Uppsala Universitet
Matematiska Institutionen
Hankyung Ko

Algebraiska strukturer
Kandidatprogrammet i matematik
HT 2020

Exam and solutions
08-01-2021

Time: 14.00-19.00. You may look at your personal notes from the course, the lecture notes, and the course book. 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 S_3 be the set of permutations (i.e., bijections) on $\{1, 2, 3\}$.
   (a) Show that $(S_3, \circ)$ is a group, where the group operation $\circ$ is the composition of permutations.

   We need to check the associativity, unit law and inverses. Composition is associative, and the identity permutation is the unit, and permutations have inverse permutations.

   (b) Is S_3 abelian? Justify your answer.

   No. For example we have $(1,2) \circ (2,3) = (1,2,3) \neq (1,3,2) = (2,3) \circ (1,2)$.

   (c) Find all subgroups of S_3.

   S_3 has the following 6 subgroups. $\{e\}, \{e, (1,2)\}, \{e, (2,3)\}, \{e, (1,3)\}, \{e, (1,2,3), (1,3,2)\}, S_3$

   (d) Find all quotient groups of S_3.

   Among the subgroups of S_3, the normal subgroups are $\{e\}, \{e, (1,2,3), (1,3,2)\}$ and S_3. The quotients by these are $S_3/\{e\} \cong S_3$, $S_3/\{e, (1,2,3), (1,3,2)\} \cong \mathbb{Z}_2$, and $S_3/S_3 \cong \{e\}$ respectively.

   (e) Is S_3 solvable? Justify your answer.

   Yes. The normal series $\{e\} \trianglelefteq \{e, (1,2,3), (1,3,2)\} \trianglelefteq S_3$ has factors $\{e, (1,2,3), (1,3,2)\}/\{e\} \cong \mathbb{Z}_3$ and $S_3/\{e, (1,2,3), (1,3,2)\} \cong \mathbb{Z}_2$ which are abelian. Thus it is a solvable series for S_3.

   (f) Show that S_3 is isomorphic to a quotient of the group G which has the following presentation by generators and relations:
   $$G = \langle b, c \mid bcb = cbc \rangle.$$

   The map $G \to S_3$ given by $b \mapsto (1,2)$, $c \mapsto (2,3)$ is a well-defined group homomorphism since the relation $(1,2)(2,3)(1,2) = (1,3) = (2,3)(1,2)(2,3)$ is satisfied in S_3. It is surjective since the elements $(1,2), (2,3)$ generate S_3:

   $$S_3 = \{e, (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\} = \{e, (1,2), (2,3), (1,2)(2,3)(1,2), (1,2)(2,3), (2,3)(1,2)\}.$$

   By the first isomorphism theorem, S_3 is isomorphic to the quotient of G by the kernel of this map.

2. (5 pt) Classify all groups of order 33. Justify your answer.

   Suppose G is a group of order 33. The prime decomposition of 33 is $3 \cdot 11$. By the first Sylow theorem, G contains a subgroup of order 3 and 11 each, which are Sylow subgroups. The groups of prime order are cyclic, so the Sylow 3-subgroup, say H of G is (isomorphic to) $\mathbb{Z}_3$ and the Sylow 11-subgroup of G, say N is $\mathbb{Z}_{11}$.

By the second Sylow theorem, the number of Sylow 3-subgroups has to divide $|G| = 33$ and one modulo 3. The only possibility is that there is a unique Sylow 3-subgroup. Similarly, the number of Sylow 11-subgroups of G is one. It follows that both Sylow subgroups H, N are normal subgroups of G.

Now note that $H \cap N = \{e\}$ since the orders of the nontrivial elements in H (resp., N) are 3 (resp., 11). By the second isomorphism theorem, we need to have $HN = G$. We conclude $G = HN = H \times N \cong \mathbb{Z}_3 \times \mathbb{Z}_{11} \cong \mathbb{Z}_{33}$.

