ALGEBRA COMPREHENSIVE EXAMINATION

Fall 2015

Brookfield, 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: $\mathbb{Q}$ denotes the rational numbers; $\mathbb{Z}_n$ denotes the integers modulo n.

Groups

(G1) Let G be a cyclic group. Let N be a subgroup of G.

(a) Prove that N is normal in G.

(b) Prove that G/N is cyclic.

`Answer:`

(a) G is cyclic, so abelian. Any subgroup of an abelian group is normal.

(b) Elements of G/N are cosets of N so have the form gN with $g \in G$. Since G is cyclic we have $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ for some $a \in G$. So elements of G/N have the form a^nN with $n \in \mathbb{Z}$. Because of the multiplication rule in G/N, $a^nN = (aN)^n$ and so, $G/N = \{(aN)^n \mid n \in \mathbb{Z}\}$, that is, $G/N = \langle aN \rangle$ is cyclic.

(G2) Let D_{2n} have the usual presentation, $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1}\rangle$. Show that every element of D_{2n}which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr both of which have order 2.

`Answer:` We know that $D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$, so an element that is not a power of r must have the form $x = sr^k$ for some $k \in \mathbb{N}$. By a simple induction from $rs = sr^{-1}$ we get $r^ks = sr^{-k}$ and so

$$x^2 = sr^ksr^k = s(r^ks)r^k = s(sr^{-k})r^k = s^2 = 1.$$

Since $x \neq 1$, this implies $|x| = 2$.

sr is not a power of r so has order 2 by the argument just made. Moreover, any subgroup of D_{2n} that contains sr and s contains $r = s(sr)$ and s, so

$$D_{2n} = \langle r, s \rangle \leq \langle sr, s \rangle \leq D_{2n}.$$

(G3) Suppose that G is a simple group of order 168.

(a) Prove that G contains exactly 8 Sylow 7-subgroups.

(b) Prove that G contains exactly 48 elements of order 7.

`Answer:` By Sylow, $n_7 \in \{1, 8\}$. But if $n_7 = 1$, then G has a unique normal subgroup of order 7 and is not simple, contrary to hypothesis. Thus G has 8 Sylow subgroups of order 7. Each of these contains 6 elements of order 7, so there are a total of 48 elements of order 7 in the group.

Rings

(R1) Suppose that R is a Principal Ideal Domain and I is a prime ideal of R. Prove that R/I is a Principal Ideal Domain.

`Answer:` Since I is prime, R/I is a domain (Fraleigh, Theorem 17.15). Let $\phi : R \to R/I$ be the canonical (natural) ring homomorphism. Let J be an ideal of R/I. Then $\phi^{-1}(J)$ is an ideal of R (The inverse image of an ideal is an ideal). Since R is a PID, $\phi^{-1}(J) = \langle r \rangle$ for some $r \in R$. We show that $\langle \phi(r) \rangle = J$.

- Since $r \in \phi^{-1}(J)$, we have $\phi(r) \in J$ and $\langle \phi(r) \rangle \leq J$.
- Conversely, suppose that $j \in J$. Because ϕ is surjective, we have $j = \phi(s)$ for some $s \in R$. Then $s \in \phi^{-1}(J) = \langle r \rangle$ and $s = xr$ for some $x \in R$. Hence

$$j = \phi(s) = \phi(xr) = \phi(x)\phi(r) \in \langle \phi(r) \rangle.$$

This holds for all $j \in J$, so we have shown that $J \leq \langle \phi(r) \rangle$.

We have now shown that any ideal J of R/I is principal, and so R/I is a PID.

(R2) Let S be a subring of R.

(a) Suppose that I is an ideal of R. Is $J = S \cap I$ an ideal of S? Proof or counterexample.

(b) Suppose that J is an ideal of S. Is $J = S \cap I$ for some ideal I of R? Proof or counterexample.

`Answer:`

(a) Yes. Since S and I are subgroups of $(R, +)$, $J = S \cap I$ is also a subgroup of $(R, +)$. (Intersections of subgroups are subgroups.)

Suppose that $s \in S$ and $j \in J$. Then $sj \in S$ because $s, j \in S$ and S is a closed under multiplication, and also $sj \in I$ because $s \in R$, $j \in I$ and I is an ideal. Thus $sj \in S \cap I = J$. Similarly, $js \in J$. Thus J is an ideal if S.

(b) No. Counterexample: Let $S = \mathbb{Z}$ and $R = \mathbb{Q}$. $\mathbb{Q}$ is a field so only has two ideals: $\{0\}$ and $\mathbb{Q}$. The intersections of these ideals with $\mathbb{Z}$ are $\{0\}$ and $\mathbb{Z}$. These are ideals of $\mathbb{Z}$, but $\mathbb{Z}$ has infinitely many other ideals than these two.

