ALGEBRA COMPREHENSIVE EXAMINATION

Spring 2008

Chabot, Krebs, Shaheen*

Directions: Answer 5 questions only. 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: If n is a positive integer, let $\mathbb{Z}_n$ denote the integers modulo n. Let $\mathbb{Q}$ denote the rational numbers.

Groups

1. Show that all groups of order 45 are abelian.

   `Answer:` *Let G be a group of order 45. By Sylow, n_3 divides 45 and is congruent to 1 modulo 3. The only such number is $n_3 = 1$, and so G contains a normal subgroup H of order 9. Similarly, n_5 divides 45 and is congruent to 1 modulo 5. The only such number is $n_5 = 1$, and so G contains a normal subgroup K of order 5. As usual, $H \cap K = \{1\}$ so $H \times K \cong HK \leq G$. But $|H \times K| = 45 = |G|$ and so $H \times K \cong G$. Since all groups of groups of order 5 and 9 are abelian, G is also abelian.*

2. Let G be a cyclic group and H a subgroup of G. Prove that H is cyclic.

   `Answer:` *[See S13] Suppose that $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$. Let H be a subgroup of G. If $H = \{1\}$ then $H = \langle 1 \rangle$ and so H is cyclic. Otherwise, H contains at least one element of the form a^k with $k \in \mathbb{N}$.*

   Let $n \in \mathbb{N}$ be the least natural number such that $a^n \in H$. Then $\langle a^n \rangle \leq H$ is automatic. We prove the opposite inclusion: Suppose that $a^k \in H$. Since $n \in \mathbb{N}$, there are $q, r \in \mathbb{Z}$ such that $k = qn + r$ and $0 \leq r < n$. Then $a^r = a^{k-qn} = a^k(a^n)^{-q}$. Because a^n and a^k are in H, so is a^r. But, by the choice of n, this is only possible if $r = 0$. Thus $k = qn$ and $a^k = (a^n)^q \in \langle a^n \rangle$. This shows that $H = \langle a^n \rangle$ and that H is cyclic.

3. Let G be a finite group with $|G| > 1$, and let $\mathrm{Inn}(G)$ be the group of inner automorphisms of G. Show that if G is isomorphic to $\mathrm{Inn}(G)$, then $|G|$ has at least two distinct prime factors. (Hint: Do a proof by contradiction.)

   `Answer:` *Reminder: For $g \in G$ the function $\phi_g : G \to G$ defined by $\phi_g(x) = gxg^{-1}$ for all $x \in G$ is an automorphism of G. ϕ_g is called an inner automorphism, the set of inner automorphisms, $\mathrm{Inn}(G)$, is a subgroup of the group of all automorphisms of G. The function $\Phi : G \to \mathrm{Inn}(G)$ defined by $\Phi(g) = \phi_g$ for all $g \in G$ is a surjective group homomorphism. The kernel of Φ is $Z = Z(G)$, the center of G, so $\mathrm{Inn}(G) \cong G/Z$. See Fraleigh, Definition 14.15, p. 141 and Dummit and Foote, Section 4.4, p. 133.*

   Suppose, to the contrary, that $|G| = p^n$ for some prime p and $n \in \mathbb{N}$. Since G is a p-group, the center of G, Z, is nontrivial (Fraleigh, Theorem 37.4, p. 329). From the above discussion, this means that $\Phi : G \to \mathrm{Inn}(G)$ is not injective, in particular, $|\mathrm{Inn}(G)| = |G|/|Z| < |G|$. Hence $\mathrm{Inn}(G)$ and G cannot be isomorphic.

Rings

1. Let p be a prime number. Let $D : \mathbb{Z}_p \to \mathbb{Z}_p$ be a function such that $D(a \cdot b) = a \cdot D(b) + b \cdot D(a)$ for all $a, b \in \mathbb{Z}_p$. Prove that D is the zero map.

   `Answer:` *Lemma: For all $a \in \mathbb{Z}_p$, $D(a^n) = na^{n-1}D(a)$. Proof: By induction. For $n = 1$, the claim is clear. Suppose that the claim is true for some n. Then*

   $$D(a^{n+1}) = D(a \cdot a^n) = a \cdot D(a^n) + a^n \cdot D(a) = a(na^{n-1}D(a)) + a^n \cdot D(a) = (n+1)a^n D(a)$$

   which proves the claim in the next case. $\square$

   To finished the question we use the facts that $a^p = a$ and $pa = 0$ for all $a \in \mathbb{Z}_p$:

   $$D(a) = D(a^p) = pa^{p-1}D(a) = 0.$$

2. Let D be a Euclidean domain and $a, b, c \in D$. Prove:

   (a) If a divides bc and $GCD(a, b) = 1$, then a divides c.

