

# Chapter 7

## Cyclotomic Extensions

A cyclotomic extension  $\mathbb{Q}(\zeta_n)$  of the rationals is formed by adjoining a primitive  $n^{\text{th}}$  root of unity  $\zeta_n$ . In this chapter, we will find an integral basis and calculate the field discriminant.

### 7.1 Some Preliminary Calculations

#### 7.1.1 The Cyclotomic Polynomial

Recall that the cyclotomic polynomial  $\Phi_n(X)$  is defined as the product of the terms  $X - \zeta$ , where  $\zeta$  ranges over all primitive  $n^{\text{th}}$  roots of unity in  $\mathbb{C}$ . Now an  $n^{\text{th}}$  root of unity is a primitive  $d^{\text{th}}$  root of unity for some divisor  $d$  of  $n$ , so  $X^n - 1$  is the product of all cyclotomic polynomials  $\Phi_d(X)$  with  $d$  a divisor of  $n$ . In particular, let  $n = p^r$  be a prime power. Since a divisor of  $p^r$  is either  $p^r$  or a divisor of  $p^{r-1}$ , we have

$$\Phi_{p^r}(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = \frac{t^p - 1}{t - 1} = 1 + t + \cdots + t^{p-1}$$

where  $t = X^{p^{r-1}}$ . If  $X = 1$  then  $t = 1$ , and it follows that  $\Phi_{p^r}(1) = p$ .

Until otherwise specified, we assume that  $n$  is a prime power  $p^r$ .

#### 7.1.2 Lemma

Let  $\zeta$  and  $\zeta'$  be primitive  $(p^r)^{\text{th}}$  roots of unity. Then  $u = (1 - \zeta')/(1 - \zeta)$  is a unit in  $\mathbb{Z}[\zeta]$ , hence in the ring of algebraic integers.

*Proof.* Since  $\zeta$  is primitive,  $\zeta' = \zeta^s$  for some  $s$  (not a multiple of  $p$ ). It follows that  $u = (1 - \zeta^s)/(1 - \zeta) = 1 + \zeta + \cdots + \zeta^{s-1} \in \mathbb{Z}[\zeta]$ . By symmetry,  $(1 - \zeta)/(1 - \zeta') \in \mathbb{Z}[\zeta'] = \mathbb{Z}[\zeta]$ , and the result follows. ♣

#### 7.1.3 Lemma

Let  $\pi = 1 - \zeta$  and  $e = \varphi(p^r) = p^{r-1}(p - 1)$ , where  $\varphi$  is the Euler phi function. Then the principal ideals  $(p)$  and  $(\pi)^e$  coincide.

*Proof.* By (7.1.1) and (7.1.2),

$$p = \Phi_{p^r}(1) = \prod_{\zeta'} (1 - \zeta') = \prod_{\zeta'} \left( \frac{1 - \zeta'}{1 - \zeta} \right) (1 - \zeta) = v(1 - \zeta)^{\varphi(p^r)}$$

where  $v$  is a unit in  $\mathbb{Z}[\zeta]$ . The result follows. ♣

We can now give a short proof of a basic result, but remember that we are operating under the restriction that  $n = p^r$ .

### 7.1.4 Proposition

The degree of the extension  $\mathbb{Q}(\zeta)/\mathbb{Q}$  equals the degree of the cyclotomic polynomial, namely  $\varphi(p^r)$ . Therefore the cyclotomic polynomial is irreducible over  $\mathbb{Q}$ .

*Proof.* By (7.1.3),  $p$  has at least  $e = \varphi(p^r)$  prime factors (not necessarily distinct) in the ring of algebraic integers of  $\mathbb{Q}(\zeta)$ . By the ram-rel identity (4.1.6),  $e \leq [\mathbb{Q}(\zeta) : \mathbb{Q}]$ . But  $[\mathbb{Q}(\zeta) : \mathbb{Q}]$  cannot exceed the degree of a polynomial having  $\zeta$  as a root, so  $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leq e$ . If  $\zeta$  were a root of an irreducible factor of  $\Phi_{p^r}$ , then the degree of the cyclotomic extension would be less than  $\varphi(p^r)$ , contradicting what we have just proved. ♣

### 7.1.5 Lemma

Let  $B$  be the ring of algebraic integers of  $\mathbb{Q}(\zeta)$ . Then  $(\pi)$  is a prime ideal (equivalently,  $\pi$  is a prime element) of  $B$ . The relative degree  $f$  of  $(\pi)$  over  $(p)$  is 1, hence the injection  $\mathbb{Z}/(p) \rightarrow B/(\pi)$  is an isomorphism.

