Since norms are not too hard to compute (they can always be found from symmetric polynomial considerations, often with short-cuts) whereas discriminants involve complicated work with determinants, the following result is sometimes useful:

Proposition 2.18. *Let $K = \mathbf{Q}(\theta)$ be a number field where θ has minimum polynomial p of degree n. The $\mathbf{Q}$-basis $\{1, \theta, \ldots, \theta^{n-1}\}$ has discriminant*

$$\Delta\left[1, \ldots, \theta^{n-1}\right] = (-1)^{n(n-1)/2}\mathrm{N}(\mathrm{D}p(\theta))$$

where $\mathrm{D}p$ is the formal derivative of p.

Proof: From the proof of Theorem 2.7 we obtain

$$\Delta = \Delta[1, \theta, \ldots, \theta^{n-1}] = \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2$$

where $\theta_1, \ldots, \theta_n$ are the conjugates of θ. Now

$$p(t) = \prod_{i=1}^{n} (t - \theta_i)$$

so that

$$\mathrm{D}p(t) = \sum_{j=1}^{n} \prod_{\substack{i=1 \\ i \ne j}}^{n} (t - \theta_i)$$

and therefore

$$\mathrm{D}p(\theta_j) = \prod_{\substack{i=1 \\ i \ne j}}^{n} (\theta_j - \theta_i).$$

Multiplying all these equations for $j = 1, \ldots, n$ we obtain

$$\prod_{j=1}^{n} \mathrm{D}p(\theta_j) = \prod_{\substack{i,j=1 \\ i \ne j}}^{n} (\theta_j - \theta_i).$$

The left-hand side is $\mathrm{N}(\mathrm{D}p(\theta))$. On the right, each factor $(\theta_i - \theta_j)$ for $i < j$ appears twice, once as $(\theta_i - \theta_j)$ and once as $(\theta_j - \theta_i)$. The product of these two factors is $-(\theta_i - \theta_j)^2$. On multiplying up, we get Δ multiplied by $(-1)^s$ where s is the number of pairs (i, j) with $1 \le i < j \le n$, which is given by

$$s = \tfrac{1}{2}n(n-1).$$

The result follows. □

We close this chapter by noting the following simple identity linking the discriminant and trace:

Proposition 2.19. *If $\{\alpha_1, \ldots, \alpha_n\}$ is any $\mathbf{Q}$-basis of K, then*

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\mathrm{T}(\alpha_i\alpha_j)).$$

Proof: $\mathrm{T}(\alpha_i\alpha_j) = \sum_{r=1}^{n} \sigma_r(\alpha_i\alpha_j) = \sum_{r=1}^{n} \sigma_r(\alpha_i)\sigma_r(\alpha_j)$. Hence

$$\begin{aligned} \Delta[\alpha_1, \ldots, \alpha_n] &= (\det(\sigma_i(\alpha_j)))^2 \\ &= (\det(\sigma_j(\alpha_i)))(\det(\sigma_i(\alpha_j))) \\ &= \det(\sum_{r=1}^{n} \sigma_r(\alpha_i)\sigma_r(\alpha_j)) \\ &= \det(\mathrm{T}(\alpha_i\alpha_j)). \end{aligned}$$

□

2.6 Rings of Integers

We now discuss how to find the ring of integers of a given number field. With the methods available to us, this involves moderately heavy calculation; but by taking advantage of short cuts the technique can be made reasonably efficient. In particular we show in Example 2.3 below that not every number field has an integral basis of the form $\{1, \theta, \ldots, \theta^{n-1}\}$.

