ALGEBRA COMPREHENSIVE EXAMINATION

Spring 2017

Akis, Brookfield*, Shaheen

Directions: *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.

Notation: $\mathbb{Q}$ is the set of rational numbers. $\mathbb{Z}_n$ is set of integers modulo n. $\mathbb{N}$ is the set of natural numbers. $\mathbb{R}$ is the set of real numbers.

Groups

(G1) Let G be a nonabelian group of order 10. Show that G contains elements r and s such that $|r| = 5$, $|s| = 2$ and $|sr| = 2$.

`Answer:` [Compare S13] Since G is not abelian it contains no elements of order 10. Thus all nonidentity elements have order 2 or 5. By the Sylow Theorems, the number of Sylow 5-subgroups, n_5, satisfies $n_5 \equiv 1 \mod 5$ and $n_5|10$. Thus $n_5 = 1$ and G has a unique normal subgroup N of order 5. Any group of order 5 is cyclic, so $N = \{1, r, r^2, r^3, r^4\}$ for some $r \in G$ with order 5. Any element of G with order 5 must be in this unique subgroup of order 5. Elements of G that are not in N must have order 2. Let s be such an element.

It remains to show that $|sr| = 2$. If, to the contrary, $|sr| \neq 2$, then $sr \in N$ and so $sr = r^k$ for some $k \in \{0, 1, 2, 3, 4\}$. But then $s = r^{k-1} \in N$, contradicting our choice of s.

(G2) Let H and K be subgroups of a group G such that

(a) $H \cap K = \{1\}$

(b) $HK = G$

(c) $hk = kh$ for all $h \in H$ and $k \in K$.

Prove that $G \cong H \times K$. Make clear in your proof where the conditions (a), (b) and (c) are used.

`Answer:` Define $\phi : H \times K \to G$ by $\phi(h, k) = hk$ for all $(h, k) \in H \times K$.

Because of (a), ϕ is injective: If $\phi(h, k) = 1$ for some $(h, k) \in H \times K$, then $hk = 1$. This implies that $h = k^{-1} \in H \cap K = \{1\}$, and $h = k = 1$. Hence $\ker \phi = \{(1, 1)\}$ and ϕ is injective.

Because of (b), ϕ is surjective.

Because of (c), ϕ is a homomorphism: If $(h_1, k_1), (h_2, k_2) \in H \times K$, then

$$\phi((h_1, k_1)(h_2, k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = (h_1k_1)(h_2k_2) = \phi(h_1, k_1)\phi(h_2, k_2)$$

This makes ϕ an isomorphism.

(G3) Let H be a subgroup of a group G. The **normalizer** of H in G is

$$N(H) = \{x \in G \mid xHx^{-1} = H\}.$$

Prove the following:

(a) $N(H)$ is a subgroup of G.

(b) H is a normal subgroup of $N(H)$.

(c) If K is a subgroup of G, and H is a normal subgroup of K, then K is a subgroup of $N(H)$.

`Answer:`

(a) We use the subgroup criteria. Of course, $1 \in N(H)$ since $1H1^{-1} = H$. If $x \in H$, then $xHx^{-1} = H$, so

$$x^{-1}Hx = x^{-1}(xHx^{-1})x = (x^{-1}x)H(x^{-1}x) = 1H1 = H,$$

so $x^{-1} \in N(H)$. If $x, y \in N(H)$, then $xHx^{-1} = H$ and $yHy^{-1} = H$ so

$$(xy)H(xy)^{-1} = x(yHy^{-1})x^{-1} = xHx^{-1} = H$$

and $xy \in N(H)$.

(b) For all $x \in N(H)$ we have, by definition, $xHx^{-1} = H$. This is one of several equivalent definitions of H is a normal subgroup of $N(H)$.

(c) If H is a normal subgroup of K, then for all $x \in K$ we have $xHx^{-1} = H$. This means that, for all $x \in K$, we have $x \in N(H)$. In other words, $K \subseteq N(H)$.

Rings

(R1) Let F be a field. Define addition and multiplication on $R = \{(a, b) \mid a, b \in F\}$ by

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$(a_1, b_1)(a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1).$$

for all $a_1, a_2, b_1, b_2 \in F$. The set R with these operations is a commutative ring with $1 = (1, 0) \neq 0 = (0, 0)$ (no need to prove this). Prove the following:

(a) R contains a square root of -1.

(b) R is a field if and only if -1 has no square root in F.

Hint: If $F = \mathbb{R}$, then R is the set of complex numbers.

`Answer:`

(a) From the definition of multiplication $(0, 1)^2 = (-1, 0) = -1$.

