ALGEBRA COMPREHENSIVE EXAMINATION
Fall 2013
Brookfield*, Krebs, Shaheen, Webster

Directions: Answer 5 questions only. If you answer more than five questions, only the first five will be graded. You must answer *at least one* from each of groups, rings, and fields. Be sure to show enough work so that your answers are adequately supported.

Groups

(1) Let G be a finite group. Let H be a normal subgroup of G such that $|H|$ and $[G : H]$ are relatively prime. (Here $|H|$ denotes the order of H, and $[G : H]$ denotes the index of H in G.) Let f be an automorphism of G, and let $J = f(H)$. Prove that $J = H$. Hint 1: Consider the orders of the subgroups $H \cap J$ and HJ. OR Hint 2: Consider the order of $\phi(f(H))$ in G/H where $\phi : G \to G/H$ is the natural homomorphism.

`Answer:` *Let $m = |H|, d = |H \cap J|$, and $n = [G : H]$. Then $d|m$. Also, $|HJ| = m^2/d$, so m^2/d divides $|G| = mn$. Because m and n are relatively prime, this forces $d = m$, which implies that $H = J$.*

OR

Consider the composition $\phi \circ f$ where $\phi : G \to G/H$ is the natural homomorphism. The image of H, $\phi(f(H))$, is isomorphic to a quotient group of H so its order divides $|H|$. In addition, $\phi(f(H))$ is a subgroup of G/H so its order divides $|G/H| = [G : H]$. Because $|H|$ and $[G : H]$ are relatively prime, this implies that $\phi(f(H))$ is trivial, and hence $f(H)$ is contained in $\ker \phi = H$. Because f is an automorphism and $|f(H)| = |H|$, and so $f(H) = H$.

(2) Prove that $\mathbb{Z}_n$ with $n > 1$ is simple if and only if n is a prime.

`Answer:` *Suppose that n is prime. Let H be a nontrivial subgroup of $\mathbb{Z}_n$. Let $a \in H$ be nonzero. Since a and n are relatively prime, there are $x, y \in \mathbb{Z}$ such that $xa + yn = 1$. In $\mathbb{Z}_n$, this equation becomes $xa = 1$ and so $1 \in H$. Since 1 generates $\mathbb{Z}_n$, this implies that $H = \mathbb{Z}_n$. We have shown that the only subgroups of $\mathbb{Z}_n$ are the trivial one and $\mathbb{Z}_n$ itself, $\mathbb{Z}_n$ is simple.*

Conversely, suppose that $\mathbb{Z}_n$ is simple. Let $a \in \mathbb{Z}_n$ be nonzero. Since the subgroup generated by a is $\mathbb{Z}_n$, $xa = 1$ must hold in $\mathbb{Z}_n$ for some $x \in \mathbb{Z}$. That means that $xa + yn = 1$ holds in $\mathbb{Z}$ for some $y \in \mathbb{Z}$, and so a and n are relatively prime. Since this holds for all $a \in \mathbb{Z}$ with $1 \leq a < n$, n is prime.

(3) Prove that any group of order 45 is abelian. Hint: You may use the fact that, if p is prime, then any group of order p^2 is abelian.

`Answer:` *Suppose that the group G has order $45 = 5 \cdot 3^2$. By Sylow, n_5 divides 45 and $n_5 \equiv 1 \mod 5$. Thus $n_5 = 1$ and G has a unique normal subgroup H of order 5. Also, n_3 divides 45 and $n_3 \equiv 1 \mod 3$, so $n_3 = 1$ and G has a unique normal subgroup K of order 9. By the usual argument $H \cap K = \{1\}$ and $H \times K \cong HK \leq G$. Since $|H \times K| = |H| \cdot |K| = |G|$ we have $H \times K \cong G$. Because H and K are abelian, G is abelian.*

Rings

(1) Let R be a commutative ring with unity. Show that the set

$$N = \{a \in R \mid a^n = 0 \text{ for some } n \geq 1\}$$

of all nilpotent elements of R (called the nilradical of R) is an ideal.
`Answer:` *Let $a, b \in N$. Then there are $n_1, n_2 \geq 1$ with $a^{n_1} = b^{n_2} = 0$. Consider the binomial theorem expansion of $(a \pm b)^{n_1+n_2}$. Each summand in this expansion contains either a sufficiently high power of a or a sufficiently high power of b so that it is zero. Hence $(a \pm b)^{n_1+n_2} = 0$ and $a \pm b \in N$. Finally since R is commutative, $(ra)^{n_1} = r^{n_1}a^{n_1} = 0$, and $(ar)^{n_1} = a^{n_1}r^{n_1} = 0$.*

(2) Let R and R' be commutative rings with unity. Let $\phi : R \to R'$ be a surjective (onto) ring homomorphism.
  (a) Prove that $\phi(1) = 1$.
  `Answer:` *Since ϕ is surjective, there is some $r \in R$ such that $\phi(r) = 1$. Then*
$$\phi(1) = \phi(1) \cdot 1 = \phi(1)\phi(r) = \phi(1 \cdot r) = \phi(r) = 1.$$
  (b) Let u be a unit in R. Prove that $\phi(u)$ is a unit in R' and that $\phi(u^{-1}) = \phi(u)^{-1}$.
  `Answer:` *Since u is a unit we have $uu^{-1} = 1$ in R. Applying the homomorphism ϕ we get $\phi(u)\phi(u^{-1}) = \phi(uu^{-1}) = \phi(1) = 1$ and so $\phi(u)$ is a unit of R' with inverse $\phi(u^{-1})$.*

