

## Algebraic number theory – Additional exercises

H. W. Lenstra, P. Stevenhagen, Fall 2008

<http://websites.math.leidenuniv.nl/ant2008/>

### 1 – Introduction to number rings

**Exercise 1.32.** In this exercise you may make use of the theorem that for every  $d \in \mathbf{Z}_{>0}$  that is not a square, there are positive integers  $x, y$  with  $x^2 = dy^2 + 1$ . By a *triangular number* we mean a number of the form  $n(n+1)/2$ , where  $n \in \mathbf{Z}_{>0}$ .

Let  $q$  be a positive rational number. Prove that the following statements are equivalent:

- (i) there are a triangular number  $T$  and a non-zero square  $S$  with  $T/S = q$ ;
- (ii) there are infinitely many pairs  $(T, S)$  as in (i);
- (iii) for each positive integer  $k$ , there is a pair  $(T, S)$  as in (i) with the additional property that  $S$  is divisible by  $k$ ;
- (iv) there does not exist a rational number  $r$  with  $q = 2r^2$ .

**Exercise 1.33.** Let  $A$  be a commutative ring, and let  $B \subset A$  be a subring for which the abelian group  $A/B$  is finite.

(a) Prove that there is an ideal  $I$  of  $A$  with  $I \subset B$  for which  $A/I$  is finite.

(b) Denote the unit group of a ring  $R$  by  $R^*$ . Prove that one has  $A^* \cap B = B^*$ , and that the abelian group  $A^*/B^*$  is finite.

**Exercise 1.34.** Let  $A$  be a commutative ring, and write  $\sqrt{0} = \{x \in A : x^n = 0 \text{ for some } n \in \mathbf{Z}_{>0}\}$ ; one calls  $\sqrt{0}$  the *radical* or the *nilradical* of  $A$ .

Prove that  $\sqrt{0}$  is an ideal of  $A$ , that one has  $1 + \sqrt{0} \subset A^*$ , and that there is an exact sequence

$$1 \rightarrow 1 + \sqrt{0} \rightarrow A^* \rightarrow (A/\sqrt{0})^* \rightarrow 1$$

of abelian groups.

**Exercise 1.35.** For an abelian group  $F$ , we define the *torsion subgroup*  $F_{\text{tor}}$  of  $F$  to be the subgroup of elements of finite order of  $F$ , and if  $F$  is finitely generated we define the *rank*  $\text{rank } F$  of  $F$  to be the unique integer  $n$  for which  $F/F_{\text{tor}}$  is isomorphic to  $\mathbf{Z}^n$  as an abelian group.

Let  $A$  and  $\sqrt{0}$  be as in Exercise 1.34, and suppose that  $\sqrt{0}$  is finitely generated as an abelian group. Prove that the multiplicative group  $1 + \sqrt{0}$  is also finitely generated, and that the abelian groups  $\sqrt{0}$  and  $1 + \sqrt{0}$  have the same rank. Can you find an example in which  $\sqrt{0}$  and  $1 + \sqrt{0}$  are non-isomorphic as abelian groups?

**Exercise 1.36.** (This exercise counts for two. You may use Dirichlet's unit theorem (see 5.13) in your solution. You may also use general results from commutative algebra, including properties of tensor products; but do mention which results you use.)

Let  $A$  be a commutative ring such that the additive group  $A^+$  of  $A$  is finitely generated and torsion free (i. e.,  $A_{\text{tor}}^+ = \{0\}$ ). Prove that  $A^*$  is a finitely generated abelian group, and that one has

$$\text{rank}(A^*) = \# \text{Spec}(A_{\mathbf{R}}) - \# \text{Spec}(A_{\mathbf{Q}}) + \text{rank}\sqrt{0},$$

where  $A_{\mathbf{Q}}$  and  $A_{\mathbf{R}}$  denote the rings  $A \otimes_{\mathbf{Z}} \mathbf{Q}$  and  $A \otimes_{\mathbf{Z}} \mathbf{R}$ , respectively, and the *spectrum*  $\text{Spec } R$  of a commutative ring  $R$  is defined to be the set of prime ideals of  $R$ .

