TheNumbersBook.com 2010

Stewart: Chapter 2, # 2, 3, 4, 8, 10, 11, 13

Problem 2.2 Express $\mathbb{Q}(\sqrt{3}, \sqrt[5]{3})$ in terms of $\mathbb{Q}(\theta)$.

We presented an explicit construction of θ using the set $S = \{\frac{\alpha - \sqrt[5]{3}}{\sqrt{3}-\beta}\}$. Now consider an element $c \notin S$, say $c = 1$ (no ratio of $\sqrt[5]{3}$ and $\sqrt{3}$ will yield 1). Then let $\theta = \alpha + c\beta = \sqrt[5]{3} + \sqrt{3}$ and we have the desired result: $\mathbb{Q}(\sqrt{3}, \sqrt[5]{3}) = \mathbb{Q}(\sqrt{3} + \sqrt[5]{3})$. ∎

Problem 2.3 Find all monomorphisms $\sigma : \mathbb{Q}(\sqrt[3]{7}) \to \mathbb{C}$.

We note that the minimal polynomial for $\sqrt[3]{7}$ is $x^3 - 7 = 0$ so that $\mathbb{Q}(\sqrt[3]{7})$ is a vector space of dimension 3. By Lemma 3 in class, there are precisely 3 different monomorphisms and each of the monomorphisms permutes the roots $\sqrt[3]{7}, \omega\sqrt[3]{7}, \omega^2\sqrt[3]{7}$ where $\omega = e^{\frac{2\pi i}{3}}$. Thus, we have the following monomorphisms:

$$\begin{aligned} 1(\sqrt[3]{7}) &= \sqrt[3]{7}, \\ \sigma_1(\sqrt[3]{7}) &= \omega\sqrt[3]{7} \\ \sigma_2(\sqrt[3]{7}) &= \omega^2\sqrt[3]{7} \end{aligned}$$

Sidenote: Note that lemma 3 is similar, but different, to the group of automorphisms of a field extension that fix a base field. It is similar in that the morphisms are determined by where the roots go but it's different in that lemma 3 specifies an embedding of $\mathbb{Q}(\sqrt[3]{7})$ (and not all roots of the minimal polynomial). It then says that the embeddings are determined by mapping $\sqrt[3]{7}$ to every root of its minimal polynomial! ∎

Problem 2.4 Find the discriminant of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

We begin by noting that $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$. Now assume that the additive subgroup of O_K, call it G, is generated by

$$\{1, \sqrt{3} + \sqrt{5}, (\sqrt{3} + \sqrt{5})^2, (\sqrt{3} + \sqrt{5})^3\} = \{1, \sqrt{3} + \sqrt{5}, 8 + 2\sqrt{15}, 18\sqrt{3} + 14\sqrt{5}\}$$

Using the four monomorphisms,

$$\begin{aligned} 1 &: \sqrt{3} + \sqrt{5} \to \sqrt{3} + \sqrt{5} \\ \sigma_1 &: \sqrt{3} + \sqrt{5} \to -\sqrt{3} + \sqrt{5} \\ \sigma_2 &: \sqrt{3} + \sqrt{5} \to \sqrt{3} - \sqrt{5} \\ \sigma_3 &: \sqrt{3} + \sqrt{5} \to -\sqrt{3} - \sqrt{5} \end{aligned}$$

we obtain a discriminant of $3686400 = 2^{14} * 3^2 * 5^2$. By Proposition 2.21, we know there may be an algebraic integer of the form $\frac{1}{2}g, \frac{1}{3}g$ and/or $\frac{1}{5}g$. Taking the norm of $\frac{1}{2}g$ yields a nasty expression in four variables that must be divisible by $2^4 = 16$ (the coefficients in front of g may be 0 or 1, as described by the Proposition). From this, we obtain that the form of the algebraic integer must be $1, \sqrt{3}+\sqrt{5}, 8+2\sqrt{15}$. Performing similar computations (using Mathematica) for $\frac{1}{3}g$ (now the coefficients may be $0, 1, 2$) and $\frac{1}{5}g$ (coefficients can now be $0, 1, 2, 3, 4$) yields the following integral basis:

$$\left\{1, \sqrt{3}+\sqrt{5}, \frac{5}{2}+\frac{1}{2}\sqrt{3}+\frac{1}{2}\sqrt{5}+\frac{1}{2}\sqrt{15}, \frac{1}{2}+3\sqrt{3}+\frac{10}{4}\sqrt{5})\right\}$$

Its discriminant is 3600. ∎

Problem 2.8 Compute integral bases and discriminants of
(a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
(b) $\mathbb{Q}(\sqrt{2}, i)$.
(c) $\mathbb{Q}(\sqrt[3]{2})$.
(d) $\mathbb{Q}(\sqrt[4]{2})$.

