Uppsala Universitet Matematiska Institutionen Hankyung Ko

Algebraiska strukturer HT 2022

Exam in Algebraic Structures
03-01-2023

Notes, books or electronic devices are not allowed. Please write your answers in English or in Swedish. Total is 40 points, of which you need 18 points for grade 3, 25 for grade 4, and 32 for grade 5.

1. (5pt)

   (a) Let S be a set and let $\cdot : S \times S \to S$ be a function. When is $(S, \cdot)$ a group? That is, what is the definition of a group?

   (b) Define a normal subgroup of a group.

   Answer: See notes/book.

2. (5 pt) Recall that a composition series of a group G is a series of (proper) normal subgroups

$$\{e_G\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G,$$

   where each quotient group G_i/G_{i-1} is simple. Can you give two different composition series of the group G below? If yes, give the two composition series; if no, justify.

   (a) $G = \mathbb{Z}$.

   Answer: G does not have a composition series. The subgroup $G_1 \cong G_1/G_0 = G_1/\{e_G\}$ in the series has to be simple, while G does not contain any simple subgroup. In fact, any subgroup $H \leq G$ is isomorphic to $n\mathbb{Z}$ for some $n \in \mathbb{Z}$ and thus has a proper normal subgroup, e.g., $2n\mathbb{Z} \lhd n\mathbb{Z}$.

   (b) $G = \mathbb{Z}/8\mathbb{Z}$.

   Answer: G has only one composition series. The only simple subgroup of G is $4G$ and thus we need to have $G_1 = 4G$. Then the only simple subgroup of $G/4G$ is $2G/4G$ and thus we need to have $G_2 = 2G$. Then $G/2G \cong \mathbb{Z}/2$ is simple. Thus a composition series of G is equal to $0 \lhd 4\mathbb{Z}/8 \lhd 2\mathbb{Z}/8 \lhd \mathbb{Z}/8$.

(c) $G = S_3 (= S_{\{1,2,3\}}$ in the notation of Problem 3).

Answer: The only proper normal subgroup of S_3 is $H = \{e, (123), (132)\}$. The latter is simple. Moreover, the quotient S_3/H is simple (for example, it has the order $6/3 = 2$). This means that the only composition series of S_3 is $\{e\} \lhd H \lhd S_3$.

Comment: The fact that G has only one proper normal subgroup, say $N \lhd G$, is not enough to show that G has a unique composition series since there can be subgroups $H_i \lhd N$ which are not normal in G. An example of such G is the alternating group A_4.

3. (5 pt) Prove that every group is isomorphic to a subgroup of $S_X = (\{f : X \to X \mid f \text{ is a bijection}\}, \circ)$ for some set X. Here, $\circ$ denotes the composition of functions.

Answer: Let G be a group and consider the group action of G on the underlying set G given by the group operation. This gives a group homomorphism $G \to S_G$ sending g to $\sigma_g : h \mapsto gh$. The homomorphism is a monomorphism since if $\sigma_g = e_{S_G} = \mathrm{Id}_G$ then $e_G = \sigma_g(e_G) = ge_G = g$. By the first ismomorphism theorem, the image of G in S_G is isomorphic to G.

4. (5 pt) Let R be a(n integral) domain and let Q be the fraction field of R.

(a) Prove or disprove: if R is finite then Q is finite.

Answer: Q is a quotient of $R \times R \setminus 0$. Since R is finite, the latter is finite, and thus Q is finite.

(b) Prove or disprove: the characteristic of R is equal to the characteristic of Q.

Answer: Let R have characteristic n, that is, we have a group (ring) momomorphism $\mathbb{Z}/n \to R$ given by $m + n\mathbb{Z} \mapsto m1_R$. Composing with the monomorphism $R \to Q$ given by $r \mapsto \frac{r}{1}$ we have a monomorphism $\mathbb{Z}/n \to Q$, showing that Q has the same characteristic n.

Turn to the next page!

5. (5 pt) Let R be a principal ideal domain (PID). Let (p) be a nonzero ideal in R. Show that the following conditions are equivalent:

   - p is prime;
   - p is irreducible;
   - (p) is prime;
   - (p) is maximal.

   Answer:

   If p is irreducible then (p) is maximal: For any inclusion $(p) \leq I \lneq R$ of ideals, we have $I = (a)$ for some $a \in R$ since R is PID. For such $a \in R$, there is $b \in R$ such that $p = ab$. So if p is irreducible then $b \in R^\times$ (we cannot have $a \in R^\times$ since $(a) \neq R$). So $(p) = Rp = Rab = Ra = (a)$.

