Uppsala Universitet | **Algebraiska strukturer**
Matematiska Institutionen | Kandidatprogrammet i matematik
Hankyung Ko | HT 2021

Exam in Algebraic Structures
07-01-2022

Time: 8.00-13.00. 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. (10 pt) Let G be a group and let $H \leq G$ be a subgroup.

   (a) Consider the set of left cosets
   $$G/H = \{gH \mid g \in G\}.$$
   Give an example of a G-action on G/H. Justify your answer.

   Answer: The assignment
   $$a(gH) = (ag)H$$
   for $a \in G$ and $gH \in G/H$ is a G-action since
   $$e_G(gH) = (e_G g)H = gH$$
   and for $a, b \in G$
   $$b(a(gH)) = b((ag)H)) = (b(ag))H = ((ba)g)H = (ba)(gH)$$
   by the associativity of the group structure on G.

   (b) When is H said to be a normal subgroup?

   Answer: When $gH = Hg$ for all $g \in G$.

   (c) Show that G/H is a group under the operation $(gH, g'H) \mapsto gg'H = (gg')H$ if and only if H is normal.

   Answer: The operation is well-defined iff $gg'H = ghg'H$ for all $g, g' \in G$ and $h \in H$. The latter equation holds iff $gg'h' = ghg'$ for some $h' \in H$ iff $g'h' = hg'$ for some $h' \in H$ iff $g'H = Hg'$. Therefore the operation $(gH, g'H) \mapsto gg'H = (gg')H$ is well-defined if and only if H is normal, and it remains to show that the operation satisfies the group axioms:

   1. $(g_1Hg_2H)g_3H = (g_1g_2)Hg_3H = ((g_1g_2)g_3)H = (g_1(g_2g_3))H = g_1H(g_2g_3)H = g_1H(g_2Hg_3H)$ for $g_1, g_2, g_3 \in G$, by the associativity of G ;
   2. Letting $e \in G$ be an identity element in G, the element $eH = H \in G/H$ is an identity element, since $eHgH = egH = gH = geH = gHeH$ for all $g \in G$;
   3. Given each $gH \in G/H$, the element $g'H \in G/H$ is its inverse if $g' \in G$ is an inverse of $g \in G$, which exists since G is a group.

(d) Show that, if $\phi : G \to L$ is a group homomorphism, then $\operatorname{Ker}\phi$ is a normal subgroup of G.

Answer: We need $g \operatorname{Ker}\phi = \operatorname{Ker}\phi g$ for $g \in G$. By symmetry, we only show "$\subseteq$".
For $h \in \operatorname{Ker}\phi$ and $g \in G$, we want to find $h' \in \operatorname{Ker}\phi$ such that $gh = h'g$. But since $\phi(gh) = \phi(g)\phi(h) = \phi(g)$, we have

$$e = \phi(g)\phi(g^{-1}) = \phi(gh)\phi(g^{-1}) = \phi(ghg^{-1})$$

so $ghg^{-1} \in \operatorname{Ker}\phi$, and we can let $h' = ghg^{-1}$.

(e) State the first isomorphism theorem for groups.

Answer: See notes/textbook.

2. (5 pt) Give a presentation of the group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ by generators and relations.

Answer:

$$F_{\{a,b\}}/N(a^2, b^2, aba^{-1}b^{-1})$$

or

$$\langle a, b \mid a^2 = e = b^2, ab = ba \rangle$$

3. (5 pt) A *Euclidean ring* is an integral domain R which admits a map

$$R \setminus \{0\} \to \mathbb{Z}_{\geq 0}, \quad a \mapsto ||a||$$

satisfying

1. for $a, b \in R$, if b divides a, then $||b|| \leq ||a||$;
2. for $a, b \in R$, if $b \neq 0$ does not divide a, then there is $q, r \in R$ with $||r|| < ||b||$ such that $a = bq + r$ holds.

(a) Prove that a Euclidean ring is a principal ideal domain (PID).