(a) We know that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. The usual guess is the set G generated by the elements $\{1, \theta, \theta^2, \theta^3\}$. The resulting discriminant is $384 = 2^7 * 3$ so by Proposition 2.21, we know there is an algebraic integer of the form $\frac{1}{2}g$ for $g \in G$.Taking the norm yields the expression

$$\begin{aligned} N_K(\alpha) = \frac{1}{16}(a^4 + 20a^3c - 2a^2\left(5b^2 + 98bd - 51c^2 + 485d^2\right) - 4ac \\ \left(b^2 + 10bd - 5c^2 + 49d^2\right) + b^4 + 20b^3d - 2b^2 \\ \left(5c^2 - 51d^2\right) - 4bd\left(c^2 - 5d^2\right) + c^4 - 10c^2d^2 + d^4) \end{aligned}$$

so the expression in parenthesis must be divisible by 16 for α to be an algebraic integer (Page 55). This is valid only for $a = c = 0, b = d = 1$ and $a = c = 1, b = d = 0$ and $a = b = c = d = 1$. Doing the trace eliminates $a = c = 0, b = d = 1$. Choosing $\frac{1}{2}\theta + \frac{1}{2}\theta^3$ for $a = c = 1, b = d = 0$ guarantees that we have a minimal polynomial with integer coefficients. Similarly, we choose $\frac{3}{4} + \frac{3}{4}\theta + \frac{1}{4}\theta^2 + \frac{1}{4}\theta^3$ for $a = b = c = d = 1$ to get a minimal polynomial with integer coefficients. Thus, our modified basis is now $G' = \langle 1, \sqrt{2}+\sqrt{3}, \frac{1}{2}\theta + \frac{1}{2}\theta^3, \frac{3}{4} + \frac{3}{4}\theta + \frac{1}{4}\theta^2 + \frac{1}{4}\theta^3 \rangle = O_K$ and since a recomputation yields nothing of integer form for $\frac{1}{2}g$, we conclude that that is the integral basis with discriminant 2304.

(b) The obvious guess is $G = \langle 1, \sqrt{2}, i, i\sqrt{2} \rangle$. Using Mathematica, we get $\Delta_G = -64$. By Proposition 2.21, O_K may contain elements of the form $\frac{1}{2}g$ for $g \in G$. Taking its norm gives:

$$N_K(\frac{1}{2}g) = \frac{1}{16}N(a + b\sqrt{2} + ci + di\sqrt{2}) = \frac{1}{16}((a^2 - c^2 - 2b^2 + 2d^2)^2 + 4(ac - 2bd)^2)$$

where $a, b, c, d = 0, 1$ and not all zero. This equality is an integer only for $b = d = 1, a = c = 0$. Thus, $\alpha = \frac{1}{2}(\theta + \theta i)$ and we note that $\alpha^4 + 1 = 0$ ($\theta = \sqrt{2}$). Thus, α is an algebraic integer. Our new guess can replace θi to yield $\{1, \theta, i, \frac{1}{2}(1+i)\}$. The discriminant is -16 and since a recalculation gives nothing of the form $\frac{1}{2}g$ with integer norm, we conclude that $O_K = G' =< \{1, \theta, i, \frac{1}{2}(1+i)\} >$.

(c) We assume $G = \langle 1, \sqrt[3]{2}, \sqrt[3]{2^2} \rangle$ (let $\sqrt[3]{2} = \theta$). The resulting discriminant is $-108 = 2^2 * 3^3$ so by Proposition 2.21, $\alpha = \frac{1}{2}(a + b\theta + c\theta^2)$ for $a, b, c = 0$ or 1 but not all 0. Similarly, $\alpha_2 = \frac{1}{5}(a + b\theta + c\theta^2)$. Stewart and Tall perform an exhaustive search and show that an algebraic integer of the form α_2 does not exist. How about α? Taking the norm, we have

$$N(\alpha) = \frac{1}{4}(a^3 - 6abc + 2b^3 + 4c^3)$$

The only possibility is if $a = b = 0$ and $c = 1$ (for $N(\alpha)$ to be a rational integer). So θ^2 may be an integer and since $x^3 - 25$ is its minimal polynomial, it is precisely an algebraic integer. We are, however, where we started so there will be no other algebraic integers. Thus, $G = \langle 1, \theta, \theta^2 \rangle = O_K$ with discriminant -108.

