ALGEBRA COMPREHENSIVE EXAMINATION

Spring 2011

Brookfield*, 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.

Groups

(1) Let p be a prime number of the form $4k+1$ for some integer k. Define $f : \mathbb{Z}_p \to \mathbb{Z}_p$ by $f(x) = x^{p-2}$.

(a) Prove that f is bijective. (Hint: Prove that f is its own inverse.)

Answer: *By Fermat, $x^p = x$ for all $x \in \mathbb{Z}_p$. So*

$$f(f(x)) = f(x^{p-2}) = (x^{p-2})^{p-2} = x^{p^2-4p+4} = (x^p)^{p-4}x^4 = x^{p-4}x^4 = x^p = x$$

for all $x \in \mathbb{Z}_p$. Since $f \circ f$ is the identity function on $\mathbb{Z}_p$, f is its own inverse and, in particular, is a bijection.

OR

If $x \neq 0$, then x is a unit and by Fermat $x^{p-1} = 1$. Hence $f(x) = x^{p-2} = x^{-1}$ in this case. Consequently $f(f(x)) = (x^{-1})^{-1} = x$. Since, also $f(0) = 0$ and so $f(f(0)) = 0$, we have $f(f(x)) = x$ for all $x \in \mathbb{Z}_p$.

(b) Regarding f as an element of the symmetric group S_p, prove that f is an odd permutation. (Hint: How many fixed points does f have?)

Answer: *Since f is its own inverse, f has order 2 in S_p, and f must be a product of disjoint transpositions. (Any element of S_n is a product of disjoint cycles. The order of such an element is the lcm of the lengths of the cycles.) The number of these transpositions is one half the number of elements of $\mathbb{Z}_p$ that are not fixed by f.*

Certainly 0 is fixed by f. And if $x \neq 0$ is fixed by f, then $x^{-1} = x$, that is $x^2 = 1$, and $x = \pm 1$ (since $p \neq 2$). Thus there are three elements of $\mathbb{Z}_p$ that are fixed by f, and $(4k+1) - 3 = 2(2k-1)$ that are not fixed by f. Thus f is a product of $2k-1$ transpositions, an odd number of transpositions, and so f is odd.

(2) Let G and H be groups and $\phi : G \to H$ be a group homomorphism. Prove that $G/\ker(\phi)$ is isomorphic to $\phi[G]$ where

$$\phi[G] = \{\phi(x) \mid x \in G\}$$

is the image of ϕ.

Answer: *Fraleigh, Theorem 14.11*

(3) Show that there are no simple groups of order 56.

Answer: *Let G be a group of order $56 = 2^3 \cdot 7$. By the Sylow theorems, G has $n_7 = 1$ or $n_7 = 8$ Sylow-7 subgroups, and $n_2 = 1$ or $n_2 = 7$ Sylow-2 subgroups. If $n_7 = 1$, then the Sylow-7 subgroup is normal and so G is not simple. Otherwise, if $n_7 = 8$, then G has 8 distinct Sylow-7 subgroups of order 7. The intersection of any pair of these subgroups is trivial, and each contains 6 elements of order 7. So there are $6 \cdot 8 = 48$ elements of order 7 in G. This leaves 8 elements of G that do not have order 7. These elements must form a*

unique Sylow-2 subgroup, which is therefore a normal subgroup of G. Once again, this means that G is not simple.