Answer: Let I be an ideal in a Euclidean ring R. We want to find $b \in I$ such that $I = (b)$. We claim we can take $b \in I$ to be such that $||b|| = \min||I||$.
If there is $a \in I$ that is not divisible by b then item 2 above implies $a - bq = r \in I$ for some $||r|| < b$, but this contradicts $||b|| = \min||I||$. This proves the claim.

(b) Is $\mathbb{Q}[X, Y]$ a Euclidean ring? Justify your answer.

Answer: No, we claim $I = (X, Y)$ is not a principal ideal, which implies $R = \mathbb{Q}[X, Y]$ is not a PID and is not a Euclidean ring by (a). Suppose $I = (f)$ for some $f \in I$. Then since $X, Y \in I$, f divides X and Y. So f has to belong to $\mathbb{Q}$, but f is also not zero. It follows that f is invertible in R and that $I = R$ which contradicts for example that $1 \notin I$.

Turn to the next page!

4. (5 pt) Given a ring R and two rings S, T that contain R as a subring, an *R-homomorphism* $\phi : S \to T$ is a ring homomorphism such that $\phi(r) = r$ for $r \in R$.

   (a) Can you give two (different) examples of surjective $\mathbb{R}$-homomorphisms $\mathbb{R}[X] \to \mathbb{C}$? If yes, give the examples; if not, justify.

   Answer: Letting ϕ_a, for $a \in \mathbb{C}$ to be the $\mathbb{R}$-homomorphism sending X to a, the ϕ_a for $a \in \mathbb{C} \setminus \mathbb{R}$ are (distinct and) exactly all surjective $\mathbb{R}$-homomorphisms $\mathbb{R}[X] \to \mathbb{C}$.
   So two examples can be ϕ_i and ϕ_{i+1}, for example.

   More explanation: An $\mathbb{R}$-homomorphism $\phi : \mathbb{R}[X] \to \mathbb{C}$ is a $\mathbb{R}$-linear map if we view $\mathbb{R}[X]$ and $\mathbb{C}$ as $\mathbb{R}$-vectorspaces with bases $\{X^n\}$ and $\{1, i\}$ respectively. Moreover, being a ring homomorphism, the values $\phi(X^n)$ are determined by the value $\phi(X) \in \mathbb{C}$. The image of ϕ is the subspace $\mathbb{R}+\mathbb{R}\phi(X)$ in $\mathbb{C}$ and is equal to $\mathbb{C}$ if and only if $\mathbb{R}\phi(X) \neq \mathbb{R}$ if and only if $\phi(X) \in \mathbb{C} \setminus \mathbb{R}$.

   (b) Can you give two (different) examples of injective $\mathbb{R}$-homomorphisms $\mathbb{R}[X] \to \mathbb{C}$. If yes, give the examples; if not, justify.

   Answer: An $\mathbb{R}$-homomorphism $\phi : \mathbb{R}[X] \to \mathbb{C}$ is a $\mathbb{R}$-linear map if we view $\mathbb{R}[X]$ and $\mathbb{C}$ as $\mathbb{R}$-vectorspaces. There is no such injective linear map because the domain $\mathbb{R}[X]$ has a ($\mathbb{R}$)-dimension strictly bigger than that of $\mathbb{C}$.

5. (5 pt) Consider the polynomial $f = X^{3^3} - X \in \mathbb{F}_3[X]$ and let E be its splitting field (over $\mathbb{F}_3$).

   (a) Is f irreducible?

   Answer: No, for example X divides f in $\mathbb{F}_3[X]$.

   (b) Compute the group $\mathrm{Aut}_{\mathbb{F}_3}(E)$ of $\mathbb{F}_3$-automorphisms on E.

   Answer: The group $\mathrm{Aut}_{\mathbb{F}_3}(E)$ is isomorphic to $\mathbb{Z}/3$.
   More precisely, we have $\mathrm{Aut}_{\mathbb{F}_3}(E) = \{\mathrm{Id}_E, \sigma, \sigma^2\} = \langle\sigma\rangle$ where $\sigma : \alpha \mapsto \alpha^3$ and $\sigma^3 = \mathrm{Id}_E$.

   More explanation: See the solution to problem 19.2 in the exercise collection.

