3

Quadratic and Cyclotomic Fields

In this chapter we investigate two special cases of number fields in the light of our previous work. The quadratic fields are those of degree 2, and are especially important in the study of quadratic forms. The cyclotomic fields are generated by pth roots of unity, and we consider only the case p prime; it is these which are central to Kummer's approach to Fermat's Last Theorem and play a substantial role in all subsequent work, including Wiles's proof. We shall return to both types of field at later stages. For the moment we content ourselves with finding the rings of integers, integral bases, and discriminants.

3.1 Quadratic Fields

A *quadratic field* is a number field K of degree 2 over $\mathbf{Q}$. Then $K = \mathbf{Q}(\theta)$ where θ is an algebraic integer, and θ is a zero of

$$t^2 + at + b \qquad (a, b \in \mathbf{Z}).$$

Thus

$$\theta = \frac{-a \pm \sqrt{(a^2 - 4b)}}{2}.$$

Let $a^2 - 4b = r^2 d$ where $r, d \in \mathbf{Z}$ and d is squarefree. (That this is always possible follows from prime factorization in $\mathbf{Z}$.) Then

$$\theta = \frac{-a \pm r\sqrt{d}}{2}$$

and so $\mathbf{Q}(\theta) = \mathbf{Q}(\sqrt{d})$. Hence we have proved:

Proposition 3.1. *The quadratic fields are precisely those of the form* $\mathbf{Q}(\sqrt{d})$ *for* d *a squarefree rational integer.* □

Next we determine the ring of integers of $\mathbf{Q}(\sqrt{d})$, for squarefree d. The answer, it turns out, depends on the arithmetic properties of d.

Theorem 3.2. *Let* d *be a squarefree rational integer. Then the integers of* $\mathbf{Q}(\sqrt{d})$ *are:*

(a) $\mathbf{Z}[\sqrt{d}]$ if $d \not\equiv 1 \pmod 4$,
(b) $\mathbf{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$ if $d \equiv 1 \pmod 4$.

Proof: Every element $\alpha \in \mathbf{Q}(\sqrt{d})$ is of the form $\alpha = r + s\sqrt{d}$ for $r, s \in \mathbf{Q}$. Hence we may write

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

where $a, b, c \in \mathbf{Z}$, $c > 0$, and no prime divides all of a, b, c. Now α is an integer if and only if the coefficients of the minimum polynomial

$$\left(t - \left(\frac{a + b\sqrt{d}}{c}\right)\right)\left(t - \left(\frac{a - b\sqrt{d}}{c}\right)\right)$$

are integers. Thus

$$\frac{a^2 - b^2 d}{c^2} \in \mathbf{Z}, \tag{3.1}$$

$$\frac{2a}{c} \in \mathbf{Z}. \tag{3.2}$$

If c and a have a common prime factor p then (3.1) implies that p divides b (since d is squarefree) which contradicts our previous assumption. Hence from (3.2) we have $c = 1$ or 2. If $c = 1$ then α is an integer of K in any

case, so we may concentrate on the case $c = 2$. Now a and b must both be odd, and $(a^2 - b^2 d)/4 \in \mathbf{Z}$. Hence

$$a^2 - b^2 d \equiv 0 \pmod 4.$$

Now an odd number $2k + 1$ has square $4k^2 + 4k + 1 \equiv 1 \pmod 4$, hence $a^2 \equiv 1 \equiv b^2 \pmod 4$, and this implies $d \equiv 1 \pmod 4$. Conversely, if $d \equiv 1 \pmod 4$ then for odd a, b we have α an integer because (3.1) and (3.2) hold.

To sum up: if $d \equiv 1 \pmod 4$ then $c = 1$ and so (a) holds; whereas if $d \equiv 1 \pmod 4$ we can also have $c = 2$ and a, b odd, whence easily (b) holds. □

The monomorphisms $K \to \mathbf{C}$ are given by

$$\begin{aligned} \sigma_1(r + s\sqrt{d}) &= r + s\sqrt{d}, \\ \sigma_2(r + s\sqrt{d}) &= r - s\sqrt{d}. \end{aligned}$$

Hence we can compute discriminants:

Theorem 3.3. *(a) If* $d \not\equiv 1 \pmod 4$ *then* $\mathbf{Q}(\sqrt{d})$ *has an integral basis of the form* $\{1, \sqrt{d}\}$ *and discriminant* $4d$. *(b) If* $d \equiv 1 \pmod 4$ *then* $\mathbf{Q}(\sqrt{d})$ *has an integral basis of the form* $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\}$ *and discriminant* d.