The method is based on the following result:

Theorem 2.20. *Let G be an additive subgroup of $\mathfrak{O}$ of rank equal to the degree of K, with $\mathbf{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$. Then $|\mathfrak{O}/G|^2$ divides $\Delta[\alpha_1, \ldots, \alpha_n]$.*

Proof: By Theorem 1.16 there exists a $\mathbf{Z}$-basis for $\mathfrak{O}$ of the form $\{\beta_1, \ldots, \beta_n\}$ such that G has a $\mathbf{Z}$-basis $\{\mu_1\beta_1, \ldots, \mu_n\beta_n\}$ for suitable $\mu_i \in \mathbf{Z}$. Now

$$\Delta[\alpha_1, \ldots, \alpha_n] = \Delta[\mu_1\beta_1, \ldots, \mu_n\beta_n]$$

since by Lemma 1.15 a basis-change has a unimodular matrix; and the right-hand side is equal to

$$(\mu_1 \ldots \mu_n)^2\Delta[\beta_1, \ldots, \beta_n] = (\mu_1 \ldots \mu_n)^2\Delta$$

where Δ is the discriminant of K and so lies in $\mathbf{Z}$. But

$$|\mu_1 \ldots \mu_n| = |\mathfrak{O}/G|.$$

Therefore

$$|\mathfrak{O}/G|^2 \text{ divides } \Delta[\alpha_1, \ldots, \alpha_n]. \qquad \square$$

In the above situation we use the notation

$$\Delta_G = \Delta[\alpha_1, \ldots, \alpha_n].$$

We then have a generalization of Theorem 2.17:

Proposition 2.21. *Suppose that $G \neq \mathfrak{O}$. Then there exists an algebraic integer of the form*

$$\frac{1}{p}(\lambda_1\alpha_1 + \ldots + \lambda_n\alpha_n) \tag{2.6}$$

where $0 \leq \lambda_i \leq p-1$, $\lambda_i \in \mathbf{Z}$, and p is a prime such that p^2 divides Δ_G.

Proof: If $G \neq \mathfrak{O}$ then $|\mathfrak{O}/G| > 1$. Therefore (by the structure theory for finite abelian groups) there exists a prime p dividing $|\mathfrak{O}/G|$ and an element $u \in \mathfrak{O}/G$ such that $g = pu \in G$. By Theorem 2.20, p^2 divides Δ_G. Further,

$$u = \frac{1}{p}g = \frac{1}{p}(\lambda_1\alpha_1 + \ldots + \lambda_n\alpha_n)$$

since $\{\alpha_i\}$ forms a $\mathbf{Z}$-basis for G. $\square$

Note that this really *is* a generalization of Theorem 2.17: if Δ_G is squarefree then no such p exists, so that $G = \mathfrak{O}$.

We may use Proposition 2.21 as the basis of a trial-and-error search for algebraic integers in $\mathfrak{O}$ but not in G, because there are only finitely many possibilities (6). The idea is:

(a) Start with an initial guess G for $\mathfrak{O}$.

(b) Compute Δ_G.

(c) For each prime p whose square divides Δ_G, test all numbers of the form (2.6) to see which are algebraic integers.

(d) If any new integers arise, enlarge G to a new G' by adding in the new number (and divide Δ_G by p^2 to get $\Delta_{G'}$).

(e) Repeat until no new algebraic integers are found.

Example 2.22. Find the ring of integers of $\mathbf{Q}(\sqrt[3]{5})$.

Let $\theta \in \mathbf{R}$, $\theta^3 = 5$. The natural first guess is that $\mathfrak{O}$ has $\mathbf{Z}$-basis $\{1, \theta, \theta^2\}$. Let G be the abelian group generated by this set. Let $\omega = e^{2\pi i/3}$ be a cube root of unity. We compute

$$\begin{aligned}
\Delta_G &= \begin{vmatrix} 1 & \theta & \theta^2 \\ 1 & \omega\theta & \omega^2\theta^2 \\ 1 & \omega^2\theta & \omega\theta^2 \end{vmatrix}^2 \\
&= \theta^6 \begin{vmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{vmatrix}^2 \\
&= 5^2 \cdot (\omega^2 + \omega^2 + \omega^2 - \omega - \omega - \omega)^2 \\
&= 5^2 \cdot 3^2 \cdot (\omega^2 - \omega)^2 \\
&= 3^2 \cdot 5^2 \cdot (-3) \\
&= -3^3 \cdot 5^2.
\end{aligned}$$

By Proposition 2.21 we must consider two possibilities.

