ALGEBRA COMPREHENSIVE EXAMINATION

Fall 2010

Brookfield, Krebs, Shaheen*

Directions: *Answer 5 questions only. Indicate CLEARLY which five you want us to grade—if you do more than five problems, we will select five to grade, and they may not be the five that you want us to grade.* You must answer *at least one* from each of groups, rings, and fields. Be sure to show enough work that your answers are adequately supported.

Notation: $\mathbb{Q}$ denotes the rational numbers; S_n denotes the symmetric group; $\mathbb{Z}_n$ denotes the integers modulo n; D_n denotes the dihedral group.

Groups

1. Let G and H be groups and $\phi : G \to H$ be a group homomorphism.

   (a) Let H' be a subgroup of H. Prove that

   $$\phi^{-1}[H'] = \{x \in G \mid \phi(x) \in H'\}$$

   is a subgroup of G.

   `Answer:` *Fraleigh Theorem 13.12(4)*

   (b) Prove or give a counterexample: If ϕ is onto and H is cyclic, then G is cyclic.

   `Answer:` *Counterexample: Let $G = S_3$, $K = A_3$ and $\phi : G \to G/K$ the natural homomorphism. Then G/K has order 2 and so is isomorphic to $\mathbb{Z}_2$ and is cyclic. But S_3 is not cyclic.*

2. Suppose that G is a simple group of order 168.

   (a) Prove that G contains exactly 8 Sylow 7-subgroups.

   (b) Prove that G contains exactly 48 elements of order 7.

   `Answer:` *By Sylow, $n_7 \in \{1, 8\}$. But if $n_7 = 1$, then G has a unique normal subgroup of order 7 and is not simple, contrary to hypothesis. Thus G has 8 Sylow subgroups of order 7. Each of these contains 6 elements of order 7, so there are a total of 48 elements of order 7 in the group.*

3. Show that A_4 is the smallest subgroup of S_4 that contains the 3-cycles $(1, 2, 3)$ and $(2, 3, 4)$.

   `Answer:` *Since $(1, 2, 3)$ and $(2, 3, 4)$ are even, these elements are in A_4 and the subgroup they generate, $H = \langle(1, 2, 3), (2, 3, 4)\rangle$, is contained in A_4. In particular, the order of H divides the order of A_4 which is 12. But H contains the identity element, $(1, 2, 3)$ and $(2, 3, 4)$ and the inverse of these element, as well as $(1, 2, 3)(2, 3, 4) = (1, 2)(3, 4)$ and $(2, 3, 4)(1, 2, 3) = (1, 3)(2, 4)$. Since we have found 7 elements of H so far, the order of H must be 12 and $H = A_4$.*

Rings

1. Let M be the ring of all 2×2 matrices with integer entries. Prove that there does not exist an ideal I of M such that M/I is isomorphic to the ring of integers. Hint: Consider the matrices $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

   `Answer:` *There is an ideal I of M such that M/I is isomorphic to $\mathbb{Z}$ if and only if I is the kernel of a surjective homomorphism $\phi : M \to \mathbb{Z}$. So we suppose that $\phi : M \to \mathbb{Z}$ is a homomorphism and we show that ϕ is not surjective.*

   Let A and B be the matrices above. Since $A^2 = B^2 = 0$ in M, we have $\phi(A)^2 = \phi(B)^2 = 0$ in $\mathbb{Z}$. This implies that $\phi(A) = \phi(B) = 0$. Let $X \in M$. Then

   $$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

   for some integers a, b, c, d. An easy calculation gives

   $$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} b & 0 \\ d & b \end{pmatrix} A + \begin{pmatrix} c & a \\ 0 & c \end{pmatrix} B$$

   Applying ϕ to both sides of this equation and using the homomorphism properties we see that $\phi(X) = 0$ for all $X \in M$. In particular, ϕ is not surjective.

   Note: The same argument shows that if M is the ring of 2×2 matrices over a commutative ring with unity, and D is a domain, and $\phi : M \to D$ is a homomorphism, then ϕ is trivial.