(d) Let G be generated by the usual set $\{1, \theta, \theta^2, \theta^3\}$ where $\theta = \sqrt[4]{2}$. The resulting discriminant is $-2048 = -2^{11}$. Thus, we may expect an algebraic integer to be of the form: $\alpha = \frac{1}{2}(a + b\theta + c\theta^2 + d\theta^3)$. Taking the norm (using Mathematica) yields an ugly expression in four variables that must be divisible by 16. Computing all possibilities by hand, we find that no value works. This suggests that no algebraic number occurs, so we conclude that $G = O_K$ and the discriminant is -2048.

■

Problem 2.10 If $\alpha_1, \cdots, \alpha_n$ are $\mathbb{Q}$-linearly independent algebraic integers in $\mathbb{Q}(\theta)$, and if

$$\Delta(\alpha_1, \cdots, \alpha_n) = d$$

where d is the discriminant of $\mathbb{Q}(\theta)$, show that $\{\alpha_1, \cdots, \alpha_n\}$ is an integral basis for $\mathbb{Q}(\theta)$.

Let $\{\beta_1, \cdots, \beta_n\}$ be the integral basis for $\mathbb{Q}(\theta)$. Then $\{\beta_1, \cdots, \beta_n\}$ is a basis of $O_{\mathbb{Q}(\theta)}$, the free abelian group of rank n also called ring of integers. Since $\alpha_1, \cdots, \alpha_n \in O_{\mathbb{Q}(\theta)}$. we can write them as linear combination of $\beta_1, \cdots, \beta_n$ with integer coefficients (by definition of integral basis, page 46). Let C be the matrix consisting of those coefficients. In class, we showed that

$$\Delta(\alpha_1, \cdots, \alpha_n) = \det(C)^2 \Delta(\beta_1, \cdots, \beta_n)$$

At the same time, problem statement tells us $\Delta(\alpha_1, \cdots, \alpha_n) = \Delta(\beta_1, \cdots, \beta_n)$. Comparing this with the above equation implies that $\det(C) = \pm 1$, or that it is unimodal. By Lemma 1.15, $\{\alpha_1, \cdots, \alpha_n\}$ forms a basis for $O_{\mathbb{Q}(\theta)}$. Thus, $\{\alpha_1, \cdots, \alpha_n\}$ is an integral basis for $\mathbb{Q}(\theta)$.

■

Problem 2.11 If $[K : \mathbb{Q}] = n, \alpha \in \mathbb{Q}$, show

$$N_K(\alpha) = \alpha^n$$

$$T_K(\alpha) = n\alpha$$

By definition, $N_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$ where σ_i is a monomorphism $K \to \mathbb{C}$. Since every embedding fixes $\mathbb{Q}$ pointwise and $\alpha \in \mathbb{Q}$, we have

$$\begin{aligned} N_K(\alpha) &= \prod_{i=1}^{n} \sigma_i(\alpha), \\ &= \prod_{i=1}^{n} \alpha, \\ &= \alpha^n, \end{aligned}$$

as desired. Similarly,

$$\begin{aligned} T_K(\alpha) &= \sum_{i=1}^{n} \sigma_i(\alpha) \text{ (by definition)} \\ &= \sum_{i=1}^{n} \alpha \text{ ($\mathbb{Q}$ is fixed pointwise)} \\ &= n\alpha \end{aligned}$$

■

Problem 2.13 The norm and trace may be generalized by considering number fields $L \subseteq K$. Suppose $K = L(\theta)$ and $[K : L] = n$. Consider monomorphisms $\sigma : K \to \mathbb{C}$ such that $\sigma(x) = x$ for all $x \in L$. Show that there are precisely n such monomorphisms $\sigma_1, \cdots, \sigma_n$ and describe them. For $\alpha \in K$, define

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

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

(Compared with our earlier notation, we have $N_K = N_{K/\mathbb{Q}}, T_K = T_{K/\mathbb{Q}}$.) Prove that

$$N_{K/L}(\alpha_1\alpha_2) = N_{K/L}(\alpha_1)N_{K/L}(\alpha_2),$$

$$T_{K/L}(\alpha_1 + \alpha_2) = T_{K/L}(\alpha_1) + T_{K/L}(\alpha_2).$$

Let $K = \mathbb{Q}(\sqrt[4]{3}), L = \mathbb{Q}(\sqrt{3})$. Calculate $N_{K/L}(\alpha), T_{K/L}(\alpha)$ for $\alpha = \sqrt[4]{3}$ and $\alpha = \sqrt[4]{3} + \sqrt{3}$.