(a) Can $\alpha = \frac{1}{3}(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2)$ be an algebraic integer, for $0 \leq \lambda_i \leq 2$?

(b) Can $\alpha = \frac{1}{5}(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2)$ be an algebraic integer, for $0 \leq \lambda_i \leq 4$?

Consider case (b), which is harder. First use the trace: we have

$$\mathrm{T}(\alpha) = 3\lambda_1/5 \in \mathbf{Z}$$

so that $\lambda_1 \in 5\mathbf{Z}$. Then

$$\alpha' = \frac{1}{5}(\lambda_2\theta + \lambda_3\theta^2)$$

is also an algebraic integer.

Now compute the norm of α'. (It is easier to do this for α' than for α because there are fewer terms, which is why we use the trace first.) We have

$$\begin{aligned}
\mathrm{N}(a\theta + b\theta^2) &= (a\theta + b\theta^2)(a\omega\theta + b\omega^2\theta^2)(a\omega^2\theta + b\omega\theta^2) \\
&= \omega \cdot \omega^2(a\theta + b\theta^2)(a\theta + \omega b\theta^2)(a\theta + \omega^2 b\theta^2) \\
&= (a\theta)^3 + (b\theta^2)^3 \\
&= 5a^3 + 25b^3.
\end{aligned}$$

It follows that for α to be an algebraic integer, we must have $\mathrm{N}(\alpha') \in \mathbf{Z}$. But $\mathrm{N}(\alpha') = (5\lambda_2^3 + 25\lambda_3^3)/125 = (\lambda_2^3 + 5\lambda_3^3)/25$. One way to finish the calculation is just to try all cases:

λ_2	λ_3	$\lambda_2^3 + 5\lambda_3^3$	Divisible by 25?
0	1	5	No
0	2	40	No
0	3	135	No
0	4	320	No
1	0	1	No
1	1	6	No
1	2	41	No
1	3	136	No
1	4	321	No
2	0	8	No
2	1	13	No
2	2	48	No
2	3	143	No
2	4	328	No
3	0	27	No
3	1	32	No
3	2	67	No
3	3	162	No
3	4	347	No
4	0	64	No
4	1	69	No
4	2	104	No
4	3	199	No
4	4	384	No

Whichever argument we use, we have shown that if there are no better ideas, brute force can suffice. But here it is not hard to find a better idea. Suppose $\lambda_2^3 + 5\lambda_3^3 \equiv 0 \pmod{25}$. If $\lambda_3 \equiv 0 \pmod 5$, then we must also have $\lambda_2 \equiv 0 \pmod 5$. If not, we have $5 \equiv (-\lambda_2/\lambda_3)^3 \pmod{25}$. Therefore 5 is a *cubic residue* (mod 25), that is, is congruent to a cube. The factor 5 shows that we must have $5 \equiv (5k)^3 \pmod{25}$, but then $5 \equiv 0 \pmod{25}$, an impossibility.

Whichever argument we use, we have shown that no new α' occurs in case (b). The analysis in case (a) is similar, and left as Exercise 6 in this chapter.

Note that it is *necessary* for $\mathrm{N}(\alpha)$ and $\mathrm{T}(\alpha)$ to be rational integers, in order for α to be an algebraic integer; but it may not be *sufficient*. If the use of norms and traces produces a candidate for a new algebraic integer, we still have to check that it is one—for example, by finding its minimum polynomial. However, our main use of $\mathrm{N}(\alpha)$ and $\mathrm{T}(\alpha)$ is to rule out possible candidates, so this step is not always needed.

