Lent Term 2008 M. Strauch

Number Fields: Example Sheet 1

(1) Which of the following are algebraic integers?

$$\frac{1}{2}, \quad \frac{\sqrt{3}+\sqrt{5}}{2}, \quad \frac{\sqrt{3}+\sqrt{7}}{\sqrt{2}}, \quad \frac{3+2\sqrt{6}}{1-\sqrt{6}}.$$

(2) Let $D \in \mathbb{Z}$, $D \neq 0$, $D \neq 1$, be a square-free integer, and put $K = \mathbb{Q}(\sqrt{D})$.

(a) Show that the ring of integers $\mathcal{O}_K$ of K is equal to $\mathbb{Z}[\sqrt{D}]$ if $D \equiv 2 \mod 4$ or $D \equiv 3 \mod 4$. Show further that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ if $D \equiv 1 \mod 4$.

(b) Denote by d_K the discriminant of K. Show that $d_K = 4D$ if $D \equiv 2 \mod 4$ or $D \equiv 3 \mod 4$, and $d_K = D$ if $D \equiv 1 \mod 4$.

(3) (a) Let $f(X) = a_0X^n + \ldots + a_n \in \mathbb{Z}[X]$, $a_0 \neq 0$, be a polynomial. Show that, if $f(\frac{a}{b}) = 0$ for $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, then $b|a_0$ and $a|a_n$.

(b) Determine which of the following polynomials are irreducible over $\mathbb{Q}$: $X^3 \pm X + 1$, $X^3 \pm X + 2$, $X^3 \pm X + 3$.

(4) (a) Let n be a positive integer and $A \in M_n(\mathbb{Z})$ be a matrix. By using elementary column and row operations, show that there are matrices $S, T \in GL_n(\mathbb{Z})$ such that SAT is a diagonal matrix.

(b) Let $N \subset \mathbb{Z}^n$ be a submodule of rank n. Show that there is a matrix $A \in M_n(\mathbb{Z})$ such that $A(\mathbb{Z}^n) = N$ and the index $[\mathbb{Z}^n : N]$ of N in $\mathbb{Z}^n$ is equal to $|\det(A)|$.

(5) Let K be a number field of degree $n = [K : \mathbb{Q}]$, and let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ be a basis of $K/\mathbb{Q}$ such that $d(\alpha_1, \ldots, \alpha_n)$ is a square-free integer. Show that $\alpha_1, \ldots, \alpha_n$ is an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$.

(6) (a) Let $f(X) \in \mathbb{Q}[X]$ be a monic irreducible polynomial of degree n and $\theta \in \mathbb{C}$ a root of f. Put $K = \mathbb{Q}(\theta)$. Show that the discriminant of the basis $(1, \theta, \ldots, \theta^{n-1})$ of K is equal to $(-1)^{\frac{n(n-1)}{2}} R(f, f')$, where $R(f, f')$ denotes the resultant of f and its derivative f'. The latter is also called the discriminant of f.

(b) Show that the discriminant of the polynomial $X^3 + cX + d$ is $-4c^3 - 27d^2$. Show further that $(1, \theta, \theta^2)$ is an integral basis of $\mathcal{O}_K$ for $K = \mathbb{Q}(\theta)$, where $\theta^3 + \theta + 1 = 0$.

(7) Let R be a commutative ring with unit. For $a, b \in R$ we say that a *divides* b (notation $a|b$) if $b = ac$ for some $c \in R$. Note that $a|1 \iff a \in R^*$. We say that a is *associated* to b iff $a = ub$ with $u \in R^*$ (notation $a \sim b$). If R is a domain, then $a \sim b \iff (a|b \wedge b|a)$. We call an element $a \in R - R^*$ *irreducible* if for any factorization $a = bc$ one of b, c is a unit in R. A non-zero non-unit a is called a *prime element* if a generates a prime ideal. An integral domain R is called a *unique factorization domain* (UFD) if the following two conditions are satisfied:

(i) every element $a \in R - \{0\}$, which is not a unit can be written as a product of (finitely many) irreducible elements;

(ii) if $a = x_1 \cdots x_r = y_1 \cdots y_s$ with all x_i, y_j irreducible, then $r = s$ and there is a permutation σ of $\{1, \ldots, r\}$ such that for all i: $x_i \sim y_{\sigma(i)}$.

