ALGEBRA COMPREHENSIVE EXAMINATION

Fall 2012

Brookfield, Krebs, Shaheen*, Webster

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 of order $2n$.

Groups

1. Let H be a subgroup of a group G. Prove that the following are equivalent:

   (a) $x^{-1}y^{-1}xy \in H$ for all $x, y \in G$.

   (b) H is a normal subgroup of G and G/H is abelian.

   `Answer:` *Suppose that $x^{-1}y^{-1}xy \in H$ for all $x, y \in G$. Then, in particular, for all $h \in H$ and $y \in G$, we have $h^{-1}y^{-1}hy \in H$, that is, $h^{-1}y^{-1}hy = h'$ for some $h' \in H$. This implies that $y^{-1}hy = hh' \in H$. Thus we have shown that $y^{-1}hy \in H$ for all $h \in H$, that is, $y^{-1}Hy \subseteq H$ for all $y \in G$. This suffices to show that H is normal.*

   Now we show that G/H is abelian. If $xH, yH \in G/H$ with $x, y \in G$, then

   $$(xH)^{-1}(yH)^{-1}(xH)(yH) = x^{-1}y^{-1}xyH = H.$$

   Multiplying this equation on the left by (xH) and then (yH) gives $(xH)(yH) = (yH)(xH)$, which shows that G/H is abelian.

   Now for the converse. Suppose that H is a normal subgroup and G/H is abelian. Then for all $x, y \in G$ we have $(xH)(yH) = (yH)(xH)$. As above, this equation can be written as

   $$(xH)^{-1}(yH)^{-1}(xH)(yH) = H,$$

   or $x^{-1}y^{-1}xyH = H$ which implies that $x^{-1}y^{-1}xy \in H$.

2. Let G be a group with center Z. Suppose that G/Z is cyclic with generator aZ for some $a \in G$.

   (a) Show that each element of G can be written in the form $a^n z$ where $n \in \mathbb{Z}$ and $z \in Z$.

   `Answer:` *Since G/Z is cyclic with generator aZ, each element of G/Z has the form $(aZ)^n = a^nZ$ for some $n \in \mathbb{Z}$. But each element of G/Z is a coset of Z in G, and these cosets form a partition of G. Thus each element of G is in a^nZ for some $n \in \mathbb{Z}$. In particular, each element of G can be written in the form a^nz with $n \in \mathbb{Z}$ and $z \in Z$.*

(b) Show that G is abelian.

Answer: *Let $a^{n_1}z_1$ and $a^{n_2}z_2$ be elements of G with $n_1, n_2 \in \mathbb{Z}$ and $z_1, z_2 \in Z$. Since z_1 and z_2 are in the center, they commute with all other elements of G. Hence $(a^{n_1}z_1)(a^{n_2}z_2) = a^{n_1+n_2}z_1z_2 = a^{n_1+n_2}z_2z_1 = (a^{n_2}z_2)(a^{n_1}z_1)$, and G is abelian.*

3. Prove that the (additive) groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Answer: *Let $\phi : \mathbb{Z} \to \mathbb{Q}$ be a homomorphism. We will show that ϕ is not surjective. Let $\phi(1) = a \in \mathbb{Q}$. Then, since ϕ is a homomorphism, $\phi(n) = na$ for all $n \in \mathbb{Z}$. If $a = 0$, then $\phi(n) = 0$ for all $n \in \mathbb{Z}$ and ϕ is not surjective in this case. If $a \neq 0$, then ϕ is not surjective because there is no $n \in \mathbb{Z}$ such that $\phi(n) = a/2$. (If there was, then $na = \phi(n) = a/2$ and so $n = 1/2$ and n is not an integer.)*

Rings

1. Let R be a commutative ring with identity 1 and let M be an ideal of R. Prove that M is a maximal ideal of R if and only if for every $r \in R \setminus M$ there is an $x \in R$ such that $1 - rx \in M$. [Note: $R \setminus M$ denotes the set of elements of R that are not contained in M.]

