Algebra Comprehensive Exam Spring 2021, old style Solutions

Brookfield, Krebs*, Shaheen

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 G be a group. Let H and K be normal subgroups of G. Prove that (i) $H \cap K$ is a subgroup of G, and (ii) $H \cap K$ is normal in G.

Solution:
https://martin-thoma.com/intersection-two-normal-subgroups-normal-subgroup/

(2) Let G be a group. Let $a, b \in G$. Let

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

be the dihedral group with $2n$ elements, where 1 denotes the identity element, and $s^2 = r^n = 1$, and $rs = sr^{n-1}$. Prove that there exists a homomorphism $\phi\colon D_{2n} \to G$ such that $\phi(r) = a$ and $\phi(s) = b$ if and only if $|a|$ divides n and $|b| \leq 2$ and $ab = ba^{-1}$. Here $|x|$ denotes the order of the element x.

Solution:
First, suppose such a homomorphism exists. We will show that $|a|$ divides n and $|b| \leq 2$ and $ab = ba^{-1}$.
Because $\phi(r) = a$, we have that $e = \phi(1) = \phi(r^n) = \phi(r)^n = a^n$, from which it follows that $|a|$ divides n. Here e denotes the identity element of G, and we make use of the fact that a homomorphism maps the identity element to the identity element.
Simlarly, because $\phi(s) = b$, we have that $1 = \phi(s^2) = \phi(s)^2 = b^2$, from which it follows that $|b|$ divides 2, so $|b| = 1$ or $|b| = 2$.
Finally, $ab = \phi(r)\phi(s) = \phi(rs) = \phi(sr^{-1}) = \phi(s)\phi(r)^{-1} = ba^{-1}$.

Now we prove the converse. That is, suppose that $|a|$ divides n and $|b| \leq 2$ and $ab = ba^{-1}$. We will show that there exists a homomorphism $\phi\colon D_{2n} \to G$ such that $\phi(r) = a$ and $\phi(s) = b$.
Define $\phi\colon D_{2n} \to G$ by $\phi(s^i r^j) = b^i a^j$ for all $i, j \in \mathbb{Z}$.
Because the same input can be represented in more than one way, we must show that ϕ is well-defined.

Suppose $s^i r^j = s^k r^m$ for some integers i, j, k, m. We will show that $b^i a^j = b^k a^m$.
From $s^i r^j = s^k r^m$ we get that $i \equiv k \pmod 2$ and $j \equiv m \pmod n$.
Because $|b| \leq 2$, we know that $|b| = 1$ or $|b| = 2$, so in either case, $b^2 = e$. Hence $b^{i-k} = e$.
Because $|a|$ divides n, we have that $a^n = e$, so $a^{j-m} = e$.
Multiplying these two equations, we get $b^{i-k} a^{j-m} = e$. Multiply by b^k on the left and a^m on the right to get $b^i a^j = b^k a^m$.
Therefore ϕ is well-defined.
Next, we will show that ϕ is a homomorphism.
Let $s^i r^j, s^k r^m \in D_{2n}$. Then

$$\phi(s^i r^j \cdot s^k r^m) = \phi(s^{i+k} \cdot r^{m-j}) = b^{i+k} \cdot a^{m-j} = b^i a^j \cdot b^k a^m = \phi(s^i r^j)\phi(s^k r^m).$$

Here we get $r^j \cdot s^k = s^k r^{-j}$ by repeatedly applying the relation $rs = sr^{n-1}$. Same goes for a and b in lieu of r and s.
Finally, $\phi(r) = \phi(s^0 r^1) = b^0 a^1 = a$ and $\phi(s) = \phi(s^1 r^0) = b^1 a^0 = b$.

(3) Let A_4 be the alternating group on 4 letters. Let $K = \{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Here ι denotes the identity element of A_4.

(i) Prove that K is a subset of A_4.

(ii) Prove that K is a subgroup of A_4.

(iii) You may assume without proof that K is a normal subgroup of A_4. (It is.) Find a familiar group isomorphic to the quotient group A_4/K, and prove that your answer is correct.

Solutions
(i) All four elements of K are even permutations.

(ii) We are given that $\iota \in K$.
Let $a = (1\ 2)(3\ 4), b = (1\ 3)(2\ 4), c = (1\ 4)(2\ 3)$.
Then $a^2 = b^2 = c^2 = \iota$. Also, $ab = ba = c, ac = ca = b, bc = cb = a$. So K is closed under the group operation.
Finally, every element in K is its own inverse, so K is closed under inverses.

(iii) We know that $|A_4| = 4!/2 = 24/2 = 12$. So $|A_4/K| = |A_4|/|K| = 12/4 = 3$. Because 3 is prime, by a corollary to Lagrange's theorem, we have that A_4/K is cyclic of order 3, hence isomorphic to the group of integers mod 3 under addition.

