ALGEBRA COMPREHENSIVE EXAMINATION

Fall 2016

Brookfield, Demeke, Shaheen*

<ins>Directions</ins>: *Answer 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 which ones to grade, and they may not be the ones that you want us to grade. Be sure to show enough work that your answers are adequately supported.

<ins>Notation</ins>: $\mathbb{Q}$ denotes the rational numbers; $\mathbb{Z}_n$ denotes the integers modulo n; $\mathbb{N}$ denotes the natural numbers.

Groups

(G1) Let G be a group. Suppose that H is a subgroup of G and N is a normal subgroup of G. Prove that

$$NH = \{nh \mid n \in N, h \in H\}$$

is a subgroup of G.

`Answer:` [See F08] Of course, $K \neq \emptyset$ and $H \neq \emptyset$, so $KH \neq \emptyset$. Suppose $x_1, x_2 \in KH$. Then $x_1 = k_1h_1$ and $x_2 = k_2h_2$, with $k_1, k_2 \in K$ and $h_1, h_2 \in H$. Since K is normal, $h_1h_2^{-1}k_2^{-1} \in h_1h_2^{-1}K = Kh_1h_2^{-1}$ and so $h_1h_2^{-1}k_2^{-1} = k_3h_1h_2^{-1}$ for some $k_3 \in K$. This implies

$$x_1x_2^{-1} = k_1h_1h_2^{-1}k_2^{-1} = k_1k_3h_1h_2^{-1} \in KH.$$

By the subgroup criterion, $KH \leq G$.

(G2) Let G be a finite group and H be a subgroup of G.

(a) Prove that for any $g \in G$, that gH and H have the same size.

(b) Prove for any $a, b \in G$, that either $aH \cap bH = \emptyset$ or $aH = bH$.

(c) Use (a) and (b) to prove Lagrange's theorem.

`Answer:` See, for example, Fraleigh, Section 10.

(G3) Find all Sylow 2-subgroups of the dihedral group

$$D_{12} = \{1, r, r^2, r^3, r^4, r^5, s, sr, sr^2, sr^3, sr^4, sr^5\}$$

with $|r| = 6$, $|s| = 2$ and $rs = sr^{-1}$. Feel free to use the fact that $r^n s = sr^{-n}$ for all $n \in \mathbb{Z}$.

`Answer:` By Sylow's Theorem the number of Sylow 2-subgroups, n_2, satisfies $n_2 \equiv 1 \mod 2$ and $n_2|12$, so $n_2 = 1$ or $n_2 = 3$. We show, in fact, that $n_2 = 3$.

Sylow 2-subgroups have order 4, and any subgroup of order 4 is a Sylow 2-subgroup. Since D_{12} contains no elements of order 4, the Sylow 2-subgroups must be isomorphic to the Klein group and so each contains 3 pairwise commuting elements of order 2. D_{12} contains 7 elements of order 2: $r^3, s, sr, sr^2, sr^3, sr^4, sr^5$. Because $sr^3 = r^3s$, r^3 commutes with all elements of D_{12}, so any subgroup generated by r^3 and another element of order 2 will be isomorphic to the Klein group. Thus the Sylow 2-subgroups are

$$G_1 = \langle r^3, s\rangle = \langle r^3, sr^3\rangle = \{1, r^3, s, sr^3\}$$
$$G_2 = \langle r^3, sr\rangle = \langle r^3, sr^4\rangle = \{1, r^3, sr, sr^4\}$$
$$G_3 = \langle r^3, sr^2\rangle = \langle r^3, sr^5\rangle = \{1, r^3, sr^2, sr^5\}$$

Rings

(R1) Prove or disprove: $2\mathbb{Z}$ and $3\mathbb{Z}$ are isomorphic as rings.

`Answer:` These rings are not isomorphic. For example, the equation $x + x = x^2$ has two solutions ($x = 0, 2$) in $2\mathbb{Z}$, but only one solution ($x = 0$) in $3\mathbb{Z}$.

OR

Suppose that $\phi : 2\mathbb{Z} \to 3\mathbb{Z}$ is a ring homomorphism. Then $\phi(2) = 3k$ for some $k \in \mathbb{Z}$. Then

$$\phi(4) = \phi(2 + 2) = \phi(2) + \phi(2) = 6k$$

and

$$\phi(4) = \phi(2 \cdot 2) = \phi(2) \cdot \phi(2) = 9k^2.$$

Thus $6k = 9k^2$. The only integer satisfying this equation is $k = 0$, and so $\phi(2) = 0$. Because we also have $\phi(0) = 0$, ϕ is not injective, and so ϕ is not an isomorphism.

(R2) Let $\phi : R \to S$ be an onto ring homomorphism with kernel K. Prove the following. [For each part prove that the given set is an ideal and that it is prime.]

(a) If P is a prime ideal of R that contains K, then $\phi(P)$ is a prime ideal of S.

(b) If Q is a prime ideal of S, then $\phi^{-1}(Q)$ is a prime ideal of R that contains K.