(b) Suppose that -1 has no square root in F. Then, for $a, b \in F$, we have $a^2 + b^2 = 0$, if and only if $a = b = 0$, if and only if $(a, b) = (0, 0) = 0$. (If, for example, $a^2 + b^2 = 0$ and $b \neq 0$, then $a/b \in F$ is a square root of -1.)

If $(a, b) \neq 0$, then

$$(a, b)\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = (1, 0) = 1.$$

This means that every nonzero element of R is a unit and hence R is a field.

Conversely, if $i \in F$ is a square root of -1, then the polynomial $x^2 + 1 \in F[x]$ has four roots in R namely $(i, 0)$, $(-i, 0)$, $(0, 1)$ and $(0, -1)$. But by Lagrange's Theorem, if R is a field, then a quadratic polynomial can have at most 2 roots. So R is not a field.

OR

If $i \in F$ is a square root of -1, then $(i, 1)(-i, 1) = (0, 0) = 0$, so R has zero divisors and is not a field.

(R2) Consider the quotient ring $F = \mathbb{Z}_3[x]/(x^2 + 1)$. Let $\alpha = x + (x^2 + 1)$.

(a) Show that F is a field.

`Answer:` Since $x^2 + 1 \in \mathbb{Z}_3[x]$ has no roots in $\mathbb{Z}_3$, this polynomial is irreducible over $\mathbb{Z}_3$. This means that the ideal $(x^2 + 1)$ is maximal and F is a field.

(b) List all elements of F and identify on your list the multiplicative inverse of $\alpha + 1$.

`Answer:` For example, every element of F can be written uniquely in the form $a + b\alpha$ with $a, b \in \mathbb{Z}_3$. Hence $F = \{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\}$. Plugging in $x = \alpha$ into the identity $x^2 + 1 = (x + 1)(x - 1) + 2$ gives $0 = (\alpha + 1)(\alpha - 1) + 2$. This can be written as $1/(\alpha + 1) = 2 + \alpha$. Reminder: $2 = -1$ in $\mathbb{Z}_3$.

(R3) Let R be a principal ideal domain. Prove, from the definitions, that every nonzero prime ideal of R is maximal.

`Answer:` Let I be a nonzero prime ideal of R. Then $I \neq R$, $I \neq \{0\}$ and, for all $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$.

Let J be an ideal such that $I \subseteq J \subseteq R$. We show that $J = I$ or $J = R$.

Since R is a PID, $I = (i)$ and $J = (j)$ for some $i, j \in R$. Because $I \neq \{0\}$ we have $i \neq 0$. If $j \in I$ then $J = I$ and we are done. Otherwise $j \notin I$ and J is strictly bigger than I. Then,

because $I \subseteq J$, we have $i = jk$ for some $k \in R$. Since I is prime and $jk \in I$ but $j \notin I$, we have $k \in I$ and so $k = mi$ for some $m \in R$. Combining these equations we get $i = jmi$, or equivalently $(1 - jm)i = 0$. Since $i \neq 0$, this implies that $jm = 1$, in particular, j is a unit of R and $J = (j) = R$.

We have shown that $I \neq R$ has the property that, if J is an ideal such that $I \subseteq J \subseteq R$, then $J = I$ or $J = R$. This means that I is maximal.

Fields

(F1) Consider the polynomial $f(x) = x^3 + 3x^2 + 3x + 2 \in \mathbb{Z}_5[x]$. Let K be the splitting field of $f(x)$ over $\mathbb{Z}_5$. Construct K. How many elements does K have? Factor $f(x)$ completely in $K[x]$.

`Answer:` (See F08, F09) $f(x)$ has the root $3 \in \mathbb{Z}_5$, so $f(x)$ factors as $f(x) = (x-3)(x^2 + x + 1)$ in $\mathbb{Z}_5[x]$. The quotient $x^2 + x + 1$ has no roots in $\mathbb{Z}_5$ so is irreducible over $\mathbb{Z}_5$. So $K = \mathbb{Z}_5[x]/(x^2 + x + 1)$ is a field that contains $\mathbb{Z}_5$ and two roots of f, namely 3 and $\alpha = x + (x^2 + x + 1) \in K$. Dividing $x^2 + x + 1$ by $x - \alpha$ gives $x^2 + x + 1 = (x - \alpha)(x - (-1 - \alpha))$ so the remaining root of f is $-1 - \alpha \in K$. This makes K the splitting field for f. Each element of K can be written uniquely in the form $a + b\alpha$ with $a, b \in \mathbb{Z}_5$, so K has 25 elements. Moreover, f factors completely over K as $f(x) = (x-3)(x-\alpha)(x-(-1-\alpha))$.

(F2) Let E be a finite extension of a field F. Show that every element of E is algebraic over F.