Proof: The assertions regarding bases are clear from Theorem 3.2. Computing discriminants we work out:

$$\begin{aligned} \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 &= (-2\sqrt{d})^2 = 4d, \\ \begin{vmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{d} \end{vmatrix}^2 &= (-\sqrt{d})^2 = d. \end{aligned}$$

□

Since the discriminants of isomorphic fields are equal, it follows that for distinct squarefree d the fields $\mathbf{Q}(\sqrt{d})$ are not isomorphic. This completes the classification of quadratic fields.

A special case, of historical interest as the first number field to be studied as such, is the *Gaussian field* $\mathbf{Q}(\sqrt{-1})$. Since $-1 \not\equiv 1 \pmod 4$ the ring of integers is $\mathbf{Z}[\sqrt{-1}]$ (known as the ring of *Gaussian integers*) and the discriminant is -4.

Incidentally, these results show that Theorem 2.17 is not always applicable: an integral basis *can* have a discriminant which is not squarefree. For instance, the Gaussian integers themselves.

For future reference we note the norms and traces:

$$\begin{aligned} \mathrm{N}(r+s\sqrt{d}) &= r^2 - ds^2, \\ \mathrm{T}(r+s\sqrt{d}) &= 2r. \end{aligned}$$

We also note some useful terminology. A quadratic field $\mathbf{Q}(\sqrt{d})$ is said to be *real* if d is positive, *imaginary* if d is negative. (A real quadratic field contains only real numbers, an imaginary quadratic field contains proper complex numbers as well.)

3.2 Cyclotomic Fields

A *cyclotomic field* is one of the form $\mathbf{Q}(\zeta)$ where $\zeta = e^{2\pi i/m}$ is a primitive complex mth root of unity. (The name means 'circle-cutting' and refers to the equal spacing of powers of ζ around the unit circle in the complex plane.) We shall consider only the case $m = p$, a prime number. Further, if $p = 2$ then $\zeta = -1$ so that $\mathbf{Q}(\zeta) = \mathbf{Q}$, hence we ignore this case and assume p odd.

Lemma 3.4. *The minimum polynomial of $\zeta = e^{2\pi i/p}$, p an odd prime, over $\mathbf{Q}$ is*

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

The degree of $\mathbf{Q}(\zeta)$ is $p-1$.

Proof: We have

$$f(t) = \frac{t^p - 1}{t - 1}.$$

Since $\zeta - 1 \neq 0$ and $\zeta^p = 1$ it follows that $f(\zeta) = 0$, so all we need prove is that f is irreducible. This we do by a standard piece of trickery. We have

$$f(t+1) = \frac{(t+1)^p - 1}{t} = \sum_{r=1}^{p} \binom{p}{r} t^{r-1}.$$

Now the binomial coefficient $\binom{p}{r}$ is divisible by p if $1 \leq r \leq p-1$, and $\binom{p}{1} = p$ is not divisible by p^2.

Hence by Eisenstein's criterion (Theorem 1.8) $f(t+1)$ is irreducible. Therefore $f(t)$ is irreducible, and is the minimum polynomial of ζ. Since $\partial f = p - 1$ we have $[\mathbf{Q}(\zeta) : \mathbf{Q}] = p - 1$ by Theorem 1.11. □

The powers $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ are also pth roots of unity, not equal to 1, and so by the same argument have $f(t)$ as minimum polynomial. Clearly

$$f(t) = (t-\zeta)(t-\zeta^2)\ldots(t-\zeta^{p-1}) \tag{3.3}$$

and thus the conjugates of ζ are $\zeta, \zeta^2, \ldots, \zeta^{p-1}$. This means that the monomorphisms from $\mathbf{Q}(\zeta)$ to $\mathbf{C}$ are given by

$$\sigma_i(\zeta) = \zeta^i \qquad (1 \leq i \leq p-1).$$

Because the minimum polynomial $f(t)$ has degree $p-1$, a basis for $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$ is $1, \zeta, \ldots, \zeta^{p-2}$, so for a general element

$$\alpha = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2} \qquad (a_i \in \mathbf{Q})$$

we have

$$\sigma_i(a_0 + \zeta + \ldots + a_{p-2}\zeta^{p-2}) = a_0 + \zeta^i + \ldots + a_{p-2}\zeta^{i(p-2)}.$$

