Algebra Comprehensive Exam Spring 2022, old style Solutions

Brookfield, Krebs*, Liu

Answer five (5) questions only. You must answer *at least one* from each of groups, rings, and fields. Indicate CLEARLY which problems you want us to grade; otherwise, we will select the first problem from each section, and then the first two additional problems answered after that. Be sure to show enough work that your answers are adequately supported. Tip: When a question has multiple parts, the later parts often (but not always) make use of the earlier parts.

Notation: Unless otherwise stated, $\mathbb{Q}, \mathbb{Z}, \mathbb{Z}_n, \mathbb{C}$, and $\mathbb{R}$ denote the sets of rational numbers, integers, integers modulo n, complex numbers, and real numbers respectively, regarded as groups or rings in the usual way.

Groups

(1) Let a and b be elements of a finite group G. Show that $|ab| = |ba|$. (Here $|x|$ denotes the order of the element $x \in G$.)
Solution: First we prove that $|a^{-1}ba| = |b|$. Define $\phi : G \to G$ and $\psi : G \to G$ by

$$\phi(x) = a^{-1}xa \qquad \psi(x) = axa^{-1}$$

for all $x \in G$. Then ϕ and ψ are inverse automorphisms. Because automorphisms send subgroups to subgroups and generators to generators, $\langle b\rangle$ is isomorphic to $\phi(\langle b\rangle) = \langle \phi(b)\rangle = \langle a^{-1}ba\rangle$. In particular, $|b| = |\langle b\rangle| = |\langle a^{-1}ba\rangle| = |a^{-1}ba|$.
Now replace b by ab in $|b| = |a^{-1}ba|$ to get $|ab| = |a^{-1}(ab)a| = |ba|$.

(2) Let G be a finite group and $p \in \mathbb{N}$ a prime number. Show the following:

(a) If every element of G is contained in a subgroup of order p, then $|G| = p^n$ for some positive integer n.
(b) If every element of G is contained in a normal subgroup of order p, then G is abelian.

Solution:

(a) Let q be a prime number that divides $|G|$. Then, by Cauchy's Theorem, G contains an element of order q. Since elements in G have order 1 or p, we have $q = p$. So the only prime number that divides $|G|$ is p, and $|G|$ is a power of p.
(b) Let $h, k \in G$. If $h = 1$ or $k = 1$ then $hk = kh$ is immediate. Otherwise $H = \langle h\rangle$ and $K = \langle k\rangle$ are normal subgroups of order p. If $H = K$, then h and k commute because all groups of order p are abelian. If $H \neq K$, then $h^{-1}k^{-1}hk \in H \cap K = \{1\}$, so $h^{-1}k^{-1}hk = 1$, which can be written as $hk = kh$.

(3) Let $n \geq 2$ be an integer. Let A_n and S_n be the alternating and symmetric groups on n letters, respectively. Let $\tau \in S_n$ be a transposition. Define $\varphi\colon A_n \to S_n$ by $\varphi(\sigma) = \tau\sigma\tau$.

(a) Prove that φ is a homomorphism.
(b) Find the kernel of φ.
(c) Is φ injective? Prove that your answer is correct. Hint: Use your answer from (b).
(d) Is φ an isomorphism from A_n to S_n? Prove that your answer is correct. Hint: Consider the orders of these groups.

Solutions
(a) For all $\sigma_1, \sigma_2 \in A_n$, we have that $\varphi(\sigma_1\sigma_2) = \tau\sigma_1\tau\tau\sigma_2\tau = \tau\sigma_1\sigma_2\tau = \varphi(\sigma_1\sigma_2)$. Here we use that $\tau^2 = \iota$, because τ is a transposition. We use ι to denote the identity element of S_n.
(b) We have that

$$\begin{aligned}\ker(\varphi) &= \{\sigma \in A_n \mid \varphi(\sigma) = \iota\} \\ &= \{\sigma \in A_n \mid \tau\sigma\tau = \iota\} \\ &= \{\sigma \in A_n \mid \sigma\tau = \tau^{-1} = \tau\} \\ &= \{\sigma \in A_n \mid \sigma = \iota\} \\ &= \{\iota\}\end{aligned}$$

(c) By part (b), because the kernel is trivial, therefore φ is injective.
(d) The mapping φ cannot be bijective, because $|A_n| = n!/2 < n! = |S_n|$. So φ is not an isomorphism.

