# Solution for Homework 13

Xiangcan Li

January 20, 2021

**Exercise 5.2.2** Prove that for any field $\mathbb{F}$ and any nonconstant polynomial $f \in \mathbb{F}[x]$, there exists a field $\mathbb{L}$ such that $f$ factors into linear factors over $\mathbb{L}$.

We claim that for any irreducible nonconstant polynomial $f \in \mathbb{F}[x]$, there exists a field $\mathbb{K}$ such that $f$ factors into linear factors over $\mathbb{K}$.

We prove by induction on the degree of $f$. Since $f$ is nonconstant, the base case is $\deg(f) = 1$, which implies that $f$ is linear. Hence, the base case holds.

Inductive hypothesis: For any irreducible nonconstant polynomial $f \in \mathbb{F}[x]$ with $\deg(f) \leq k$, where $k > 1$, there exists a field $\mathbb{K}$ such that $f$ factors into linear factors over $\mathbb{K}$.

Inductive step: Suppose $f \in \mathbb{F}[x]$ is an arbitrary irreducible nonconstant polynomial with degree $k+1$. By Theorem 5.2.2, $\mathbb{K} = \mathbb{F}[x]/((p))$ is a field and $\alpha = \pi(x) \in \mathbb{K}$, where $x \in \mathbb{F}[x]$ and $\pi : \mathbb{F}[x] \to \mathbb{F}[x]/((p))$. Then $\alpha$ is a root of $f \in \mathbb{K}[x]$. Hence, $(x - \alpha)$ is a linear factor of $f$. Then $f = (x-\alpha)g$ for some $g \in \mathbb{K}[x]$. Note that $\deg(g) = k+1-1 = k$. By theorem 2.3.6, $g = ap_1 \cdots p_n$, where $a \in \mathbb{K}$ and $p_1, \ldots, p_n \in \mathbb{K}[x]$ are irreducible polynomial. For any $p_i$, where $1 \leq i \leq n$ and $i \in \mathbb{Z}$, if $p_i$ is linear, then we are done. Otherwise, since $\deg(p_i) \leq \deg(g)$, by inductive hypothesis, there exists a field $\mathbb{K}_i$ such that $p_i$ factors into linear factors over $\mathbb{K}_i$. Suppose there are $m$ nonlinear irreducible polynomials, then by applying inductive hypothesis $m$ times, we have $\mathbb{K} \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_m$ such that all $m$ nonlinear irreducible polynomials factor into linear factor over $K_m$. Then $g$ factors into linear factors over $\mathbb{K}_m$. Hence, $f = (x-\alpha)g$ factors into linear factors over $\mathbb{K}_m$.

We conclude for any irreducible nonconstant polynomial $f \in \mathbb{F}[x]$, there exists a field $\mathbb{K}$ such that $f$ factors into linear factors over $\mathbb{K}$.

Then for any field $\mathbb{F}$ and for any nonconstant polynomial $f \in \mathbb{F}[x]$, by Theorem 2.3.6, we can write $f$ as a product of irreducible factors. By applying our claim above for each nonlinear irreducible factors, we have $\mathbb{F} \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n$, where $n$ is the number of nonlinear irreducible factors. then $f$ factors into linear factors over $\mathbb{K}_n$.

We conclude for any field $\mathbb{F}$ and any nonconstant polynomial $f \in \mathbb{F}[x]$, there exists a field $\mathbb{L}$ such that $f$ factors into linear factors over $\mathbb{L}$.

**Exercise 5.2.3** Suppose $\mathbb{F} \subset \mathbb{K}$ is a field extension. Prove that if $\sigma \in \mathrm{Aut}(\mathbb{K}, \mathbb{F})$, then $\sigma : K \to K$ is a linear transformation, when we view $\mathbb{K}$ as a vector space over $\mathbb{F}$.

Let $\mathbb{F}$ be a field and $\mathbb{K} \subset \mathbb{F}$ is a subfield of a field $\mathbb{F}$. Then $\mathbb{F}$ is a vector space over $\mathbb{K}$.

Since $\sigma \in \mathrm{Aut}(\mathbb{K}, \mathbb{F})$ and $\mathrm{Aut}(\mathbb{F}, \mathbb{K}) = \{\sigma \in \mathrm{Aut}(\mathbb{F}) \mid \sigma(a) = a \text{ for all } a \in \mathbb{K}\}$, then for all $a \in \mathbb{F}$ and $v, w \in \mathbb{K}$,

$$\sigma(ax) = ax = a\sigma(x) \text{ and } \sigma(x+y) = x+y = \sigma(x) + \sigma(y).$$

We conclude $\sigma$ is a linear transformation.

**Exercise 5.2.5** Consider the subfield $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{R}$.
a. Prove that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ by proving that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and that $x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})[x]$, then appeal to Proposition 5.2.6 and Exercise 5.2.4.
b. Prove that $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.
c. Prove that $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

a. Suppose $x = p/q \in \mathbb{Q}$, where $p, q$ are two integers with no common factors (If there are any common factors, we cancel them in the numerator and denominator). Then $(p/q)^2 - 2 = 0$. Hence, $p^2 = 2q^2$, which implies $p^2$ is even. Then $p$ is even. We write $p$ as $p = 2k$ for some integer $k$. Then $4k^2 = 2q^2$, i.e., $2k^2 = q^2$. Hence, $q^2$ is even. then $q$ is even. Then 2 is a common factor, which is a contradiction. We conclude $x^2 - 2$ is irreducible in $\mathbb{Q}$.