Answer: *[See F08] Suppose that M is maximal. If $r \in R \setminus M$, then the ideal containing M and r is strictly bigger than M so is the whole ring R. Specifically, $\langle r \rangle + M = R$. In particular, $1 \in \langle r \rangle + M$ and so there are $x \in R$ and $m \in M$ such that $1 = rx + m$. Consequently $1 - rx = m \in M$.*

Conversely, suppose that for every $r \in R \setminus M$ there is an $x \in R$ such that $1 - rx \in M$. Let I be an ideal such that $M \subseteq I \subseteq R$. If $I = M$ we are done. Otherwise, I contains an element r that is not in M. By assumption, there exists $x \in R$ and $m \in M$ such that $1 = rx + m$. This implies that $1 \in \langle r \rangle + M$ and so $\langle r \rangle + M = R$. Because $r \in I$ we also have $\langle r \rangle + M \subseteq I$, and so $I = R$. This shows that M is maximal.

2. Let c be an element of a finite commutative ring R with $1 \neq 0$. Show that exactly one (but not both) of the following conditions holds:

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

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

   Hint: Consider the function $\phi : R \to R$ defined by $\phi(x) = xc$ for all $x \in R$.

   Answer: *If $\phi(b) = 1$ for some $b \in R$, we have $bc = 1$ and, because b must be nonzero for this to be true, (a) holds. Otherwise, ϕ is not surjective, and, because R is finite, ϕ is not injective either. This means that there are distinct $b_1, b_2 \in R$ such that $\phi(b_1) = \phi(b_2)$. 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 $b_2 = b_2 1 = b_2 b_1 c = b_1 0 = 0$, contradicting $b_2 \neq 0$. Thus (a) and (b) cannot both be true.

3. The eighth cyclotomic polynomial is $f(x) = x^4 + 1$.

   (a) Factor f into irreducible polynomials over $\mathbb{C}$. It may be convenient to express your answer in terms of powers of $\alpha = e^{2\pi i/8} = (1+i)/\sqrt{2}$, an eighth root of unity.

   `Answer:` $f = (x - \alpha)(x - \alpha^3)(x - \alpha^5)(x - \alpha^7)$

   (b) Factor f into irreducible polynomials over $\mathbb{R}$.

   `Answer:` *Since* α *and* α^7 *are complex congugates,* $(x-\alpha)(x-\alpha^7) = x^2 - \sqrt{2}x + 1 \in \mathbb{R}[x]$. *Similarly,* $(x - \alpha^3)(x - \alpha^5) = x^2 + \sqrt{2}x + 1 \in \mathbb{R}[x]$, *and so*

$$f = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1).$$

   These quadratic polynomials are irreducible over $\mathbb{R}$ *because they have no zeros in* $\mathbb{R}$

   (c) Factor f into irreducible polynomials over $\mathbb{Q}$. Hint: Show f is irreducible over $\mathbb{Q}$.

   `Answer:` *By the Rational Zeros Theorem, the only possible rational zeros of* f *are* ± 1. *Since these numbers are not zeros,* f *has not degree 1 factor in* $\mathbb{Q}$. *That leaves degree 2 factors to consider.*

   Suppose $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ *with* $a, b, c, d \in \mathbb{Q}$. *Because of Gauss's Lemma, can assume* $a, b, c, d \in \mathbb{Z}$. *Multiplying this out and matching coefficients we get* $a + c = 0$, $b + d + ac = 0$, $bc + ad = 0$ *and* $bd = 1$. *The last of these equations has two solutions: If* $b = d = 1$, *then we get* $a^2 = c^2 = 2$, *with no solutions in* $\mathbb{Z}$. *If* $b = d = -1$, *then we get* $a^2 = c^2 = -2$, *with no solutions in* $\mathbb{Z}$. *Thus* f *does not factor over* $\mathbb{Q}$.

   OR

   Any factorization of f *over* $\mathbb{Q}$ *is, in particular, a factorization of* f *over* $\mathbb{R}$. *But, from above, the* ***only*** *factorization over* $\mathbb{R}$ *is* $f = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$, *and this is is not a factorization over* $\mathbb{Q}$ *since* $\sqrt{2} \notin \mathbb{Q}$. *Thus* f *is irreducible over* $\mathbb{Q}$.

   (d) Factor f into irreducible polynomials over $\mathbb{Z}_3$.

