

1 Homework 6.

1. Suppose A is a unital commutative ring and G is a finite subgroup of the group automorphisms of A . Let

$$A^G := \{a \in A \mid \forall g \in G, g(a) = a\}.$$

- (a) Prove that A/A^G is an integral extension.
- (b) Suppose $\mathfrak{p} \in \text{Spec}(A^G)$. Prove that G acts transitively on

$$\{\mathfrak{q} \in \text{Spec}(A) \mid \mathfrak{q}^c = \mathfrak{p}\};$$

in particular, this is a finite set. (This means $\text{Spec}(A) \rightarrow \text{Spec}(A^G)$ has finite fibers.)

(**Hint.** Notice that $a \in A$ is a zero of

$$f_{a;G}(x) := \prod_{g \in G} (x - g(a)).$$

Argue why $f_{a;G}(x) \in A^G[x]$.

Suppose $\mathfrak{q}_1^c = \mathfrak{q}_2^c = \mathfrak{p}$. For every $a \in \mathfrak{q}_1$, we have

$$N_G(a) := \prod_{g \in G} g(a) \in A^G \cap \mathfrak{q}_1.$$

Hence, for all $a \in \mathfrak{q}_1$, $N_G(a) \in \mathfrak{q}_2$. Obtain that for all $a \in \mathfrak{q}_1$, $g(a) \in \mathfrak{q}_2$ for some $g \in G$. Hence,

$$\mathfrak{q}_1 \subseteq \bigcup_{g \in G} g(\mathfrak{q}_2).$$

Deduce that $\mathfrak{q}_1 = g(\mathfrak{q}_2)$ for some $g \in G$.)

2. In this exercise, you get an alternative approach for proving the Going-down theorem.
 - (a) Suppose E/F is a finite normal extension. Let $F' := \text{Fix}(\text{Aut}(E/F))$. Prove that E/F' is a finite Galois extension, $F' = F$ if the characteristic of F is zero, and $(F')^\times/F^\times$ is a p -group if the characteristic of F is $p > 0$.

- (b) Suppose A is an integrally closed integral domain and F is a field of fractions of A . Let E/F be a finite normal extension of F , and B be the integral closure of A in E . Let $f : A \rightarrow B$ be the inclusion of ring homomorphism, and $f^* : \text{Spec}(B) \rightarrow \text{Spec}(A)$, the map given by the contraction on prime ideals. Prove that for every $\mathfrak{p} \in \text{Spec}(A)$, $\text{Aut}(E/F)$ acts transitively on the fiber $(f^*)^{-1}(\mathfrak{p})$.
- (c) (Going-down) Suppose A is integrally closed, B/A is an integral extension, and B is an integral domain. Suppose $\mathfrak{p} \subsetneq \mathfrak{p}'$ are prime ideals of A and $\mathfrak{q}'$ is a prime ideal of B such that $f^*(\mathfrak{q}') = \mathfrak{p}'$. Prove that there exists $\mathfrak{q} \in \text{Spec}(B)$ such that $\mathfrak{q} \subsetneq \mathfrak{q}'$ and $f^*(\mathfrak{q}) = \mathfrak{p}$.

(**Hint.** (a) The first part is part of Galois theory. When the characteristic is 0, E/F is a Galois extension, and so the second part follows. Suppose the characteristic is $p > 0$. For $\alpha \in F'$, let $\alpha' \in E$ be a zero of $m_{\alpha, F}(x)$. Then there exists $\sigma \in \text{Aut}(E/F)$ such that $\sigma(\alpha) = \alpha'$. Deduce that $m_{\alpha, F}(x) = (x - \alpha)^d$. Argue why d has to be a power of p .

(b) Recall that we have proved f^* is surjective and so the fiber is non-empty. We also showed that the dimension of the fiber is zero. Now, suppose to the contrary that there are $\mathfrak{q}, \mathfrak{q}' \in (f^*)^{-1}(\mathfrak{p})$ and for every $\sigma \in \text{Aut}(E/F)$, $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$. Argue why

$$\mathfrak{q}' \not\subseteq \bigcup_{\sigma \in \text{Aut}(E/F)} \sigma^{-1}(\mathfrak{q})$$

(see P1 HW5). Deduce that there exists $x \in \mathfrak{q}'$ such that $\sigma(x) \notin \mathfrak{q}$ for all $\sigma \in \text{Aut}(E/F)$. Use part (a) to show that

$$\left(\prod_{\sigma \in \text{Aut}(E/F)} \sigma(x) \right)^q \in F,$$

where $q = 1$ if the characteristic of F is zero and a large power of p if the characteristic of F is $p > 0$. Deduce that

$$\left(\prod_{\sigma \in \text{Aut}(E/F)} \sigma(x) \right)^q \in \mathfrak{p} \subseteq \mathfrak{q}.$$

Get a contradiction.

Using part (b), one can prove a similar result without the assumption that E/F is a finite extension. In the next part, you should use the extended result.

(c) Notice that a field $Q(B)$ of fractions of B is an algebraic extension of F . Let L be a normal closure of $Q(B)$ over F , and C be the algebraic closure of B in L . Argue why there exists $\mathfrak{Q}' \in \text{Spec}(C)$ such that $\mathfrak{Q}' \cap B = \mathfrak{q}'$. Say why there exist $\bar{\mathfrak{Q}} \subsetneq \bar{\mathfrak{Q}}' \in \text{Spec}(C)$ such that

$$\bar{\mathfrak{Q}} \cap A = \mathfrak{p} \quad \text{and} \quad \bar{\mathfrak{Q}}' \cap A = \mathfrak{p}'.$$

Using part (b) deduce $\exists \sigma \in \text{Aut}(L/F)$ such that $\bar{\mathfrak{Q}}' = \sigma(\bar{\mathfrak{Q}})$. Show that

$$\sigma^{-1}(\bar{\mathfrak{Q}}) \subsetneq \mathfrak{Q}' \quad \text{and} \quad \sigma^{-1}(\bar{\mathfrak{Q}}) \cap A = \mathfrak{p}.$$

Then $\mathfrak{q} := \sigma^{-1}(\bar{\mathfrak{Q}}) \cap B$ satisfies the desired properties.