Rings

(1) Let R be a commutative ring with identity such that $x^2 = x$ for all $x \in R$. Let $f : R \to R$ be a function such that $f(ab) = a \cdot f(b) + b \cdot f(a)$ for all $a, b \in R$. Prove that $f(a) = 0$ for all $a \in R$.
`Answer:` *Using $x^2 = x$ for all $x \in R$, we get $2a = (2a)^2 = 4a^2 = 4a$ and cancelling $2a$ from this gives $0 = 2a$. Then $f(a) = f(a^2) = a \cdot f(a) + a \cdot f(a) = 2af(a) = 0f(a) = 0$.*

(2) Let R and S be commutative rings. Let I be an ideal of R. Let $\phi : R \to S$ be an onto ring homomorphism. Prove that

$$\phi[I] = \{\phi(x) \mid x \in I\}$$

is an ideal of S.
`Answer:` *Let $J = \phi[I]$. Since ϕ is, among other things, a group homomorphism from $(R, +)$ to $(S, +)$, we know that J is an additive subgroup of $(S, +)$.*

Let $s \in S$ and $j \in J$. Then $j = \phi(i)$ for some $i \in I$ and, since ϕ is surjective, $s = \phi(r)$ for some $r \in R$. Because I is an ideal, $ri \in I$ and $ir \in I$. Then $sj = \phi(r)\phi(i) = \phi(ri) \in \phi[I] = J$ and similarly, $js \in J$. Thus J is an ideal of S.

(3) Let f be a monic polynomial with integer coefficients. Show that any rational root of f is an integer.
`Answer:` *Fraleigh Theorem 23.12.*

Fields

(1) Let $f(x)$ be a polynomial with integer coefficients. Show that $\alpha = \dfrac{1+\sqrt{5}}{2}$ is a root of $f(x)$ if and only if $\beta = \dfrac{1-\sqrt{5}}{2}$ is a root of $f(x)$.
`Answer:` *Since $\sqrt{5}$ is not rational, neither are α and β, and so the degree of α and β over $\mathbb{Q}$ is bigger than 1. On the other hand, both α and β are a roots of $p(x) = x^2 - x - 1$, a monic polynomial in $\mathbb{Q}[x]$ of degree 2. So p is the minimal polynomial for both α and β over $\mathbb{Q}$.*

If α is a root of $f(x) \in \mathbb{Q}[x]$, then p divides f, and then β is a root of f too. Similarly, if β is a root then so is α.

(2) Let F and E be fields and $\phi : F \to E$ be a ring homomorphism.
   (a) Prove that the only two ideals of F are F and $\{0\}$.
   (b) Prove that ϕ is one-to-one if and only if ϕ is not the zero map.
`Answer:`
   (a) *Let I be an ideal of F and suppose that I is not $\{0\}$. Then I contains a nonzero element a. Since F is a field, a^{-1} exists. Now for any $r \in F$ we have $r = r(1) = (ra^{-1})a \in I$. This implies that $F \subseteq I$, and so $I = F$.*
   (b) *If ϕ is one-to-one, then $\phi(1) \neq \phi(0) = 0$ so ϕ is not the zero map. Conversely, if ϕ is not the zero map, then $\ker \phi$ is a proper ideal of F. By (a), $\ker \phi = \{0\}$. This implies that ϕ is injective.*

(3) Let F be a field and $f \in F[x]$ a monic polynomial. Suppose that E is the splitting field for f over F so that $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ has

roots α_1, α_2,..., α_n in E. Let ϕ be an automorphism of E over F. Show that ϕ restricts to a permutation of the set $A = \{\alpha_1, \alpha_2, \ldots, \alpha_m\} \subseteq E$.
`Answer:` *We need to show that* $\phi(A) \subseteq A$. *If* $\alpha \in A$, *then* $f(\alpha) = 0$. *Writing* $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + x^n$, *we have*

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + \alpha^n = 0.$$

Applying the automorphism ϕ *to both sides of this equation and using the homomorphism properties of* ϕ *we get*

$$a_0 + a_1\phi(\alpha) + a_2\phi(\alpha)^2 + \cdots + \phi(\alpha)^n = 0,$$

which shows that $\phi(\alpha)$ *is a root of* f *and hence* $\phi(\alpha) \in A$. *Therefore* ϕ *restricts to a function from* A *to* A.

By definition, ϕ *is injective on* E, *and so is also injective when restricted to* A. *Since* A *is finite, this means* ϕ, *restricted to* A, *is surjective.*