Example 2.23.

(a) Find the ring of integers of $\mathbf{Q}(\sqrt[3]{175})$.

(b) Show that it has no $\mathbf{Z}$-basis of the form $\{1, \theta, \theta^2\}$.

Solution:

(a) Let $t = \sqrt[3]{175} = \sqrt[3]{(5^2 \cdot 7)}$. Consider also $u = \sqrt[3]{5 \cdot 7^2} = \sqrt[3]{245}$. We have

$$\begin{aligned} ut &= 35 \\ u^2 &= 7t \\ t^2 &= 5u. \end{aligned}$$

Let $\mathfrak{O}$ be the ring of integers of $K = \mathbf{Q}(\sqrt[3]{175})$.

We have $u = 35/t \in K$. But $u^3 - 245 = 0$ so $u \in \mathbf{B}$. Therefore $u \in \mathbf{B} \cap K = \mathfrak{O}$.

A good initial guess is that $\mathfrak{O} = G$, where G is the abelian group generated by $\{1, t, u\}$.

To see if this is correct, we compute Δ_G. The monomorphisms $K \to \mathbf{C}$ are $\sigma_1, \sigma_2, \sigma_3$ where $\sigma_1(t) = t$, $\sigma_2(t) = \omega t$, $\sigma_3(t) = \omega^3 t$. Since $tu = 35$ which must be fixed by each σ_i, we have $\sigma_1(u) = u$, $\sigma_2(u) = \omega^2 u$, $\sigma_3(u) = \omega u$. Therefore

$$\Delta_G = \begin{vmatrix} 1 & t & u \\ 1 & \omega t & \omega^2 u \\ 1 & \omega^2 t & \omega u \end{vmatrix}^2$$

which works out as $-3^3 \cdot 5^2 \cdot 7^2$.

There are now three primes to try: $p = 3, 5$, or 7.

If $p = 5$ or 7 then, as in Example 2.22, use of the trace lets us assume that our putative integer is $\frac{1}{p}(at + bu)$ for $a, b, \in \mathbf{Z}$. Now

$$\mathrm{N}(at + bu) = 175a^3 + 245b^3$$

and we must see whether this can be congruent to 0 (mod 5^3 or 7^3) for a, b not congruent to zero.

Suppose $175a^3 + 245b^3 \equiv 0 \pmod{125}$, that is, $35a^3 + 49b^3 \equiv 0 \pmod{25}$. Write this as $10a^3 - b^3 \equiv 0 \pmod{25}$. If $a \equiv 0 \pmod 5$ then also $b \equiv 0 \pmod 5$. If not, $10 \equiv (b/a)^3 \pmod{25}$ is a cubic residue; but then $10 \equiv (5k)^3 \pmod{25}$, hence $10 \equiv 0 \pmod{25}$ which is absurd. The case $p = 7$ is dealt with in the same way.

When $p = 3$ the trace is no help, and we must compute the norm of

$$\frac{1}{3}(a + bt + cu)$$

for $a, b, c \in \mathbf{Z}$. The calculation is more complicated, but not too bad since we only have to consider $a, b, c = 0, 1, 2$. No new integers occur.

Therefore $\mathfrak{O} = G$ as we hoped.

(b) Now we have to show that there is no $\mathbf{Z}$-basis of the form $\{1, \theta, \theta^2\}$, where $\theta = a + bt + cu$. Note that $\{1, \theta, \theta^2\}$ is a $\mathbf{Z}$-basis if and only if $\{1, \theta+1, (\theta+1)^2\}$ is a $\mathbf{Z}$-basis; so we may without loss of generality assume that $a = 0$. Now

$$\begin{aligned}(bt + cu)^2 &= b^2t^2 + 2bctu + c^2u^2 \\ &= 5b^2u + 70bc + 7c^2t.\end{aligned}$$

Therefore $\{1, bt + cu, (bt + cu)^2\}$ is a $\mathbf{Z}$-basis if and only if the matrix

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & b & c \\ 70bc & 7c^2 & 5b^2 \end{vmatrix}$$

is unimodular; that is,

$$5b^3 - 7c^3 = \pm 1.$$

Consider this modulo 7. Cubes are congruent to 0, 1, or $-1 \pmod 7$, so we have $5(-1,\ 0,\ \text{or}\ 1) \equiv \pm 1 \pmod 7$, a contradiction.