From this formula the norm and trace may be calculated using the basic definitions

$$\mathrm{N}(\alpha) = \prod_{i=1}^{p-1} \sigma_i(\alpha),$$

$$\mathrm{T}(\alpha) = \sum_{i=1}^{p-1} \sigma_i(\alpha).$$

In particular

$$\mathrm{N}(\zeta) = \zeta \cdot \zeta^2 \ldots \zeta^{p-1}.$$

Now ζ and $\zeta^i (1 \leq i \leq p-1)$ are conjugates, so have the same norm, which can be calculated by putting $t = 0$ in (3.3) to give

$$\mathrm{N}(\zeta) = \mathrm{N}(\zeta^i) = (-1)^{p-1}$$

and since p is odd,

$$\mathrm{N}(\zeta^i) = 1 \quad (1 \leq i \leq p-1). \tag{3.4}$$

The trace of ζ^i can be found by a similar argument. We have

$$\mathrm{T}(\zeta^i) = \mathrm{T}(\zeta) = \zeta + \zeta^2 + \ldots + \zeta^{p-1},$$

and using the fact that

$$f(\zeta) = 1 + \zeta + \ldots + \zeta^{p-1} = 0$$

we find

$$\mathrm{T}(\zeta^i) = -1 \quad (1 \le i \le p-1). \tag{3.5}$$

For $a \in \mathbf{Q}$ we trivially have

$$\begin{aligned} \mathrm{N}(a) &= a^{p-1} \\ \mathrm{T}(a) &= (p-1)a. \end{aligned}$$

Since $\zeta^p = 1$, we can use these formulas to extend (3.4) and (3.5) to

$$\mathrm{N}(\zeta^s) = 1 \qquad \text{for all } s \in \mathbf{Z} \tag{3.6}$$

and

$$\mathrm{T}(\zeta^s) = \begin{cases} -1 & \text{if } s \not\equiv 0 \pmod{p} \\ p-1 & \text{if } s \equiv 0 \pmod{p}. \end{cases} \tag{3.7}$$

For a general element of $\mathbf{Q}(\zeta)$, the trace is easily calculated:

$$\begin{aligned} \mathrm{T}\left(\sum_{i=0}^{p-2} a_i \zeta^i\right) &= \sum_{i=0}^{p-2} \mathrm{T}(a_i \zeta^i) \\ &= \mathrm{T}(a_0) + \sum_{i=1}^{p-2} \mathrm{T}(a_i \zeta^i) \\ &= (p-1)a_0 - \sum_{i=0}^{p-2} a_i \end{aligned}$$

and so

$$\mathrm{T}\left(\sum_{i=0}^{p-2} a_i \zeta^i\right) = pa_0 - \sum_{i=1}^{p-2} a_i. \tag{3.8}$$

The norm is more complicated in general, but a useful special case is

$$\mathrm{N}(1-\zeta) = \prod_{i=1}^{p-1} (1 - \zeta^i)$$

which can be calculated by putting $t = 1$ in (3.3) to obtain

$$\prod_{i=1}^{p-1} (1 - \zeta^i) = p, \tag{3.9}$$

so

$$\mathrm{N}(1-\zeta) = p. \tag{3.10}$$

We can put these computations to good use, first by showing that the integers of $\mathbf{Q}(\zeta)$ are what one naively might expect:

Theorem 3.5. *The ring $\mathfrak{O}$ of integers of $\mathbf{Q}(\zeta)$ is $\mathbf{Z}[\zeta]$.*

Proof: Suppose $\alpha = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}$ is an integer in $\mathbf{Q}(\zeta)$. We must demonstrate that the rational numbers a_i are actually rational integers.

For $0 \le k \le p-2$ the element

$$\alpha\zeta^{-k} - \alpha\zeta$$

is an integer, so its trace is a rational integer. But

$$\begin{aligned} & \mathrm{T}(\alpha\zeta^{-k} - \alpha\zeta) \\ = \; & \mathrm{T}(a_0\zeta^{-k} + \ldots + a_k + \ldots + a_{p-2}\zeta^{p-k-2} - a_0\zeta - \ldots - a_{p-2}\zeta^{p-1}) \\ = \; & pa_k - (a_0 + \ldots + a_{p-2}) - (-a_0 - \ldots - a_{p-2}) \\ = \; & pa_k. \end{aligned}$$

Hence $b_k = pa_k$ is a rational integer.