*Proof.* If  $(\pi)$  were not prime,  $(p)$  would have more than  $\varphi(p^r)$  prime ideal factors, which is impossible, in view of the ram-rel identity. This identity also gives  $f = 1$ . ♣

We will need to do several discriminant computations, and to prepare for this, we do some calculations of norms. The symbol  $N$  with no subscript will mean the norm in the extension  $\mathbb{Q}(\zeta)/\mathbb{Q}$ .

### 7.1.6 Proposition

$N(1 - \zeta) = \pm p$ , and more generally,  $N(1 - \zeta^{p^s}) = \pm p^{p^s}$ ,  $0 \leq s < r$ .

*Proof.* The minimal polynomial of  $1 - \zeta$  is  $\Phi_{p^r}(1 - X)$ , which has constant term  $\Phi_{p^r}(1 - 0) = p$  by (7.1.1). This proves the first assertion. If  $0 < s < r$ , then  $\zeta^{p^s}$  is a primitive  $(p^{r-s})^{\text{th}}$  root of unity, so by the above calculation with  $r$  replaced by  $r - s$ ,

$$N_1(1 - \zeta^{p^s}) = \pm p$$

where  $N_1$  is the norm in the extension  $\mathbb{Q}(\zeta^{p^s})/\mathbb{Q}$ . By transitivity of norms [see (2.1.7)] applied to the chain  $\mathbb{Q}(\zeta), \mathbb{Q}(\zeta^{p^s}), \mathbb{Q}$ , and the formula in (2.1.3) for the norm of an element of the base field, we get

$$N(1 - \zeta^{p^s}) = N_1((1 - \zeta^{p^s})^b)$$

where  $b = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta^{p^s})] = \varphi(p^r)/\varphi(p^{r-s}) = p^s$ . Thus  $N(1 - \zeta^{p^s}) = \pm p^b$ , and the result follows. ♣

In (7.1.6), the sign is  $(-1)^{\varphi(n)}$ ; see (2.1.3).

### 7.1.7 Proposition

Let  $D$  be the discriminant of the basis  $1, \zeta, \dots, \zeta^{\varphi(p^r)-1}$ . Then  $D = \pm p^c$ , where  $c = p^{r-1}(pr - r - 1)$ .

*Proof.* By (2.3.6),  $D = \pm N(\Phi'_{p^r}(\zeta))$ . Differentiate the equation

$$(X^{p^{r-1}} - 1)\Phi_{p^r}(X) = X^{p^r} - 1$$

to get

$$(X^{p^{r-1}} - 1)\Phi'_{p^r}(X) + p^{r-1}X^{p^{r-1}-1}\Phi_{p^r}(X) = p^r X^{p^r-1}.$$

Setting  $X = \zeta$  and noting that  $\zeta$  is a root of  $\Phi_{p^r}$ , we have

$$(\zeta^{p^{r-1}} - 1)\Phi'_{p^r}(\zeta) + 0 = p^r \zeta^{p^r-1}.$$

Thus

$$\Phi'_{p^r}(\zeta) = \frac{p^r \zeta^{p^r-1}}{\zeta^{p^{r-1}} - 1}.$$

The norm of the denominator has been computed in (7.1.6). The norm of  $\zeta$  is  $\pm 1$ , as  $\zeta$  is a root of unity. The norm of  $p^r$  is  $p^{r\varphi(p^r)} = p^{rp^{r-1}(p-1)}$ . By (2.1.3), the norm is multiplicative, so the norm of  $\Phi'_{p^r}(\zeta)$  is  $\pm p^c$ , where

