ALGEBRA COMPREHENSIVE EXAMINATION

Fall 2011

Brookfield, Krebs, 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: $\mathbb{C}$ denotes the complex numbers; $\mathbb{Q}$ 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 be a group and let N be a normal subgroup of index n. Show that $g^n \in N$ for all $g \in G$.

   `Answer:` *Note that the index of N in G is the same as the order of the group G/N. If $g \in G$, then gN is an element of the group G/N. Since this group has order n, by Lagrange, $(gN)^n = N$. That is, $g^nN = N$, so the coset that contains g^n is the coset N and $g^n \in N$.*

2. a. Prove that every group of order 15 is abelian.

   b. Is it true that every group of order 15 is cyclic? Prove or give a counterexample.

   `Answer:` *[See F08] We actually show that such groups are cyclic. Let G be a group of order 15. By Sylow, n_3 divides 15 and is congruent to 1 modulo 3. Thus $n_3 = 1$, and G has a unique normal subgroup H of order 3. Similarly, n_5 divides 15 and is congruent to 1 modulo 5. Thus $n_5 = 1$, and G has a unique normal subgroup K of order 5. $H \cap K$ is a subgroup of H and a subgroup of K, so its order divides both 3 and 5, and so $H \cap K = \{1\}$. By HW11(2), $H \times K \cong HK \leq G$. But $|H \times K| = 15 = |G|$ and so $H \times K \cong G$. Now we recall that groups of order 3 and 5 are isomorphic to $\mathbb{Z}_3$ and $\mathbb{Z}_5$ respectively and so $G \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$.*

3. Let G be a group of order n. Let f be an automorphism of G. Prove that $f^{n!}$ is the identity map. (Here $f^{n!}$ means f composed with itself $n!$ times.)

   `Answer:` *An automorphism of G is, in particular, a permutation of the elements of G, so is an element of the symmetric group on G. This group has order $n!$. By Lagrange, the $n!$ power of any element of this group is the identity element of the group. Specifically, $f^{n!}$ is the identity map.*

Rings

1. Let a, b and d be positive integers. Prove that d is the least common multiple of a and b if and only if $\langle a\rangle \cap \langle b\rangle = \langle d\rangle$.

2. Let R and R' be rings. Let J be an ideal of R'. Let $\phi : R \to R'$ be a ring homomorphism. Prove that $\phi^{-1}(J) = \{x \in R \mid \phi(x) \in J\}$ is an ideal of R.

3. Let F be a field, and let $F[x, y]$ be the ring of polynomials with indeterminates x and y. Let J be the principal ideal of $F[x, y]$ generated by $x^2 + y^2 - 1$. Let $R = F[x, y]/J$. Prove that R is not a Euclidean domain. You may assume, without proving it, that $x + J$, $1 + y + J$, and $1 - y + J$ are irreducible elements of R, no two of which are associates.

Fields

1. Let $\sigma = e^{2\pi i/5} \in \mathbb{C}$, and let $F = \mathbb{Q}(\sigma)$. Let G be the Galois group of F over $\mathbb{Q}$. Describe the group G. Is G abelian? Is G cyclic? Prove your answers.

2. Let p be a prime number. Let F be a finite field of order $q = p^k$ for some positive integer k. Let n be a positive integer.

   a. Show that if $x \in F$ and $x^n = 1$, then $x = 1$ or $\gcd(n, q - 1) > 1$.

   b. Show that if $x^{n-1} + x^{n-2} + \cdots + x + 1$ has a root in F, then p divides n or $\gcd(n, q - 1) > 1$.

3. Let $\alpha = \sqrt[14]{2}$, and let $\beta = \sqrt[45]{2}$. Let $a_0, a_1 \ldots, a_{13}$ be rational numbers, and let $x = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{13}\alpha^{13}$. Prove that if $x = b_0 + b_1\beta + b_2\beta^2 + \cdots + b_{44}\beta^{44}$ for some rational numbers $b_0, b_1, \ldots, b_{44}$, then $a_1 = a_2 = \cdots = a_{13} = 0$. [Hint: Find two simple extensions of $\mathbb{Q}$ that each contain x, and consider their intersection.]

   `Answer:` *$x^{14} - 2$ and $x^{45} - 2$ are irreducible over $\mathbb{Q}$ by Eisenstein and so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 14$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = 45$. Let $F = \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)$. Then $[F : \mathbb{Q}]$ divides both 14 and 45. This implies $[F : \mathbb{Q}] = 1$ and $F = \mathbb{Q}$. We have $x = a_0 + a_1\alpha + a_2\alpha^2 \cdots + a_{13}\alpha^{13} \in \mathbb{Q}(\alpha)$ and $x = b_0 + b_1\beta + b_2\beta^2 \cdots + b_{44}\beta^{44} \in \mathbb{Q}(\beta)$, and so $x \in K = \mathbb{Q}$.*

   But $x \in \mathbb{Q}(\alpha)$ can be written ***uniquely*** *in the form $x = a_0 + a_1\alpha + a_2\alpha^2 \cdots + a_{13}\alpha^{13}$ with $a_0, a_1, \ldots, a_{13} \in \mathbb{Q}$. Since $x \in \mathbb{Q}$, this means that $a_0 = x$ and $a_1 = a_2 = \cdots = a_{13} = 0$.*