ALGEBRA COMPREHENSIVE EXAMINATION

Spring 2012

Brookfield, Krebs*

Directions: *Answer 5 questions only.* You must answer *at least one* from each of groups, rings, and fields. The five questions you choose are worth 20 points each. 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 ones that you want us to grade. Be sure to show enough work that your answers are adequately supported.

Notation: $\mathbb{Z}$ denotes the set of integers, $\mathbb{Q}$ denotes the set of rational numbers, and $\mathbb{C}$ denotes the set of complex numbers, each endowed with the usual definitions of addition and multiplication.

Groups

1. Let X be a nonempty set, S_X the group of permutations on X and $\phi : G \to S_X$ a group homomorphism. For $g \in G$, we write $\phi_g : X \to X$ (rather than $\phi(g)$) for the permutation of X corresponding to g. For $x \in X$, the set $\{\phi_g(x) \mid g \in G\}$ is called the **orbit** of x. Suppose that G is finite. For any $x \in X$, show that the number of elements in the orbit of x divides the order of G.

   `Answer:` *The stabilizer of x is the subgroup $H = \{g \in G \mid \phi_g(x) = x\}$. The elements of the orbit of x are in bijection with the left cosets of H in G. Thus the number of elements in the orbit of x divides the order of G. For details, see Fraleigh, Section 16 and/or Dummit and Foote, Proposition 2, p. 114.*

2. Let $\phi : S_4 \to S_5$ be a homomorphism such that $(1, 2, 3, 4)$ and $(1, 2, 3)$ are in the kernel. Fill in the blank in the sentence below to make a true statement, and then prove that your answer is correct. Be as specific as possible.
   The image of ϕ is _____.

   `Answer:` $\ker \phi$ *is a normal subgroup of S_4 whose order must be a multiple of 4 and of 3, the orders of $(1, 2, 3, 4)$ and $(1, 2, 3)$, respectively. Thus the kernel is A_4 or S_4, the only subgroups of S_4 with order 12 or more. But $(1, 2, 3, 4)$ is odd so is not contained in A_4. This means that* $\ker \phi = S_4$ *and the image of ϕ is the trivial subgroup of S_5, namely $\{e\}$.*

3. Let G be a group, and let H be a subgroup of G such that H has order 2. Prove that H is normal in G if and only if H is contained in the center of G.

   `Answer:` *Let $H = \{1, h\}$ with $h \in G$ of order 2.*

   If H is normal, then for all $g \in G$, $g^{-1}Hg = H$. Since $g^{-1}1g = 1$, this implies that $g^{-1}hg = h$, that is, $hg = gh$. Thus h commutes with all elements $g \in G$, and H is contained in the center of G.

   Conversely, if H is contained in the center of G, then h commutes with all elements $g \in G$ and $g^{-1}hg = h$. Hence H is normal.

Rings

1. Let K be a field. Let K^* be the group of nonzero elements of K, under multiplication. Let $S = \{x^2 \mid x \in K^*\}$.

   (a) Prove that S is a subgroup of K^*.

   (b) Prove that if $-1 \in S$, then there does not exist a group homomorphism $f : S \to K^*$ such that $(f(y))^2 = y$ for all $y \in S$.

   `Answer:`

   (a) It is easy to check that S is closed under multiplication and taking inverses.

   (b) Suppose, to the contrary, that $f : S \to K^*$ is a group homomorphism such that $(f(y))^2 = y$ for all $y \in S$. In S we have $(-1)^2 = 1$. Applying f to this equation gives $(f(-1))^2 = f(1) = 1$, that is, $f(-1)$ is a root of $x^2 - 1$. Since K is a field, $f(-1) = \pm 1$ and so $(f(-1))^2 = 1$. But, because $(f(y))^2 = y$ for all $y \in S$, we also have $(f(-1))^2 = -1$. This contradiction means that no such homomorphism exists.

   NOTE: The contradiction depends on $-1 \neq 1$ in K, so the proof (and the claim) is false if K has characteristic 2.

2. Let

$$R = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \text{ is not divisible by } 3 \right\}.$$

   Notice that under usual addition and multiplication, R is a subring of the rational numbers. (You do not need to prove that.) Let $I = \langle 3 \rangle$ be the ideal of R generated by 3. Prove that I is the *unique* maximal ideal of R . (In other words, prove that I is maximal, and also prove that there are no other maximal ideals of R .)

   `Answer:` *First, observe that an element of R is a unit if and only if it is not in I. Now, we will show that I is maximal. So any ideal properly containing I must contain a unit and hence be all of R; so I is maximal. Any other ideal must either be properly contained in I (hence not maximal), or else contain an element not in I, which must then be a unit, therefore making the ideal all of R.*

OR

Here is a more detailed answer:

Lemma: Every nonzero ideal J of R has the form $\langle 3^n \rangle$ for some $n \in \{0, 1, 2, \dots\}$. Proof: Suppose that J contains an element a/b with $a, b \in \mathbb{Z}$ and b is not divisible by 3. Write $a = 3^k c$ with $k \in \{0, 1, 2, \dots\}$ and $c \in \mathbb{Z}$ such that c is not divisible by 3. Then $b/c \in R$ and $3^k = (a/b)(b/c) \in J$. Thus J contains a power of 3. Now let $n \in \{0, 1, 2, \dots\}$ be the smallest nonnegative integer such that $3^n \in J$. Then, of course, $\langle 3^n \rangle \subseteq J$. To show

that $J \subseteq \langle 3^n \rangle$, suppose that $a/b \in J$. Exactly as above, $a/b = (c/b)3^k$ with $3^k \in J$. By the choice of n, we have $n \leq k$ and so $a/b = ((c/b)3^{k-n})3^n \in \langle 3^n \rangle$. Thus $J = \langle 3^n \rangle$. □

By this lemma, the set of all ideals of R is linearly ordered:

$$\{0\} \subset \cdots \subset \langle 3^5 \rangle \subset \langle 3^4 \rangle \subset \langle 3^3 \rangle \subset \langle 3^2 \rangle \subset \langle 3 \rangle = I \subset \langle 3^0 \rangle = R.$$

In particular, I is the unique maximal ideal.