   (b) If a is irreducible, then a is prime.

   `Answer:`

   (a) Suppose that $GCD(a, b) = 1$. This means that that if d is a common divisor of a and b, then d divides 1, that is d is a unit of D (Fraleigh p. 395). Since Euclideans domains are PIDs, there is some $e \in D$ such that $Da + Db = De$. Then $a \in De$ and $b \in De$ which means that e is a common divisor of a and b. By assumption e is a unit and so $Da + Db = De = D$. In particular, there are $x, y \in D$ such that $ax + by = 1$ (See also Dummit and Foote, Theorem 4, p. 275). Hence, if a divides bc, then a divides $bcy + acx = c$.

   (b) Suppose that a is irreducible. This means that a is not a unit, but, if $a = bc$, then either b is a unit or c is a unit. To show that a is prime we need to show that if a divides bc, then either a divides b or a divides c.

   Suppose that a divides bc. If a divides b we are done. Otherwise, a does not divide b. Let d be a common divisor of a and b. Then $a = de$ for some $e \in D$. Since a is irreducible, either e or d is a unit. But if e is a unit, then a divides d ($ae^{-1} = dee^{-1} = d$) which implies that a divides b contrary to assumption. This means that d is a unit. Since the only common divisors of a and b are units, $GCD(a, b) = 1$, then, by (1), a divides c.

3. Let R be a commutative ring with identity 1. Prove that an ideal M is maximal if and only if R/M is a field.

   `Answer:` *Fraleigh, Theorem 27.9, p. 247. Dummit and Foote, Proposition 12, p. 254.*

Fields

1. Let $\mathbb{Q}$ be the field of rationals and let $p(x) = x^3 - 4x + 5$. Assume α is a root of $p(x)$.

   (a) Prove that $p(x)$ is irreducible over $\mathbb{Q}$.

   (b) Find $a, b, c \in \mathbb{Q}$ such that $(\alpha + 1)^{-1} = a + b\alpha + c\alpha^2$.

   `Answer:`

   (a) By the Rational Zeros Theorem (or Fraleigh, Corollary 23.12, p. 215), the only possible rational zeros of p are ± 5 and ± 1. It is easy to check that these integers are not, in fact, zeros of p and so p has no rational zeros and is irreducible over $\mathbb{Q}$.

   (b) Dividing p by $x + 1$ using long division we get $p(x) = (x^2 - x - 3)(x + 1) + 8$. Setting $x = \alpha$ in this and using $p(\alpha) = 0$, we get $0 = (\alpha^2 - \alpha - 3)(\alpha + 1) + 8$. This can be written as

   $$\frac{1}{\alpha + 1} = -\frac{1}{8}(\alpha^2 - \alpha - 3).$$

2. Let F be a field. Let G be a finite subgroup of the group of units of F. Prove that G is cyclic. (Hint: Do a proof by contraction. First show that G is a finite abelian group. To get a contradiction, find a positive integer n such that the polynomial $x^n - 1$ has more than n zeroes. You will need to use a major theorem about finite abelian groups.)

   `Answer:` *Dummit and Foote, Proposition 18, p. 314. Since multiplication in F is commutative, G is an abelian group. By the Classification Theorem for Finite Abelian Groups, G is isomorphic to a direct product of cyclic groups:*

   $$G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$$

   where $p_1, p_2, \ldots, p_k$ are prime and $a_1, a_2, \ldots, a_k \in \mathbb{N}$. If there is only one prime, or if all the primes are distinct, then G is cyclic. If G is not cyclic, then at least two of the primes are equal. WLOG, suppose that $p_1 = p_2 = p$. Since $\mathbb{Z}_{p^{a_1}}$ and $\mathbb{Z}_{p^{a_2}}$ each have subgroups isomorphic to $\mathbb{Z}_p$, G has a subgroup H isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. The order of $\mathbb{Z}_p \times \mathbb{Z}_p$ is p^2 and each element $x \in \mathbb{Z}_p \times \mathbb{Z}_p$ satisfies $px = 0$. So H has order p^2 and each element $h \in H$ satisfies $h^p = 1$. But this implies that $x^p - 1$ has at least p^2 zeros in F, contrary to Lagrange's Theorem.

3. Let $\xi = e^{2\pi i/n}$ be a primitive n-th root of unity. Prove that $Gal(\mathbb{Q}(\xi)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$. Note: $\mathbb{Z}_n^\times$ is the group of units under multiplication in $\mathbb{Z}_n$.

   `Answer:` *Dummit and Foote, Theorem 26, p. 596.*