Math 311 – Algebraic number theory – Practice problemd

Instructor: Matthew Greenberg

December 11, 2016

1. Let A be an abelian group. Define the *rank of A* to be
$$\sup\{|X| : X \subseteq A \text{ is } \mathbb{Z}\text{-linearly independent}\}.$$
   (a) Define what it means for an abelian group to be:
      - free,
      - finitely generated,
      - torsion-free.

   (b) State the structure theorem for finitely-generated abelian groups. Use it to prove that an abelian group is free of rank $r < \infty$ if and only if $A \approx \mathbb{Z}^n$.

   (c) State the *elementary divisors theorem.* Use it to prove that if A and B are abelian groups such that if B is free of rank $n < \infty$ and $A \subseteq B$, then A is free of rank $m \leq n$ with equality if and only if B/A is finite. Further, show that if $m = n$ then $[B : A]$ is the product of the elementary divisors of A with respect to B.

2. Let K be a number field of degree n with ring of integers $\mathcal{O}_K$.
   (a) Prove that $\mathcal{O}_K$ is a free abelian group of rank at most n.
$$\operatorname{rank} \mathcal{O}_K \leq \dim K.$$
   (Hint: Explain why (i) $\mathcal{O}_K$ is torsion-free and (ii) a set of $> n$ elements of K are $\mathbb{Z}$-linearly dependent.)

   (b) Let $a \in K$. Prove that there is an integer $n > 0$ such that $na \in \mathcal{O}_K$.

   (c) Prove that $\mathcal{O}_K$ contains a $\mathbb{Q}$-basis of K. (Use the preceding exercise.) Deduce that
$$\operatorname{rank} \mathcal{O}_K \geq n.$$

3. Let V be an n-dimensional $\mathbb{Q}$-vector space and let L be an abelian subgroup of V.
   (a) Prove that if L is free of rank $\leq n$ if and only if L is finitely generated. (Use the structure theorem for finitely generated abelian groups.)

   (b) Prove that a subset X of V is $\mathbb{Q}$-linearly independent if and only if it is $\mathbb{Z}$-linearly independent.

   (c) Prove that
$$\sup\{|X| : X \text{ is a linearly independent subset of } L\} \leq n.$$
   (We are *not* assuming L is finitely generated.)

   (d) Give an example of an abelian subgroup of V that is not finitely generated.

4. Let V be an F-vector space and let
$$B : V \times V \longrightarrow F$$
   be an F-bilinear form.

(a) Prove that the following conditions are equivalent:

1. $B(x, V) = 0$ if and only if $x = 0$.
2. The *duality map*
$$\delta : V \longrightarrow V^* := \mathrm{Hom}_F(V, F)$$
defined by
$$\delta(x)(y) = B(x, y)$$
is injective.

If B satisfies these conditions, it is called *nondegenerate*.

(b) Suppose B is nondegenerate and V is finite-dimensional. Prove that δ is an isomorphism. (Hint: What is the dimension of V^*?)

(c) Suppose that B is nondegenerate and $\mathbf{v} = (v_1, \ldots, v_n)$ is an F-basis of V. Prove that there are is a unique B-*dual basis* $\mathbf{v}^B = (v_1^B, \ldots, v_n^B)$ of V such that
$$B(v_i, w_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$
(Hint: Since $\mathbf{v}$ is an F-basis of V, there are unique F-linear functionals
$$\ell_j : V \longrightarrow F$$
such that
$$\ell_j(v_i) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$
Now use the injectivity of δ.)

(d) Suppose that $\dim V = n$, that B is nondegenerate and that $\mathbf{v}$ is an F-basis of V. Let $[B]_{\mathbf{v}} \in F^{n \times n}$ be the matrix whose (i, j)-component is $B(v_i, v_j)$. Show that
$$B(x, y) = [x]_{\mathbf{v}}^t [B]_{\mathbf{v}} [y_{\mathbf{v}}],$$
where $[x]_{\mathbf{v}}, [y]_{\mathbf{v}} \in F^{n \times 1}$ are the coordinate vectors of x and y with respect to $\mathbf{v}$, respectively.

