HOMEWORK 14

Due date: Week 15

Exercise 7.1, ($\delta = \sqrt{-5}$ in problem 7.1), 7.3, (in exercise 7.3, R is the integer ring of $\mathbb{Q}(\sqrt{-26})$), Page 410 of Artin's book,

Let F be an algebraic number field and $\mathcal{O}_F$ be its ring of integers. Let $\mathfrak{a} \subset \mathcal{O}_F$ be a nonzero ideal. Recall that $\mathcal{O}_F/\mathfrak{a}$ is finite. We have defined

$$\mathrm{Nm}(\mathfrak{a}) = |\mathcal{O}_F/\mathfrak{a}|,$$

which is a positive integer.

Problem 1. (1) *For $a \in \mathbb{Z}$, show that $\mathrm{Nm}(a\mathcal{O}_F) = |\mathrm{Nm}_{F/\mathbb{Q}}(a)| = a^n$, where $n = [F : \mathbb{Q}]$.*
(2) *Show that $\mathrm{Nm}(\alpha\mathcal{O}_F) = |\mathrm{Nm}_{F/\mathbb{Q}}(\alpha)|$ for any $\alpha \in \mathcal{O}_F$.*

The first one is proved in class. The second one follows from the structure theorem of finitely generated abelian group, see Exercise 4.6 of page 438.

Problem 2. *Let $\mathfrak{a}, \mathfrak{b}$ be two nonzero ideals. Show that $\mathrm{Nm}(\mathfrak{ab}) = \mathrm{Nm}(\mathfrak{a})\mathrm{Nm}(\mathfrak{b})$.*

Problem 3. *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_F$. Show that $\mathrm{Nm}(\mathfrak{p}) = p^f$ for some prime integer $p \in \mathbb{Z}$ and some positive integer f.*

Problem 4 $(*)$**.** *Let F be an algebraic number field and $\mathcal{O}_F$ be its ring of integers. From Hurwitz lemma, there exists an integer $M = M_F$ such that for any $\alpha, \beta \in \mathcal{O}_F$ with $\beta \neq 0$, there exists an integer t with $1 \leq t \leq M$ and an element $\omega \in \mathcal{O}_F$ such that*

$$|\mathrm{Nm}_{F/\mathbb{Q}}(t\alpha - \omega\beta)| < |\mathrm{Nm}_{F/\mathbb{Q}}(\beta)|.$$

Re-examine the proof given in class and try to find an explicit form of M_F. For the field $F = \mathbb{Q}(\sqrt{-13})$, find an explicit $M = M_F$. The constant M should be as small as possible.

We know that $M_F > 1$ since $\mathcal{O}_F$ is not a PID when $F = \mathbb{Q}(\sqrt{-13})$. Is $M = 2$ enough? If so, prove it. If not, find one counter example and try the next one.

Problem 5. *Let F be an algebraic number field. Show that $\mathcal{O}_F$ is a PID iff for every $\alpha \in F, \alpha \notin \mathcal{O}_F$, there exists $\beta, \gamma \in \mathcal{O}_F$ such that*

$$0 < |\mathrm{Nm}_{F/\mathbb{Q}}(\alpha\beta - \gamma)| < 1.$$

This is Dedekind-Hasse property of PID. The proof is easy.

Problem 6. *Let K be an algebraic number field. Show that there exists a finite extension L/K such that for every ideal $\mathfrak{a} \subset \mathcal{O}_K$, the ideal $\mathfrak{a}\mathcal{O}_L$ is principal in $\mathcal{O}_L$.*

Hint: use finiteness of class numbers. See this link for a solution.

Given a matrix $A = (a_{i,j}) \in \mathrm{Mat}_{n\times n}(\mathbb{C})$, recall that the Hilbert-Schimidt norm is defined to be

$$||A||_{HS} = \sqrt{\sum_{i,j} |a_{ij}|^2}.$$

Problem 7. *Show that*

$$||A + B||_{HS} \leq ||A||_{HS} + ||B||_{HS}$$

for all $A, B \in \mathrm{Mat}_{n\times n}(\mathbb{C})$.

