ALGEBRA COMPREHENSIVE EXAMINATION

Fall 2017

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: $\mathbb{Q}$ denotes the rational numbers; $\mathbb{Z}$ is the set of integers; $\mathbb{Z}_n$ is the set of integers modulo n; and $\mathbb{C}$ is the set of complex numbers.

Groups

(G1) Let H and K be subgroups of a group G. Show that $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.

`Answer:` If $H \subseteq K$ or $K \subseteq H$, then $H \cup K$ is either K or H, so $H \cup K$ is a subgroup.

Conversely, suppose that $H \cup K$ is a subgroup. If the claim is not true, then there are $h_0 \in H$ and $k_0 \in K$ such that $h_0 \notin K$ and $k_0 \notin H$. Since $h_0, k_0 \in H \cup K$ and $H \cup K$ is a group, we have $h_0 k_0 \in H \cup K$. So $h_0 k_0 \in H$ or $h_0 k_0 \in K$. But both of these conditions lead to contradictions: If $h_0 k_0 \in H$, then $h_0 k_0 = h_1$ for some $h_1 \in H$ and then $k_0 = h_0^{-1} h_1 \in H$, a contradiction. Similarly, if $h_0 k_0 \in K$, then $h_0 \in K$. Thus the claim must be true.

(G2) Let G be a group such that (i) and (ii) below are true:

(i) For every nontrivial group H, there exists a nontrivial homomorphism from G to H, and

(ii) If f is a homomorphism from G to G and $f \circ f = f$, then either $f(x) = x$ for all $x \in G$, or else $f(x) = e$ for all $x \in G$. (Here e denotes the identity element of G.)

(a) Show that there is a surjective homomorphism g from G to $\mathbb{Z}$, where $\mathbb{Z}$ is the group of integers under addition. [Hint: Use (i).]

(b) Using your answer from (a), let $p \in G$ such that $g(p) = 1$. Define $h\colon \mathbb{Z} \to G$ by $h(n) = p^n$. Prove that h is a homomorphism.

(c) Using your answer from (b), prove that $g \circ h$ is the identity function on $\mathbb{Z}$.

(d) Prove that G is isomorphic to $\mathbb{Z}$. [Hint: Let $f = h \circ g$, and apply (ii). Use your answer from (c).]

`Answer:`

(a) By (i), there exists a nontrivial homomorphism j from G to $\mathbb{Z}$. Then $j(G)$ is a nontrivial subgroup of $\mathbb{Z}$, and $j(G)$ is generated by some positive integer k. Define $g : G \to \mathbb{Z}$ by $g(x) = j(x)/k$ for all $x \in G$. It is straightforward to show that g is a surjective homomorphism.

(b) $h(n+m) = p^{n+m} = p^n p^m = h(n)h(m)$

(c) Observe that for all $n \in \mathbb{Z}$, we have that $g(h(n)) = g(p^n) = ng(p) = n \cdot 1 = n$.

(d) Note that f is a homomorphism, because it is a composition of homomorphisms. So $f \circ f(x) = h(g(h(g(x)))) = h(g(x)) = f(x)$, using (c). Also, f is nontrivial, because $f(p) = h(g(p)) = h(1) = p$. So by (ii), f is the identity function. So $h \circ g$ is the identity function. That plus (c) implies that g and h are inverse functions.

(G3) Let G be a group of order 15. Prove that G is abelian.
`Answer:` See F08 and F11.