   If (p) is maximal then (p) is prime: If (p) is maximal then $R/(p)$ is a field (a proper ideal $(p) \lneq J \lneq R/(p)$ gives a proper ideal $(p) \lneq J + (p) \lneq R$ which does not exists) and thus an integral domain. This means that for $a, b \in R$ with $ab \in (p)$ we have $a \in (p)$ or $b \in (p)$, that is, (p) is prime.

   If (p) is prime then p is prime: Suppose (p) is prime. Then if $p \mid ab$ then $ab \in (p)$ and thus $a \in (p)$ or $b \in (p)$, i.e., $p \mid a$ or $p \mid b$. This shows that p is prime.

   If p is prime then p is irreducible: Let $p \in R$ be prime and suppose $p = ab$. Then $p \mid ab$, so p wlog divides a, i.e., $pc = a$ for some $c \in R$. But this implies $pcb = ab = p$ which, by cancellation, give $cb = 1$, so $b \in R^\times$. This shows that p is irreducible.

6. (5 pt) Let K be a field, let $f \in K[X]$ be irreducible, and let $\alpha, \beta \in \overline{K}$ be such that $f(\alpha) = f(\beta) = 0$. Prove or disprove:

   (a) We have $K(\alpha) = K(\beta)$.

   Answer: This is not true. For example, if $K = \mathbb{Q}$, $f = X^3 - 2$, $\alpha = \sqrt[3]{2}$ and $\beta = \sqrt[3]{2}e^{2\pi i/3}$, then $\alpha, \beta \in \overline{\mathbb{Q}}$ are roots of the irreducible polynomial $f \in \mathbb{Q}[X]$ such that $K(\alpha) \neq K(\beta)$. In fact, $K(\alpha) \subset \mathbb{R}$ while $K(\beta) \not\subset \mathbb{R}$.

   (b) There is a K-isomorphism between $K(\alpha)$ and $K(\beta)$.

   Answer: This is true. The K-homomorphism given by $\alpha \mapsto \beta$ is well-defined since f, which has α as a root, is the minimal polynomial of β (up to scalar). Similarly the K-homomorphism sending β to α is well-defined and is the inverse to the above.

   (c) There is a K-isomorphism between $K(\alpha)$ and $K(\beta + 1)$.

   Answer: This is true. By part (b) it is enough to show that $K(\beta) = K(\beta + 1)$. But since $1 \in K$ we have $\beta = (\beta + 1) - 1 \in K(\beta + 1)$ and similarly $\beta + 1 \in K(\beta)$, which implies $K(\beta) = K(\beta + 1)$.

7. (5 pt) Consider the field extension $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$ of $\mathbb{Q}$. Let $G = Aut_{\mathbb{Q}}(E)$.

(a) Is the extension $\mathbb{Q} \subset E$ simple?

Answer: Yes, we have $E = \mathbb{Q}[\sqrt{2} + \sqrt{3} + \sqrt{5}]$. The answer 'yes' also follows by the primitive element theorem, using part (b),(c).

(b) Is the extension $\mathbb{Q} \subset E$ separable?

Answer: Yes, every extension in characteristic zero is separable.

(c) Is the extension $\mathbb{Q} \subset E$ normal?

Answer: Yes, the field E is a splitting field of the polynomial $(X^2 - 2)(X^2 - 3)(X^2 - 5)$ over $\mathbb{Q}$.

(d) Show that, for $\sigma \in G \setminus \{e_G\}$, we have $|\sigma| = 2$. (Hint: what are the roots of $X^2 - 2 \in \mathbb{Q}[X]$ in E?)

Answer: Let $\sigma \in G \setminus \{e_G\}$. We need to show that $\sigma^2 = \mathrm{Id}_E$. For this, it is enough to show $\sigma^2(\alpha) = \alpha$ for $\alpha \in \{\sqrt{2}, \sqrt{3}, \sqrt{5}\}$ since the latter generates E over $\mathbb{Q}$.
Since σ sends a root of $X^2 - 2 \in \mathbb{Q}[X]$ to a root of $X^2 - 2$, we have either $\sigma(\sqrt{2}) = \sqrt{2}$ or $\sigma(\sqrt{2}) = -\sqrt{2}$. In either case, we have $\sigma^2(\sqrt{2}) = \sqrt{2}$. Similarly, σ^2 fixes $\sqrt{3}$ and $\sqrt{5}$ as desired.

8. (5 pt) If $E \supset \mathbb{R}$ is finite, then $[E : \mathbb{R}] = 2^r$ for some r. Use this fact to prove that the field $\mathbb{C}$ is algebraically closed. (Hint: use the Galois theorem and Sylow's theorem.)

Answer: See S19.2 in the notes.

The exam ends here.