < 2 so every ideal class contains R. In other words, every ideal is principal.

Here is another perspective towards Corollary 5.4. It states a lower bound for $|\operatorname{disc}(R)|$. In particular, we have

$$\sqrt{|\operatorname{disc}(R)|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s.$$

The number on the right is > 1 whenever $n \geq 2$. Hence, $|\operatorname{disc}(R)| > 1$ whenever $R \neq \mathbb{Z}$.

The significance of this is that it enables us to complete the proof of the Kronecker-Weber theorem: $\operatorname{disc}(R)$ must have a prime divisor, which is necessarily ramified in R. Thus for each $K \neq \mathbb{Q}$ there is a prime of $\mathbb{Z}$ which is ramified in K, as promised in Chapter 4.

To prove Theorem 5.3, we need the following theorem of Minkowski (Theorem 5.4).

Theorem 5.4 (Minkowski's convex body theorem). Let $\wedge$ be an n-dimensional lattice in $\mathbb{R}^n$ and let E be a convex, measurable, centrally symmetric subset of $\mathbb{R}^n$ such that

$$\operatorname{vol}(E) > 2^n \operatorname{vol}(\mathbb{R}^n/\wedge).$$

Then E contains some non-zero point of $\wedge$. If E is also compact, then the strict

inequality can be weakened to $\geq$.

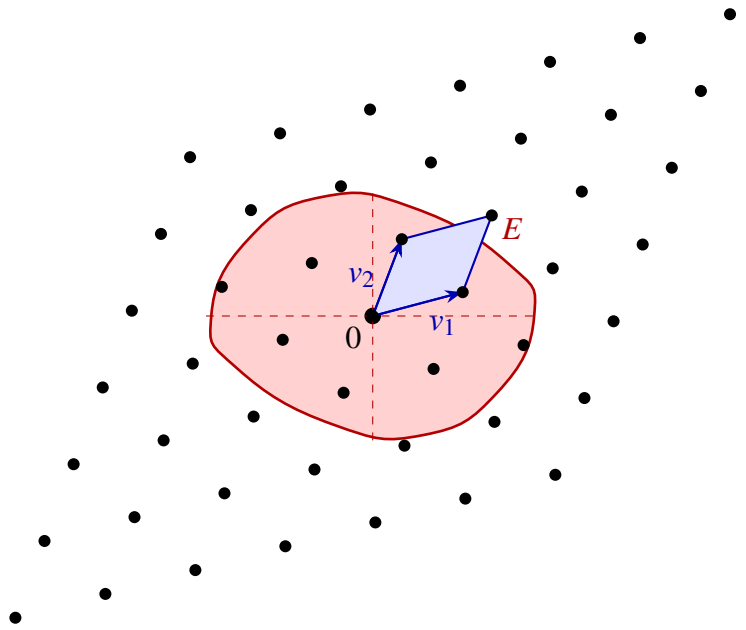


Figure 5.2: An example application of Minkowski's theorem in $\mathbb{R}^2$

By convex, we mean that if x and y are in E, then so is the entire line segment joining them. Next, measurable refers to the Lebesgue measure in $\mathbb{R}^n$, which we will not explain further except to say that the Lebesgue measure $\mathrm{vol}(E)$ coincides with any reasonable intuitive concept of n-dimensional volume, and Lebesgue measure is countably additive in the sense that if E_1, E_2 are pairwise disjoint measurable sets, then

$$\mathrm{vol}\left(\bigcup_{i=1}^{\infty} E_i\right) = \sum_{i=1}^{\infty} \mathrm{vol}(E_i).$$

Finally, centrally symmetric means symmetric around the origin. That is to say, if $x \in E$, then so is $-x$.

