**Uppsala Universitet**
Matematiska Institutionen
Hankyung Ko

**Algebraiska strukturer**
HT 2023

**Exam in Algebraic Structures**
**11-01-2024**

*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) Let $S_n$ denote the symmetric group on $n$ letters, i.e., the group of permutations on $\{1, \cdots, n\}$.
   (a) Find all homomorphisms $S_2 \to S_3$.
   (b) Find all homomorphisms $S_3 \to S_2$.

   **Answer:** See problem session 1.

2. (5 pt) Let $G$ be a group and let $H \leq G$ be a subgroup and consider the set of left cosets

$$G/H = \{gH \mid g \in G\}.$$

   (a) Show that $G/H$ is a group under the operation $(g_1H, g_2H) \mapsto g_1g_2H$ if $H$ is normal.

   **Answer:** The assignment is well-defined iff $g_1g_2H = g_1hg_2H$ for all $g_1, g_2 \in G$ and $h \in H$. The latter equation holds iff $g_1g_2h' = g_1hg_2$ for some $h' \in H$ iff $g_2h' = hg_2$ for some $h' \in H$ iff $g_2H = Hg_2$. (Then check the group axioms.)

   (b) If $H$ is normal, then the set of right cosets $H\backslash G = \{Hg \mid g \in G\}$ also has a group structure given by $(Hg_1, Hg_2) \mapsto Hg_1g_2$. Prove or disprove: if $H$ is normal, then $H\backslash G$ and $G/H$ are isomorphic as groups.

   **Answer:** We have $H\backslash G = G/H$ as sets and the group operations are the same. Alternatively, $Hg \mapsto gH$ is an isomorphism.

3. (5 pt) Let $G$ be a finite group. Recall that the first Sylow theorem states that, given a prime number $p$ and a natural number $r$ such that $p^r \bigm| |G|$, there exists a subgroup $H \leq G$ with $|H| = p^r$. Prove the first Sylow theorem. (Hint: consider the center $Z(G) \leq G$ and the orbits under the conjugation action.)

   **Answer:** See Lecture 8.

4. (5 pt)

(a) What is the characteristic of a ring $R$? Give (any of the) definition(s). **Answer:** See Lecture 10.

(b) Show that if $R$ is an integral domain then the characteristic of $R$ is either zero or a prime integer. **Answer:** See Lecture 12.

**Turn to the next page!**

5. (5 pt)
   (a) Use Eisenstein's criterion to show that the polynomial $f = x^3 + 3x^2 - 6x + 3 \in \mathbb{Q}[x]$ is irreducible.

   **Answer:** Eisenstein's criterion applies to $x^3 + 3x^2 - 6x + 3 \in \mathbb{Z}[x]$ to show that the polynomial is irreducibble in $\mathbb{Z}[x]$. Since $f$ is primitive $f \in \mathrm{Frac}(\mathbb{Z})[x] = \mathbb{Q}[x]$ is irreducible.

   (b) Use part (a) to show that $\mathbb{Q}[x]/(f)$ is a field.

   **Answer:** Since $\mathbb{Q}[x]$ is a PID $f$ being irreducible implies that $(f)$ is a maximal ideal. It follows that $\mathbb{Q}[x]/(f)$ has no proper ideal and thus is a field.

6. (5 pt) Let $F$ be a field of order $q \in \mathbb{Z}_{>0}$.
   (a) Show that there is a ring homomorphism $\mathbb{F}_p \hookrightarrow F$ for some prime number $p$.

   **Answer:** The characteristic of $F$ is not zero because it then has $|\mathbb{Z}|$ distinct elements $n1_F$ and is infinite. So the characteristic is a prime number $p$ and then $\mathbb{F}_p \cong \{n1_F\}$ is a subfield in $F$.

   (b) Show that $q = p^r$ for some prime integer $p$ and $r \in \mathbb{Z}_{>0}$.

   **Answer:** $F$ is an $\mathbb{F}_p$-vector space of finite dimension say $r$ so has order $p^r$.

   (c) Show that $F^\times$ is a cyclic group (Hint: use the classification of finite(ly generated) abelian groups) .

   **Answer:** See Lecture 15.

7. (5 pt) Consider the irreducible polynomial $f = x^3 + 3x^2 - 6x + 3 \in \mathbb{Q}[x]$ (see Problem 5) and let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ be its roots, that is,

$$x^3 + 3x^2 - 6x + 3 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \in \mathbb{C}[x].$$

   Below we use that $x^3 + 3x^2 - 6x + 3$ has exactly one real root (with multiplicity one) to assume $\alpha_1 \in \mathbb{R}$ and $\alpha_2, \alpha_3 \notin \mathbb{R}$.

   (a) Show that $\mathbb{Q}[\alpha_i] = \mathbb{Q}(\alpha_i)$ holds for each $i$.

   **Answer:** Since $\alpha_i$ are roots of a polynomial $f \in \mathbb{Q}[x]$, we have that $\mathbb{Q}[\alpha_i] \cong \mathbb{Q}[x]/f$ is a field. This proves the claim.

   (b) Find the degrees $[\mathbb{Q}[\alpha_i] : \mathbb{Q}]$ of the field extensions $\mathbb{Q} \subset \mathbb{Q}[\alpha_i]$, for $i = 1, 2, 3$.

   **Answer:** Since each $\alpha_i$ has the minimal polynomial $f$, we have the $\mathbb{Q}$-isomorphism $\mathbb{Q}[\alpha_i] \cong \mathbb{Q}[x]/f$. The latter has dimension $\deg f = 3$ over $\mathbb{Q}$. Thus the degree is 3 for all $i = 1, 2, 3$.

(c) Does $|Aut_{\mathbb{Q}}(\mathbb{Q}[\alpha_i])| = [\mathbb{Q}[\alpha_i] : \mathbb{Q}]$ hold? Justify your answer, for $i = 1, 2, 3$.

**Answer:** We have $|Aut_{\mathbb{Q}}(\mathbb{Q}[\alpha_i])| \neq [\mathbb{Q}[\alpha_i] : \mathbb{Q}] = 3$ for each $i = 1, 2, 3$. Let us justify.
We first show $Aut_{\mathbb{Q}}(\mathbb{Q}[\alpha_1])$ is trivial. Since $\mathbb{Q}$-automorphisms permute roots of a polynomial and since $\alpha_2, \alpha_3 \notin \mathbb{Q}[\alpha_1] \subset \mathbb{R}$, any $\mathbb{Q}$-automorphism on $\mathbb{Q}[\alpha_1]$ sends $\alpha_1$ to $\alpha_1$ and thus is the identity map.
Now, since $\mathbb{Q}[\alpha_i]$, for $i = 1, 2, 3$, are all $\mathbb{Q}$-isomorphic (see part (b)), their $\mathbb{Q}$-automorphism groups are isomorphic. For example, if $f : \mathbb{Q}[\alpha_1] \to \mathbb{Q}[\alpha_2]$ is a $\mathbb{Q}$-isomorphicm, then one can check that $\phi \mapsto f \circ \phi \circ f^{-1}$ gives a group isomorphism $Aut_{\mathbb{Q}}(\mathbb{Q}[\alpha_1]) \xrightarrow{\cong} Aut_{\mathbb{Q}}(\mathbb{Q}[\alpha_2])$. It follows that each $Aut_{\mathbb{Q}}(\mathbb{Q}[\alpha_i])$ is trivial.

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 the first Sylow theorem.)

**Answer:** See S19.2 in the notes.

**The exam ends here.**