(e) Suppose that $\dim V = n$, that B is nondegenerate, and that $\mathbf{v}$ and $\mathbf{v}'$ are F-bases of V. Let $A \in F^{n \times n}$ be the matrix mapping the $\mathbf{v}$-coordinates of $x \in V$ to its $\mathbf{v}'$ -coordinates:
$$A[x]_{\mathbf{v}} = [x]'_{\mathbf{v}}.$$
Prove that
$$A^t [B]_{\mathbf{v}'} A = [B]_{\mathbf{v}}.$$

(f) Set
$$\operatorname{disc} \mathbf{v} = \det [B]_{\mathbf{v}},$$
Prove that
$$\operatorname{disc} \mathbf{v} \equiv \operatorname{disc} \mathbf{v}' \pmod{F^{\times 2}},$$
where $\mathbf{v}'$ is another F-basis of V and $F^{\times 2} = \{x^2 : x \in F^{\times}\}$. (Hint: Use the preceding exercise and properties of the determinant.)

The *discriminant of* B, denoted $\operatorname{disc} B$, is defined to be the image of $\operatorname{disc} \mathbf{v}$ in $F^{\times}/F^{\times 2}$. By the above,
$$\operatorname{disc} B \in F^{\times}/F^{\times 2}$$
does not depend on our choice of $\mathbf{v}$.

5. Suppose that V is an n-dimensional $\mathbb{Q}$-vector space equipped with a nondegenerate, symmetric, $\mathbb{Q}$-bilinear form

$$B : V \times V \longrightarrow \mathbb{Q}$$

Let L be an abelian subgroup of V.

(a) Suppose that $\mathbf{v} = (v_1, \dots, v_n)$ and $\mathbf{v}' = (v'_1, \dots, v'_n)$ are $\mathbb{Z}$-bases of L. Prove that

$$\operatorname{disc} \mathbf{v} = \operatorname{disc} \mathbf{v}'.$$

Define $\operatorname{disc}(L, B)$ to be this common value.

(b) Suppose that M is an abelian subgroup of V with $L \subseteq M$. Show that M is B-integral and that

$$\operatorname{disc}(M, B) = [L : M]^2 \operatorname{disc}(L, B).$$

(Hint: Use the elementary divisors theorem.) Conclude that if $\operatorname{disc}(L, B)$ is squarefree then L is a maximal B-integral subgroup of V.

(c) Define the *T-dual subgroup*

$$L^T = \{x \in V : T(x, L) \subseteq \mathbb{Z}\}.$$

Prove that $L_1 \subseteq L_2$ implies $L_2^T \subseteq L_1^T$.

(d) Suppose that $\mathbf{v} = (v_1, \dots, v_n)$ is a basis of L. Prove that $\mathbf{v}^T = (v_1^T, \dots, v_n^T)$ is a basis of L^T.

(e) Prove that

$$|\operatorname{disc}(L, B)| = [L^T : L].$$

6. (a) Define the *trace map*

$$t : K \longrightarrow \mathbb{Q}.$$

(b) Prove that t is $\mathbb{Q}$-linear.

(c) Define the *trace form*

$$T : K \times K \longrightarrow \mathbb{Q}.$$

(d) Prove that T is $\mathbb{Q}$-bilinear. (Use the fact that t is $\mathbb{Q}$-linear.)

(e) We proved in class that T is nondegenerate. Remind yourself why this is.

(f) Prove that $\mathcal{O}_K \subset \mathcal{O}_K^T$, i.e., that

$$T(\mathcal{O}_K, \mathcal{O}_K) \subseteq \mathbb{Z}.$$

(g) Let L be a subgroup of $\mathcal{O}_K$. Prove that $\mathcal{O}_K^T \subseteq L^T \subset$.

(h) Let $\mathbf{v} = (v_1, \dots, v_n)$ be a basis of K with $v_i \in \mathcal{O}_K$ (such a basis exists by a previous exercise) and let

$$L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n.$$

Then L^T free abelian group of rank n containing $\mathcal{O}_K$. (Why?) Deduce that $\operatorname{rank} \mathcal{O}_K \leq n$. Combine this with the result of a previous exercise to deduce that $\operatorname{rank} \mathcal{O}_K = n$.

