HOMEWORK 13

Due date: Week 14
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.*

Primitive element theorem can be used to simplify many proofs in Galois theory. Artin book adopted this approach. The following is one example.

Problem 7. *Let K be a field of characteristic zero. Let $H \leq \mathrm{Aut}(K)$ be a finite subgroup and let $F = K^H$. Show that K/F is a finite extension and $[K : F] = |H|$.*

This is Theorem 16.5.4, page 487 of Artin's book. You are advised to read the proof given in the book and compare the proof given in our class. Moreover, check how primitive element theorem can be used to simplify its proof.

Problem 8. *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.*