$$c = r(p-1)p^{r-1} - p^{r-1} = p^{r-1}(pr - r - 1). \quad \clubsuit$$

### 7.1.8 Remarks

In (4.2.5), we related the norm of an ideal  $I$  to the field discriminant  $d$  and the discriminant  $D(z)$  of a basis  $z$  for  $I$ . It is important to notice that the same argument works if  $I$  is replaced by any free  $\mathbb{Z}$ -module  $J$  of rank  $n$ . Thus if  $B$  is the ring of algebraic integers, then

$$D(z) = |B/J|^2 d.$$

Applying this result with  $z = \{1, \zeta, \dots, \zeta^{\varphi(p^r)-1}\}$  and  $J = \mathbb{Z}[\zeta]$ , we find that

$$D = |B/\mathbb{Z}[\zeta]|^2 d.$$

Thus if we can show that the powers of  $\zeta$  form an integral basis, so that  $\mathbb{Z}[\zeta] = B$ , then in view of (7.1.7), we are able to calculate the field discriminant up to sign. Also, by the exercises in Section 4.2, the only ramified prime is  $p$ .

Let  $\pi = 1 - \zeta$  as in (7.1.3), and recall the isomorphism  $\mathbb{Z}/(p) \rightarrow B/(\pi)$  of (7.1.5).

### 7.1.9 Lemma

For every positive integer  $m$ , we have  $\mathbb{Z}[\zeta] + p^m B = B$ .

*Proof.* We first prove the identity with  $p$  replaced by  $\pi$ . If  $b \in B$ , then  $b + (\pi) = t + (\pi)$  for some integer  $t$ , hence  $b - t \in (\pi)$ . Thus  $\mathbb{Z}[\zeta] + \pi B = B$ , and consequently  $\pi\mathbb{Z}[\zeta] + \pi^2 B = \pi B$ . Now iterate: If  $b \in B$ , then  $b = b_1 + b_2$ ,  $b_1 \in \mathbb{Z}[\zeta]$ ,  $b_2 \in \pi B$ . Then  $b_2 = b_3 + b_4$ ,  $b_3 \in \pi\mathbb{Z}[\zeta] \subseteq \mathbb{Z}[\zeta]$ ,  $b_4 \in \pi^2 B$ . Observe that  $b = (b_1 + b_3) + b_4$ , so  $\mathbb{Z}[\zeta] + \pi^2 B = B$ . Continue in this fashion to obtain the desired result. Now by (7.1.3),  $\pi^{\varphi(p^r)}$  is  $p$  times a unit, so if  $m = \varphi(p^r)$ , we can replace  $\pi^m B$  by  $pB$ , so that  $\mathbb{Z}[\zeta] + pB = B$ . But we can iterate this equation exactly as above, and the result follows. ♣

### 7.1.10 Theorem

The set  $\{1, \zeta, \dots, \zeta^{\varphi(p^r)-1}\}$  is an integral basis for the ring of algebraic integers of  $\mathbb{Q}(\zeta_{p^r})$ .

*Proof.* By (7.1.7) and (7.1.8),  $|B/\mathbb{Z}[\zeta]|$  is a power of  $p$ , so  $p^m(B/\mathbb{Z}[\zeta]) = 0$  for sufficiently large  $m$ . Therefore  $p^m B \subseteq \mathbb{Z}[\zeta]$ , hence by (7.1.9),  $\mathbb{Z}[\zeta] = B$ . ♣

## Problems For Section 7.1

This problem set will indicate how to find the sign of the discriminant of the basis  $1, \alpha, \dots, \alpha^{n-1}$  of  $L = \mathbb{Q}(\alpha)$ , where the minimal polynomial  $f$  of  $\alpha$  has degree  $n$ .