(i) Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Prove that $\mathfrak{a}$ contains a positive integer n. It follows that $n\mathcal{O}_K \subseteq \mathfrak{a}$. Deduce that $\operatorname{rank} \mathfrak{a} = n$.

(j) Let $\mathbf{v} = (v_1, \dots, v_n)$ be an integral basis of K, i.e., $\mathbb{Z}$-basis of $\mathcal{O}_K$. Define the *discriminant d_K of K* by

$$d_K = \operatorname{disc}(\mathcal{O}_K, T).$$

Explain why d_K is well-defined, i.e., is independent of our choice of basis.

(k) Let $\mathcal{O}$ is a subring of $K \cap \bar{\mathbb{Z}}$ with $\operatorname{rank} \mathcal{O} = n$. Suppose that $\operatorname{disc}(\mathcal{O}, T)$ is squarefree. Show that $\mathcal{O} = \mathcal{O}_K$ and that $d_K = \operatorname{disc}(\mathcal{O}, T)$.

(l) Let $\mathcal{O}$ be a subring of $K \cap \bar{\mathbb{Z}}$ with $\operatorname{rank} \mathcal{O} = n$. Suppose that $\operatorname{disc}(\mathcal{O}, T) = p^2$, where p is a prime number. Show that $\mathcal{O} = \mathcal{O}_K$ and that $d_K = \operatorname{disc}(\mathcal{O}, T)$.

7. Let a be a root of $f(x)$ and let $K = \mathbb{Q}(a)$. Compute:

- $\operatorname{disc}(1, a, \ldots, a^{\deg f - 1})$
- $r_1(K)$, $r_2(K)$, $\operatorname{rank} \mathcal{O}_K^\times$

In the cases where $\operatorname{rank} \mathcal{O}_K^\times \geq 1$, can you write down any units of infinite order? How about a linearly independent subset of $\mathcal{O}_K^\times$ of maximal rank?)

(a) $f(x) = x^2 - m$

(b) $f(x) = x^2 - x + \dfrac{1-m}{4}$, $\quad m \in \mathbb{Z}$, $m \equiv 1 \pmod 4$.

(c) $f(x) = x^3 + x^2 - 1$

(d) $f(x) = x^3 + x^2 - 2x - 1$

(e) $f(x) =$ minimal polynomial of $\zeta_7 + \zeta_7^{-1}$, where $\zeta_7 = e^{2\pi i/7}$

(f) $f(x) =$ minimal polynomial of $\dfrac{1}{\sqrt{2}}(1 + \sqrt{-1})$

(g) $f(x) =$ minimal polynomial of $\sqrt{5} + \sqrt{-1}$

8. Let $K = \mathbb{Q}(\sqrt{-5})$.

(a) Prove that 2 ramifies in K.

(b) Let $\mathfrak{p}_2$ be the unique (prime) ideal of $\mathcal{O}_K$ such that $\mathfrak{p}^2 = 2\mathcal{O}_K$. Prove that $\mathfrak{p}_2$ is not a principal ideal. Deduce that the class number of K is at least 2.

(c) By computing the Minkowski bound for K, show that K has class number 2.

(d) Prove that $\mathfrak{p}_2 = (2, 1 + \sqrt{-5})$. (Hint: It suffices to show (why?) that $(2, 1 + \sqrt{-5})^2 = 2\mathcal{O}_K$.)

(e) Prove that 3 splits in $\mathcal{O}_K$; write $3\mathcal{O}_K = \mathfrak{p}_3\bar{\mathfrak{p}}_3$. Show that $\mathfrak{p}_3$ and $\bar{\mathfrak{p}}_3$ is not principal.

(f) Explain why $\mathfrak{p}_2\mathfrak{p}_3$ and $\mathfrak{p}_2\bar{\mathfrak{p}}_3$ are a principal ideals. Identify generators. (You don't need to a presentation of $\mathfrak{p}_3$ to do this.)

