Prof. A. Baker

Number Fields Examples

Michaelmas Term 2002

Sheet 1

1. Find the minimum polynomials over $\mathbb{Q}$ of $(1+i)\sqrt{3}, i+\sqrt{3}, i+e^{i\pi/3}$.

2. Find the field polynomials of i and $\sqrt[3]{5}$ in $\mathbb{Q}(i+\sqrt[3]{5})$.

3. By the symmetric function theorem, or otherwise, prove that any zero of a monic polynomial $p(x)$ with algebraic integer coefficients is an algebraic integer.

4. Which of the following are algebraic integers?

$$1/2, (\sqrt{3}+\sqrt{5})/2, (\sqrt{3}+\sqrt{7})/\sqrt{2}, (1+\sqrt[3]{10}+\sqrt[3]{100})/3.$$

5. Let $K=\mathbb{Q}(\alpha)$, where $\alpha=\sqrt[4]{2}$. Calculate the relative norm $N_{K/k}(\alpha)$ where $k=\mathbb{Q}(\sqrt{2})$. Compute $N_{K/k}(\alpha+\alpha^2)$ and also the relative traces $T_{K/k}(\alpha)$ and $T_{K/k}(\alpha+\alpha^2)$.

6. Explain why the equation

$$2.11=(5+\sqrt{3})(5-\sqrt{3})$$

is not inconsistent with the fact that $\mathbb{Q}(\sqrt{3})$ has unique factorisation.

7. Find equations to show that $\mathbb{Q}(\sqrt{d})$ does not have unique factorisation for $d=-10,-13,-14$ and -15.

8. Using unique factorisation in $\mathbb{Z}[i]$, show that, if a prime number p divides x^2+y^2 for some $x,y\in\mathbb{Z}$ with $(x,y)=1$, then there exist $a,b\in\mathbb{Z}$ such that $p=a^2+b^2$.

9. We know that the kernel of the map 'evaluation at i' given by $\mathbb{Z}[X]\longrightarrow\mathbb{Z}[i]$, that is $g(X)\mapsto g(i)$, is $\mathbb{Z}[X]\cap(X^2+1)\mathbb{Q}[X]$. Show that in fact the kernel is $(X^2+1)\mathbb{Z}[X]$ and deduce that the above map induces an isomorphism of rings $\mathbb{Z}[X]/(X^2+1)\to\mathbb{Z}[i]$.

10. Show that, if π is a prime (ie. an irreducible element) of $\mathbb{Z}[i]$, then $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is a finite field with $N(\pi)=\pi\bar{\pi}$ elements.

11. Let K be a field with characteristic $\neq 2$. Show that every extension L/K of degree 2 is of the form $L_a=K(\sqrt{a})$ with $a\in K^*$, $a\notin K^{*2}$. Show further that $L_a=L_b$ if and only if $a/b\in K^{*2}$.

12. Show that, for $a,b\in\mathbb{Q}^*$, the degree of $\mathbb{Q}(\sqrt{a},\sqrt{b})$ is equal to the order of the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ generated by a,b. Determine whether the field $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is of the form $\mathbb{Q}(\sqrt{a},\sqrt{b})$ with $a,b\in\mathbb{Q}$.

13. (Tripos 96) Let G denote the Galois group of $k = \mathbb{Q}(\sqrt{2}, \sqrt{7})$ over $\mathbb{Q}$. You may assume that $G = \{1, \alpha, \beta, \alpha\beta\}$, where

$$\alpha(\sqrt{2}) = \sqrt{2}, \quad \alpha(\sqrt{7}) = -\sqrt{7}, \quad \beta(\sqrt{2}) = -\sqrt{2}, \quad \beta(\sqrt{7}) = \sqrt{7}.$$

By considering the relative traces $\theta + \sigma(\theta)$, where σ runs through the elements of G other than the identity, show that the algebraic integers in k have the form

$$\theta = \frac{1}{2}(a + b\sqrt{7} + c\sqrt{2} + d\sqrt{14}),$$

where a, b, c, d are rational integers.
By computing the relative norm $\theta\sigma(\theta)$, where σ takes $\sqrt{2}$ to $-\sqrt{2}$, or otherwise, show that a and b are even and that $c \equiv d (\mathrm{mod}\ 2)$. Hence prove that an integral basis for k is $1, \sqrt{2}, \sqrt{7}, \frac{1}{2}(\sqrt{2} + \sqrt{14})$.

14. Let $K \subset L$ be number fields. Show that, for $\alpha \in \mathcal{O}_L$, the trace and norm $T_{L/K}(\alpha)$, $N_{L/K}(\alpha)$ are in $\mathcal{O}_K$. Let now $L = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. For $\theta = a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} \in L$ compute $T_{L/K_j}(\theta)$, $N_{L/K_j}(\theta)$ for the three quadratic subfields $K_j = \mathbb{Q}(\sqrt{j})$ with $j = 3, 5, 15$. Hence find $\mathcal{O}_L$.