1. Let  $c_1, \dots, c_{r_1}$  be the real conjugates of  $\alpha$ , that is, the real roots of  $f$ , and let  $c_{r_1+1}, \overline{c_{r_1+1}}, \dots, c_{r_1+r_2}, \overline{c_{r_1+r_2}}$  be the complex (=non-real) conjugates. Show that the sign of the discriminant is the sign of

$$\prod_{i=1}^{r_2} (c_{r_1+i} - \overline{c_{r_1+i}})^2.$$

2. Show that the sign of the discriminant is  $(-1)^{r_2}$ , where  $2r_2$  is the number of complex embeddings.

3. Apply the results to  $\alpha = \zeta$ , where  $\zeta$  is a primitive  $(p^r)^{\text{th}}$  root of unity. (Note that a nontrivial cyclotomic extension has no real embeddings.)

## 7.2 An Integral Basis of a Cyclotomic Field

In the previous section, we found that the powers of  $\zeta$  form an integral basis when  $\zeta$  is a power of a prime. We will extend the result to all cyclotomic extensions.

### 7.2.1 Notation and Remarks

Let  $K$  and  $L$  be number fields of respective degrees  $m$  and  $n$  over  $\mathbb{Q}$ , and let  $KL$  be the composite of  $K$  and  $L$ . Then  $KL$  consists of all finite sums  $\sum a_i b_i$  with  $a_i \in K$  and  $b_i \in L$ . This is because the composite can be formed by adjoining basis elements of  $K/\mathbb{Q}$  and  $L/\mathbb{Q}$  one at a time, thus allowing an induction argument. Let  $R, S, T$  be the algebraic integers of  $K, L, KL$  respectively. Define  $RS$  as the set of all finite sums  $\sum a_i b_i$  with  $a_i \in R, b_i \in S$ . Then  $RS \subseteq T$ , but equality does not hold in general. For example,

look at  $K = \mathbb{Q}(\sqrt{m_1})$  and  $L = \mathbb{Q}(\sqrt{m_2})$ , where  $m_1 \equiv 3 \pmod{4}$ ,  $m_2 \equiv 3 \pmod{4}$ , hence  $m_1 m_2 \equiv 1 \pmod{4}$ .

### 7.2.2 Lemma

Assume that  $[KL : \mathbb{Q}] = mn$ . Let  $\sigma$  be an embedding of  $K$  in  $\mathbb{C}$  and  $\tau$  an embedding of  $L$  in  $\mathbb{C}$ . Then there is an embedding of  $KL$  in  $\mathbb{C}$  that restricts to  $\sigma$  on  $K$  and to  $\tau$  on  $L$ .

*Proof.* The embedding  $\sigma$  has  $[KL : K] = n$  distinct extensions to embeddings of  $KL$  in  $\mathbb{C}$ , and if two of them agree on  $L$ , then they agree on  $KL$  (because they coincide with  $\sigma$  on  $K$ ). This contradicts the fact that the extensions are distinct. Thus we have  $n$  embeddings of  $KL$  in  $\mathbb{C}$  with distinct restrictions to  $L$ . But there are only  $n$  embeddings of  $L$  in  $\mathbb{C}$ , so one of them must be  $\tau$ , and the result follows. ♣

### 7.2.3 Lemma

Again assume  $[KL : \mathbb{Q}] = mn$ . Let  $a_1, \dots, a_m$  and  $b_1, \dots, b_n$  be integral bases for  $R$  and  $S$  respectively. If  $\alpha \in T$ , then

$$\alpha = \sum_{i=1}^m \sum_{j=1}^n \frac{c_{ij}}{r} a_i b_j, \quad c_{ij} \in \mathbb{Z}, \quad r \in \mathbb{Z}$$

with  $r$  having no factor (except  $\pm 1$ ) in common with all the  $c_{ij}$ .

*Proof.* The assumption that  $[KL : \mathbb{Q}] = mn$  implies that the  $a_i b_j$  form a basis for  $KL/\mathbb{Q}$ . [See the process of constructing  $KL$  discussed in (7.2.1).] In fact the  $a_i b_j$  form an integral basis for  $RS$ . (This is because  $RS$  consists of all finite sums  $\sum v_i w_i$ ,  $v_i \in R$ ,  $w_i \in S$ . Each  $v_i$  is a linear combination of the  $a_k$  with integer coefficients, and so on.) It follows that  $\alpha$  is a linear combination of the  $a_i b_j$  with rational coefficients. Form a common denominator and eliminate common factors to obtain the desired result. ♣

### 7.2.4 Proposition

We are still assuming that  $[KL : \mathbb{Q}] = mn$ . If  $d$  is the greatest common divisor of the discriminant of  $R$  and the discriminant of  $S$ , then  $T \subseteq \frac{1}{d}RS$ . Thus if  $d = 1$ , then  $T = RS$ .