9. Let $f(x) = x^3 - ax^2 - (a+3)x - 1$.

(a) Prove that $f(x)$ is irreducible.

(b) Let $\rho = \rho_1$ be a root of $f(x)$ and let $K = \mathbb{Q}(\rho)$. Verify that

$$\rho_2 := \frac{-1}{1+\rho_1} \quad \text{and} \quad \rho_3 := \frac{-1}{1+\rho_3}$$

are the other roots of $f(x)$:

$$f(x) = (x - \rho_1)(x - \rho_2)(x - \rho_2).$$

Deduce that K is totally real:

$$r_1(K) = 3.$$

(c) Show that the ρ_j are units:

$$\rho_j \in \mathcal{O}_K^\times, \quad j = 1, 2, 3.$$

(d) Prove that

$$\operatorname{disc}(1, \rho, \rho^2) = (a^2 + 3a + 9)^2.$$

(e) Suppose

$$p := a^2 + 3a + 9$$

is prime. For example, $a = -1$, 1, and 2 give $p = 7$, 13, and 19, respectively. Prove that $\mathcal{O}_K = \mathbb{Z}[\rho]$.

(f) (**) Show that $p \equiv 1 \pmod 3$, making $\frac{p-1}{3}$ an integer. Let $q \neq p$ be another prime. Prove that

$$q^{\frac{p-1}{3}} \equiv \begin{cases} 1 & \text{if } q \text{ splits of } K, \\ -1 & \text{if } q \text{ is inert in } K. \end{cases} \pmod p.$$

In other words, $q \neq p$ splits in K if and only if q is a cube modulo p.

10. Let K be a Galois number fields. Let $p \in \mathbb{Z}$ be a prime and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ such that $\mathfrak{p} \mid p$. Assume that p is unramified in K.

    (a) Define the *decomposition group* $D_{\mathfrak{p}|p}$.

    (b) Define the *Frobenius automorphism* $\mathrm{Fr}_{\mathfrak{p}|p} \in D_{\mathfrak{p}|p}$.

    (c) Let K be a quadratic field and let d_K be its discriminant. Let p be a prime with $p \nmid d_K$. Identify the image of $\mathrm{Fr}_{\mathfrak{p}|p}$ under the natural (unique) map

    $$\mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \{\pm 1\}.$$

    You don't need to justify your answer for this part.

11. Let K and L be a Galois number fields with $K \subset L$. Let $p \in \mathbb{Z}$ be a prime and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ such that $\mathfrak{p} \mid p$, and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ such that $\mathfrak{P} \mid \mathfrak{p}$. Assume that p is unramified in L and, hence, in K.

    Show that the natural map

    $$\mathrm{Gal}(L/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$$

    maps $D_{\mathfrak{P}|p}$ into $D_{\mathfrak{p}|p}$ and $\mathrm{Fr}_{\mathfrak{P}|p}$ onto $\mathrm{Fr}_{\mathfrak{p}|p}$.

12. Let

    $$K = \mathbb{Q}(\sqrt{5}, \sqrt{-1}).$$

    (a) For a prime $p \in \mathbb{Z}$, define e, f, and g by

    $$p\mathcal{O}_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e, \quad f = [k(\mathfrak{P}_i)/k(p)].$$

    Here, $k(\mathfrak{P}_i)$ and $k(p)$ are the residue class fields of $\mathfrak{P}_i$ and p, respectively.

    Enumerate all possible triples (e, f, g). For each triple (e, f, g), provide a corresponding p.

    (b) There is a third quadratic subfield of K; find it. Call it E.

    (c) Determine the triples (e', f', g') and (e'', f'', g'') characterized by

    $$\begin{aligned} 2\mathcal{O}_E &= (\mathfrak{p}_1 \cdots \mathfrak{p}_{g'})^{e'} \qquad & f' &= [k(\mathfrak{p}_i)/k(p)], \\ \mathfrak{p}_i\mathcal{O}_K &= (\mathfrak{P}_1 \cdots \mathfrak{P}_{g''})^{e''} \qquad & f'' &= [k(\mathfrak{P}_j)/k(\mathfrak{p}_i)]. \end{aligned}$$