   Since $\sqrt{2} \in \mathbb{R}$, $\sqrt{2}$ is a root for $f = x^2 - 2$ in $\mathbb{R}$. By Theorem 5.2.2 and Proposition 5.2.6, $\mathbb{Q}[x]/((x^2-2)) = \mathbb{Q}(\sqrt{2})$. Hence, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

   Suppose there is $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ so that $(a + b\sqrt{2})^2 - 3 = 0$ for some $a, b \in \mathbb{Q}$.

   Then we have $a^2 + 2\sqrt{2}ab + 2b^2 - 3 = 0$, i.e., $(a+1)(a-1) + 2(b+1)(b-1) = -2\sqrt{2}ab$.

   Clearly, $(a+1)(a-1) + 2(b+1)(b-1) \in \mathbb{Q}$, then $-2\sqrt{2}ab \in \mathbb{Q}$, which implies either $a = 0$ or $b = 0$.

   - $a = 0$: $(a+1)(a-1) + 2(b+1)(b-1) = 0 \implies 2(b+1)(b-1) = 1$. Suppose $b = p/q$, where $p, q$ are two integers with no common factors (If there are any common factors, we cancel them in the numerator and denominator). Then $2(p/q+1)(p/q-1) = 1$, i.e., $p^2/q^2 = 3/2$. Then $3q^2 = 2p^2$. Then $2 \mid 3q^2$ since $p^2 \in \mathbb{Z}$. Since $2 \nmid 3$, $2 \mid q^2$. Then $q$ is even. We write $q$ as $q = 2k$ for some integer $k$. Then $q^2 = 4k^2$. Hence, $2p^2 = 3(4k^2)$, i.e., $q^2 = 2(3k^2)$. Then $q^2$ is even, which implies $q$ is even. Then 2 is a common factor, which is a contradiction.
   - $b = 0$: $(a+1)(a-1) + 2(b+1)(b-1) = 0 \implies (a+1)(a-1) = 2$. Then $a^2 = 3$. Suppose $a = p/q$, where $p, q$ are two integers with no common factors (If there are any common factors, we cancel them in the numerator and denominator). Then $p^2/q^2 = 3$, i.e., $p^2 = 3q^2$. Then $3 \mid p^2$, which implies $3 \mid p$. We write $p$ as $p = 3k$ for some integer $k$. Then $9k^2 = 3q^2$. Hence, $q^2 = 3k^2$. Then $3 \mid q^2$, which implies $3 \mid q$ (If $q = 3n+1$ or $q = 3n+2$, then $q^2 = 9n^2 + 6n + 2$ or $q^2 = 9n^2 + 12n + 4$, respectively, which implies $3 \nmid q^2$, a contradiction). Then 3 is a common factor, which is a contradiction.

   We conclude $x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})[x]$.

   Note that $\sqrt{3} \in \mathbb{R}$ is a root of $f = x^2 - 3$.

   By Theorem 5.2.2 and Proposition 5.2.6, $\mathbb{Q}(\sqrt{2})[x]/((x^2-3)) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Hence, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.

   By Exercise 5.2.4, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

b. Since $\sqrt{2}$ and $-\sqrt{2}$ are roots for $p = x^2 - 2$, by Theorem 5.2.2, we have $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/((x^2-2))$.

   Similarly, since $\sqrt{3}$ and $-\sqrt{3}$ are roots for $p = x^2 - 3$, we have $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})[x]/((x^2-3))$, where $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

   Then we have

$$\begin{aligned}\mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \{a' + b'\sqrt{3} \mid a', b' \in \mathbb{Q}(\sqrt{2})\} \\ &= \{(a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3} \mid a, b, c, d \in \mathbb{Q}\} \\ &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}\end{aligned}$$

   Hence, $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ is a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

c. We refer readers to the Example 5.2.14. Note that $x^2 - 2$ and $x^2 - 3$ are irreducible in $\mathbb{Q}$ since they have no roots in $\mathbb{Q}$ and they have degree 2. Hence, the minimal polynomial of $\sqrt{2}$ and $-\sqrt{2}$ is $x^2 - 2$ and the minimal polynomial of $\sqrt{3}, -\sqrt{3}$ is $x^2 - 3$.

   On the other hand, $G = \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q})$ acts on the roots of these polynomials $\{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}\}$. The orbit of $\sqrt{2}$ is $G \cdot \sqrt{2} = \{\sqrt{2}, -\sqrt{2}\}$, and the orbit of $\sqrt{3}$ is $G \cdot \sqrt{3} = \{\sqrt{3}, -\sqrt{3}\}$.

   Hence, $[G : \mathrm{stab}_G(\sqrt{2})] = 2$ and $[G : \mathrm{stab}_G(\sqrt{3})] = 2$ and $\mathrm{stab}_G(\sqrt{2}) \cap \mathrm{stab}_G(\sqrt{3}) = \{e\}$. We conclude $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.