*Proof.* It suffices to show that in (7.2.3),  $r$  divides  $d$ . To see this, write

$$\frac{c_{ij}}{r} = \frac{c_{ij}(d/r)}{d}.$$

In turn, it suffices to show that  $r$  divides the discriminant of  $R$ . Then by symmetry,  $r$  will also divide the discriminant of  $S$ , and therefore divide  $d$ .

Let  $\sigma$  be an embedding of  $K$  in  $\mathbb{C}$ . By (7.2.2),  $\sigma$  extends to an embedding (also called  $\sigma$ ) of  $KL$  in  $\mathbb{C}$  such that  $\sigma$  is the identity on  $L$ . By (7.2.3), if  $\alpha \in T$  we have

$$\sigma(\alpha) = \sum_{i,j} \frac{c_{ij}}{r} \sigma(a_i) b_j.$$

If we set

$$x_i = \sum_{j=1}^n \frac{c_{ij}}{r} b_j,$$

we have the system of linear equations

$$\sum_{i=1}^m \sigma(a_i) x_i = \sigma(\alpha)$$

where there is one equation for each of the  $m$  embeddings  $\sigma$  from  $K$  to  $\mathbb{C}$ . Solving for  $x_i$  by Cramer's rule, we get  $x_i = \gamma_i/\delta$ , where  $\delta$  is the determinant formed from the  $\sigma(a_i)$  and  $\gamma_i$  is the determinant obtained by replacing the  $i^{\text{th}}$  column of  $\delta$  with the  $\sigma(\alpha)$ . Note that by (2.3.3),  $\delta^2$  is the discriminant of  $R$ , call it  $e$ . Since all the  $\sigma(a_i)$  and  $\sigma(\alpha)$  are algebraic integers, so are  $\delta$  and all the  $\gamma_i$ . Now

$$x_i = \frac{\gamma_i}{\delta} = \frac{\gamma_i \delta}{\delta^2} = \frac{\gamma_i \delta}{e}$$

so  $e x_i = \gamma_i \delta$  is an algebraic integer. By definition of  $x_i$ ,

$$e x_i = \sum_{j=1}^n \frac{e c_{ij}}{r} b_j,$$

an algebraic integer in  $RS$ . But  $e$  is a  $\mathbb{Z}$ -linear combination of the  $a_i$ , and the  $a_i b_j$  are an integral basis for  $RS$ , so  $e c_{ij}/r$  is an integer. Thus  $r$  divides every  $e c_{ij}$ . By (7.2.3),  $r$  has no factor (except the trivial  $\pm 1$ ) in common with every  $c_{ij}$ . Consequently,  $r$  divides  $e$ , the discriminant of  $R$ . ♣

We need one more preliminary result.

### 7.2.5 Lemma

Let  $\zeta$  be a primitive  $n^{\text{th}}$  root of unity, and denote the discriminant of  $\{1, \zeta, \dots, \zeta^{\varphi(n)-1}\}$  by  $\text{disc}(\zeta)$ . Then  $\text{disc}(\zeta)$  divides  $n^{\varphi(n)}$ .