Rings

(R1) Let R be the set of all rational numbers of the form $a/2^k$ where a is an integer and k is a nonnegative integer.
(a) Prove that R is a commutative ring with unity, under usual addition and multiplication.
(b) Prove that R is not a field.
(c) Is $\mathbb{Z}$ an ideal of R? Prove that your answer is correct.
`Answer:` (a) It is easy to show that R is a subring of $\mathbb{Q}$. The only nontrivial part is to show that R is closed under addition: Suppose that $a/2^k, b/2^m \in R$. Without loss of generality we can assume that $k \leq m$, then

$$\frac{a}{2^k} + \frac{b}{2^m} = \frac{a2^{m-k} + b}{2^m} \in R$$

(b) We show that $3 \in R$ has no inverse in R. Suppose, to the contrary, that $3(a/2^k) = 1$ for some $a, k \in \mathbb{Z}$ with $k \geq 0$. Then $3a = 2^k$, which is impossible because 3 is prime and not equal to 2.
(c) No, it is not, because $1 \in \mathbb{Z}$, but $(1/2)(1) \notin \mathbb{Z}$.

(R2) Let $R = \mathbb{Z}_3[x]/I$ where $I = (x^2 - 1)$.
(a) List the elements of R. Show how you got these elements.
`Answer:` Every element of R has the form $a + bx + I$ with $a, b \in \mathbb{Z}_3$. Hence

$$R = \{0 + I, 1 + I, 2 + I, x + I, 1 + x + I, 2 + x + I, 2x + I, 1 + 2x + I, 2 + 2x + I\}.$$

(b) Is R a field? An integral domain? Prove that your answer is correct.
`Answer:` Neither. For example, $(x - 1 + I)(x - 1 + I) = x^2 - 1 + I = 0 + I$, so R has zero divisors. OR $x^2 - 1$ is reducible over $\mathbb{Z}_3$, so I is not maximal, and hence R/I is not a field. Since finite domains are fields, R/I is not a domain either.
(c) Let G be the group of units of R. List the elements of G. Also, find a familiar group that is isomorphic to G and prove it.
`Answer:` The group of units of R is $\{1+I, 2+I, x+I, 2x+I\}$. Since $(2+I)^2 = 1+I$ and $(x + I)^2 = x^2 + I = x^2 - (x^2 - 1) + I = 1 + I$, this group has at least two elements of order 2, so must be isomorphic to the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(R3) Let R be commutative ring with identity $1 \neq 0$.
(a) Prove that R is an integral domain if and only if $R[x]$ is an integral domain.
(b) Let R be an integral domain. Prove that the set of units of $R[x]$ is equal to the units in R.

`Answer:` Dummit and Foote, Proposition 4, page 235.

Fields

(F1) Let R be a finite integral domain. Prove that R is a field.
`Answer:` Dummit and Foote, Corollary 3, page 228. See also F07, F08, F10.
Let $a \in R$ be nonzero. Consider the function $\phi : R \to R$ defined by $\phi(x) = ax$ for all $x \in R$. We show that ϕ is injective: If $\phi(x) = \phi(y)$ for some $x, y \in R$, then $ax = ay$ and $a(x - y) = 0$. Since R is a domain and $a \neq 0$, this implies $x - y = 0$, that is $x = y$.

Because, R is finite and ϕ is injective, ϕ is also surjective. In particular, there is some $b \in R$ such that $\phi(b) = 1$. This means that $ab = 1$, that is, $b = a^{-1}$.

Since all nonzero elements of R have inverses, R is a field.

(F2) Let p be prime. Let $f \in \mathbb{Q}[x]$. Let $\zeta = e^{2\pi i/p}$.

(a) Prove that $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$ are linearly independent over $\mathbb{Q}$.

(b) Prove that if $f(\zeta) = f(\zeta^a)$ for all $a = 1, ..., p-1$, then $f(\zeta)$ in $\mathbb{Q}$. [Hint: First use your answer in (a) to prove that this statement is true when f is of the form $c_1x + c_2x^2 + ... + c_{p-1}x^{p-1}$.]

`Answer:` (a) We have that ζ is a root of $1 + x + x^2 + \cdots + x^{p-1}$, which is irreducible.