**Exercise 1.37.** Can you do Exercise 1.36 without the condition that  $A^+$  be torsion free? (Again, state the results from commutative algebra that you use.)

**Exercise 1.38.** Let  $\mathcal{P}$  denote the set of prime numbers. Prove there is a bijection

$$\begin{array}{ccc} \{\text{subrings of } \mathbf{Q}\} & \longrightarrow & \{\text{subsets of } \mathcal{P}\} \\ R & \longmapsto & R^* \cap \mathcal{P}. \end{array}$$

**Exercise 1.39.** Let  $K$  be an algebraic extension of  $\mathbf{Q}$  and  $R$  be a subring of  $K$ .

(a) Show that if  $I$  is a nonzero ideal of  $R$ , then  $I \cap \mathbf{Z}$  is a nonzero ideal of  $\mathbf{Z}$ .

(b) Suppose that  $K$  is the field of fractions of  $R$ , so that every element of  $K$  can be written as  $a/b$  with  $a, b \in R$ ,  $b \neq 0$ . Show that actually every element of  $K$  can be written as  $a/b$  with  $a \in R$ ,  $b \in \mathbf{Z} \setminus \{0\}$ .

**Exercise 1.40.** Let  $K$  be an algebraic number field such that  $K \neq \mathbf{Q}$ . Show that  $K$  contains infinitely many orders (i. e., subrings that are finitely generated as additive groups and that have  $K$  as field of fractions).

## 2 – Ideal arithmetic

**Exercise 2.57.** Recall that the set  $\text{Hom}_R(M, N)$  of all  $R$ -linear homomorphisms between two modules  $M, N$  over a commutative ring  $R$  is naturally endowed with the structure of an  $R$ -module. When  $M = N$ , the multiplication  $(f, g) \mapsto f \circ g$  turns the set  $\text{Hom}_R(M, M)$  of endomorphisms of  $M$  into a (non-necessarily commutative) ring, denoted  $\text{End}_R(M)$ . Let  $R$  be a domain and  $I, J$  two fractional ideals of  $R$ .

(a) Show that the quotient  $I : J$  and  $\text{Hom}_R(J, I)$  are isomorphic as  $R$ -modules.

(b) Show that  $I : I$  and  $\text{End}_R(I)$  are isomorphic as rings.

**Exercise 2.58.** For a number ring  $R$ , we denote by  $\mathcal{F}(R)$  the set of fractional  $R$ -ideals.

Let  $R$  be a number ring, and let  $S$  be the set of non-zero prime ideals of  $R$ . Write  $\bigoplus_{\mathfrak{p} \in S} \mathcal{F}(R_{\mathfrak{p}})$  for the set of sequences  $(J_{\mathfrak{p}})_{\mathfrak{p} \in S}$  with  $J_{\mathfrak{p}} \in \mathcal{F}(R_{\mathfrak{p}})$  for all  $\mathfrak{p} \in S$  and  $J_{\mathfrak{p}} = R_{\mathfrak{p}}$  for all but finitely many  $\mathfrak{p} \in S$ .

(a) Prove: the maps  $\mathcal{F}(R) \rightarrow \bigoplus_{\mathfrak{p} \in S} \mathcal{F}(R_{\mathfrak{p}})$  and  $\bigoplus_{\mathfrak{p} \in S} \mathcal{F}(R_{\mathfrak{p}}) \rightarrow \mathcal{F}(R)$  sending  $I$  to  $(I_{\mathfrak{p}})_{\mathfrak{p} \in S}$  (with  $I_{\mathfrak{p}}$  denoting the localization of  $I$  at  $\mathfrak{p}$ ) and  $(J_{\mathfrak{p}})_{\mathfrak{p} \in S}$  to  $\bigcap_{\mathfrak{p} \in S} J_{\mathfrak{p}}$ , respectively, are well-defined and bijective, and they are each other's two-sided inverse.

(b) The maps in (a) preserve inclusion, sum, product, intersection, quotient, and invertibility of ideals. Make these statements precise, and prove them.

(c) For  $I \in \mathcal{F}(R)$  and  $a$  in the field of fractions of  $R$ , prove that one has  $I = Ra$  if and only if for all  $\mathfrak{p} \in S$  one has  $I_{\mathfrak{p}} = R_{\mathfrak{p}}a$ . Is it also true that an element  $I \in \mathcal{F}(R)$  is principal if and only if each  $I_{\mathfrak{p}}$  is principal? Give a proof or a counterexample.