(R3) Let R and S be rings and I be an ideal of R. Let $\phi : R \to S$ be an onto ring homomorphism. Prove that $\phi(I)$ is an ideal of S.

`Answer:` From the definition of ideal, we have two things to prove:

(a) $\phi(I)$ is a additive subgroup of S: Suppose $j_1, j_2 \in \phi(I)$. Then $j_1 = \phi(i_1)$ and $j_2 = \phi(i_2)$ for some $i_1, i_2 \in I$. Then $j_1 - j_2 = \phi(i_1) - \phi(i_2) = \phi(i_1 - i_2) \in \phi(I)$ because $i_1 - i_2 \in I$. Thus $j_1 - j_2 \in \phi(I)$.

(b) If $j \in \phi(I)$ and $s \in S$, then sj and js are in $\phi(I)$: If $j \in \phi(I)$ then $j = \phi(i)$ for some $i \in I$. Since ϕ is onto (surjective), $s = \phi(r)$ for some $r \in R$. Then $sj = \phi(r)\phi(i) = \phi(ri) \in \phi(I)$ (since $ri \in I$) and similarly, $js = \phi(i)\phi(r) = \phi(ir) \in \phi(I)$ (since $ir \in I$).

Fields

(F1) Let F, L, K be fields with $F \subseteq L \subseteq K$, $[K : L] = n$, and $[L : F] = m$. Prove that $[K : F] = mn$. [Hint: Think about bases and vector spaces.]

`Answer:` Fraleigh, Theorem 31.4. Dummit and Foote, Theorem 14, p. 523.

(F2) Let $\alpha \in \mathbb{C}$ be a zero of $f(x) = x^4 - 2x^2 + 9 \in \mathbb{Q}[x]$.

(a) Show that f is irreducible over $\mathbb{Q}$.

(b) Express $1/(1-\alpha)$ as a $\mathbb{Q}$-linear combination of $\{1, \alpha, \alpha^2, \alpha^3\}$.

`Answer:`

(a) (Eisenstein is no help!) By the rational zeros theorem, the only possible rational zeros of f are ± 1, ± 3 and ± 9. It is easy to check that none these numbers is in fact a zero, so f has no linear factors in $\mathbb{Q}[x]$.

If f has quadratic factors in $\mathbb{Q}[x]$, then by Gauss's Lemma,

$$f(x) = (x^2 + ax + b)(x^2 + cx + d)$$

for some $a, b, c, d \in \mathbb{Z}$. Matching coefficients we get $a + c = 0$, $b + d + ac = -2$, $ad + bc = 0$ and $bd = 9$. From the first and third of these equations we get $a = -c$ and $a(b - d) = 0$. Case 1: If $a = 0$, then $c = 0$, $b + d = -2$ and $bd = 9$. These equations in b and d have no solution in $\mathbb{Z}$. Case 2: If $b = d$, then $2b - a^2 = -2$ and $b^2 = 9$. Thus $b = \pm 3$ and $\pm 6 - a^2 = -2$, that is, $a^2 = 2 \pm 6$. There is no integer a satisfying this equation. Since Case 1 and Case 2 are both impossible, f has no quadratic factors in $\mathbb{Q}[x]$.

Since f has no linear or quadratic factors it is irreducible over $\mathbb{Q}$.

(b) Using long division we find

$$f(x) = (x-1)(x^3 + x^2 - x - 1) + 8.$$

Plugging in α into this gives

$$0 = (\alpha - 1)(\alpha^3 + \alpha^2 - \alpha - 1) + 8,$$

which can be solved for $1/(1-\alpha)$:

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

(F3) Let F be the Galois field with 2^n elements. Prove that any $\alpha \in F$ has a square root in F.

`Answer:` Consider the function $\phi : F \to F$ defined by $\phi(x) = x^2$ for all $x \in F$. (ϕ is called the Frobenius homomorphism.) We show that ϕ is injective.

Suppose that $\phi(x) = \phi(y)$ for some $x, y \in F$ so that that $x^2 = y^2$. Since F has characteristic 2, we have $2xy = 0$ and $-y^2 = y^2$, and so

$$(x-y)^2 = x^2 + 2xy + y^2 = 0.$$

This implies $x - y = 0$, that is, $x = y$.

This shows that ϕ is injective. Since F is finite, ϕ is also surjective. Then for any $\alpha \in F$ there is some $\beta \in F$ such that $\phi(\beta) = \alpha$. In other words, $\beta^2 = \alpha$.