2. Prove that any ring (with unity) having three elements is isomorphic to $\mathbb{Z}_3$.

   `Answer:` *Let R be a ring with 3 elements. By the ring axioms, two of these elements are 0 and 1. Let's temporarily call the third element a, so that $R = \{0, 1, a\}$. Consider the element $1 + a \in R$. The equation $1 + a = a$ is not possible, since by cancellation in the group $(R, +, 0)$ it would imply $1 = 0$. Similarly, $1 + a = 1$ would imply that $a = 0$, contrary to our assumptions about a. Thus $1 + a = 0$, that is, $a = -1$, the (additive) inverse of 1. Similarly $1 + 1 = 1$ is impossible since it implies $1 = 0$, and $1 + 1 = 0$ is impossible since (with $1 + a = 0$) it implies $1 = a$. Thus $1 + 1 = a$, and equivalently, $a = 2$. These facts enables us to fill in the addition table for R and to confirm that addition in R is identical to addition in $\mathbb{Z}_3$. (This argument shows that, up to isomorphism, there is only one group of order 3.)*

   Most of the multiplication table for R is determined by the ring axiom $1x = x1 = x$ for all $x \in R$, and one of the consequences of the axioms, that $0x = x0 = 0$ for all $x \in R$. The only entry left to be determined is $2 \cdot 2$. But, by distributivity, $2 \cdot 2 = 2 \cdot (1 + 1) = 2 \cdot 1 + 2 \cdot 1 = 2 + 2 = 1$, and so multiplication in R is identical to multiplication in $\mathbb{Z}_3$.

3. Let c be an element of a finite commutative ring R with unity 1. Show that exactly one of the following two conditions holds:

   (a) $bc = 1$ for some nonzero $b \in R$.

   (b) $bc = 0$ for some nonzero $b \in R$.

   [Hint: Consider the function ϕ_c defined by $\phi_c(x) = xc$ for $x \in R$.]

   `Answer:` *If $\phi_c(b) = 1$ for some $b \in R$, we have $bc = 1$ and, because b must be nonzero (a) holds. Otherwise, ϕ_c is not surjective, and, because R is finite, ϕ_c is not injective either. This means that there are distinct $b_1, b_2 \in R$ such that $\phi_c(b_1) = \phi_c(b_2)$. Hence $b_1c = b_2c$ and we have $bc = 0$ with $b = b_1 - b_2 \neq 0$, and so (b) holds.*

   Now suppose that both (a) and (b) hold. Then $b_1c = 1$ and $b_2c = 0$ for nonzero elements $b_1, b_2 \in R$. But this implies $b_2 = b_21 = b_2b_1c = b_10 = 0$, contradicting $b_2 \neq 0$. Thus (a) and (b) cannot both be true.

Fields

1. 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:` *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*

$$\underbrace{\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{5})}_{3} \underbrace{\subseteq \mathbb{Q}(\omega, \sqrt[3]{5})}_{2}}_{6} = E$$

   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* $\mathrm{Gal}(E : \mathbb{Q}) \cong S_3$*.*

2. Let p be a prime number, and let F be a field with p^a elements for some positive integer a. How many elements x of F are there such that $x^{p-1} = 1$? Prove that your answer is correct.

   `Answer:` *The multiplicative group* F^* *is cyclic of order* $p^a - 1$ *(Fraleigh Theorem 33.5). So* F^* *has a unique subgroup of order* d *for each* $d \in \mathbb{N}$ *that divides* $p^a - 1$ *(Fraleigh Theorem 6.14). Since*

   $$p^a - 1 = (p-1)(p^{a-1} + p^{a-2} + \cdots + p + 1),$$

   $p - 1$ *divides* $p^a - 1$*, and* F^* *has a unique subgroup of order* $p - 1$*. By Lagrange, all of the* $p - 1$ *elements of this group are solutions of* $x^{p-1} = 1$*. There can be no other solutions since a degree* $n - 1$ *polynomial over a field can have at most* $n - 1$ *zeros.*

3. Let $F \subseteq E$ be fields and $\alpha \in E$. Show that α^2 is algebraic over F if and only if α^3 is algebraic over F.

   `Answer:` *Suppose that* α^2 *is algebraic over* F*. Then* α^2 *is the root of a nonzero polynomial* $f \in F[x]$*. Then* α *is a root of* $f(x^2) \in F[x]$ *and* α *is algebraic over* F*. This implies,* $[F(\alpha) : F] = \deg(\alpha, F)$ *is finite. Since* $\alpha^3 \in F(\alpha)$*, a finite extension of* F*,* α^3 *is the root of a nonzero polynomial in* $F[x]$*, and so* α^3 *is algebraic over* F*.*

   The converse can be proved by similarly by interchanging 2 *and* 3*.*