`Answer:`

(a) Suppose that P is a prime ideal of R that contains K.

a)) Let $s_1, s_2 \in \phi(P)$. Then $s_1 = \phi(r_1)$ and $s_2 = \phi(r_2)$ for some $r_1, r_2 \in P$. Then $s_1 - s_2 = \phi(r_1) - \phi(r_2) = \phi(r_1 - r_2) \in \phi(P)$ because $r_1 - r_2 \in P$. This means that $\phi(P)$ is a subgroup of $(S, +)$.

b)) If $q \in \phi(P)$ and $s \in S$, then, since ϕ is surjective, $\phi(r) = s$ and $q = \phi(p)$ for some $r \in R$ and $p \in P$. Then $sq = \phi(r)\phi(p) = \phi(rp) \in \phi(P)$ because P is an ideal and $rp \in P$. This shows that $\phi(P)$ is an ideal.

c)) Suppose that $s_1, s_2 \in S$ are such that $s_1 s_2 \in \phi(P)$. Then there are $r_1, r_2 \in R$ and $p \in P$ such that $s_1 = \phi(r_1)$, $s_2 = \phi(r_2)$ and $s_1 s_2 = \phi(p)$. This implies $\phi(p) = s_1 s_2 = \phi(r_1)\phi(r_2) = \phi(r_1 r_2)$ and so $r_1 r_2 - p \in \ker \phi = K \subseteq P$. Since P is closed under addition $r_1 r_2 \in P$. Because P is prime, either $r_1 \in P$ and hence $s_1 \in \phi(P)$, or $r_2 \in P$ and hence $s_2 \in \phi(P)$. This makes $\phi(P)$ a prime ideal.

(b) Suppose that Q is a prime ideal of S.

a)) Let $q_1, q_2 \in \phi^{-1}(Q)$. Then $\phi(q_1), \phi(q_2) \in Q$ and so $\phi(q_1 - q_2) = \phi(q_1) - \phi(q_2) \in \mathbb{Q}$, that is, $q_1 - q_2 \in \phi^{-1}(Q)$. This means that $\phi^{-1}(Q)$ is a subgroup of $(R, +)$.

b)) Let $r \in R$ and $q \in \phi^{-1}(Q)$. Then $\phi(q) \in Q$ and $\phi(rq) = \phi(r)\phi(q) \in Q$, since Q is an ideal, and so $rq \in \phi^{-1}(Q)$. This means that $\phi^{-1}(Q)$ is an ideal of R.

c)) If $k \in K$, then $\phi(k) = e \in Q$ and so $k \in \phi^{-1}(Q)$. This means that $K \leq Q$.

d)) Suppose that $r_1, r_2 \in R$ satisfy $r_1 r_2 \in \phi^{-1}(Q)$. Then $\phi(r_1)\phi(r_2) = \phi(r_1 r_2) \in Q$. Since Q is prime, either $\phi(r_1) \in Q$ or $\phi(r_2) \in Q$. Thus either $r_1 \in \phi^{-1}(Q)$ or $r_2 \in \phi^{-1}(Q)$. This means that $\phi^{-1}(Q)$ is a prime ideal.

(R3) Let I and J be ideals of a domain R. Show that $K = \{r \in R \mid rI \subseteq J\}$ is an ideal of R.

`Answer:` First $0 \in K$ because $0I = \{0\} \subseteq J$.

Let $a, b \in K$. Then, for all $i \in I$, we have $ai \in aI \subseteq J$ and $bi \in bI \subseteq J$. Since J is an ideal, $(a - b)i = ai - bi \in J$. Since this holds for all $i \in I$, we have shown that $a - b \in K$, and that K is a subgroup of $(R, +)$.

Let $a \in K$ and $r \in R$. Then, for all $i \in I$, we have $ai \in aI \subseteq J$. Since J is an ideal, $(ra)i = r(ai) \in J$. Since this holds for all $i \in I$, we have $(ra)I \subseteq J$, that is, $ra \in K$.

Fields

(F1) Let σ be a field automorphism of $\mathbb{Q}$. Prove that σ is the identity map.

`Answer:` [See F04] Because σ is a field homomorphism we have $\sigma(1) = 1$, and then, because σ is a group homomorphism from $(\mathbb{Q}, +)$ to itself, we have $\sigma(n) = n$ for all $n \in \mathbb{Z}$. (For example, $\sigma(2) = \sigma(1+1) = \sigma(1) + \sigma(1) = 1 + 1 = 2$.)

Now let $r = p/q \in \mathbb{Q}$ with $p, q \in \mathbb{Z}$ and $q \neq 0$. Then $\sigma(p) = p$, $\sigma(q) = q$ and $p = rq$, so

$$p = \sigma(p) = \sigma(rq) = \sigma(r)\sigma(q) = \sigma(r)q.$$

Dividing by q we get $\sigma(r) = p/q = r$.

Since this holds for all $r \in \mathbb{Q}$, σ is the identity map.

(F2) Prove that every finite integral domain is a field.

`Answer:` [See F02, F07, F08] Fraleigh, Theorem 19.11

(F3) Let E be the splitting field for $f(x) = x^3 + 2$ over $\mathbb{Z}_7$. Calculate $[E : \mathbb{Z}_7]$. Hint: $\mathbb{Z}_7$ contains three cube roots of unity. Find them.

`Answer:` From the table below we see that 1, 2 and 4 are cube roots of 1 and that f has no zeros in $\mathbb{Z}_7$.

$x =$	0	1	2	3	4	5	6
$x^3 =$	0	1	1	6	1	6	6
$f(x) = x^3 + 2 =$	2	3	3	1	3	1	1

Thus f is irreducible over $\mathbb{Z}_7$ and, if α is a zero of f in E, then $[\mathbb{Z}_7(\alpha) : \mathbb{Z}_7] = \deg f = 3$. Because 1, 2 and 4 are cube roots of 1, the zeros of f are α, 2α and 4α. Thus all zeros of f are in $\mathbb{Z}_7(\alpha)$, the slitting field for f is $\mathbb{Z}_7(\alpha)$, $E = \mathbb{Z}_7(\alpha)$ and $[E : \mathbb{Z}_7] = [\mathbb{Z}_7(\alpha) : \mathbb{Z}_7] = 3$.