ALGEBRA COMPREHENSIVE EXAMINATION

Spring 2016

Brookfield*, Webster, (Krebs)

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: $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{C}$ denote the set of integers, rational numbers and complex numbers respectively.

Groups

(G1) Show that no group of order 105 is simple.

`Answer:` Suppose, contrary to the claim that G is a simple a group with $|G| = 105$. By the Sylow theorems, the number of Sylow 5-subgroups n_5 satisfies $n_5 \equiv 1 \mod 5$ and $n_5 \mid 21$. Thus $n_5 = 1, 21$. Similarly, $n_7 \equiv 1 \mod 7$ and $n_7 \mid 15$. Thus $n_7 = 1, 15$. But, because G is simple, it has no nontrivial proper normal subgroups, and so $n_5 = 1$ and $n_7 = 1$ are not possible. Thus $n_5 = 21$ and $n_7 = 15$. By the usual argument, this implies that G has $21 \cdot 4 = 84$ elements of order 5 and $15 \cdot 6 = 90$ elements of order 7—an obvious impossibility in a group of order 105.

(G2) Let G be a group and $Z(G)$ the center of this group. Prove that if $G/Z(G)$ is cyclic then G is abelian.

`Answer:` See F12 Algebra Exam.

(G3) Prove that $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic (as groups under addition).

`Answer:` Let $\phi : \mathbb{Z} \to \mathbb{Q}$ be a homomorphism. We show that ϕ is not surjective, so, in particular, ϕ is not an isomorphism.

Let $q = \phi(1) \in \mathbb{Q}$. Then by familiar properties of homomorphisms, $\phi(n) = nq$ for all $n \in \mathbb{Z}$. If $q = 0$, then $\phi(n) = 0$ for all $n \in \mathbb{Z}$, so ϕ is not surjective in this case.

If $q \neq 0$, then the image of ϕ is the set of all integer multiples of q. In particular, $q/2$ is not in the image of ϕ. (If it were, then $q/2 = nq$ for some integer $n \in \mathbb{Z}$. After cancelation, this implies that $1/2 = n$, an obvious contradiction.)

Rings

(R1) Let F be a field and $F^* = \{x \in F \mid x \neq 0\}$ the group of units of F (under multiplication). Show that for each $n \in \mathbb{N}$, F^* has at most one subgroup of order n.

`Answer:` Let G be a subgroup of F^* with order n. By Lagrange's Theorem, $u^n = 1$ for all $u \in G$, that is, all elements of G are roots of $x^n - 1 \in \mathbb{Z}[x]$. But this polynomial can have at most n roots. Because G has n elements, this means that G is precisely the set of roots of $x^n - 1 \in \mathbb{Z}[x]$, that is, $G = \{x \in F^* \mid x^n - 1 = 0\}$.

If H is another subgroup of F^* with order n, then the same argument shows $H = \{x \in F^* \mid x^n - 1 = 0\}$, and so $H = G$.

(R2) Let a and b be elements of an integral domain D. If $a|b$ and $b|a$, then a and b are called **associates**, which we denote by $a \approx b$. Prove the following for $a, b, c \in D$ with $c \neq 0$.

(a) $a \approx 1$ if and only if a is a unit.

(b) $ac \approx bc$ if and only if $a \approx b$.

(c) $a \approx b$ if and only if $b = ua$ and $a = u^{-1}b$ for some unit $u \in D$.

`Answer:`

(a) If $a \approx 1$, then in particular, $a|1$ so there is some $u \in D$ such that $au = 1$. This means that a is a unit.
Conversely, if a is a unit, then there is some $u \in D$ such that $au = 1$. This means that $a|1$. Also, since $a = 1a$, we have $1|a$ and so $a \approx 1$.

(b) Suppose that $ac \approx bc$. Then $ac|bc$, that is $acs = bc$ for some $s \in D$. Since c is nonzero, we can cancel c from this equation to get $as = b$, and so $a|b$. Similarly, $bc|ac$ implies that $b|a$.
Suppose that $a \approx b$. Then $a|b$ and $b|a$. As above, these imply that $ac|bc$ and $bc|ac$, so $ac \approx bc$.

(c) Suppose first that $a \approx b$ with $a \neq 0$. Then $a|b$ and $b|a$, so there are $u, v \in D$ such that $av = b$ and $bu = a$. Eliminating b from these equations gives $a(uv - 1) = 0$. Since $a \neq 0$, this implies that $uv = 1$, that is, u is a unit and $v = u^{-1}$.
Suppose next that $a \approx b$ with $a = 0$. Then $a|b$ implies that $b = 0$, and $b = ua$ and $a = u^{-1}b$ holds with $u = 1$.
The converse is easy, since if $b = ua$ and $a = u^{-1}b$, then $a|b$ and $b|a$ and so $a \approx b$.

(R3) Suppose that R is a principal ideal domain and $p \in R$. Prove that p is prime if and only if p is irreducible.

`Answer:` (Dummit and Foote, 8.3, Proposition 11) The definitions of prime and irreducible both include the requirement that p is nonzero and not a unit. Then, by definition, p is prime if $p|ab$ implies $p|a$ or $p|b$, and p is irreducible if $p = ab$ implies a is a unit or b is a unit.