Put $\lambda = 1 - \zeta$. Then

$$\begin{aligned} p\alpha &= b_0 + b_1\zeta + \ldots + b_{p-2}\zeta^{p-2} \\ &= c_0 + c_1\lambda + \ldots + c_{p-2}\lambda^{p-2} \end{aligned} \tag{3.11}$$

where (substituting $\zeta = 1 - \lambda$ and expanding)

$$c_i = \sum_{j=i}^{p-2} (-1)^i \binom{j}{i} b_j \in \mathbf{Z}.$$

Since $\lambda = 1 - \zeta$ we also have, symmetrically,

$$b_i = \sum_{j=i}^{p-2} (-1)^i \binom{j}{i} c_j. \tag{3.12}$$

We claim that all c_i, are divisible by p. Proceeding by induction, we may assume this for all c_i with $i \le k-1$, where $0 \le k \le p-2$. Since $c_0 =$

$b_0 + \ldots + b_{p-2} = p(-\mathrm{T}(\alpha) + b_0)$, we have $p|c_0$, so it is true for $k = 0$. Now by (3.9)

$$\begin{aligned} p &= \prod_{i=1}^{p-1}(1-\zeta^i) \\ &= (1-\zeta)^{p-1}\prod_{i=1}^{p-1}(1+\zeta+\ldots+\zeta^{i-1}) \\ &= \lambda^{p-1}\kappa \end{aligned} \tag{3.13}$$

where $\kappa \in \mathbf{Z}[\zeta] \subseteq \mathfrak{O}$. Consider (3.11) as a congruence modulo the ideal $\langle\lambda^{k+1}\rangle$ of $\mathfrak{O}$. By (3.13) we have

$$p \equiv 0 \pmod{\langle\lambda^{k+1}\rangle}.$$

and so the left-hand side of (3.11), and the terms up to $c_{k-1}\lambda^{k-1}$, vanish; further the terms from $c_{k+1}\lambda^{k+1}$ onwards are multiples of λ^{k+1} and also vanish. There remains:

$$c_k\lambda^k \equiv 0 \pmod{\langle\lambda^{k+1}\rangle}.$$

This is equivalent to

$$c_k\lambda^k = \mu\lambda^{k+1}$$

for some $\mu \in \mathfrak{O}$, from which we obtain

$$c_k = \mu\lambda.$$

Taking norms we get

$$c_k^{p-1} = \mathrm{N}(c_k) = \mathrm{N}(\mu)\mathrm{N}(\lambda) = p\mathrm{N}(\mu),$$

since $\mathrm{N}(\lambda) = p$ by (3.10). Hence $p|c_k^{p-1}$, so $p|c_k$. Hence by induction $p|c_k$ for all k, and then (3.12) shows that $p|b_k$ for all k. Therefore $a_k \in \mathbf{Z}$ for all k and the theorem is proved. □

Now we can compute the discriminant.

Theorem 3.6. *The discriminant of* $\mathbf{Q}(\zeta)$, *where* $\zeta = e^{2\pi i/p}$ *and* p *is an odd prime, is*

$$(-1)^{(p-1)/2} \cdot p^{p-2}.$$

Proof: By Theorem 3.5 an integral basis is $\{1, \zeta, \ldots, \zeta^{p-2}\}$. Hence by Proposition 2.18 the discriminant is equal to

$$(-1)^{(p-1)(p-2)/2} \cdot \mathrm{N}(\mathrm{D}f(\zeta))$$

with $f(t)$ as above. Since p is odd the first factor reduces to $(-1)^{(p-1)/2}$. To evaluate the second, we have

$$f(t) = \frac{t^p - 1}{t - 1},$$

so that

$$\mathrm{D}f(t) = \frac{(t-1)pt^{p-1} - (t^p - 1)}{(t-1)^2}$$

whence

$$\mathrm{D}f(\zeta) = \frac{-p\zeta^{p-1}}{\lambda}$$

where $\lambda = 1 - \zeta$ as before. Hence

$$\begin{aligned} \mathrm{N}(\mathrm{D}f(\zeta)) &= \frac{\mathrm{N}(p)\mathrm{N}(\zeta)^{p-1}}{\mathrm{N}(\lambda)} \\ &= \frac{(-p)^{p-1}1^{p-1}}{p} \\ &= p^{p-2}. \end{aligned}$$

□

The case $p = 3$ deserves special mention, for $\mathbf{Q}(\zeta)$ has degree $p - 1 = 2$, so it is a quadratic field. Since

$$e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2}$$

it is equal to $\mathbf{Q}(\sqrt{-3})$. As a check on our discriminant calculations: Theorem 3.3 gives -3 (since $-3 \equiv 1 \pmod 4$), and Theorem 3.6 gives $(-1)^{2/2}3^1 = -3$ as well.