Rings

(1) Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$, a subring of $\mathbb{C}$, and define the function $\phi : R \to \{0, 1, 2, 3, ...\}$ by

$$\phi(a + b\sqrt{-5}) = a^2 + 5b^2$$

for all $a, b \in \mathbb{Z}$. Show the following for all $\alpha, \beta \in R$:

(a) $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$
(b) $\phi(\alpha) = 1$ if and only if α is a unit of R.
(c) If $\phi(\alpha)$ is prime, then α is irreducible.

Solution:

(a)

$$\begin{aligned}\phi\left((a + b\sqrt{-5})(c + d\sqrt{-5})\right) &= \phi(ac - 5bd + (bc + ad)\sqrt{-5}) \\ &= (ac - 5bd)^2 + 5(bc + ad)^2 \\ &= a^2c^2 + 25b^2d^2 + 5b^2c^2 + 5a^2d^2 \\ &= (a^2 + 5b^2)(c^2 + 5d^2) \\ &= \phi(a + b\sqrt{-5})\phi(c + d\sqrt{-5})\end{aligned}$$

(b) If $\alpha \in R$ is a unit, then there exists some $\beta \in R$ such that $\alpha\beta = 1$. Applying ϕ to this equation gives $\phi(\alpha)\phi(\beta) = 1$ and so $\phi(\alpha) = 1$ (from the definition $\phi(\alpha) \geq 0$).

Conversely, if $\phi(\alpha) = 1$ with $\alpha = a + b\sqrt{-5}$, then $a^2 + 5b^2 = 1$. The only solution in integers of this is $a = \pm 1$ and $b = 0$. So $\alpha = \pm 1$ and α is obviously a unit.

(c) Suppose that $\phi(\alpha) = p$ is prime. Since $p \neq 1$, α is not a unit. Now suppose that $\alpha = \beta\gamma$ for some $\beta, \gamma \in R$. Then $\phi(\beta)\phi(\gamma) = \phi(\alpha) = p$. Since p is prime, either $\phi(\beta) = 1$ or $\phi(\gamma) = 1$, and so β or γ is a unit. This shows that α is irreducible.

(2) Let

$$R = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z} \right\}.$$

You may assume without proof that R is a ring under ordinary matrix multiplication. Let

$$K = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \;\middle|\; a \in \mathbb{Z} \right\}.$$

(a) Define $\phi\colon R \to \mathbb{Z}$ by

$$\phi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\right) = a - b.$$

Prove that ϕ is a homomorphism.

(b) Prove that K is the kernel of ϕ.

(c) Prove that $R/K \cong \mathbb{Z}$.

(d) Prove that K is a prime ideal of R.

(e) Prove that K is not a maximal ideal of R.

Solution:
See the last problem at:
http://ramanujan.math.trinity.edu/rdaileda/teach/m4363s07/HW4_soln.pdf

(3) A polynomial $p(x) \in \mathbb{Z}[x]$ is called *primitive* if the greatest common divisor of all its coefficients is 1.

(a) Let $g(x), h(x)$ be primitive polynomials in $\mathbb{Z}[x]$. Prove that $g(x)h(x)$ is also primitive in $\mathbb{Z}[x]$.

(b) Use (a) to show that $p(x)$ is irreducible in $\mathbb{Z}$ if and only if it is irreducible in $\mathbb{Q}$.