(3) Let R be a commutative ring with unity. Let $I = \langle x + 1 \rangle$ be the ideal of $R[x]$ generated by $x + 1$. Show that I is a prime ideal of $R[x]$ if and only if R is an integral domain. (Here $R[x]$ denotes the ring of polynomials in the indeterminate x with coefficients in R.)
`Answer:` *Consider the ring automorphism $x \mapsto x + 1$. So $I = \langle x + 1 \rangle$ is prime iff $\langle x \rangle$ is prime iff $R[x]/\langle x \rangle \cong R$ is an integral domain.*

OR

Consider the (surjective) evaluation homomorphism $\phi : R[x] \to R$ defined by $f(x) \mapsto f(-1)$. The kernel of ϕ is I and so $R[x]/I \cong R$. Now use the fact that I is prime if and only if R/I is a domain.

Fields

(1) Let E/F be a field extension of degree 3.
  (a) Show that $E = F(\alpha)$ for some $\alpha \in E$.
  (b) With α as in (a), show that any element $\beta \in E$ can be written in the form
$$\beta = \frac{a + b\alpha}{c + d\alpha}$$
  for suitable $a, b, c, d \in F$. Hint: Can the set $\{1, \alpha, \beta, \alpha\beta\}$ be linearly independent over F?

`Answer:`
  (a) *Choose α in E but not F. Then $F \subset F(\alpha) \subseteq E$. Since $[F(\alpha) : F]$ is not one and divides $[E : F] = 3$, we have $F(\alpha) = E$.*
  (b) *Since $[E : F] = 3$, the set $\{1, \alpha, \beta, \alpha\beta\}$ must be dependent over F, and so there are constants a, b, c, d, not all zero, such that $a + b\alpha + c\beta + d\beta\alpha = 0$. Supposing that $c + d\alpha \neq 0$, this can be solved for β, giving the claimed form (with a sign change). So it remains to show that $c + d\alpha \neq 0$.*

Suppose, to the contrary that $c + d\alpha = 0$. If $d \neq 0$, this would imply $\alpha \in F$ so we must have $d = c = 0$. But then $a + b\alpha = 0$, which similarly leads to $a = b = 0$. But $a = b = c = d = 0$ contradicts the requirement that not all of a, b, c, d are zero.

(2) Find the minimal polynomial (over $\mathbb{Q}$) for $\alpha = e^{2\pi i/8}$, a primitive eighth root of unity. Prove your claim.

`Answer:` *Since $\alpha^4 = -1$, α is a root of $f(x) = x^4 + 1 \in \mathbb{Q}[x]$. This is the minimal polynomial for α over $\mathbb{Q}$. To prove this, we show that $f(x)$ is irreducible over $\mathbb{Q}$. Here are two ways:*

(a) *$f(x + 1) = x^4 + 4x^3 + 6x^2 + 4x + 2$ is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$. Thus f is also irreducible over $\mathbb{Q}$.*

(b) *By the rational roots theorem, f has no rational roots and hence no linear factors in $\mathbb{Q}[x]$. We look for a quadratic factor of form $x^2 + bx + c \in \mathbb{Z}[x]$. (We know that, f has a quadratic factor in $\mathbb{Q}[x]$ if and only if it has a monic quadratic factor in $\mathbb{Z}[x]$.) To see if $x^2 + bx + c$ is a factor of f we use long division:*

$$f(x) = (x^2 + bx + c)(x^2 - bx + (b^2 - c)) + (2bc - b^3)x + (1 - c(b^2 - c)).$$

So x^2+bx+c divides f if and only if the remainder, $(2bc-b^3)x+(1-c(b^2-c))$ is zero, that is, if and only if $2bc - b^3 = 0$ and $1 - c(b^2 - c) = 0$. The second of these equations implies $1 = c(b^2-c)$, and so either $c = b^2-c = 1$ or $c = b^2 - c = -1$. These imply $b^2 = \pm 2$ and so there are no $b, c \in \mathbb{Z}$ such that $x^2 + bx + c$ is a factor of f.

Since we have now shown that f has no linear or quadratic factors in $\mathbb{Q}[x]$, f is irreducible over $\mathbb{Q}$.

(3) Let E/F be a Galois extension, $\phi \in \mathrm{Gal}(E/F)$ and $\alpha \in E$. Show that $\phi(\alpha)$ and α are conjugate over F.

`Answer:` *Suppose that $f(\alpha) = 0$ for some $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$. Applying ϕ to the equation $f(\alpha) = 0$, using the fact that ϕ is an automorphism of E that fixes all elements of F, we get*

$$\begin{aligned} 0 &= \phi(f(\alpha)) \\ &= \phi(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= a_0 + a_1\phi(\alpha) + \cdots + a_n\phi(\alpha)^n \\ &= f(\phi(\alpha)). \end{aligned}$$

Thus any polynomial in $F[x]$ having α is a root, also has $\phi(\alpha)$ as a root. The converse is also true because $\phi^{-1} \in \mathrm{Gal}(E/F)$. If this does not correspond to your definition of conjugate, there's one more step:

Let $m \in F[x]$ be the minimal polynomial of α over F, then from above, $m(\phi(\alpha)) = 0$ and so m divides the minimal polynomial of $\phi(\alpha)$ over F. Similarly, the minimal polynomial of $\phi(\alpha)$ over F divides the minimal polynomial of α over F. Thus the two minimal polynomials are equal, and α and $\phi(\alpha)$ are conjugate over F.