Proof. Let F be a fundamental parallelotope for $\wedge$. Then, $\mathbb{R}^n$ is the disjoint union of translates $x+F$, where $x \in \wedge$. It follows that

$$\frac{1}{2}E = \bigcup_{x \in \wedge} \left(\left(\frac{1}{2}E \right) \cap (x+F) \right).$$

Here, for any $t \in \mathbb{R}$, tE means the set $\{te : e \in E\}$. Hence, assuming the strict inequality,

$$\begin{aligned} \mathrm{vol}(F) < \frac{1}{2^n}\mathrm{vol}(E) &= \mathrm{vol}\left(\frac{1}{2}E\right) \\ &= \sum_{x \in \wedge} \mathrm{vol}\left(\left(\frac{1}{2}E \right) \cap (x+F) \right) \\ &= \sum_{x \in \wedge} \mathrm{vol}\left(\left(\left(\frac{1}{2}E \right) - x \right) \cap F \right) \end{aligned}$$

with the latter equality holding because the Lebesgue measure of a set is invariant under translation. The above shows that the sets $\left(\left(\frac{1}{2}E\right)-x\right)\cap F$ cannot be pairwise disjoint.

Fix any two points $x,y\in\wedge$ such that $\left(\frac{1}{2}E\right)-x$ and $\left(\frac{1}{2}E\right)-y$ intersect; then $x-y$ is a non-zero point of $\wedge$ and from the convex and symmetric properties of E we show easily that E contains $x-y$.

Now, suppose E is compact, for which in $\mathbb{R}^n$ means closed and bounded by the Heine-Borel theorem. Also, we shall weaken the strict inequality to $\geq$. For each $m=1,2,\ldots$, the first part of the theorem shows that the set $\left(1+\frac{1}{m}\right)E$ contains some non-zero point x_m of $\wedge$. The x_m are bounded as $m\to\infty$ since they are all in $2E$, and all x_m are in $\wedge$. It follows that there can be only finitely many distinct points x_m. Then, one of them is in $\left(1+\frac{1}{m}\right)E$ for infinitely many m, hence in the closure $\overline{E}$, which is E. □

Corollary 5.5. Suppose there is a compact, convex, centrally symmetric set A with $\mathrm{vol}(A)>0$, and the property

$$a\in A\Rightarrow |N(a)|\leq 1.$$

Then every n-dimensional lattice $\wedge$ contains a nonzero point x with

$$|N(x)|\leq \frac{2^n}{\mathrm{vol}(A)}\mathrm{vol}\left(\mathbb{R}^n/\wedge\right).$$

Proof. Apply Theorem 5.4 with $E=tA$, where

$$t^n=\frac{2^n}{\mathrm{vol}(A)}\mathrm{vol}\left(\mathbb{R}^n/\wedge\right).$$

The result follows. □

Example 5.3 (Marcus p. 104 Question 4). Prove that the subset of $\mathbb{R}^n$ defined by the inequalities

$$|x_1|+\cdots+|x_r|+2\left(\sqrt{x_{r+1}^2+x_{r+2}^2}+\cdots+\sqrt{x_{n-1}^2+x_n^2}\right)\leq n$$

is convex[1].

Solution. We give a *somewhat different* proof as to what the hint suggested. Define

$$F(x)=|x_1|+\cdots+|x_r|+2\left(\sqrt{x_{r+1}^2+x_{r+2}^2}+\cdots+\sqrt{x_{n-1}^2+x_n^2}\right).$$

[1] A hint is to first reduce the problem to showing that the set is closed under taking midpoints. Then use the inequality

$$\sqrt{(a+b)^2+(c+d)^2}\leq\sqrt{a^2+c^2}+\sqrt{b^2+d^2},$$

which is just the triangle inequality in $\mathbb{R}^2$.

Then, it suffices to prove that F is a convex function since sublevel sets of convex functions are also convex. That is to say, for any $x, y \in \mathbb{R}^n$ and $t \in [0,1]$, we wish to prove that

$$F(tx+(1-t)y) \leq tF(x)+(1-t)F(y).$$

For the first r coordinates, by the triangle inequality,

$$|tx_i+(1-t)y_i| \leq t|x_i|+(1-t)|y_i|.$$

For the remaining coordinates, for instance, we have

$$\sqrt{(tx_{r+1}+(1-t)y_{r+1})^2+(tx_{r+2}+(1-t)y_{r+2})^2}$$

which is the Euclidean norm of $t(x_{r+1},x_{r+2})+(1-t)(y_{r+1},y_{r+2})$. As such, the result follows. □

We now prove Theorem 5.3.