   `Answer:` *In* $\mathbb{Z}_3$, $x^4 \in \{0, 1\}$ *for any* x, *and so* f *has no zeros in* $\mathbb{Z}_3$. *To look for a factorization into two quadratic polynomials, we suppose* $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ *with* $a, b, c, d \in \mathbb{Z}_3$. *Then just as in (c), we get* $a + c = 0$, $b + d + ac = 0$, $bc + ad = 0$ *and* $bd = 1$. *The last of these equations has two solutions in* $\mathbb{Z}_3$: *either* $b = d = 1$ *or* $b = d = -1 = 2$. *If* $b = d = 1$, *then we get* $a^2 = c^2 = 2$, *with no solutions in* $\mathbb{Z}_3$. *If* $b = d = -1$, *then we get* $a^2 = c^2 = -2 = 1$, *which* has *solutions in* $\mathbb{Z}_3$. *Since* $a = -c$, *we get the factorization* $f(x) = (x^2 + x - 1)(x^2 - x - 1)$ *in* $\mathbb{Z}_3[x]$. *The two quadratic polynomials in this factorization must be irreducible since they can't have any zeros (otherwise* f *would have zeros).*

Fields

1. Let K be a field extension of a field F of degree n and let $f(x) \in F[x]$ be an irreducible polynomial of degree $m > 1$. Show that if $\gcd(m, n) = 1$, then f has no root in K.

   `Answer:` *If α is root of f and is contained in K, then $F \subseteq F(\alpha) \subseteq K$ with $[F(\alpha) : F] = m > 1$ and $[K : F] = n$. This would imply that m divides n, contrary to* $\gcd(m, n) = 1$.

2. The polynomial $x^5 - 1 \in \mathbb{Q}[x]$ factors into irreducible polynomials over $\mathbb{Q}$ as follows:

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1).$$

   Let $\sigma = e^{2\pi i/5}$ and $E = \mathbb{Q}(\sigma)$, the splitting field of $x^5 - 1$. Since the degree of σ over $\mathbb{Q}$ is 4, elements of E can be written uniquely in the form

$$\alpha = a + b\sigma + c\sigma^2 + d\sigma^3$$

   with $a, b, c, d \in \mathbb{Q}$. Let $G = \mathrm{Gal}(E, \mathbb{Q})$ be the Galois group of E over $\mathbb{Q}$ and $\phi \in G$ be such that $\phi(\sigma) = \sigma^4$. Which elements of the form $\alpha = a + b\sigma + c\sigma^2 + d\sigma^3$ are in the fixed field of ϕ?

   `Answer:` *Applying the automorphism to α we get*

$$\begin{aligned}\phi(\alpha) &= \phi(a + b\sigma + c\sigma^2 + d\sigma^3)\\ &= a + b\phi(\sigma) + c(\phi(\sigma))^2 + d(\phi(\sigma))^3\\ &= a + b\sigma^4 + c\sigma^3 + d\sigma^2\\ &= (a - b) + (-b)\sigma + (d - b)\sigma^2 + (c - b)\sigma^3,\end{aligned}$$

   using $\sigma^4 = -1 - \sigma - \sigma^2 - \sigma^3$. So $\phi(\alpha) = \alpha$ if and only if $a = a - b$, $b = -b$, $c = d - b$ and $d = c - b$. These equations imply $b = 0$ and $c = d$. So α is fixed by ϕ if and only if $\alpha = a + c(\sigma^2 + \sigma^3)$ for some $a, c \in \mathbb{Q}$.

3. Let $F \subseteq E$ be fields. Let $\alpha, \beta \in E$ be the zeros of a quadratic polynomial in $F[x]$. Show that $F(\alpha) = F(\beta)$.

   `Answer:` *If $\alpha = \beta$, then the claim is obvious. Otherwise, the quadratic polynomial must be $a(x - \alpha)(x - \beta) = ax^2 - a(\alpha + \beta)x + a\alpha\beta \in F[x]$. Since $a \neq 0$ and $a(\alpha + \beta)$ are both in F, we have $r = \alpha + \beta \in F$.*

   Since $r, \alpha \in F(\alpha)$, $\beta = r - \alpha$ is also in $F(\alpha)$ and so $F(\beta) \subseteq F(\alpha)$. Similarly, $F(\alpha) \subseteq F(\beta)$.

   OR

   Let $f \in F[x]$ be the quadratic polynomial with roots α and β. Since $f \in F(\alpha)[x]$ and α is a root of f, $f(x) = (x - \alpha)g(x)$ for some polynomial $g \in F(\alpha)[x]$ with degree 1. Since β is a root of f, either it is a root of $x - \alpha$ or of $g(x)$, either way, β has degree 1 over $F(\alpha)$ and hence $\beta \in F(\alpha)$ and $F(\beta) \subseteq F(\alpha)$. Similarly, $F(\alpha) \subseteq F(\beta)$.