Solution:
https://web.ma.utexas.edu/users/lpbowen/m373k/notes20.pdf

Fields

(1) Prove that $\pi + \sqrt{2}$ is transcendental over $\mathbb{Q}$. You can assume that π is transcendental over $\mathbb{Q}$.

Solution: Let $\alpha = \pi + \sqrt{2}$. Suppose, to the contrary, that α is algebraic over $\mathbb{Q}$. Then $\mathbb{Q}(\alpha)$ is a finite extension of $\mathbb{Q}$. Since $(\alpha - \pi)^2 = 2$, π is a root of the polynomial $x^2 - 2\alpha x + \alpha^2 - 2 \in \mathbb{Q}(\alpha)[x]$, and so π has at most degree 2 over $\mathbb{Q}(\alpha)$, in particular, $\mathbb{Q}(\alpha, \pi)$ is a finite extension of $\mathbb{Q}(\alpha)$. Since each of the extensions in the tower

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \pi)$$

is finite, $\mathbb{Q}(\alpha, \pi)$ is a finite extension of $\mathbb{Q}$. But then, because $\pi \in \mathbb{Q}(\alpha, \pi)$, this implies that π is algebraic over $\mathbb{Q}$, a contradiction.

(2)

(a) Prove that $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$.

(b) Prove that $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ is reducible over $\mathbb{Q}(\sqrt{5})$. Hint: Suppose that $f(x) = (x^2 + ax + 1)(x^2 + bx + 1)$ for some $a, b \in \mathbb{C}$. What are a and b?

Solution:

(a) Let $g(x) = f(x+1) = x^4 + 5x^3 + 10x^2 + 10x + 5$. Then $g(x)$ is irreducible over $\mathbb{Q}$ by the Eisenstein criterion with $p = 5$. Specifically, 5 divides all terms except the first and 5^2 does not divide the constant term. Since $f(x)$ is just a translation of $g(x)$, $f(x)$ is also irreducible over $\mathbb{Q}$.

(b) Matching coefficients in $f(x) = (x^2 + ax + 1)(x^2 + bx + 1)$ we get $a + b = 1$ and $ab = -1$. Thus a and b are the roots of $x^2 - x - 1$, namely $a, b = (1 \pm \sqrt{5})/2 \in \mathbb{Q}(\sqrt{5})$. (Or eliminating b from $a + b = 1$ and $ab = -1$ gives $a^2 - a - 1 = 0$, so $a = (1 \pm \sqrt{5})/2 \in \mathbb{Q}(\sqrt{5})$.) Hence $f(x)$ is reducible over $\mathbb{Q}(\sqrt{5})$.

(3) Let $f(x) = (x^2 - 7)(x^2 - 11)(x^2 - 13) \in \mathbb{Q}[x]$. Let E be the splitting field of f over $\mathbb{Q}$.

(a) Determine the Galois group G of E over $\mathbb{Q}$.

(b) Explicitly write down the elements of a subgroup of G whose fixed field is $\mathbb{Q}(\sqrt{77})$.

Solution:

(a) The Galois group G contains elements

$$\alpha\colon \sqrt{7} \mapsto -\sqrt{7}, \sqrt{11} \mapsto \sqrt{11}, \sqrt{13} \mapsto \sqrt{13} \text{ and}$$

$$\beta\colon \sqrt{7} \mapsto \sqrt{7}, \sqrt{11} \mapsto -\sqrt{11}, \sqrt{13} \mapsto \sqrt{13} \text{ and}$$

$$\gamma\colon \sqrt{7} \mapsto \sqrt{7}, \sqrt{11} \mapsto \sqrt{11}, \sqrt{13} \mapsto -\sqrt{13} \text{ and}$$

Then α, β, γ generate G, which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) Let $H = \{\mathrm{id}, \alpha, \beta\gamma, \alpha\beta\gamma\}$. Then the fixed field of H is $\mathbb{Q}(\sqrt{77})$.