3.3 Exercises

1. Find integral bases and discriminants for:
   (a) $\mathbf{Q}(\sqrt{3})$
   (b) $\mathbf{Q}(\sqrt{-7})$

(c) $\mathbf{Q}(\sqrt{11})$
(d) $\mathbf{Q}(\sqrt{-11})$
(e) $\mathbf{Q}(\sqrt{6})$
(f) $\mathbf{Q}(\sqrt{-6})$

2. Let $K = \mathbf{Q}(\zeta)$ where $\zeta = e^{2\pi i/5}$. Calculate $\mathrm{N}_K(\alpha)$ and $\mathrm{T}_K(\alpha)$ for the following values of α:

   (i) ζ^2 (ii) $\zeta + \zeta^2$ (iii) $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4$.

3. Let $K = \mathbf{Q}(\zeta)$ where $\zeta = e^{2\pi i/p}$ for a rational prime p. In the ring of integers $\mathbf{Z}[\zeta]$, show that $\alpha \in \mathbf{Z}[\zeta]$ is a unit if and only if $\mathrm{N}_K(\alpha) = \pm 1$.

4. If $\zeta = e^{2\pi i/3}$, $K = \mathbf{Q}(\zeta)$, prove that the norm of $\alpha \in \mathbf{Z}[\zeta]$ is of the form $\frac{1}{4}(a^2+3b^2)$ where a, b are rational integers which are either both even or both odd. Using the result of Exercise 3, deduce that there are precisely six units in $\mathbf{Z}[\zeta]$ and find them all.

5. If $\zeta = e^{2\pi i/5}$, $K = \mathbf{Q}(\zeta)$, prove that the norm of $\alpha \in \mathbf{Z}[\zeta]$ is of the form $\frac{1}{4}(a^2-5b^2)$ where a, b are rational integers. (Hint: in calculating $\mathrm{N}(\alpha)$, first calculate $\sigma_1(\alpha)\sigma_4(\alpha)$ where $\sigma_i(\zeta) = \zeta^i$. Show that this is of the form $q + r\theta + s\phi$ where q, r, s are rational integers, $\theta = \zeta + \zeta^4$, $\phi = \zeta^2 + \zeta^3$. In the same way, establish $\sigma_2(\alpha)\sigma_3(\alpha) = q + s\theta + r\phi$.) Using Exercise 3, prove that $\mathbf{Z}[\zeta]$ has an infinite number of units.

6. Let $\zeta = \mathrm{e}^{2\pi i/5}$. For $K = \mathbf{Q}(\zeta)$, use the formula $\mathrm{N}_K(a + b\zeta) = (a^5 + b^5)/(a + b)$ to calculate the following norms:

   (i) $\mathrm{N}_K(\zeta + 2)$ (ii) $\mathrm{N}_K(\zeta - 2)$ (iii) $\mathrm{N}_K(\zeta + 3)$.

   Using the fact that if $\alpha\beta = \gamma$, then $\mathrm{N}_K(\alpha)\mathrm{N}_K(\beta) = \mathrm{N}_K(\gamma)$, deduce that $\zeta + 2$, $\zeta - 2$, $\zeta + 3$ have no proper factors (i.e. factors which are not units) in $\mathbf{Z}[\zeta]$.

   Factorize 11, 31, 61 in $\mathbf{Z}[\zeta]$.

7. If $\zeta = e^{2\pi i/5}$, as in Exercise 6, calculate

   (i) $\mathrm{N}_K(\zeta + 4)$ (ii) $\mathrm{N}_K(\zeta - 3)$.

   Deduce that any proper factors of $\zeta + 4$ in $\mathbf{Z}[\zeta]$ have norm 5 or 41. Given $\zeta - 1$ is a factor of $\zeta + 4$, find another factor. Verify $\zeta - 3$ is a unit times $(\zeta^2 + 2)^2$ in $\mathbf{Z}[\zeta]$.