Hence no such $\mathbf{Z}$-basis exists.

Example 2.24. Find the ring of integers of $\mathbf{Q}(\sqrt{2}, i)$.

(Here, our initial guess turns out not to be good enough, so this example illustrates how to continue the analysis when this unfortunate event occurs.)

The obvious guess is $\{1, \sqrt{2}, i, i\sqrt{2}\}$. Let G be the group these generate. We have $\Delta_G = -64$, so $\mathfrak{O}$ may contain elements of the form $\frac{1}{2}g$ (and then possibly $\frac{1}{4}g$ or $\frac{1}{8}g$) for $g \in G$. The norm is

$$\mathrm{N}(a + b\sqrt{2} + ci + di\sqrt{2}) = (a^2 - c^2 - 2b^2 + 2d^2)^2 + 4(ac - 2bd)^2.$$

We must find whether this is divisible by 16 for $a, b, c, d = 0$ or 1, and not all zero. By trial and error the only case where this occurs is $b = d = 1$, $a = c = 0$. So

$$\alpha = \tfrac{1}{2}(\theta + \theta i)$$

may be an integer (where $\theta = \sqrt{2}$). In fact

$$\alpha^2 = i$$

so that

$$\alpha^4 + 1 = 0$$

and α *is* an integer.

We therefore revise our initial guess to

$$G' = \{1, \theta, i, \theta i, \tfrac{1}{2}\theta(1 + i)\}.$$

Since $2 \cdot \frac{1}{2}\theta(1 + i) = \theta + \theta i$ this has a $\mathbf{Z}$-basis

$$\{1, \theta, i, \tfrac{1}{2}\theta(1 + i)\}.$$

Now

$$\Delta_{G'} = -64/2^2 = -16.$$

A recalculation of the usual kind shows that nothing of the form $\frac{1}{2}g$ (where we may now assume that the term in $\frac{1}{2}\theta(1 + i)$ occurs with nonzero coefficient) has integer norm. So no new integers arise and $\mathfrak{O} = G'$.

2.7 Exercises

1. Which of the following complex numbers are algebraic? Which are algebraic *integers*?
   (a) $355/113$
   (b) $e^{2\pi i/23}$
   (c) $e^{\pi i/23}$
   (d) $\sqrt{17} + \sqrt{19}$
   (e) $(1 + \sqrt{17})/(2\sqrt{-19})$
   (f) $\sqrt{(1 + \sqrt{2})} + \sqrt{(1 - \sqrt{2})}$.

2. Express $\mathbf{Q}(\sqrt{3}, \sqrt[3]{5})$ in the form $\mathbf{Q}(\theta)$.

3. Find all monomorphisms $\mathbf{Q}(\sqrt[3]{7}) \to \mathbf{C}$.

4. Find the discriminant of $\mathbf{Q}(\sqrt{3}, \sqrt{5})$.

5. Let $K = \mathbf{Q}(\sqrt[4]{2})$. Find all monomorphisms $\sigma : K \to \mathbf{C}$ and the minimum polynomials (over $\mathbf{Q}$) and field polynomials (over K) of (i) $\sqrt[4]{2}$ (ii) $\sqrt{2}$ (iii) 2 (iv) $\sqrt{2}+1$. Compare with Theorem 2.6.

