LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Fabien Morel
Laurenz Wiesenberger

# Tutorial Sheet 12
## Algebra
### Suggested Solutions

Winter term 25/26

**Exercise 1.** Let $G$ be a finite group of order 35.

(i) Show that $G$ has a unique Sylow 5-subgroup, and that this subgroup is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. Moreover, show that $G$ has a unique Sylow 7-subgroup, and that this subgroup is isomorphic to $\mathbb{Z}/7\mathbb{Z}$.

*Suggested solution.* We have $|G| = 35 = 5 \cdot 7$. By Sylow I, there exists a Sylow 5-subgroup of $G$. Moreover, Sylow III implies that

$$n_5 \mid 7 \quad \text{and} \quad n_5 \equiv 1 \pmod 5,$$

which forces $n_5 = 1$. Hence, $G$ has a unique Sylow 5-subgroup, and this subgroup is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. The same argument shows that $G$ also has a unique Sylow 7-subgroup, which is isomorphic to $\mathbb{Z}/7\mathbb{Z}$.

□

(ii) Deduce that $G$ is abelian.

*Hint:* You may find Exercise Sheet 5 helpful.

*Suggested solution.* By Exercise Sheet 5, Exercise 2, we conclude that

$$G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

In particular, $G$ is abelian.

□

**Exercise 2.**
Answer each question with "Yes" or "No". (Each correct answer is worth one point. Incorrect answers will not be counted.)

(i) The quotient ring $\mathbb{Z}[i]/(3)$ is a field.

*Suggested solution.* True. We have

$$\mathbb{Z}[i]/(3) \cong \big(\mathbb{Z}[X]/(X^2+1)\big)\big/\big((3, X^2+1)/(X^2+1)\big) \cong (\mathbb{Z}/3\mathbb{Z})[X]/(X^2+1).$$

Moreover, the polynomial $X^2 + 1$ has no roots in $\mathbb{Z}/3\mathbb{Z}$, and hence it is irreducible over $\mathbb{Z}/3\mathbb{Z}$. Therefore the quotient is a field. □

(ii) The quotient ring $\mathbb{Z}[i]/(2)$ is a field.

*Suggested solution.* False. In $\mathbb{Z}[i]$ we have the factorization $2 = (1+i)(1-i)$. □

(iii) $\mathbb{R}[X]/(X^2-2)$ is isomorphic to $\mathbb{C}$.

*Suggested solution.* False. The polynomial $X^2-2$ is reducible in $\mathbb{R}[X]$. In particular, the quotient ring cannot be a field. □

(iv) In $\mathbb{Z}$, one has $(9, 21) = (3)$.

*Suggested solution.* True. Indeed, we have $\gcd(9, 21) = 3$. □

(v) In a factorial ring, every nonzero prime ideal is maximal.

*Suggested solution.* False. Consider the ring $\mathbb{Z}[X]$. Then $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$, which shows that $(X)$ is a prime ideal, but not a maximal ideal. □

(vi) The element $X$ is prime in $\mathbb{Z}[X, Y]$.

*Suggested solution.* True. We have $\mathbb{Z}[X, Y]/(X) \cong \mathbb{Z}[Y]$, and $\mathbb{Z}[Y]$ is an integral domain. □

(vii) The polynomial ring $K[X]$ is a principal ideal domain if and only if $K$ is a field.

*Suggested solution.* True. This was proved in the lecture. □

(viii) The polynomial $2X^{17} + \frac{10}{7}X^7 + \frac{10}{7}$ is irreducible in $\mathbb{Q}[X]$.

*Suggested solution.* True. Multiplying by 7 yields the polynomial $14X^{17}+10X^7+10$, which is irreducible by Eisenstein's criterion with $p = 5$. □

(ix) Let $K$ be a field and let $f(X), g(X) \in K[X]$ be irreducible. Then the composition $f(g(X))$ is irreducible in $K[X]$.

*Suggested solution.* False. For example, let $K = \mathbb{R}$ and consider the polynomials $f(X) = X - 1$ and $g(X) = X^2 + 1$. Then

$$f(g(X)) = g(X) - 1 = (X^2 + 1) - 1 = X^2 = X \cdot X,$$

so $f(g(X))$ is reducible in $K[X]$. □

(x) Let $K$ be a field. Then every nontrivial ring homomorphism $K \to S$ is injective.

*Suggested solution.* True. This was proved in the tutorials. □

(xi) Let $p$ be a prime and let $a \in \mathbb{Z}$. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

*Suggested solution.* True. Since $\overline{a} \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, the claim follows from Lagrange's theorem. □

(xii) A commutative ring $R$ is a field if and only if $\{0\}$ is a maximal ideal of $R$.

*Suggested solution.* True. If $K$ is a field, the only ideals of $K$ are $\{0\}$ and $K$. Conversely, every noninvertible element of a commutative ring is contained in a maximal ideal. Since the only maximal ideal is $\{0\}$, it follows that every nonzero element is invertible, i.e. $K^\times = K \setminus \{0\}$. □

(xiii) Every field extension $K/\mathbb{Q}$ of degree 3 is Galois.

*Suggested solution.* False. For instance, consider the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, whose minimal polynomial is $f(X) = X^3 - 2$. This extension is not normal. □

(xiv) Let $L/K$ be a finitely generated algebraic field extension. Then $[L : K] < \infty$.

*Suggested solution.* True. This was proved in the lecture. □

(xv) There exists a finite algebraically closed field.