(b) First assume that f is of the form $c_1x + c_2x^2 + ... + c_{p-1}x^{p-1}$. Because p is prime, for all $j = 1, \ldots, p-1$, there exists k such that kj is congruent to 1 mod p. Then $c_1\zeta + c_2\zeta^2 + ... + c_{p-1}\zeta^{p-1} = f(\zeta) = f(\zeta^k) = c_1\zeta^k + c_2\zeta^2 k + ... + c_{p-1}\zeta^{p-1}k$. Comparing coefficients and using (a), we get that $c_1 = c_j$. Because j was arbitrary, we get $c_1 = \cdots = c_{p-1}$. So

$$f(\zeta) = c_1\zeta + c_2\zeta^2 + ... + c_{p-1}\zeta^{p-1} = c_1(\zeta + \cdots + \zeta^{p-1}) = -c_1 \in \mathbb{Q}.$$

Now take an arbitrary $f = c_0 + c_1x + c_2x^2 + ... + c_{p-1}x^{p-1} + \cdots + c_nx^n$. Then by what we proved earlier, $f(\zeta) = c_0 + [c_1x + c_2x^2 + ... + c_{p-1}x^{p-1}] + c_p\zeta^p + x^p[c_{p+1}x + c_{p+2}x^2 + ... + c_{2p-1}x^{p-1}] + \cdots + \zeta^{bp} + x^{bp}[c_{bp+1}x + c_{bp+2}x^2 + ... + c_{(b+1)p-1}x^{p-1}] \in \mathbb{Q}$ for some b.

(F3) Suppose that $\alpha, \beta \in \mathbb{C}$ satisfy $\beta^3 = 2$ and $\alpha = \beta + \beta^2$.

(a) Find $a_0, a_1, a_2 \in \mathbb{Q}$ such that $\beta = a_0 + a_1\alpha + a_2\alpha^2$.

`Answer:` Plugging $\alpha = \beta + \beta^2$ into the equation $\beta = a_0 + a_1\alpha + a_2\alpha^2$ and simplifying using $\beta^3 = 2$ gives

$$\beta = (a_0 + 4a_2) + (a_1 + 2a_2)\beta + (a_1 + a_2)\beta^2.$$

Because of the linear independence of $\{1, \beta, \beta^2\}$ over $\mathbb{Q}$ we get the linear equations $0 = a_0 + 4a_2$, $1 = a_1 + 2a_2$ and $a_1 + a_2 = 0$. This system has the solution $a_0 = -4$, $a_1 = -1$, $a_2 = 1$, that is, $\beta = -4 - \alpha + \alpha^2$.

(b) Show $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$.

`Answer:` We are given $\alpha = \beta + \beta^2 \in \mathbb{Q}(\beta)$ which implies $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta)$. From (a), $\beta = -4 - \alpha + \alpha^2 \in \mathbb{Q}(\alpha)$, and so $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$.

OR

Since β is a root of the polynomial $x^3 - 2 \in \mathbb{Q}[x]$, which is irreducible over $\mathbb{Q}$ by Eisenstein, we have $[\mathbb{Q}(\beta), \mathbb{Q}] = 3$. As above $\alpha \in \mathbb{Q}(\beta)$ and so $[\mathbb{Q}(\alpha), \mathbb{Q}] = 3$ in which case $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$, or $[\mathbb{Q}(\alpha), \mathbb{Q}] = 1$ in which case $\alpha \in \mathbb{Q}$.

But $\alpha \in \mathbb{Q}$ is not possible since otherwise, β is a root of the degree 2 polynomial $x^2 + x - \alpha \in \mathbb{Q}[x]$.

(c) Find the minimal polynomial for α over $\mathbb{Q}$.

`Answer:` Because $[\mathbb{Q}(\alpha), \mathbb{Q}] = 3$ we are looking a monic cubic polynomial in $\mathbb{Q}[x]$ with α as a root. Some calculation using $\beta^3 = 2$ gives $\alpha^3 = 6 + 6\beta + 6\beta^2 = 6 + 6\alpha$, and so $\alpha^3 - 6\alpha - 6 = 0$. So the minimal polynomial for α over $\mathbb{Q}$ is $x^3 - 6x - 6 \in \mathbb{Q}[x]$.