**Exercise 2.59.** Let  $R$  be a number ring with field of fractions  $K$ , and let  $I$  be an  $R$ -submodule of  $K$ . For any prime ideal  $\mathfrak{p}$  of  $R$ , we write  $I_{\mathfrak{p}}$  for the  $R_{\mathfrak{p}}$ -module  $\{a/s : a \in I, s \in R, s \notin \mathfrak{p}\}$ .

Suppose that each  $I_{\mathfrak{p}}$  is finitely generated as an  $R_{\mathfrak{p}}$ -module. Does it follow that  $I$  is finitely generated as an  $R$ -module? Give a proof or a counterexample.

**Exercise 2.60.** Let  $R$  be a noetherian domain of Krull dimension 1, and let  $I$  be a non-zero ideal of  $R$ . Prove that the  $R$ -module  $R/I$  has finite length. (If you do not know what *length* means, check it in the literature, e. g. in Atiyah-Macdonald.)

*Note.* All algebraic results in §2 about number rings, including Exercise 2.58, extend with very little change to general noetherian one-dimensional domains, the present exercise playing the role of Theorem 2.11.

**Exercise 2.61.** Let  $R$  be a noetherian one-dimensional domain, and denote by  $K$  its field of fractions.

(a) Let  $V$  be a finite dimensional  $K$ -vector space,  $I$  a non-zero ideal of  $R$ , and  $M$  an  $R$ -submodule of  $V$ . Prove: the length of  $M/IM$  as an  $R$ -module is finite. (*Hint.* First do the case  $M$  is finitely generated and  $I$  is principal.)

(b) Let  $L$  be a finite field extension of  $K$ , and let  $A \subset L$  be a subring containing  $R$ . Prove:  $A$  is a noetherian domain of Krull dimension 0 or 1.

**Exercise 2.62.** Let  $\mathcal{N} : \mathcal{F}(R) \rightarrow \mathbf{Q}_{>0}$  denote the counting norm of a number ring  $R$ .

(a) \* Show by providing an example that the condition  $\mathcal{N}(I^2) = \mathcal{N}(I)^2$  does not imply that the fractional ideal  $I$  is invertible.

(b) \*\* Can you find an example where  $\mathcal{N}(I^2) < \mathcal{N}(I)^2$  ?

**Exercise 2.63.** Recall that a fractional ideal  $I$  in a domain  $R$  is said to be *proper* if  $r(I) = R$ . This problem illustrates that proper ideals need not be invertible.

Let  $f \in \mathbf{Z}[x]$  be a monic irreducible polynomial of degree 3, and consider the number ring  $A = \mathbf{Z}[\alpha]$ , where  $\alpha$  is a root of  $f$ .

- (a) For  $p$  a prime number, show that  $R = \mathbf{Z} + pA$  is a subring of  $A$ .
- (b) Let  $I = R + R\alpha$ . Prove that  $I$  is a proper fractional ideal of  $R$ .
- (c) Show that  $r(I^2) = A$ , and use this to deduce that  $I$  is not invertible.

### 3 – Explicit ideal factorization

**Exercise 3.32.** Let  $\alpha$  be a root of the irreducible polynomial  $X^4 - X - 1 \in \mathbf{Q}[X]$ . Compute (by hand!) the minimal polynomial  $f_{\mathbf{Q}}^{\beta}$  of  $\beta = \alpha^3 - \alpha + 1$ .

**Exercise 3.33.** Let  $R$  be a domain with field of fractions  $K$ . Show that the set  $\mathcal{S}$  of monic polynomials with coefficients in  $R$  is a multiplicative subset of  $R[X]$ , and that we have

$$(\mathcal{S}^{-1}R[X]) \cap K[X] = R[X].$$

Use this to prove that the cyclotomic polynomial  $\Phi_n(X)$  has integer coefficients.