Proof. We note first that we can obtain a weaker result very easily by taking A to be the set defined by the inequalities

$$|x_1| \leq 1, \ldots, |x_r| \leq 1 \quad \text{and} \quad x_{r+1}^2+x_{r+2}^2 \leq 1, \ldots, x_{n-1}^2+x_n^2 \leq 1.$$

Then, $\mathrm{vol}(A) = 2^r\pi^s$ and we obtain the fact that every $\wedge$ contains a non-zero point x with

$$|N(x)| \leq \left(\frac{4}{\pi}\right)^s \mathrm{vol}(\mathbb{R}^n/\wedge).$$

However, we can do better. Define A by

$$|x_1|+\cdots+|x_r|+2\left(\sqrt{x_{r+1}^2+x_{r+2}^2}+\cdots+\sqrt{x_{n-1}^2+x_n^2}\right) \leq n.$$

Then, A is convex by Example 5.3. Also, the condition $a \in A \Rightarrow |N(a)| \leq 1$ is obtained by comparing the geometric mean of the n positive real numbers

$$|x_1|, \ldots, |x_r|, \sqrt{x_{r+1}^2+x_{r+2}^2}, \sqrt{x_{r+1}^2+x_{r+2}^2}, \ldots, \sqrt{x_{n-1}^2+x_n^2}, \sqrt{x_{n-1}^2+x_n^2}$$

with their arithmetic mean. The geometric mean is $\sqrt[n]{|N(a)|}$, hence $\sqrt[n]{|N(a)|}$ is at most the arithmetic mean, which is at most 1. Moreover we will prove that

$$\mathrm{vol}(A) = \frac{n^n}{n!}2^r\left(\frac{\pi}{2}\right)^s.$$

That will prove Theorem 5.3. In general, let $V_{r,s}(t)$ denote the volume of the subset of $\mathbb{R}^{r+2s}$ defined by

$$|x_1|+\cdots+|x_r|+2\left(\sqrt{x_{r+1}^2+x_{r+2}^2}+\cdots+\sqrt{x_{r+2s-1}^2+x_{r+2s}^2}\right) \leq t.$$

Then, $V_{r,s}(t) = t^{r+2s}V_{r,s}(1)$. We claim that

$$V_{r,s}(1) = \frac{1}{(r+2s)!}2^r\left(\frac{\pi}{2}\right)^s.$$

If $r > 0$ we have

$$V_{r,s}(1) = 2\int_0^1 V_{r-1,s}(1-x)\,dx = 2\int_0^1 (1-x)^{r-1+2s}\,dx V_{r-1,s}(1) = \frac{2}{r+2s}V_{r-1,s}(1).$$

Applying this repeatedly, we obtain

$$V_{r,s}(1) = \frac{2^r}{(r+2s)(r+2s-1)\cdots(2s+1)}V_{0,s}(1).$$

We leave it to the reader to consider what happens when $s = 0$. It remains to determine $V_{0,s}(1)$ for $s > 0$. We have

$$V_{0,s}(1) = \iint V_{0,s-1}\left(1-2\sqrt{x^2+y^2}\right)dxdy$$

with the integral taken over the circular region $x^2+y^2 \leq \frac{1}{4}$. Transforming to polar coordinates, it is easy to deduce that

$$V_{0,s}(1) = V_{0,s-1}(1)\,\frac{\pi}{2}\,\frac{1}{(2s)(2s-1)}.$$

Thus,

$$V_{0,s}(1) = \left(\frac{\pi}{2}\right)^s \frac{1}{(2s)!}.$$

Putting things together, we obtain the desired value for $V_{r,s}(1)$. The formula for $\mathrm{vol}(A)$ follows immediately. □

5.2 The Unit Group

Consider the multiplicative group of units U in a number ring R. We will show that U is the direct product of a finite cyclic group (consisting of the roots of unity in R) and a free abelian group. In fact, this free abelian group has rank $r+s-1$. Thus, in the imaginary quadratic case, U just consists of the roots of unity. In the real quadratic case, the roots of unity are just 1 and -1, and the free abelian part has rank 1. Thus,

$$U = \left\{\pm u^k : k \in \mathbb{Z}\right\}$$

for some unit u, called a fundamental unit in R. Subject to the condition $u > 1$, the fundamental unit is uniquely determined. The fundamental unit in $\mathbb{Z}\left[\sqrt{2}\right]$ is $1+\sqrt{2}$ and in $\mathbb{Z}\left[\sqrt{3}\right]$ is $2+\sqrt{3}$.