(a) Show that in any domain R the prime elements are irreducible, and that in an UFD the irreducible elements are prime elements. Show further that a domain in which (i) holds and in which the irreducible elements are prime elements is an UFD.

(b) Recall that a *principal ideal domain* (PID) is an integral domain in which every ideal is principal (that is, generated by a single element). Show that a PID is a Dedekind domain. Show further that a PID is an UFD.

Remark. Conversely, we will see later that a Dedekind domain which is an UFD is a PID.

(8) An integral domain R is called a *euclidian domain* if there is a map $N : R - \{0\} \to \mathbb{Z}_{>0}$ such that for all $a, b \in R$, $b \neq 0$, there are $d, r \in R$ with the property that

$$a = db + r\,,$$

with either $r = 0$ or $r \neq 0$ and $N(r) < N(b)$.

(a) Show that the ring of Gaussian integers $\mathbb{Z}[i]$ is an euclidian ring. (Hint: take $N = N_{\mathbb{Q}(i)/\mathbb{Q}}$ and use the graphic interpretation of elements of $\mathbb{Z}[i]$ as lattice points in $\mathbb{C}$.)

(b) Show that any euclidian domain is a principal ideal domain. Deduce that $\mathbb{Z}[i]$ is a UFD.

(c) Show that the group of units of $\mathbb{Z}[i]$ is $\{1, -1, i, -i\}$.

(9) (a) Let p be an odd prime number. Show that the congruence $x^2 \equiv -1 \mod p$ has a solution $x \in \mathbb{Z}$ if and only if $p \equiv 1 \mod 4$. (Hint: use the fact that the multiplicative group $\mathbb{F}_p^*$ is cyclic.)

(b) Use (a) and the preceding exercise to show that a prime p which is congruent to $1 \mod 4$ is of the form $a^2 + b^2$ with $a, b \in \mathbb{Z}$. (Hint: p can not be a prime element in $\mathbb{Z}[i]$ because $p|(x^2+1)$ would then imply $p|(x+i)$ or $p|(x-i)$. Thus p is not irreducible in $\mathbb{Z}[i]$.)

(c) Show that a prime number p which is congruent to $3 \mod 4$ is a prime element in $\mathbb{Z}[i]$.

(10) *Prime elements in* $\mathbb{Z}[i]$. Use the preceding two exercises two show that the prime elements of $\mathbb{Z}[i]$ are, up to associated elements, given as follows:

(1) $1 + i$,
(2) p, with $p \equiv 3 \mod 4$,
(3) $a + ib$, with $p = a^2 + b^2$ a prime number $\equiv 1 \mod 4$ and $a > |b|$.

(11) The ring of integers $\mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{-5})$ is by exercise 2 equal to $\mathbb{Z}[\sqrt{-5}]$. Show that $3, 7, 1+2\sqrt{-5}$ and $1 - 2\sqrt{-5}$ are all irreducible elements in $\mathcal{O}_K$. (Hint: use the norm $N_{K/\mathbb{Q}}$.) Deduce from the equation $3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})$ that $\mathcal{O}_K$ is not a UFD.

(12) Show that the rings of integers $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{D})$, are euclidian domains for $D = -3, -2, 2, 3$. These rings are in particular all unique factorization domains. (Hint: proceed as in exercise 8.)

(13) Explain why the equation $2 \cdot 11 = (5 + \sqrt{3}) \cdot (5 - \sqrt{3})$ is not inconsistent with the fact that $\mathbb{Z}[\sqrt{3}]$ has unique factorization.

(14) Let G be 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

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

By considering the relative traces $\theta + \sigma(\theta)$, where σ runs through the elements of G other than the identity, show that the 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 $\sigma \in G$ takes $\sqrt{2}$ to $-\sqrt{2}$, or otherwise, show that a and b are even and that $c \equiv d \mod 2$. Hence prove that an integral basis for $\mathcal{O}_K$ is $1, \sqrt{2}, \sqrt{7}, \frac{1}{2}(\sqrt{2} + \sqrt{14})$.

(15) Show that an integral domain with finitely many elements is a field.

Comments, corrections and queries can be send to me at M.Strauch@dpmms.cam.ac.uk