**Exercise 3.34.** Let  $p$  be a prime number and  $F$  a field of characteristic  $p$ .

- (a) Show directly, without using the binomial formula, that the identity

$$X^p - 1 = (X - 1)^p$$

holds in  $F[X]$ . [*Hint:* Show that if  $X^p - 1$  has a non-trivial root in an algebraic closure  $\overline{F}$  of  $F$ , then its  $p$  roots are distinct.]

- (b) Show that the identity

$$X^p + Y^p = (X + Y)^p$$

holds in  $\mathbf{F}_p[X, Y]$ . [*Hint:* Apply the first part to a suitably chosen field  $F$ .]

(c) Conclude that for any commutative ring  $R$  of characteristic  $p$ , the Frobenius map  $x \mapsto x^p$  is a ring homomorphism.

**Exercise 3.35.** If  $n$  is a positive integer which is not a prime power, show that  $\zeta_n - 1$  is a unit in  $\mathbf{Z}[\zeta_n]$ .

**Exercise 3.36.** Let  $p$  be a prime number and  $m$  a positive integer which is not divisible by  $p$ . Show that, for every  $k \geq 0$ ,

$$\Phi_{p^k m}(X) \equiv \Phi_m(X)^{\varphi(p^k)} \pmod{p}.$$

**Exercise 3.37.** (a) Suppose that  $p$  is a prime number such that  $2^p - 1$  is prime (the latter is then called a *Mersenne prime*). Show that  $(2 - \zeta_p)$  is a prime ideal of  $\mathbf{Z}[\zeta_p]$ .

(b) Suppose that  $k$  is an integer such that  $2^{2^k} + 1$  is prime (a *Fermat prime*). Show that  $(2 - \zeta_{2^{k+1}})$  is a prime ideal of  $\mathbf{Z}[\zeta_{2^{k+1}}]$ .

**Exercise 3.38.** Show that the reduction modulo 3 of the cyclotomic polynomial  $\Phi_{13}$  factors as the product of all the monic cubic irreducible polynomials  $f \in \mathbf{F}_3[X]$  such that  $f(0) = -1$ . How many such polynomials are there?

**Exercise 3.39.** Compute the prime decomposition of  $(p)$  in  $\mathbf{Z}[\zeta_{12}]$  for all primes  $p < 30$ . What is the prime factorization of  $(4370)$ ?

**Exercise 3.40.** Prove that for every integer  $n > 1$  there are infinitely many pairwise non-isomorphic number fields  $K$  of degree  $n$  for which the ring of integers is of the form  $\mathbf{Z}[\alpha]$ , with  $\alpha \in \mathcal{O}_K$ . [*Hint:* You might want to look at Exercise 4.39(c) first.]

#### 4 – Linear algebra for number rings

**Exercise 4.33.** Prove Swan's formula: for  $a, b, c \in \mathbf{Z}$ ,  $a \neq 0$ , and  $n > 1$ ,

$$\Delta(aX^n + bX + c) = (-1)^{\frac{1}{2}n(n-1)} a^{n-2} (n^n ac^{n-1} + (-1)^{n-1} (n-1)^{n-1} b^n).$$

[Recall that the discriminant of a non-monic polynomial  $f = a \prod (X - \alpha_i)$  is defined as  $\Delta(f) = a^{2n-2} \prod (\alpha_i - \alpha_j)^2$ , so that  $\Delta(f) = (-1)^{\frac{1}{2}n(n-1)} a^{-1} R(f, f')$ .]

**Exercise 4.34.** A *lattice* in a number field  $K$  of degree  $n$  is an additive subgroup of the form  $\mathbf{Z}\omega_1 \oplus \cdots \oplus \mathbf{Z}\omega_n$ , where  $\omega_1, \dots, \omega_n$  is a  $\mathbf{Q}$ -basis for  $K$ . Given any nonzero  $\mathbf{Q}$ -linear map  $t : K \rightarrow \mathbf{Q}$ , we can define the *t-dual* of a lattice  $M$  in  $K$  by

$$M^t = \{x \in K : t(xM) \subset \mathbf{Z}\}.$$

(a) Show that  $M^t$  is a lattice in  $K$  and that we have  $(M^t)^t = M$ .

(b) If  $M_1 \supset M_2$ , show that  $M_2^t \supset M_1^t$  and that  $[M_1 : M_2] = [M_2^t : M_1^t]$ .

