HOMEWORK 13

Due date:
Exercise: M.4, page 511-512 of Artin's book.
Exercise 8.2, page 474 of Artin's book.
Exercise 2.1, 5.1, page 408-409 of Artin's book.

1. Algebraic closure

Problem 1. *Let F be a field and $\overline{F}$, $\overline{F}'$ be two algebraic closure of F. Show that there is an isomorphism $\phi : \overline{F} \to \overline{F}'$ such that $\phi(a) = a, \forall a \in F$.*

Hint: Consider the set $\mathcal{P}$ of all pairs (E, ι), where E is an intermediate field of F and $\overline{F}$, namely, $F \subset E$, and $\iota : E \to \overline{F}'$ is an F-homomorphism. Define a partial order on $\mathcal{P}$ by

$$(E, \iota) \leq (E_1, \iota_1) \text{ if and only if } E \subset E_1 \text{ and } \iota_1|_E = \iota.$$

The set $\mathcal{P}$ is nonempty because it contains $(F, F \hookrightarrow \overline{F}')$. Show $\mathcal{P}$ is contains a maximal element (E, ϕ) using Zorn's lemma. Then show $E = \overline{F}$ and $\phi : E \to \overline{F}'$ is an isomorphism.

Problem 2. *Show that every algebraically closed field is infinite.*

We know that every finite field is of the form $\mathbb{F}_q$ and over $\mathbb{F}_q$ there is a quadratic extension. This means that there is an irreducible quadratic irreducible polynomial $f \in \mathbb{F}_q[x]$. Thus $\mathbb{F}_q$ is not algebraically closed. Try to give a very direct proof of the above problem without using the structures of finite fields.

Let p be a prime integer and $q = p^r$. We consider the finite field $\mathbb{F}_q$ with q elements. Let a, b be two positive integers such that $a|b$. It is known that $\mathbb{F}_{q^a} \subset \mathbb{F}_{q^b}$. In particular, we can consider the following

$$\mathbb{F}_q \subset \mathbb{F}_{q^{2!}} \subset \mathbb{F}_{q^{3!}} \subset \mathbb{F}_{q^{4!}} \subset \cdots \subset \mathbb{F}_{q^{n!}} \subset \ldots.$$

Consider

$$\overline{\mathbb{F}}_q = \cup_{n \geq 1} \mathbb{F}_{q^{n!}}.$$

Problem 3. *Show that $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$.*

2. Primitive element theorem

Theorem 2.1 (Primitive element theorem)**.** *Let E/F be a finite separable extension. There there exists an element $\gamma \in E$ such that $E = F(\gamma)$.*

For a proof of this fact when characteristic of F is zero, see Theorem 15.8.1, page 462 of Artin's book. Such an element γ is called a *primitive element* for the extension E/F. With this theorem, many proofs in Galois theory could be simplified. Try to read Artin's book and see how this theorem is used in the proof of many theorems. We will prove this theorem in the following problems.

Problem 4. *Let F be a finite field and E/F be a finite extension, show that there exists an element γ such that $E = F(\gamma)$.*

This is Exercise 8.1, page 474 of Artin's book. After this problem, to prove Theorem 2.1, it suffices to consider the case when F is infinite.

Problem 5. *Let F be an infinite field and $E = F[\alpha, \beta]$ be a finite extension over F such that β is separable over F. Then there exists an element $\gamma \in E$ such that $E = F(\gamma)$.*

In the above problem, we don't assume that α is separable over F. The proof is essentially the same with the characteristic zero case in Theorem 15.8.1, page 462 of Artin's book. Here are some hints anyway. Consider elements of the form

$$\alpha + c\beta, c \in F.$$

Since F is infinite, there are infinite such elements. Let f (resp. g) be the minimal polynomial of α (resp. β). The assumption says that g has no multiple roots. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s$ and $\beta_1 = \beta, \ldots, \beta_t$ be roots of f and g in an algebraic closure $\overline{F}$. Show that one choose a $c \in F$ such that

$$\alpha_i + c\beta_j \neq \alpha + c\beta, \text{ unless } i = j = 1.$$

Let $\gamma = \alpha + c\beta$. Show that $E = F[\gamma]$. The rest of the proof is identical to the proof in the characteristic zero case.

Problem 6. *Prove Theorem 2.1.*

3. A little bit algebraic number theory

Problem 7. *Consider the ring $R = \mathbb{Z}[\sqrt{2}]$. Show that for any $n \in \mathbb{Z}$, $(3 + 2\sqrt{2})^n \in R^\times$. Thus $R^\times$ is infinite.*

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

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

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

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

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

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,

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

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*

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

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

Hint: this follows from a matrix calculation which roughly appeared in the previous HW 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 $\mathcal{B} = \{1, \beta, \ldots, \beta^{-1}\}$ be the basis of $\mathbb{Q}[\beta]/\mathbb{Q}$. Then show that $\det([\psi]_{\mathcal{B}}) = \det(A)^2$, where A is the matrix $(\sigma_i(\beta^j))_{1 \leq i,j \leq n} = (\beta_i^j)_{1 \leq i,j \leq n}$, 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 $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ be an integral basis of $\mathcal{O}_K$. Then we know that $\mathcal{O}_K = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$ is a free abelian group of rank n. Moreover, we know that

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

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 $\mathrm{disc}(\mathcal{O}_K)$.

Problem 9. *Let K be an algebraic number field and let $\mathcal{O}_K$ be the ring of integers of K. Suppose that $\mathrm{rank}(\mathcal{O}_K) = n$. 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*
$$|\Delta(\mathcal{B}')| = \mathrm{disc}(\mathcal{O}_K) |\mathcal{O}_K/\mathbb{Z}[\mathcal{B}']|^2.$$
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 3.1. 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.