   (c) Find all subfields of E.

   Answer: $\mathbb{F}_3$ and E are the only subfields of E.

   More explanation: The field E by construction contains $\mathbb{F}_3$ as a subfield and any other subfield, say K, needs to contain this $\mathbb{F}_3$. Moreover, since $K \subset E$, the order of E needs to be a power of $|K|$. But E has $3^3 = 27$ elements, so either $K = E$ or $|K| \leq 3$. In the latter case we have to have $K = \mathbb{F}_3$.
   Alternatively, since f is separable and E over $\mathbb{F}_3$ is Galois, the fields between $\mathbb{F}_3$ and E corresponds to the subgroups of the Galois group. The latter is isomorphic to $\mathbb{Z}/3$ by (b) which has only the trivial subgroup and itself. The corresponding fields are $\mathbb{F}_3$ and E.

6. (5 pt) Show that, if $E \supset \mathbb{R}$ is finite Galois, then $[E : \mathbb{R}] = 2^r$ for some r. (Use the Galois theorem, the first Sylow theorem for $p = 2$ and the fact that an odd degree polynomial has a real root.)

Answer: Let $G = Gal(E/\mathbb{R})$ and let $H \leq G$ be a Sylow 2-subgroup. By the Galois theorem, we have an extension $\mathbb{R} \subseteq E^H \subseteq E$ with $[E^H : \mathbb{R}]$ odd. So for $\alpha \in E^H$, the minimal polynomial of α over $\mathbb{R}$ is of odd degree. But every odd degree polynomial has a zero in $\mathbb{R}$, by the intermediate value theorem, so $\alpha \in \mathbb{R}$. It follows $E^H = \mathbb{R}$. By the Galois theorem, we have $H = G$ and thus $|G| = |H|$ is a power of 2.

7. (5 pt) Let $E \supset K$ be a field extension where $\operatorname{char} K = 0$. Recall that $E \supset K$ is said to be *solvable by radicals* if there exist field extensions

$$K = F_0 \subset F_1 \subset \cdots \subset F_l = E$$

such that, for each i, we have $F_i = F_{i-1}(\alpha_i)$ with $\alpha_i^{m_i} \in F_{i-1}$ for some $m_i \in \mathbb{N}$.

(a) Show that $\operatorname{char} E = 0$.

Answer: Since $\text{char}K = 0$, we have $n1_K \neq 0$ for all $n \in \mathbb{Z}$. But since $E \supset K$, we have $1_E = 1_K$ and $n1_E = n1_K \neq 0$ for all $n \in \mathbb{Z}$. The latter says $\text{char}E = 0$.

(b) If E is the splitting field of some $f \in K[X]$ with $\deg f = 2$, then is E solvable over K? Justify your answer.

Answer: Yes. Since $\deg f = 2$, we have $E = K[\alpha]$ for any root $\alpha \in \overline{K}$ of f. If we write $f = aX^2 + bX + c$ for $a, b, c \in K$, then $\alpha = \frac{-b \pm \gamma}{2a}$ for some $\gamma \in \overline{K}$ with $\gamma^2 = b^2 - 4ac \in K$. So γ is radical and $E = K[\alpha] = K[\gamma]$ is solvable over K.

Alternatively, since $[E : K] \leq 2$ and E is Galois over K, the Galois group is either trivial or S_2 and thus solvable. It follows E is solvable over K.

(c) If $[E : K] = 2$, then is E solvable over K? Justify your answer.

Answer: Yes. If $[E : K] = 2$ then for any $\alpha \in E \setminus K$ we have $E = K[\alpha]$. Let f be the minimal polynomial for α over K. We have $\deg f = 2$.

Then the other root of f belongs to $K[\alpha]$, so E is the splitting field of f over K. Now the claim follows from (b). (More concretely, writing $f = X^2 + bX + c$ for $b, c \in K$, we have $\alpha \in \frac{-b \pm \gamma}{2}$ where $\gamma^2 = b^2 - 4c \in K$. Since $K[\alpha] = K[\gamma]$ and γ is radical over K, the extension $K[\alpha] \supset K$ is solvable.)