(c) For an order  $R$  in  $K$ , show that  $M$  is a fractional  $R$ -ideal if and only if  $M^t$  is, and that we have  $M^t = R^t : M$ .

**Exercise 4.35.** Taking  $t = \text{Tr}_{K/\mathbf{Q}}$  in the previous problem, one recovers the definition of the trace dual  $M^\dagger$  of a lattice  $M$  in  $K$ .

(a) If  $M$  is contained in  $\mathcal{O}_K$ , show that  $M \subset M^\dagger$  and that  $|\Delta(M)| = [M^\dagger : M]$ .

(b)\* Can you give a similar formula in the general case?

**Exercise 4.36.** Let  $R = \mathbf{Z}[\alpha]$  be a number ring with  $\alpha$  integral over  $\mathbf{Z}$  of degree  $n$ . Show that every fractional  $R$ -ideal  $I$  satisfies  $(I^{-1})^{-1} = I$ . [Hint: Show that  $I^{-1} = I^t$ , where  $t : \mathbf{Q}(\alpha) \rightarrow \mathbf{Q}$  is the linear map  $\sum_{i=0}^{n-1} a_i \alpha^i \mapsto a_{n-1} \cdot$ ]

**Exercise 4.37.** Give an example of an order  $R$  and a fractional  $R$ -ideal  $I$  such that  $(I^{-1})^{-1} \neq I$ .

**Exercise 4.38.** This exercise aims to strengthen Theorem 4.17 by proving that for every prime  $\mathfrak{p}$  of the ring of integers  $\mathcal{O}_K$  of a number field  $K$ , we have

$$\begin{aligned} \text{ord}_{\mathfrak{p}}(\mathfrak{D}_K) &= e(\mathfrak{p}/p) - 1 && \text{when } \mathfrak{p} \text{ is tamely ramified, and} \\ \text{ord}_{\mathfrak{p}}(\mathfrak{D}_K) &\geq e(\mathfrak{p}/p) && \text{when } \mathfrak{p} \text{ is wildly ramified.} \end{aligned}$$

(a) If  $B$  an algebra which is free of finite rank over a commutative ring  $A$ , the *trace radical* of  $B$  over  $A$  is defined by

$$\mathcal{R}(B) = \{x \in B : \text{Tr}_{B/A}(xB) = 0\}.$$

Show that this is an ideal of  $B$ , and that  $\mathcal{R}(B_1 \times B_2) = \mathcal{R}(B_1) \times \mathcal{R}(B_2)$ .

(b) Let  $\mathfrak{p}$  be a prime ideal of  $\mathcal{O}_K$  of ramification index  $e = e(\mathfrak{p}/p)$ , and let  $B$  denote the  $\mathbf{F}_p$ -algebra  $\mathcal{O}_K/\mathfrak{p}^e$ . Using the filtration

$$0 = \mathfrak{p}^e/\mathfrak{p}^e \subset \mathfrak{p}^{e-1}/\mathfrak{p}^e \subset \cdots \subset \mathfrak{p}/\mathfrak{p}^e \subset \mathcal{O}_K/\mathfrak{p}^e = B,$$

show that  $\text{Tr}_{B/\mathbf{F}_p}(x) = e(\mathfrak{p}/p) \text{Tr}_{\overline{B}/\mathbf{F}_p}(\overline{x})$ , where  $\overline{x}$  denotes the image in  $\overline{B} = \mathcal{O}_K/\mathfrak{p}$  of an element  $x \in B$ . Use this to conclude that

$$\mathcal{R}(\mathcal{O}_K/\mathfrak{p}^e) = \begin{cases} \mathcal{O}_K/\mathfrak{p}^e & \text{if } p \mid e, \\ \mathfrak{p}/\mathfrak{p}^e & \text{else.} \end{cases}$$

(c) Prove that the trace radical of  $\mathcal{O}_K/p\mathcal{O}_K$  over  $\mathbf{F}_p$  is  $((p\mathfrak{D}_K^{-1}) \cap \mathcal{O}_K)/p\mathcal{O}_K$ . Deduce that  $(p\mathfrak{D}_K^{-1}) \cap \mathcal{O}_K$  is the product of all the tamely ramified primes of  $\mathcal{O}_K$  dividing  $p$ .