*Suggested solution.* False. Suppose there exists a finite algebraically closed field $K$. Consider the polynomial $f(X) = 1 + \prod_{\alpha \in K}(X - \alpha)$. Then for every $\alpha \in K$ we have $f(\alpha) = 1$, and hence $f$ has no roots in $K$. This contradicts the assumption that $K$ is algebraically closed, since $\deg f \geq 1$. □

**Exercise 3.** Let $p, q$ be prime numbers. Determine the degree of the field extension $K := \mathbb{Q}\big(\zeta_p, \sqrt[p]{q}\big)$ over $\mathbb{Q}$, and prove that $\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\sqrt[p]{q}) = \mathbb{Q}$.

*Suggested solution.* We have $\deg_{\mathbb{Q}}(\zeta_p) = p - 1$ and $\deg_{\mathbb{Q}}(\sqrt[p]{q}) = p$. Hence, by Corollary 3.2.12 from the script, we obtain $[\mathbb{Q}(\zeta_p, \sqrt[p]{q}) : \mathbb{Q}] = p \cdot (p-1)$. Now set $E := \mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\sqrt[p]{q})$. By the degree formula and using that $[\mathbb{Q}(\zeta_p, \sqrt[p]{q}) : \mathbb{Q}(\sqrt[p]{q})] = p - 1$, we obtain

$$p - 1 = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = [\mathbb{Q}(\zeta_p) : E] \cdot [E : \mathbb{Q}].$$

Therefore we must have $[E : \mathbb{Q}] = 1$. Hence $E = \mathbb{Q}$. □

**Exercise 4.** Let $K := \mathbb{Q}(\zeta_5, \sqrt[5]{3})$.

(i) Show that $K/\mathbb{Q}$ is a Galois extension.

*Suggested solution.* Since $\mathrm{char}(\mathbb{Q}) = 0$, the extension is separable. Moreover, $K$ is the splitting field of the polynomial $f(X) = X^5 - 3$. Therefore $K/\mathbb{Q}$ is a Galois extension. □

(ii) Determine whether $\mathrm{Gal}(K/\mathbb{Q})$ is abelian.

*Suggested solution.* The group $\mathrm{Gal}(K/\mathbb{Q})$ is not abelian. Consider the automorphisms $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$ defined by

$$\sigma(\zeta_5) = \zeta_5^2, \quad \sigma(\sqrt[5]{3}) = \sqrt[5]{3}, \qquad \tau(\zeta_5) = \zeta_5, \quad \tau(\sqrt[5]{3}) = \zeta_5\sqrt[5]{3}.$$

Then

$$\sigma\tau(\sqrt[5]{3}) = \zeta_5^2\sqrt[5]{3} \neq \zeta_5\sqrt[5]{3} = \tau\sigma(\sqrt[5]{3}),$$

and hence $\sigma\tau \neq \tau\sigma$. Therefore, $\mathrm{Gal}(K/\mathbb{Q})$ is not abelian. □

**Exercise 5.** Let $K := \mathbb{F}_{16}(Y)$ and let $f \in K[X]$ be an irreducible polynomial of degree 3. Let $L$ be the splitting field of $f$ over $K$. Show that $L/K$ is a Galois extension, and prove that $\mathrm{Gal}(L/K) \cong S_3$ or $\mathrm{Gal}(L/K) \cong A_3$.

*Suggested solution.* We have $\mathrm{char}(K) = 2$. Hence $f' \neq 0$, and therefore $f$ is separable. Consequently, its splitting field $L$ yields a Galois extension $L/K$. In particular, $\mathrm{Gal}(L/K)$ embeds into $S_3$ via its action on the three distinct roots of $f$. Moreover, we have $|\mathrm{Gal}(L/K)| \geq 3$. It follows that $\mathrm{Gal}(L/K)$ is isomorphic to either $S_3$ or $A_3$. □

**Exercise 6.** Let $a, b \in \mathbb{Q}$ and assume that the polynomial $f(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$ is irreducible. Let $K$ be the splitting field of $f$ over $\mathbb{Q}$.

(i) Let $\alpha \in K$ be a root of $f$. Show that $[K : \mathbb{Q}(\alpha)] \leq 2$.

*Suggested solution.* First note that the roots of $f$ occur in pairs. That is, there exist $\alpha, \beta \in L$ such that the roots of $f$ are given by $\pm\alpha$ and $\pm\beta$. Now consider the field $\mathbb{Q}(\alpha)$. In $\mathbb{Q}(\alpha)[X]$, we may divide $f$ by $(X - \alpha)(X + \alpha)$, which yields a quadratic polynomial with coefficients in $\mathbb{Q}(\alpha)$ whose roots are $\pm\beta$. In particular, we obtain $[K : \mathbb{Q}(\alpha)] \leq 2$. □

(ii) Prove that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to one of the following groups:

$$D_4, \quad \mathbb{Z}/4\mathbb{Z}, \text{ or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

*Suggested solution.* Since $f$ is irreducible of degree 4, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. By the degree formula, we obtain

$$[L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [L : \mathbb{Q}(\alpha)] \leq 4 \cdot 2 = 8.$$

In particular, $[L : \mathbb{Q}] \in \{4, 8\}$.

If $[L : \mathbb{Q}] = 4$, then $\mathrm{Gal}(L/\mathbb{Q})$ has order 4, and hence

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \quad \text{or} \quad \mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

If $[L : \mathbb{Q}] = 8$, then $|\mathrm{Gal}(L/\mathbb{Q})| = 8$. Since $\mathrm{Gal}(L/\mathbb{Q})$ embeds into $D_4$, we conclude that $\mathrm{Gal}(L/\mathbb{Q}) \cong D_4$. □