15. What is the Galois group of the field $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ where p, q are distinct primes?
Find an integral basis for the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Calculate the discriminant of the field.

16. (Tripos 97) Prove that, if $k = \mathbb{Q}(\alpha)$ is an algebraic number field with degree n and if the discriminant $\Delta(1, \alpha, ..., \alpha^{n-1})$ is square-free, then $1, \alpha, ..., \alpha^{n-1}$ is an integral basis for k.
Show that the zeros α, β, γ of the polynomial $x^3 - x - 1$ satisfy

$$\alpha(\alpha - \beta)(\alpha - \gamma) = 2\alpha + 3.$$

By computing the field norms on either side, or otherwise, verify that $1, \alpha, \alpha^2$ is an integral basis for $\mathbb{Q}(\alpha)$.

17. (Tripos 98) Explain what is meant by an integral basis of an algebraic number field. Specify such a basis for the quadratic field $k = \mathbb{Q}(\sqrt{2})$.
Let K be the quartic field $\mathbb{Q}(\alpha)$ with $\alpha = \sqrt[4]{2}$. By computing the relative traces $T_{K/k}(\theta)$ and $T_{K/k}(\alpha\theta)$, show that the algebraic integers in K have the form

$$\theta = a + b\alpha + c\alpha^2 + d\alpha^3,$$

where $2a, 2b, 2c$ and $4d$ are rational integers. By further computing the relative norm $N_{K/k}(\theta)$, show that the expressions

$$a^2 + 2c^2 - 4bd \quad \text{and} \quad 2ac - b^2 - 2d^2$$

are rational integers. Deduce that $1, \alpha, \alpha^2, \alpha^3$ is an integral basis for K.

18. (Tripos 99) Let $K/\mathbb{Q}$ be a finite extension of degree n, and let $\alpha_1, \ldots, \alpha_n$ be algebraic integers in K such that the discriminant $D(\alpha_1, \ldots, \alpha_n)$ is a square-free non-zero integer. Show that $\alpha_1, \ldots, \alpha_n$ is an integral basis of K, i.e. $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$ where $\mathcal{O}_K$ is the ring of integers of K.
Show that the discriminant of the polynomial $X^3 + aX + b$ is equal to $-4a^3 - 27b^2$.
Let α be a root of the polynomial $X^3 + X + 1$. Show that the ring of algebraic integers in $K = \mathbb{Q}(\alpha)$ is equal to $\mathbb{Z}[\alpha]$.

19. (Tripos 00 - adapted) Let $K = \mathbb{Q}(\delta)$ where $\delta = \sqrt[3]{d}$ for a square-free integer $d \neq 0, \pm 1$. Show that $\Delta(1, \delta, \delta^2) = -27d^2$. By calculating the traces of $\alpha, \alpha\delta, \alpha\delta^2$, where $\alpha = u + v\delta + w\delta^2$ is the general element of K with u, v, w rational, show that the ring of algebraic integers $\mathcal{O}_K$ of K satisfies

$$\mathbb{Z}[\sqrt[3]{d}] \subseteq \mathcal{O}_K \subseteq \frac{1}{3}\mathbb{Z}[\sqrt[3]{d}].$$

20. (Tripos 01) Let $K = \mathbb{Q}(\alpha)$ be a number field, where $\alpha \in \mathcal{O}_K$. Let f be the (normalized) minimal polynomial of α over $\mathbb{Q}$. Show that the discriminant $\mathrm{disc}(f)$ of f is equal to $(\mathcal{O}_K : \mathbb{Z}[\alpha])^2 D_K$.
Show that $f(x) = x^3 + 5x^2 - 19$ is irreducible over $\mathbb{Q}$. Determine $\mathrm{disc}(f)$ and the ring of algebraic integers $\mathcal{O}_K$ of $K = \mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{C}$ is a root of f.

21. (Tripos 02) Explain what is meant by an integral basis $\omega_1, \ldots, \omega_n$ of a number field K. Give an expression for the discriminant of K in terms of the traces of the $\omega_i\omega_j$.
Let $K = \mathbb{Q}(i, \sqrt{2})$. By computing the traces $T_{K/k}(\theta)$, where k runs through the three quadratic subfields of K, show that the algebraic integers θ in K have the form $\frac{1}{2}(\alpha + \beta\sqrt{2})$, where $\alpha = a + ib$ and $\beta = c + id$ are Gaussian integers. By further computing the norm $N_{K/k}(\theta)$, where $k = \mathbb{Q}(\sqrt{2})$, show that a and b are even and that $c \equiv d \pmod 2$. Hence prove that an integral basis for K is $1, i, \sqrt{2}, \frac{1}{2}(1+i)\sqrt{2}$.
Calculate the discriminant of K.