(d) Let  $0 \leq k \leq e(\mathfrak{p}/p)$  be an integer. Show that

$$\mathfrak{p}^k \mid \mathfrak{D}_K \iff (p\mathfrak{D}_K^{-1}) \cap \mathcal{O}_K \mid \mathfrak{p}^{e(\mathfrak{p}/p)-k}.$$

Conclude that  $\mathfrak{p}^{e(\mathfrak{p}/p)-1}$  divides  $\mathfrak{D}_K$ , and that  $\mathfrak{p}^{e(\mathfrak{p}/p)} \mid \mathfrak{D}_K \iff \mathfrak{p}$  is wildly ramified.

**Exercise 4.39.** (a) Prove that for every number field  $K$  there exists a unique positive integer  $d_K$  dividing  $[K : \mathbf{Q}]$  with the property  $d_K \mathbf{Z} = \text{Tr}_{K/\mathbf{Q}} \mathcal{O}_K$ .

(b) With  $K$  and  $d_K$  as in (a), and  $p$  prime, prove:  $p$  divides  $d_K$  if and only if each prime  $\mathfrak{p}$  of  $\mathcal{O}_K$  over  $p$  is wildly ramified. (You may use the result of Exercise 4.38.)

(c) Construct for each positive integer  $n$  a number field  $K$  with  $[K : \mathbf{Q}] = n = d_K$ .

**Exercise 4.40.** For  $A$  a commutative ring and  $n \geq 0$ , write  $A[X]_n$  for the set of polynomials with coefficients in  $A$  and degree strictly less than  $n$ , considered as a free  $A$ -module of rank  $n$  with basis  $\{X^{n-1}, \dots, X, 1\}$ . For  $f = a_m X^m + \dots + a_1 X + a_0$  and  $g = b_n X^n + \dots + b_1 X + b_0$ , the Sylvester matrix  $S_{m,n}(f, g)$  is the square matrix of size  $m+n$  with coefficients in  $A$  defined as the transpose of the matrix representing the  $A$ -linear map

$$A[X]_m \times A[X]_n \longrightarrow A[X]_{m+n}, \quad (h, k) \mapsto hg + kf.$$

Let  $R_{m,n}(f, g) \in A$  denote the determinant of  $S_{m,n}(f, g)$ . Prove the following:

(a)  $R_{n,m}(g, f) = (-1)^{mn} R_{m,n}(f, g)$ .

(b)  $R_{m,n}(af, bg) = a^n b^m R_{m,n}(f, g)$  for  $a, b \in A$ .

(c) If  $d = \deg g \leq n$ , then  $R_{m,n}(f, g) = a_m^{n-d} R_{m,d}(f, g)$ .

(d) There exists  $h \in A[X]_m$  and  $k \in A[X]_n$  such that  $R_{m,n}(f, g) = hg + kf$ . [*Hint:* In  $A[X]$ , there is an obvious solution  $Y_i = X^i$  to the system of equations

$$S_{m,n}(f, g) \cdot (Y_{m+n-1}, \dots, Y_1, Y_0)^t = (X^{m-1}g, \dots, Xg, g, X^{n-1}f, \dots, Xf, f)^t.$$

If  $R_{m,n}(f, g) \neq 0$ , use Cramer's rule to write  $X^0 = 1$  in a creative way.]

(e) Suppose  $A$  is a domain with field of fractions  $K$ . Prove that  $R_{m,n}(f, g) = 0$  if and only if both  $\deg f < m$  and  $\deg g < n$  or if  $f$  and  $g$  have a common factor in  $K[X]$ .

(f) Let  $A_1, \dots, A_m, B_1, \dots, B_n$  be algebraically independent indeterminates and consider the polynomials  $f = \prod_i (X - A_i)$  and  $g = \prod_j (X - B_j)$  with coefficients in the polynomial ring  $\mathbf{Z}[A_1, \dots, A_m, B_1, \dots, B_n]$ . Prove that

$$R_{m,n}(f, g) = \prod_{i,j} (A_i - B_j).$$

[*Hint:* First show that the right-hand side divides the left one. Comparing degrees, one finds that they differ by a multiplicative constant which can be found by inspection.]