3. Let R be a commutative ring with unity. Let $f : R \to \mathbb{Z}$ be a surjective ring homomorphism.

   (a) Prove that the kernel of f is a prime ideal of R.

   (b) Prove that the kernel of f is not a maximal ideal of R.

   `Answer:` *$R/\ker(f)$ is isomorphic to $\mathbb{Z}$, which is an integral domain but not a field. Now use the theorems that for an ideal I of R, (1) R/I is a field if and only if I is a maximal, (2) R/I is a domain if and only if I is a prime. See Fraleigh, Theorem 27.9, p. 247 and Theorem 27.15, p. 248.*

Fields

1. Let F be a finite field of order n . Prove that the polynomial $x^2 + x + 1$ has a root in F iff $n - 1$ is divisible by 3 . Hint: $(x^2 + x + 1)(x - 1) = x^3 - 1$.

   `Answer:` *The set of nonzero elements of F, F^*, is a cyclic group under multiplication with order $n-1$ (Fraleigh, Corollary 23.6, p.213). So x^2+x+1 has a root in F if and only if x^3-1 has a root in F other than 1, if and only if F^* contains an element of order 3, if and only if F^* contains a subgroup of order 3, if and only if 3 divides $n-1$. (A cyclic group of order k contains a unique subgroup of order d for each positive divisor d of k.)*

2. Let $\sigma = e^{2\pi i/5} \in \mathbb{C}$, a primitive fifth root of unity, and $F = \mathbb{Q}(\sigma)$.

   (a) Show that F is Galois over $\mathbb{Q}$.

   `Answer:` *Since σ is a zero of $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1$ and $\sigma \neq 1$, σ is a zero of $f(x) = x^4 + x^3 + x^2 + x + 1$. This polynomial is irreducible over $\mathbb{Q}$ by Eisenstein applied to $f(x+1)$ with $p = 5$. The zeros of f are σ, σ^2, σ^3 and σ^4 and so F is the splitting field of f over $\mathbb{Q}$.*

   (b) Show that the Galois group of F over $\mathbb{Q}$ is cyclic.

   `Answer:` *Since F is Galois over $\mathbb{Q}$ and $[F : \mathbb{Q}] = \deg(\sigma, \mathbb{Q}) = 4$, the Galois group has order 4. Any automorphism of F over $\mathbb{Q}$ sends σ to one of its conjugates, and is determined by that conjugate. Let $\phi : F \to F$ be the automorphism such that $\phi(\sigma) = \sigma^2$. Then $\phi^2(\sigma) = \sigma^4$, $\phi^3(\sigma) = \sigma^8 = \sigma^3$ and $\phi^4(\sigma) = \sigma^{16} = \sigma$. Thus ϕ^4 is the identity automorphism, and the Galois group is cyclic with generator ϕ.*

(c) Let $\alpha = \sigma + \sigma^4$. Show that α has degree two over $\mathbb{Q}$.

Answer: *$\phi(\alpha) = \sigma^2 + \sigma^3$ is not α because, otherwise σ is a root of $x^4 - x^3 - x^2 + x$, contradicting the uniqueness of minimal polynomials. This means that $\alpha \notin \mathbb{Q}$. On the other hand α is fixed by ϕ^2 meaning that α is contained in the fixed field of the subgroup generated by ϕ^2, namely, $\{\phi^0, \phi^2\}$. Thus α has degree 2 over $\mathbb{Q}$.*

OR

Since $\alpha^2 = (\sigma + \sigma^4)^2 = \sigma^2 + 2 + \sigma^3$ and $\sigma^4 + \sigma^3 + \sigma^2 + \sigma + 1 = 0$, α is a zero of $x^2 + x - 1$ which is irreducible over $\mathbb{Q}$ by the rational zeros theorem. Thus $\deg(\alpha, \mathbb{Q}) = 2$.

3. Let E/F be fields and $f \in F[x]$. Suppose that $\alpha_1, \alpha_2 \in E$ are conjugate over F. Show that $\beta_1 = f(\alpha_1)$ and $\beta_2 = f(\alpha_2)$ are conjugate over F.

Answer: *By definition, α_1 and α_2 have the same minimal (irreducible) polynomial over F, call it $g \in F[x]$. Let $h \in F[x]$ be the minimal polynomial for β_1 over F. Then $h(f(\alpha_1)) = h(\beta_1) = 0$. Thus $h \circ f$ has α_1 as a zero and g divides $h \circ f$. This implies that α_2 is also a zero of $h \circ f$, that is $0 = h(f(\alpha_2)) = h(\beta_2)$. Since β_2 is a zero of h and h is irreducible over F, this implies that h is the minimal polynomial for β_2 over F. That is, β_1 and β_2 are conjugate over F.*