

HOMEWORK 14

Due date:

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

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

which is a positive integer.

Problem 1. Suppose $[F : \mathbb{Q}] = n$. For $a \in \mathbb{Z}$, show that $\text{Nm}(a\mathcal{O}_F) = a^n = \text{Nm}_{F/\mathbb{Q}}(a)$.

This is proved in class. Repeat it here.

Problem 2. Let $\mathfrak{a}, \mathfrak{b}$ are two coprime nonzero ideals. Show that $\text{Nm}(\mathfrak{a}\mathfrak{b}) = \text{Nm}(\mathfrak{a})\text{Nm}(\mathfrak{b})$.

This is a consequence of Chinese remainder theorem.

Problem 3. Let \mathfrak{p} be a nonzero prime ideal of \mathcal{O}_F . Show that $\text{Nm}(\mathfrak{p}) = p^f$ 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

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

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

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

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 $A = (a_{i,j}) \in \text{Mat}_{n \times n}(\mathbb{C})$, recall that the Hilbert-Schmidt 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 $A, B \in \text{Mat}_{n \times n}(\mathbb{C})$.

1. A THEOREM OF DEDEKIND ON GALOIS GROUPS

Let $\psi_p : \mathbb{Z}[x] \rightarrow \mathbb{F}_p[x]$ be the mod p map for a prime p .

Theorem 1.1 (Dedekind). *Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial with degree $n \geq 1$. Let p be a prime such that*

$$\psi_p(f) = g_1 \cdots g_k$$

*with $g_1, \dots, g_k \in \mathbb{F}_p[x]$ irreducible and **distinct**. Assume $\deg(g_i) = n_i$ so that $n = n_1 + \cdots + n_k$. Then G_f (as a subgroup of S_n) contains an element with cycle length n_1, n_2, \dots, n_k . In other words, G_f contains an element of the form*

$$(i_1 i_2 \dots i_{n_1})(i_{n_1+1} \dots i_{n_1+n_2}) \cdots$$

The proof of this theorem is not easy. We assume it in the following. If you want a proof, see page 145 of [this link](#).

The following is one example of how we apply the above theorem.

Problem 8. Consider $f = x^5 - x - 1 \in \mathbb{Z}[x]$.

- (1) Show that $\psi_3(f)$ is irreducible and conclude that f itself is irreducible.
- (2) Show that G_f contains a cycle of order 5.
- (3) Factorize $\psi_2(f)$ and show that G_f contains a transposition using the above Dedekind's theorem.
- (4) Conclude that $G_f \cong S_5$.

For part (3), we cannot get a transposition directly using Dedekind's theorem. But certain power would suffice.

The following is a special case of the above theorem.

Proposition 1.2. *Let α be an algebraic integer such that $K := \mathbb{Q}(\alpha)$ is a Galois extension. Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of α . If there exists a prime integer p such that ψ_p is irreducible, then $\text{Gal}(K/F) = G_f$ is cyclic.*

Note that, the relation between α and K in the above is: α is a primitive element of K . In particular, $[K : \mathbb{Q}] = \deg(f)$.

Problem 9. Show that Theorem 1.1 implies Proposition 1.2.

Problem 10. Consider the polynomial $f = x^4 - 10x^2 + 1$. Show that for any prime p , $\psi_p(f)$ is irreducible. Moreover, $\psi_p(f)$ cannot have a degree 3 irreducible factor.

This is M.4 page 476 of Artin's book.

Problem 11. Consider the polynomial $f = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9 \in \mathbb{Z}[x]$. Show that $\psi_p(f)$ is reducible for any prime p .

Hint: Consider the splitting field of $x^3 - 2$ and the element $\alpha + \omega$, where $\alpha = \sqrt[3]{2}, \omega = e^{2\pi i/3}$. Moreover, try to factorize $\psi_p(f)$ for some small p , like $p = 2, 3, 5, 7$. As a comparison, for example, for the polynomial $g = x^6 + 2x^5 + 6x^4 + 3x^3 + 9x + 9 \in \mathbb{Z}[x]$, $\psi_p(g)$ is indeed irreducible for $p = 23, 73, 79$ as you may check. The reason for it is that a single root of g does not generate the splitting field of g . In fact, $G_g \cong S_6$. Thus $[Spl(g, \mathbb{Q}) : \mathbb{Q}] = 72$, and $Spl(g, \mathbb{Q})$ cannot be generated by a single root of a polynomial of degree 6.

Warning: in Proposition 1.2, the element α is a primitive element is necessary. Otherwise, the conclusion is false. For example, for $f = x^5 - x - 1$ in Problem 8, we know that $\psi_3(f)$ is irreducible. But this does not mean G_f is cyclic because f is not the minimal polynomial of some primitive element of $K = Spl(f, \mathbb{Q})$. Actually, any single root of f won't generate K . This, of course, just means that $[K : \mathbb{Q}] > 5$.