8. Show that the multiplicative group of non-zero elements of $\mathbf{Z}_7$ is cyclic with generator the residue class of 3. If $\zeta = \mathrm{e}^{2\pi i/7}$, define the monomorphism $\sigma : \mathbf{Q}(\zeta) \to \mathbf{C}$ by $\sigma(\zeta) = \zeta^3$. Show that all other monomorphisms from $\mathbf{Q}(\zeta)$ to $\mathbf{C}$ are of the form $\sigma^i (1 \le i \le 6)$ where

$\sigma^6 = 1$. For any $\alpha \in \mathbf{Q}(\zeta)$, define $c(\alpha) = \alpha\sigma^2(\alpha)\sigma^4(\alpha)$, and show $\mathrm{N}(\alpha) = c(\alpha) \cdot \sigma c(\alpha)$. Demonstrate that $c(\alpha) = \sigma^2 c(\alpha) = \sigma^4 c(\alpha)$. Using the relation $1 + \zeta + \ldots + \zeta^6 = 0$, show that every element $\alpha \in \mathbf{Q}(\zeta)$ can be written uniquely as $\sum_{i=1}^{6} a_i \zeta^i (a_i \in \mathbf{Q})$. Deduce that $c(\alpha) = a_1\theta_1 + a_3\theta_2$ where $\theta_1 = \zeta + \zeta^2 + \zeta^4$, $\theta_2 = \zeta^3 + \zeta^5 + \zeta^6$. Show $\theta_1 + \theta_2 = -1$ and calculate $\theta_1\theta_2$. Verify that $c(\alpha)$ may be written in the form $b_0 + b_1\theta_1$ where b_0, $b_1 \in \mathbf{Q}$, and show $\sigma c(\alpha) = b_0 + b_1\theta_2$. Deduce

$$\mathrm{N}(\alpha) = b_0^2 - b_0 b_1 + 2b_1^2.$$

Now calculate $\mathrm{N}(\zeta + 5\zeta^6)$.

9. Suppose p is a rational prime and $\zeta = e^{2\pi i/p}$. Given that the group of non-zero elements of $\mathbf{Z}_p$ is cyclic (see Appendix 1, Proposition 6 for a proof) show that there exists a monomorphism $\sigma : \mathbf{Q}(\zeta) \to \mathbf{C}$ such that σ^{p-1} is the identity and all monomorphisms from $\mathbf{Q}(\zeta)$ to $\mathbf{C}$ are of the form $\sigma^i (1 \le i \le p-1)$. If $p - 1 = kr$, define $c_k(\alpha) = \alpha\sigma^r(\alpha)\sigma^{2r}(\alpha)\ldots\sigma^{(k-1)r}(\alpha)$. Show

$$\mathrm{N}(\alpha) = c_k(\alpha) \cdot \sigma c_k(\alpha) \ldots \sigma^{r-1} c_k(\alpha).$$

Prove every element of $\mathbf{Q}(\zeta)$ is uniquely of the form $\sum_{i=1}^{p-1} a_i \zeta^i$, and by demonstrating that $\sigma^r(c_k(\alpha)) = c_k(\alpha)$, deduce that $c_k(\alpha) = b_1\eta_1 + \ldots + b_k\eta_k$, where

$$\eta_1 = \zeta + \sigma^r(\zeta) + \sigma^{2r}(\zeta) + \ldots + \sigma^{(k-1)r}(\zeta)$$

and $\eta_{i+1} = \sigma^i(\eta_1)$.

Interpret these results in the case $p = 5$, $k = r = 2$, by showing that the residue class of 2 is a generator of the multiplicative group of non-zero elements of $\mathbf{Z}_5$. Demonstrate that $c_2(\alpha)$ is of the form $b_1\eta_1 + b_2\eta_2$ where $\eta_1 = \zeta + \zeta^4$, $\eta_2 = \zeta^2 + \zeta^3$.

Calculate the norms of the following elements in $\mathbf{Q}(\zeta)$:

(i) $\zeta + 2\zeta^2$ (ii) $\zeta + \zeta^4$ (iii) $15\zeta + 15\zeta^4$ (iv) $\zeta + \zeta^2 + \zeta^3 + \zeta^4$.

10. In $\mathbf{Z}[\sqrt{-5}]$, prove 6 factorizes in two ways as

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Verify that $2, 3, 1 + \sqrt{-5}$, $1 - \sqrt{-5}$ have no proper factors in $\mathbf{Z}[\sqrt{-5}]$. (Hint: Take norms and note that if γ factorizes as $\gamma = \alpha\beta$, then $\mathrm{N}(\gamma) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ is a factorization of rational integers.) Deduce that it is possible in $\mathbf{Z}[\sqrt{-5}]$ for 2 to have no proper factors, yet 2 divides a product $\alpha\beta$ without dividing either α or β.