1. Integer rings in algebraic number fields

We have defined two discriminant now. Recall that, if $f \in F[x]$ we have defined

$$\operatorname{disc}(f) = \prod_{1 \le i < j \le n} (\beta_i - \beta_j)^2,$$

where $\{\beta_1, \dots, \beta_n\}$ is the set of all roots of f in an algebraic closure.

Let E/F be a field extension and let $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ be an ordered basis of E/F, we have defined

$$\Delta(\mathcal{B}) = \Delta(\alpha_1, \dots, \alpha_n) = \det[\psi]_{\mathcal{B}},$$

where $\psi : E \times E \to F$ is the bilinear form $\psi(\alpha, \beta) = \operatorname{tr}_{E/F}(\alpha\beta)$, and $[\psi]_{\mathcal{B}}$ is the matrix of the bilinear form with respect to $\mathcal{B}$. More precisely,

$$[\psi]_{\mathcal{B}} = \begin{bmatrix} \psi(\alpha_1, \alpha_1) & \psi(\alpha_2, \alpha_1) & \dots & \psi(\alpha_n, \alpha_1) \\ \dots & \dots & \dots & \dots \\ \psi(\alpha_1, \alpha_n) & \psi(\alpha_2, \alpha_n) & \dots & \psi(\alpha_n, \alpha_n) \end{bmatrix}.$$

A different way to describe the matrix is as follows. Let $[\alpha]_{\mathcal{B}}$ be the coordinate of α with respect to the ordered basis $\mathcal{B}$, then

$$\psi(\alpha, \beta) = [\beta]_{\mathcal{B}}^t [\psi]_{\mathcal{B}} [\alpha]_{\mathcal{B}}.$$

Think about how $[\psi]_{\mathcal{B}}$ changes if we change basis. We learned this in our linear algebra course. Check page 360-363 of Hoffman-Kunze.

Problem 8. *Let $\beta \in \overline{\mathbb{Q}}$ be an algebraic element over $\mathbb{Q}$. Let μ_β be the minimal polynomial of β over $\mathbb{Q}$. Show that*

$$\Delta(1, \beta, \dots, \beta^{n-1}) = \operatorname{disc}(\mu_\beta),$$

where $n = \deg(\mu_\beta)$.

Hint: this follows from a matrix calculation which roughly appeared in previous homework problems and also in linear algebra when we talked about bilinear forms, see HW 10. Let $\sigma_i : \mathbb{Q}[\beta] \to \mathbb{C}$ be the embeddings defined by μ_β (namely, $\sigma_i(\beta)$ is a root of μ_β for each i). Let $\mathcal{B} = \left\{1, \beta, \dots, \beta^{-1}\right\}$ be the basis of $\mathbb{Q}[\beta]/\mathbb{Q}$. Then show that $\det([\psi]_{\mathcal{B}}) = \det(A)^2$, where A is the matrix $(\sigma_i(\beta^j))_{1 \le i,j \le n} = (\beta_i^j)_{1 \le i,j \le n}$, where $\beta_i = \sigma_i(\beta)$, which is a root of μ_β.

Let K be an algebraic number field, i.e., $K/\mathbb{Q}$ is an extension of degree n. Let $\mathcal{O}_K$ be the ring of integers of K. Let $\mathcal{B} = \{\beta_1, \dots, \beta_n\}$ be an integral basis of $\mathcal{O}_K$. Then we know that $\mathcal{O}_K = \mathbb{Z}\beta_1 + \dots + \mathbb{Z}\beta_n$ is a free abelian group of rank n. Moreover, we know that

$$|\Delta(\beta_1, \dots, \beta_n)| \in \mathbb{Z}_{>0}$$

is minimal. Moreover, if $\mathcal{B}$ and $\mathcal{B}'$ are two integral basis, then there exists a matrix $P \in \mathrm{GL}_n(\mathbb{Z})$ such that $\mathcal{B}' = \mathcal{B}P$. Thus