Rings

(1) Let R be a commutative ring with identity $1 \neq 0$. Let I be an ideal of R. Prove that I is a prime ideal if and only if R/I is an integral domain.
Solution:
https://math.stackexchange.com/questions/1052380/prove-that-i-subseteq-r-is-prime-if-and-only-if-r-i-is-an-integ
1052392

(2) Let R be a commutative ring with identity $1 \neq 0$. Prove that R is a field if and only if the only ideals of R are the ideals $\{0\}$ and R.
https://math.stackexchange.com/questions/101157/a-commutative-ring-is-a-field-iff-the-only-ideals-are-0-and-1

(3) Let $\mathbb{R}[x]$ be the ring of polynomials over the real numbers. Find a maximal ideal I of $\mathbb{R}[x]$ so that $\mathbb{R}[x]/I \cong \mathbb{R}$, and prove that your answer is correct.

Solution:
Let $I = \langle x \rangle$. Define $\phi\colon \mathbb{R}[x] \to \mathbb{R}$ by $\phi(f) = f(0)$. Then ϕ is a surjective ring homomorphism with kernel I. By the first isomorphism theorem, we have that $\mathbb{R}[x]/I \cong \mathbb{R}$. Hence $\mathbb{R}[x]/I$ is a field, which implies that I is a maximal ideal.

Fields

(1) Let $f(x) = (x^2-2)(x^2-3)(x^2-5) \in \mathbb{Q}[x]$. Let E be the splitting field of f over $\mathbb{Q}$.

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

(ii) Explicitly write down the elements of a subgroup of G whose fixed field is $\mathbb{Q}(\sqrt{15})$.

The Galois group G contains elements

$$\alpha\colon \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}, \sqrt{5} \mapsto \sqrt{5} \text{ and}$$

$$\beta\colon \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}, \sqrt{5} \mapsto \sqrt{5} \text{ and}$$

$$\gamma\colon \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3}, \sqrt{5} \mapsto -\sqrt{5} \text{ and}$$

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

(ii) Let $H = \{\mathrm{id}, \alpha, \beta\gamma, \alpha\beta\gamma\}$. Then the fixed field of H is $\mathbb{Q}(\sqrt{15})$.

(2) Let F be a finite field containing exactly 81 elements. Prove that every element of F has a ninth root. In other words, prove that for every $y \in F$, there exists $x \in F$ such that $x^9 = y$. Hint: Use what you know about $F^\times$, the group of units of F.

Solution: Here's a solution that works more generally when $|F| = 3^n$ for some positive integer n.
Let $y \in F$. If $y = 0$, then by taking $x = 0$, we are done. So we assume that $y \neq 0$.
Let $F^\times$ be the group of units of F, so $y \in F^\times$. Then $F^\times$ is a cyclic group of order $3^n - 1$. Let g be a generator for $F^\times$, so g has order $3^n - 1$. We have that $y = g^b$ for some integer b. Note that 3 does not divide $3^n - 1$, so 3 and $3^n - 1$ are relatively prime, which implies that 9 and $3^n - 1$ are relatively prime. Let a be a multiplicative inverse of 9 modulo $3^n - 1$. Thus $9a \equiv 1 \pmod{3^n - 1}$, from which it follows that $9a = 1 + k(3^n - 1)$ for some integer k. Let $x = y^a = g^{ab}$. Then

$$x^9 = \left(g^{9a}\right)^b = \left(g^{1+k(3^n-1)}\right)^b = \left(g \cdot g^{k(3^n-1)}\right)^b = g^b = y.$$

(3) Let $F \subseteq E$ be fields and $\alpha, \beta \in E$. Prove the equivalence of the following two statements:

(i) α and β have the same minimal polynomial over F.

(ii) For all $f \in F[x]$, $f(\alpha) = 0$ if and only if $f(\beta) = 0$.

(Aside: Either of these conditions could be used as the definition of α and β being conjugate over F.)
Solution:

First we will show that (i) implies (ii). Suppose (i) holds. We will show that (ii) holds.
Let $f \in F[x]$. Suppose $f(\alpha) = 0$. We will show that $f(\beta) = 0$.
Let m_α be the minimal polynomial of α over F, and let m_β be the minimal polynomial of β over F. We are given that $m_\alpha = m_\beta$. Because $f(\alpha) = 0$, it follows that m_α divides f in $F[x]$. So $f = m_\alpha g = m_\beta g$ for some $g \in F[x]$. Hence $f(\beta) = m_\beta(\beta)g(\beta) = 0 \cdot g(\beta) = 0$.
Reversing the roles of α and β proves the other direction.

First we will show that (ii) implies (i). Suppose (ii) holds. We will show that (i) holds.
Let m_α be the minimal polynomial of α over F, and let m_β be the minimal polynomial of β over F.
We know that $m_\alpha(\alpha) = 0$. So by (ii), we have that $m_\beta(\alpha) = 0$. Therefore m_α divides m_β in $F[x]$. That is, $m_\alpha \cdot g = m_\beta$ for some $g \in F[x]$.
Reversing the roles of α and β, we get that $m_\beta \cdot h = m_\alpha$ for some $h \in F[x]$.
Hence $m_\alpha \cdot g \cdot h = m_\alpha$. But m_α is irreducible, and $F[x]$ is a UFD. Therefore gh is a unit. In other words, $gh = c$ for some constant polynomial c. Because minimal polynomials are monic, it follows that $c = 1$, which gives us $m_\alpha = m_\beta$.