`Answer:` Suppose that $[E : F] = n \in \mathbb{N}$ and $\alpha \in E$. Since E is an n-dimensional vector space over F, the set $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ is linearly dependent over F. In other words, there are $a_0, a_1, a_2, \ldots, a_n \in F$, not all zero, such that

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0.$$

Hence α is a root of the nonzero polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$ and α is algebraic over F.

(F3) Let E be the splitting field of $f(x) = x^3 - 5$ over $\mathbb{Q}$. Is $\mathrm{Gal}(E, \mathbb{Q})$ abelian? Find a familiar group (like $\mathbb{Z}_n, S_n, D_n, \ldots$) that is isomorphic to $\mathrm{Gal}(E, \mathbb{Q})$.

`Answer:` [See F10] The roots of $x^3 - 5$ are $\sqrt[3]{5}$, $\omega\sqrt[3]{5}$ and $\omega^2\sqrt[3]{5}$ where $\omega = e^{2\pi i/3}$. So $E = \mathbb{Q}(\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5})$. Since $\omega = (\omega\sqrt[3]{5})/\sqrt[3]{5} \in E$, it follows that $E = \mathbb{Q}(\omega, \sqrt[3]{5})$. Consider

$$\begin{array}{ccccc} \mathbb{Q} & \subseteq & \mathbb{Q}(\sqrt[3]{5}) & \subseteq & \mathbb{Q}(\omega, \sqrt[3]{5}) = E \\ & {\scriptstyle 3} & & {\scriptstyle 2} & \\ & & {\scriptstyle 6} & & \end{array}$$

By Eisenstein, $x^3 - 5$ is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$. Because, ω is a root of $x^2 + x + 1 \in \mathbb{Q}(\sqrt[3]{5})[x]$, the degree of ω over $\mathbb{Q}(\sqrt[3]{5})$ is at most 2. But $\mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{R}$ and $\omega \notin \mathbb{R}$, so ω has degree 2 over $\mathbb{Q}(\sqrt[3]{5})$. This implies $[E : \mathbb{Q}(\sqrt[3]{5})] = 2$ and $[E : \mathbb{Q}] = 6$.

Since E is a splitting field, $\mathrm{Gal}(E, \mathbb{Q})$ is a group of order 6 and is isomorphic to $\mathbb{Z}_6$ or S_3. Each automorphism in $\mathrm{Gal}(E, \mathbb{Q})$ sends $\sqrt[3]{5}$ to one of its three conjugates $\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}$, and sends ω to one of its two conjugates ω, ω^2. Moreover, since $\sqrt[3]{5}$ and ω generate E over $\mathbb{Q}$, each automorphism is determined by where it sends these generators. Hence $\mathrm{Gal}(E, \mathbb{Q}) = \{\phi_0, \phi_1, \phi_2, \phi_3, \phi_4, \phi_5\}$ where

x	$\sqrt[3]{5}$	ω	$\sqrt[3]{5}$	$\omega\sqrt[3]{5}$	$\omega^2\sqrt[3]{5}$
$\phi_0(x)$	$\sqrt[3]{5}$	ω	$\sqrt[3]{5}$	$\omega\sqrt[3]{5}$	$\omega^2\sqrt[3]{5}$
$\phi_1(x)$	$\omega\sqrt[3]{5}$	ω	$\omega\sqrt[3]{5}$	$\omega^2\sqrt[3]{5}$	$\sqrt[3]{5}$
$\phi_2(x)$	$\omega^2\sqrt[3]{5}$	ω	$\omega^2\sqrt[3]{5}$	$\sqrt[3]{5}$	$\omega\sqrt[3]{5}$
$\phi_3(x)$	$\sqrt[3]{5}$	ω^2	$\sqrt[3]{5}$	$\omega^2\sqrt[3]{5}$	$\omega\sqrt[3]{5}$
$\phi_4(x)$	$\omega\sqrt[3]{5}$	ω^2	$\omega\sqrt[3]{5}$	$\sqrt[3]{5}$	$\omega^2\sqrt[3]{5}$
$\phi_5(x)$	$\omega^2\sqrt[3]{5}$	ω^2	$\omega^2\sqrt[3]{5}$	$\omega\sqrt[3]{5}$	$\sqrt[3]{5}$

This group is isomorphic to S_3, for example, because it is not abelian: $\phi_1(\phi_3(\sqrt[3]{5})) = \phi_1(\sqrt[3]{5}) = \omega\sqrt[3]{5}$, whereas, $\phi_3(\phi_1(\sqrt[3]{5}) = \phi_3(\omega\sqrt[3]{5})) = \omega^2\sqrt[3]{5}$. In addition, from the table we see that the Galois group acts as the set of all permutations of $\{\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}\}$, which shows explicitly that $\mathrm{Gal}(E, \mathbb{Q}) \cong S_3$.