(g) If  $f$  and  $g$  are polynomials of degrees  $m$  and  $n$ , respectively, with coefficients in a field, show that  $R_{m,n}(f, g)$  agrees with the definition of the resultant  $R(f, g)$  given in the notes.

## 5 – The geometry of numbers

**Exercise 5.35.** (a) For  $1 \leq i \leq m$ , let  $V_i$  be a Euclidean space of positive dimension and  $X_i \subset V_i$  a bounded symmetric convex subset. Write  $V = V_1 \times \cdots \times V_m$  and suppose that  $L$  is a complete lattice in  $V$ . Adapt the proof of Minkowski's theorem to show that  $X = X_1 \times \cdots \times X_m$  contains a non-zero lattice point provided

$$\text{vol}(X) \geq 2^{\dim V} \cdot \text{vol}(V/L)$$

and at least one of the  $X_i$  is closed.

(b) Modify slightly the proof of Theorem 5.4 to show that if  $R$  is an order, every ideal class in  $\text{Pic}(R)$  contains an integral ideal  $I$  such that  $N(I) \leq |\Delta(R)|^{1/2}$ , with strict inequality when  $R \neq \mathbf{Z}$ . Deduce from this, without using Theorem 5.8, that

$$|\Delta(R)| = 1 \iff R = \mathbf{Z}.$$

## 8 – Galois theory for number rings

**Exercise 8.12.** Let  $A$  be a commutative ring,  $G \subset \text{Aut } A$  a subgroup of finite order  $n$ , and  $B = \{a \in A : \sigma(a) = a \text{ for all } \sigma \in G\}$ . Let further  $I$  be an ideal of  $B$ , and put  $J = (I \cdot A) \cap B$ .

- (a) Prove:  $J^n \subset I \subset J$ ; here  $J^n$  denotes the ideal product of  $n$  copies of  $J$ .
- (b) Prove: if  $I$  is a prime ideal of  $B$ , then  $J = I$ .
- (c) Give an example where  $J \neq I$ .

**Exercise 8.13.** Let  $A, G, B$  be as in Exercise 8.12, and let  $\mathfrak{p} \subset B$  be a prime ideal. Prove that there is a prime ideal  $\mathfrak{q}$  of  $A$  with  $\mathfrak{q} \cap B = \mathfrak{p}$ . [*Hint 1:* Start from Exercise 8.12(b). *Hint 2:* Check the “going up”-theorem in the literature.]

**Exercise 8.14.** Let  $A, G, B$  be as in Exercise 8.12, let  $\mathfrak{q}$  be a prime ideal of  $A$ , and put  $\mathfrak{p} = \mathfrak{q} \cap B$ . Write  $G_{\mathfrak{q}}$  and  $I_{\mathfrak{q}}$  for the decomposition group and the inertia group of  $\mathfrak{q}$ ; so  $G_{\mathfrak{q}} = \{\sigma \in G : \sigma\mathfrak{q} = \mathfrak{q}\}$  and  $I_{\mathfrak{q}} = \{\sigma \in G_{\mathfrak{q}} : \sigma a \equiv a \pmod{\mathfrak{q}} \text{ for all } a \in A\}$ .

Prove that the index of  $I_{\mathfrak{q}}$  in  $G_{\mathfrak{q}}$  equals the separability degree of the field of fractions of  $A/\mathfrak{q}$  over the field of fractions of  $B/\mathfrak{p}$ .

**Exercise 8.15.** Let  $K \subset L$  be an Galois extension of number fields, and assume that its Galois group  $G$  is abelian. Let  $\mathfrak{p} \subset \mathcal{O}_K$  be a prime ideal, and put  $\mathcal{N}(\mathfrak{p}) = \#(\mathcal{O}_K/\mathfrak{p})$ . Prove that  $\mathfrak{p}$  is unramified in  $L$  if and only if there is an element  $\sigma \in G$  such that for all  $a \in \mathcal{O}_L$  one has  $\sigma(a) \equiv a^{\mathcal{N}(\mathfrak{p})} \pmod{\mathfrak{p} \cdot \mathcal{O}_L}$ ; prove also that if such an element  $\sigma$  exists, it is unique.