The fundamental unit in a real quadratic field is often surprisingly large. For example, in $\mathbb{Z}\left[\sqrt{31}\right]$, the fundamental unit is $1520+273\sqrt{31}$ and worse yet, in $\mathbb{Z}\left[\sqrt{94}\right]$, it is $2143295+221064\sqrt{94}$. On the other hand in $\mathbb{Z}\left[\sqrt{95}\right]$, it is only $39+4\sqrt{95}$. There are algorithms for determining these units, say for example using continued fractions.

There are certain other number rings in which the free abelian part of U is cyclic. Cubic fields which have only one embedding in $\mathbb{R}$ have this property since $r = s = 1$. Moreover,

the only roots of unity are ± 1 since the field has an embedding in $\mathbb{R}$. Thus, as in the real quadratic case

$$U = \left\{ \pm u^k : k \in \mathbb{Z} \right\}$$

for some unit u.

Fields of degree 4 over $\mathbb{Q}$ having no embedding in $\mathbb{R}$ have $r = 0$ and $s = 2$, hence

$$U = \left\{ \theta u^k : k \in \mathbb{Z},\ \theta \text{ a root of unity} \right\} \quad \text{where } u \text{ is a unit.}$$

for some unit u. Also, since the degree is 4, there are only a few possibilities for θ. An example is the fifth cyclotomic field. Here u can be taken to be $1+\omega$, where $\omega = e^{\frac{2\pi i}{5}}$.

Theorem 5.5. Let U be the group of units in a number ring $R = \mathbb{A} \cap K$. Let r and $2s$ denote the number of real and non-real embeddings of K in $\mathbb{C}$. Then U is the direct product $W \times V$ where W is a finite cyclic group consisting of the roots of unity in K, and V is a free abelian group of rank $r+s-1$.

In other words, V consists of products

$$u_1^{k_1} u_2^{k_2} \cdots u_{r+s-1}^{k_{r+s-1}} \quad \text{where } k_i \in \mathbb{Z}$$

for some set of $r+s-1$ units $u_1, \ldots, u_{r+s-1}$; such a set is called a fundamental system of units in R. The exponents $k_1, \ldots, k_{r+s-1}$ are uniquely determined for a given member of V.

Lemma 5.1. Fix any k, $1 \le k \le r+s$. For each non-zero $\alpha \in R$ there exists a non-zero $\beta \in R$ with

$$\left| N_{\mathbb{Q}}^K(\beta) \right| \le \left(\frac{2}{\pi} \right)^s \sqrt{|\operatorname{disc}(R)|}$$

such that if

$$\log(\alpha) = (a_1, \ldots, a_{r+s}) \quad \text{and} \quad \log(\beta) = (b_1, \ldots, b_{r+s}),$$

then $b_i < a_i$ for all $i \neq k$. The actual value of the bound for $\left| N_{\mathbb{Q}}^K(\beta) \right|$ does not matter. All we need to know is that there is some bound which is independent of α.

Lemma 5.2. Fix any k, $1 \le k \le r+s$. Then there exists $u \in U$ such that if $\log(u) = (y_1, \ldots, y_{r+s})$, then $y_i < 0$ for all $i \neq k$.

Chapter 6

The Distribution of Ideals in a Number Ring

Chapter 7

The Dedekind Zeta Function and the Class Number Formula

7.1 The Class Number Formula

Bibliography

[1] Marcus, D. A. *Number Fields*. 2nd ed., Springer, Cham, 2018. ISBN: 9783319902326.