3. (5 pt)
   (a) Does the element $X^3 - 3X + 9 \in \mathbb{Q}[X]$ generate a prime ideal in $\mathbb{Q}[X]$? Is the ideal maximal? Justify your answers.
   (b) Does the element $X^3 - 3X + 9 \in \mathbb{Z}[X]$ generate a prime ideal in $\mathbb{Z}[X]$? Is the ideal maximal? Justify your answers.

   We claim that $f = X^3 - 3X + 9$ is irreducible over $\mathbb{Z}$. By Gauss' lemma, f is then irreducible over $\mathbb{Q}$. Since $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ are UFD, this will imply that the ideal generated by f is prime.
   Since $\mathbb{Q}[X]$ is a PID, the prime ideal is maximal, while for $\mathbb{Z}[X]$ the ideal (f) is properly contained in, for example, $(f, 2) < \mathbb{Z}[X]$, thus is not maximal.
   Now we prove the claim. Suppose for contradiction $f = gh$ over $\mathbb{Z}$ where neither of g, h is a constant polynomial. Then $X^3 - 3X + 9 = X^3 - X + 1 \in \mathbb{Z}_2[X]$ would have the same decomposition into g and h. Since f is monic, g and h are monic so remain non-constant over $\mathbb{Z}_2$. But since 0 and 1 (the only elements in $\mathbb{Z}_2$) are not roots of $X^3 - X + 1$, the element $X^3 - X + 1 \in \mathbb{Z}_2[X]$ is irreducible, a contradiction.
   (c) Does the element $X^3 - 3X + 9 \in \mathbb{Z}_7[X]$ generate a prime ideal in $\mathbb{Z}_7[X]$? Is the ideal maximal? Justify your answers.

   The element $1 \in \mathbb{Z}_7$ is a root of $X^3 - 3X + 9$ since $1^3 - 3 + 9 = 7 = 0 \in \mathbb{Z}_7$. Thus, $X^3 - 3X + 9$ is reducible over $\mathbb{Z}_7$. Since $\mathbb{Z}_7[X]$ is a PID, this implies $X^3 - 3X + 9$ generates an ideal that is neither prime nor maximal.

4. (5 pt) Let R be a commutative ring and suppose the set $R \setminus R^\times$ is an ideal in R.
   (a) Prove that the characteristic of R is either zero or a power of a prime.

   Let R be as above and suppose for contradiction that the characteristic of R is (not zero and is) divisible by two prime numbers $p \neq q$. Consider the ideals (p) and (q) in R (where $p = p1_R$ and $q = q1_R$ are elements in R). Since p, q are coprime, there is k, m such that $pk + qm = 1$, so the ideal generated by p and q is R. It follows that either (p) or (q) is not contained in the ideal $I := R \setminus R^\times$. However, any proper ideal of R is contained in $R \setminus R^\times$; otherwise it contains some $u \in R^\times$ but $uR = R$. Therefore, we have either $(p) = R$ or $(q) = R$, which contradicts the assumption that p, q divide the characteristic of R.
   (b) Given n, either zero or a prime power, can you find a ring R as above such that $\operatorname{char} R = n$?

   Yes. If R is a field then $R \setminus R^\times = \{0\}$ is an ideal, so for $n = 0$ we can take any field of characteristic zero. For $n = p^r$ for a prime p and $r \in \mathbb{N}$, the ring $R = \mathbb{Z}/p^r$ satisfy the condition since $R \setminus R^\times = pR$ is an ideal in R.

5. (5 pt) Let K be a field, $f \in K[X]$ be an irreducible polynomial, and let $\alpha, \beta \in \overline{K} \setminus K$ be such that $f(\alpha) = f(\beta) = 0$.
   (a) Is the field extension $K \subseteq K(\alpha)$ finite? Justify your answer.

   Yes. Since α is a root of f, the degree $[K(\alpha) : K]$ is bounded by the degree of f.

(b) Show that $K(\alpha)$ is K-isomorphic to $K(\beta)$. (Construct a K-isomorphism $K(\alpha) \to K(\beta)$.)