$$[\psi]_{\mathcal{B}'} = P^t [\psi]_B P.$$

Thus $\det([\psi]_{P'}) = \det(P)^2 \det([\psi]_{\mathcal{B}}) = \det([\psi]_{\mathcal{B}})$, since $\det(P) = \pm 1$. Thus the number $\det([\psi]_{\mathcal{B}})$ is thus independent on the choice of the basis $\mathcal{B}$ and we denote it by $\operatorname{disc}(\mathcal{O}_K)$.

Problem 9. *Let K be an algebraic number field and let $\mathcal{O}_K$ be the ring of integers of K. Suppose that $\operatorname{rank}(\mathcal{O}_K) = n$. Let $\mathcal{B}' = \{\alpha_1, \dots, \alpha_n\} \subset \mathcal{O}_K$. Consider the sub abelian group (submodule as an $\mathbb{Z}$ module)*

$$\mathbb{Z}[\mathcal{B}'] = \left\{ \sum a_i \alpha_i : a_i \in \mathbb{Z}, 1 \le i \le n \right\}$$

of $\mathcal{O}_K$. Suppose $\Delta(\alpha_1, \dots, \alpha_n) \neq 0$.

1. *Show that $\mathbb{Z}[\mathcal{B}']$ is also a free abelian group of rank n and $\mathcal{O}_K/\mathbb{Z}[\mathcal{B}']$ is finite.*
2. *Show that*
$$|\Delta(\mathcal{B}')| = \operatorname{disc}(\mathcal{O}_K) |\mathcal{O}_K/\mathbb{Z}[\mathcal{B}']|^2.$$
In particular, $|\Delta(\mathcal{B}')|$ is also an integer.
3. *If $|\Delta(\mathcal{B}')|$ is square free, show that $\mathcal{O}_K = \mathbb{Z}[\mathcal{B}']$, namely, $\mathcal{B}'$ is an integral basis.*

This is an application of the structure theorem of finitely generated abelian group.

Problem 10. *Let $\alpha \in \mathbb{C}$ be a root of $x^3 - x - 1 \in \mathbb{Q}[x]$. Consider the field $F = \mathbb{Q}[\alpha]$. Show that $1, \alpha, \alpha^2$ is an integral basis of $\mathcal{O}_F$, namely, $\mathcal{O}_F = \mathbb{Z}[\alpha] = \left\{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Z}\right\}$. Here $\mathcal{O}_F$ is the ring of integers of F.*

Hint: Compute $\Delta(1, \alpha, \alpha^2)$ and then use the above problem.

Problem 11 $(*)$**.** *Use the same method as the above problem to find an integral basis of the ring of integers of the following algebraic number fields.*

(1) *$F = \mathbb{Q}[\alpha]$, where $\alpha \in \mathbb{C}$ is a root of $x^3 + x + 1$.*
(2) *$F = \mathbb{Q}[\alpha]$, where $\alpha \in \mathbb{C}$ is a root of $x^5 - x - 1$.*

Remark 1.1. If $F = \mathbb{Q}(\alpha)$ with $\mathrm{disc}(\mu_\alpha)$ not square-free, it can be very hard to find an integral basis of $\mathcal{O}_F$. Here is one example. Consider $F = \mathbb{Q}(\alpha)$ with $\mu_\alpha = x^3 + x^2 - 2x + 8$. Then $\mathrm{disc}(\mu_\alpha) = -4 \times 503$. Dedekind showed that $\mathcal{O}_F \neq \mathbb{Z}[\alpha]$. Thus by Problem 9, $[\mathcal{O}_F : \mathbb{Z}[\alpha]] = 2$. In fact, Dedekind showed that there is no integral basis of the form $1, \beta, \beta^2$. In other words, $\mathcal{O}_F \neq \mathbb{Z}[\beta]$ for any β.