*Proof.* Let  $f$  ( $= \Phi_n$ , the  $n^{\text{th}}$  cyclotomic polynomial) be the minimal polynomial of  $\zeta$  over  $\mathbb{Q}$ . Since  $\zeta$  is a root of  $X^n - 1$ , we have  $X^n - 1 = f(X)g(X)$  for some  $g \in \mathbb{Q}[X]$ . But  $f \in \mathbb{Z}[X]$  (because  $\zeta$  is an algebraic integer), and  $f$ , hence  $g$ , is monic, so  $g \in \mathbb{Z}[X]$ . Differentiate both sides of the equation to get  $nX^{n-1} = f(X)g'(X) + f'(X)g(X)$ . Setting  $X = \zeta$ , which is a root of  $f$ , we have  $n\zeta^{n-1} = f'(\zeta)g(\zeta)$ . But  $\zeta^{n-1} = \zeta^n/\zeta = 1/\zeta$ , so

$$n = \zeta f'(\zeta)g(\zeta).$$

Now  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ , so taking the norm of each side yields

$$n^{\varphi(n)} = N(f'(\zeta))N(\zeta g(\zeta)).$$

But by (2.3.6),  $N(f'(\zeta)) = \pm \text{disc}(\zeta)$ , and  $N(\zeta g(\zeta)) \in \mathbb{Z}$  by (2.2.2). The desired result follows. ♣

### 7.2.6 Theorem

If  $\zeta$  is a primitive  $n^{\text{th}}$  root of unity, then the ring of algebraic integers of  $\mathbb{Q}(\zeta)$  is  $\mathbb{Z}[\zeta]$ . In other words, the powers of  $\zeta$  form an integral basis.

*Proof.* We have proved this when  $\zeta$  is a prime power, so let  $n = m_1 m_2$  where the  $m_i$  are relatively prime and greater than 1. Now

$$\zeta^{m_1} = (e^{i2\pi/n})^{m_1} = e^{i2\pi m_1/n} = e^{i2\pi/m_2} = \zeta_2,$$

a primitive  $(m_2)^{\text{th}}$  root of unity, and similarly  $\zeta^{m_2} = \zeta_1$ , a primitive  $(m_1)^{\text{th}}$  root of unity. Thus  $\mathbb{Q}(\zeta_1)$  and  $\mathbb{Q}(\zeta_2)$  are contained in  $\mathbb{Q}(\zeta)$ . On the other hand, since  $m_1$  and  $m_2$  are relatively prime, there are integers  $r, s$  such that  $rm_2 + sm_1 = 1$ . Thus

$$\zeta = \zeta^{rm_2 + sm_1} = \zeta_1^r \zeta_2^s.$$

It follows that  $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1)\mathbb{Q}(\zeta_2)$ , and we can apply (7.2.4). In that proposition, we take  $K = \mathbb{Q}(\zeta_1)$ ,  $L = \mathbb{Q}(\zeta_2)$ ,  $KL = \mathbb{Q}(\zeta)$ ,  $R = \mathbb{Z}[\zeta_1]$ ,  $S = \mathbb{Z}[\zeta_2]$  (induction hypothesis),  $T = RS$ . The hypothesis on the degree  $[KL : \mathbb{Q}]$  is satisfied because  $\varphi(n) = \varphi(m_1)\varphi(m_2)$ . By (7.2.5),  $\text{disc}(\zeta_1)$  divides a power of  $m_1$  and  $\text{disc}(\zeta_2)$  divides a power of  $m_2$ . Thus the greatest common divisor of  $\text{disc}(R)$  and  $\text{disc}(S)$  is 1, and again the hypothesis of (7.2.4) is satisfied. The conclusion is that the ring  $T$  of algebraic integers of  $KL$  coincides with  $RS$ . But the above argument that  $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1)\mathbb{Q}(\zeta_2)$  may be repeated verbatim with  $\mathbb{Q}$  replaced by  $\mathbb{Z}$ . We conclude that  $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta_1]\mathbb{Z}[\zeta_2] = RS = T$ . ♣

### 7.2.7 The Discriminant of a General Cyclotomic Extension

The field discriminant of  $\mathbb{Q}(\zeta)$ , where  $\zeta$  is a primitive  $n^{\text{th}}$  root of unity, is given by

$$\frac{(-1)^{\varphi(n)/2} n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

A direct verification, with the aid of (7.1.7) and Problem 3 of Section 7.1, shows that the formula is correct when  $n = p^r$ . The general case is handled by induction, but the computation is very messy.

In the next chapter, we will study factorization of primes in Galois extensions. The results will apply, in particular, to cyclotomic extensions.