Since f is irreducible, it is the minimal polynomial of both α and β. Thus, we have the K-isomorphism $\phi : K[X]/(f) \cong K(\alpha)$ sending X to α and similarly the K-isomorphism $\psi : K[X]/(f) \cong K(\beta)$ sending X to β. Then $\psi \circ \phi^{-1}$ is a K-isomorphism from $K(\alpha)$ to $K(\beta)$.

(c) Can the group $Aut_K(K(\alpha))$ be infinite? Can it be trivial? Justify your answers.

No and yes.

Since a K-automorphism on $K(\alpha)$ is determined by it s values on α. But α must be sent to a root of f in $K(\alpha)$. Thus the order of $Aut_K(K(\alpha)$ is bounded by the degree of f which is finite. Moreover, if f has only one root, namely α, in $K(\alpha)$ then $Aut_K(K(\alpha))$ is trivial. An example of the latter is when $f = X^3 - 3$ and $K = \mathbb{Q}$. See Proplem 7.

6. (5 pt) Let E be a finite field and let $K \subseteq E$ be a subfield. Prove or disprove: the extension $K \subseteq E$ is

(a) normal;

(b) separable.

Let q be the order of E. Since $E^\times = E \setminus \{0\}$ is cyclic, any nonzero element of E is a root of $X^{q-1} - 1 \in K[X]$ and all elements of E are roots of $X(X^{q-1} - 1) = X^q - X =: f$. For degree reason, it follows that E consists exactly of the roots of $f \in K[X]$. So E is a splitting field of f over K, that is, $K \subseteq E$ is normal. Again, for degree reason, the polynomial f has q distinct roots and is separable. Thus $K \subseteq E$ is separable.

7. (5 pt) Consider the polynomial $f = X^3 - 3 \in \mathbb{Q}[X]$ and let E be its splitting field (over $\mathbb{Q}$).

(a) Prove that $\mathbb{Q} \subseteq E$ is Galois.

Over $\overline{\mathbb{Q}} \subset \mathbb{C}$, we have $f = (X - \sqrt[3]{3})(X - \sqrt[3]{3}\zeta)(X - \sqrt[3]{3}\zeta^2)$ where ζ is a third root of 1 in $\mathbb{C}$ (we can let $\zeta = e^{2\pi i/3}$). Thus E is a splitting field of a separable polynomial, thus Galois.

(b) Compute the Galois group $Gal(E/\mathbb{Q})$.

Since E is generated over $\mathbb{Q}$ by $a = \sqrt[3]{3}$, $b = a\zeta$, $c = a\zeta^2$, a $\mathbb{Q}$-automophism on E is determined by its values on a, b, c. It also needs to send a, b, c, which are the roots of f, to the roots of f. Therefore, we can view the $\mathbb{Q}$-automorphisms as permuataions on the set $\{a, b, c\} \cong \{1, 2, 3\}$, providing $G := Gal(E/\mathbb{Q}) \hookrightarrow S_3$. Since the order of G is $[E : \mathbb{Q}] = [E : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] = 2 \cdot 3 = |S_3|$ we have in fact $G \cong S_3$.

(c) Find all subfields $\mathbb{Q} \subseteq F \subseteq E$.

By the Galois correspondence, such subfields are exactly the fixed fields of the subgroups of G which we found in Problem 1 (c). They are $E, \mathbb{Q}(b), \mathbb{Q}(a), \mathbb{Q}(c), \mathbb{Q}(\zeta), \mathbb{Q}$.

(d) Which of these F are Galois over $\mathbb{Q}$, and what are their Galois groups $Gal(F/\mathbb{Q})$?

By the Galois correspondence, these F are exactly the fixed fields of the normal subgroups of G and the Galois groups are the quotients groups. We found these in Problem 1(d). They are $E, \mathbb{Q}(\zeta), \mathbb{Q}$ and the corresponding Galois groups $S_3, \mathbb{Z}_2, \{e\}$ respectively.