3. (Simple extensions) Suppose E/F is a finite field extension. Prove that there exists $\alpha \in E$ such that $E = F[\alpha]$ if and only if $\text{Int}(E/F)$ is finite.

(**Hint.** $(\Rightarrow)$ For every $K \in \text{Int}(E/F)$, let $m_{\alpha,K}(x) | m_{\alpha,F}(x)$ in $K[x]$. Hence, there exists a well-defined map Ψ from $\text{Int}(E/F)$ to the set of divisors of $m_{\alpha,F}(x)$ in $E[x]$. For $K \in \text{Int}(E/F)$, let $\bar{K}$ be the subfield of E which is generated by F and the coefficients of $m_{\alpha,K}(x)$. Prove that $m_{\alpha,\bar{K}}(x) = m_{\alpha,K}(x)$, and deduce that $[\bar{K}[\alpha] : \bar{K}] = [K[\alpha] : K]$. Show that this implies $K = \bar{K}$. Use this to prove that Ψ is injective.

($\Leftarrow$) If F is finite, then E is finite. In this case, $E^\times$ is cyclic. Deduce the claim. Next, suppose F is infinite. Since $\text{Int}(E/F)$ is finite, there exists a maximal intermediate subfield K . Use induction and deduce that $K = F[\alpha]$ for some α . Let $\beta \in E \setminus K$. Argue why $E = F[\alpha, \beta]$. Consider the following function

$$\Phi : F \rightarrow \text{Int}(E/F), \quad \Phi(c) := F[\alpha + c\beta].$$

Argue why there exists $K \in \text{Int}(E/F)$ such that $K = F[\alpha + c\beta]$ for infinitely many $c \in F$. Show that $\alpha, \beta \in K$, and deduce that $E = K$.)

4. (Primitive element) Suppose E/F is a finite separable field extension. Prove that there exists $\alpha \in E$ such that $E = F[\alpha]$.

(**Hint.** Consider the normal closure L of E/F . Then L/F is a finite Galois extension. Deduce that $\text{Int}(L/F)$ is finite.)

5. Suppose E/F is a finite separable field extension and $\overline{F}$ is an algebraic closure of E . Prove that there exists an $\overline{F}$ -algebra isomorphism

$$\theta : E \otimes_F \overline{F} \rightarrow \underbrace{\overline{F} \oplus \cdots \oplus \overline{F}}_{[E:F] \text{ many}}, \text{ such that } \theta(\alpha \otimes 1) = (\sigma_1(\alpha), \dots, \sigma_d(\alpha)),$$

where $\text{Embed}_F(E, \overline{F}) = \{\sigma_1, \dots, \sigma_d\}$.

(**Hint.** $E = F[\alpha] \simeq F[x]/\langle m_{\alpha, F}(x) \rangle$ for some $\alpha \in E$.)

6. Suppose E/F is a finite separable field extension. Suppose $\mathfrak{B} := \{e_1, \dots, e_d\}$ is an F -basis of E . For $e \in E$, let $\ell_e : E \rightarrow E, \ell_e(x) := ex$. Prove that $\det(\ell_e) = \prod_{i=1}^d \sigma_i(e)$ and $\text{tr}(\ell_e) = \sum_{i=1}^d \sigma_i(e)$, where $\text{Embed}_F(E, \overline{F}) = \{\sigma_1, \dots, \sigma_d\}$.

(**Hint.** Notice that $\ell_e \otimes 1_{\overline{F}}$ is an $\overline{F}$ -linear map, and ℓ_e and $\ell_e \otimes 1$ can be represented by the same matrix, and deduce that $\text{tr}(\ell_e \otimes 1) = \text{tr}(\ell_e)$ and $\det(\ell_e \otimes 1) = \det(\ell_e)$. Notice that

$$\begin{array}{ccc} E \otimes_F \overline{F} & \longrightarrow & \overline{F} \oplus \cdots \oplus \overline{F} \\ \downarrow \ell_e \otimes 1 & & \downarrow \ell_{(\sigma_1(e), \dots, \sigma_d(e))} \\ E \otimes_F \overline{F} & \longrightarrow & \overline{F} \oplus \cdots \oplus \overline{F} \end{array}$$

Use the standard basis of $\overline{F} \oplus \cdots \oplus \overline{F}$ and complete the proof.)

For a finite separable extension E/F , we let

$$N_{E/F}(e) := \det(\ell_e) \quad \text{and} \quad T_{E/F}(e) := \text{tr}(\ell_e).$$

7. Suppose E/F is a finite separable field extension. Let

$$k : E \times E \rightarrow F, \quad k(x, y) := T_{E/F}(xy).$$

Prove that k is an F -bilinear non-degenerate form – non-degenerate means

$$k(x, y) = 0 \text{ for all } y \text{ implies } x = 0.$$

(**Hint.** It is easy to see that k is F -bilinear. To prove non-degeneracy, you have to prove that there exists $e \in E$ such that $T_{E/F}(e) \neq 0$. By P4, there exists $\alpha \in E$ such that $E = F[\alpha]$. Notice that $\sigma_1(\alpha), \dots, \sigma_d(\alpha)$ are distinct. Deduce that the matrix $[\sigma_j(\alpha^i)]_{d \times d}$ is invertible.)