6. Complete Example 2.22 above by discussing the case $p = 3$.

7. Complete Example 2.23 above by discussing the case $p = 3$.

8. Compute integral bases and discriminants of
   (a) $\mathbf{Q}(\sqrt{2}, \sqrt{3})$
   (b) $\mathbf{Q}(\sqrt{2}, i)$
   (c) $\mathbf{Q}(\sqrt[3]{2})$
   (d) $\mathbf{Q}(\sqrt[4]{2})$.

9. Let $K = \mathbf{Q}(\theta)$ where $\theta \in \mathfrak{O}_K$. Among the elements

$$\frac{1}{d}(a_0 + \ldots + a_i\theta^i)$$

   $(0 \neq a_i; a_0, \ldots, a_i \in \mathbf{Z})$, where d is the discriminant, pick one with minimal value of $|a_i|$ and call it x_i. Do this for $i = 1, \ldots, n = [K : \mathbf{Q}]$ show that $\{x_1, \ldots, x_n\}$ is an integral basis.

10. If $\alpha_1, \ldots, \alpha_n$ are $\mathbf{Q}$-linearly independent algebraic integers in $\mathbf{Q}(\theta)$, and if

$$\Delta[\alpha_1, \ldots, \alpha_n] = d$$

    where d is the discriminant of $\mathbf{Q}(\theta)$, show that $\{\alpha_i, \ldots, \alpha_n\}$ is an integral basis for $\mathbf{Q}(\theta)$.

11. If $[K : \mathbf{Q}] = n$, $\alpha \in \mathbf{Q}$, show

$$\begin{aligned} \mathrm{N}_K(\alpha) &= \alpha^n, \\ \mathrm{T}_K(\alpha) &= n\alpha. \end{aligned}$$

12. Give examples to show that for fixed α, $\mathrm{N}_K(\alpha)$ and $\mathrm{T}_K(\alpha)$ depend on K. (This is to emphasize that the norm and trace must always be defined in the context of a specific field K; there is no such thing as the norm or trace of α without a specified field.)

13. The norm and trace may be generalized by considering number fields $K \supseteq L$. Suppose $K = L(\theta)$ and $[K : L] = n$. Consider monomorphisms $\sigma : K \to \mathbf{C}$ such that $\sigma(x) = x$ for all $x \in L$. Show that there are precisely n such monomorphisms $\sigma_1, \ldots, \sigma_n$ and describe them. For $\alpha \in K$, define

$$\mathrm{N}_{K/L}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

$$\mathrm{T}_{K/L}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

    (Compared with our earlier notation, we have $\mathrm{N}_K = \mathrm{N}_{K/\mathbf{Q}}$, $\mathrm{T}_K = \mathrm{T}_{K/\mathbf{Q}}$.) Prove that

$$\mathrm{N}_{K/L}(\alpha_1\alpha_2) = \mathrm{N}_{K/L}(\alpha_1)\mathrm{N}_{K/L}(\alpha_2),$$

$$\mathrm{T}_{K/L}(\alpha_1 + \alpha_2) = \mathrm{T}_{K/L}(\alpha_1) + \mathrm{T}_{K/L}(\alpha_2).$$

    Let $K = \mathbf{Q}(\sqrt[4]{3})$, $L = \mathbf{Q}(\sqrt{3})$. Calculate $\mathrm{N}_{K/L}(\sqrt{\alpha})$, $\mathrm{T}_{K/L}(\alpha)$ for $\alpha = \sqrt[4]{3}$ and $\alpha = \sqrt[4]{3} + \sqrt{3}$.

14. For $K = \mathbf{Q}(\sqrt[4]{3})$, $L = \mathbf{Q}(\sqrt{3})$, calculate $\mathrm{N}_{K/L}(\sqrt{3})$ and $\mathrm{N}_{K/\mathbf{Q}}(\sqrt{3})$. Deduce that $\mathrm{N}_{K/L}(\alpha)$ depends on K and L (provided that $\alpha \in K$). Do the same for $\mathrm{T}_{K/L}$.