Since $[K : L] = n = \deg(m_{\theta,L}(x))$,

$$m_{\theta,L}(x) = (x - \theta)(x - \theta_2) \cdots (x - \theta_n)$$

We now show that θ and $\theta_i, 2 \leq i \leq n$ are all distinct. Consider an irreducible polynomial $f(x)$ and suppose $f(x) = (x - \theta_i)^2 g(x)$ for some $\theta_i \in K$. Then applying the formal derivative,

$$\begin{aligned} Df(x) &= D((x-\theta_i)^2 g(x)) \\ &= 2(x-\theta_i)g(x) + (x-\theta_i)^2 D(g(x)) \\ &= (x-\theta_i)(2g(x) + (x-\theta_i)D(g(x))) \end{aligned}$$

Thus, θ_i is a root of $f(x)$ and $Df(x)$, and so $m_{\theta_i,L}(x)$ must divide both $f(x)$ and $Df(x)$. Since $Df(x)$ is of degree $n-1$, $m_{\theta_i,L}$ is of degree less than (or equal to) $n-1$, contradicting the irreducibility of $f(x)$. Thus, an irreducible polynomial of degree n has n distinct roots. It follows that θ and $\theta_i, 2 \leq i \leq n$ are all distinct.

Now consider monomorphisms $\sigma : K \to \mathbb{C}$ such that $\sigma(x) = x$ for all $x \in L$. Since each root of m_θ, θ_i, has a minimal polynomial that must divide m_θ and m_θ is irreducible, we have that

$$\mathbb{Q}[x]/\langle m_\theta(x) \rangle \cong \mathbb{Q}[x]/\langle m_{\theta_i}(x) \rangle$$

so there is a unique field isomorphism $\sigma_i : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i)$ given by

$$\sigma_i(\theta) = \theta_i$$

Since there are n distinct roots, there are n distinct mappings and so there are precisely n distinct monomorphisms described above. We now prove some properties.

Property 1: $N_{K/L}(\alpha_1\alpha_2) = N_{K/L}(\alpha_1)N_{K/L}(\alpha_2)$.
Proof:

$$\begin{aligned} N_{K/L}(\alpha_1\alpha_2) &= \prod_{i=1}^{n} \sigma_i(\alpha_1\alpha_2) \text{ (definition)} \\ &= \prod_{i=1}^{n} \sigma_i(\alpha_1)\sigma_i(\alpha_2) \text{ (since } \sigma_i \text{ is a ring homomorphism)} \\ &= \prod_{i=1}^{n} \sigma_i(\alpha_1) \prod_{i=1}^{n} \sigma_i(\alpha_2) \text{ (assuming commutative ring)} \\ &= N_{K/L}(\alpha_1)N_{K/L}(\alpha_2) \end{aligned}$$

Property 2: $T_{K/L}(\alpha_1 + \alpha_2) = T_{K/L}(\alpha_1) + T_{K/L}(\alpha_2)$.
Proof:

$$\begin{aligned} T_{K/L}(\alpha_1+\alpha_2) &= \sum_{i=1}^{n} \sigma_i(\alpha_1+\alpha_2) \text{ (definition)} \\ &= \sum_{i=1}^{n} \sigma_i(\alpha_1) + \sigma_i(\alpha_2) \text{ (since } \sigma_i \text{ is a ring homomorphism)} \\ &= \sum_{i=1}^{n} \sigma_i(\alpha_1) + \sum_{i=1}^{n} \sigma_i(\alpha_2) \\ &= T_{K/L}(\alpha_1) + T_{K/L}(\alpha_2) \end{aligned}$$

Finally, we calculate specific examples.
Note that $[Q(\sqrt[4]{3}) : \mathbb{Q}(\sqrt{3})] = 2$ because $x^2 - \sqrt{3} \in \mathbb{Q}(\sqrt{3})[x]$ is a minimal polynomial of $\sqrt[4]{3}$. Thus the monomorphisms are the identity and $\sigma : \sqrt[4]{3} \to -\sqrt[4]{3}$. This allows us to compute the norm and trace:

- $N_{K/L}(\sqrt[4]{3}) = \sqrt[4]{3}(-\sqrt[4]{3}) = -\sqrt{3}$ and $T_{K/L}(\alpha) = \sqrt[4]{3} - \sqrt[4]{3} = 0$.
- $N_{K/L}(\sqrt[4]{3} + \sqrt{3}) = (\sqrt[4]{3} + \sqrt{3})(-\sqrt[4]{3} + \sqrt{3}) = 3 - \sqrt{3}$ and $T_{K/L}(\alpha) = (\sqrt{3} + \sqrt[4]{3}) + \sqrt{3} - \sqrt[4]{3} = 2\sqrt{3}$.

■