Suppose that p is prime. If $p = ab$ for some $a, b \in R$, then $p|ab$ and so $p|a$ or $p|b$. Without loss of generality, suppose that $p|a$, that is $ps = a$ for some $s \in R$. Combining these equations we get $p(sb - 1) = 0$, and since $p \neq 0$, we can cancel p to get $sb = 1$ showing that b is a unit.

Suppose that p is irreducible. We show first that (p) is maximal. Suppose that I is an ideal that contains (p). Since I is principal, $I = (r)$ for some $r \in R$, and then $p \in (r)$ implies that $p = rs$ for some $s \in R$. Because p is irreducible we have two cases: If r is a unit, then $I = (r) = R$. Otherwise s is a unit. In this case $r = s^{-1}p$ and so $r \in (p)$, and $(r) \subseteq (p)$. Combined with $(p) \subseteq I = (r)$ we get $I = (p)$. We have shown that, if I contains (p) then $I = R$ or $I = (p)$.

Now suppose $p|ab$ for some $a, b \in R$. We suppose that p does not divide a and show that p must divide b. Because $a \notin (p)$, (p, a) is strictly bigger than (p), and so, because (p) is maximal, we have $(p, a) = R$. In particular, there

are $x, y \in \mathbb{R}$ such that $xp+ya = 1$. Multiplying this by b we get $xpb+yab = b$. Since both xpb and yab are divisible by p, the same is true of b, that is $p|b$.

Fields

(F1) Let $f(x) = x^3 + 9x + 6$ and let $\theta \in \mathbb{C}$ be a root of $f(x)$.

(a) Show that $f(x)$ is irreducible over $\mathbb{Q}$.
`Answer:` This follows from Eisenstein with $p = 3$

(b) Express $\dfrac{1}{\theta+1}$ as a $\mathbb{Q}$-linear combination of $\{1, \theta, \theta^2\}$.
`Answer:` Using long division we get $f(x) = (x^2 - x + 10)(x + 1) - 4$. Plugging in $x = \theta$ in this gives $0 = (\theta^2 - \theta + 10)(\theta + 1) - 4$ which can be written as

$$\frac{1}{\theta+1} = \frac{1}{4}(\theta^2 - \theta + 10)$$

(c) Express $\dfrac{1}{(\theta+1)^2}$ as a $\mathbb{Q}$-linear combination of $\{1, \theta, \theta^2\}$.
`Answer:` Many tricks can be used to answer this question.

- Using the Euclidean Algorithm we find

$$(-4 - 3x)f(x) + (3x^2 - 2x + 28)(x + 1)^2 = 4.$$

Plugging in $x = \theta$ in this gives $(3\theta^2 - 2\theta + 28)(\theta + 1)^2 = 4$ which be written as

$$\frac{1}{(\theta+1)^2} = \frac{1}{4}(3\theta^2 - 2\theta + 28)$$

- Squaring the result in (b) we find

$$\begin{aligned}\frac{1}{(\theta+1)^2} &= \frac{1}{16}(\theta^2 - \theta + 10)^2 \\ &= \frac{1}{16}(\theta^4 - 2\theta^3 + 21\theta^2 - 20\theta + 100) \\ &= \frac{1}{4}(3\theta^2 - 2\theta + 28)\end{aligned}$$

using $\theta^3 + 9\theta + 6 = 0$ and $\theta^4 + 9\theta^2 + 6\theta = 0$.

(F2) Find a complex number $\alpha \in \mathbb{C}$ such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$. Prove your claim.
`Answer:` (See S04 Algebra Exam) Many answers are possible, for example, $\alpha = \sqrt[6]{3}$. Since $\sqrt{3} = \alpha^3 \in \mathbb{Q}(\alpha)$ and $\sqrt[3]{3} = \alpha^2 \in \mathbb{Q}(\alpha)$ we have $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) \subseteq \mathbb{Q}(\alpha)$, and since $\alpha = \sqrt{3}/\sqrt[3]{3} \in \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$ we have $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$.

Alternatively, suppose that $\alpha = \sqrt{3} + \sqrt[3]{3}$. Then $\alpha \in \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$ so $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$. To prove the opposite inclusion, we note that $(\alpha - \sqrt{3})^3 = 3$, that is, $\alpha^3 - 3\sqrt{3}\,\alpha^2 + 9\alpha - 3\sqrt{3} = 3$. This can be solved for $\sqrt{3}$ to give,

$$\sqrt{3} = \frac{\alpha^3 + 9\alpha - 3}{3\alpha^2 + 3} \in \mathbb{Q}(\alpha)$$

This implies $\sqrt[3]{3} = \alpha - \sqrt{3} \in \mathbb{Q}(\alpha)$, and so $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) \subseteq \mathbb{Q}(\alpha)$.

(F3) Let F be a finite field. Show that $|F| = p^n$ for some $p, n \in \mathbb{N}$ with p prime.
`Answer:` (Fraleigh, Theorem 33.2) Let $K \subseteq F$ be the prime subfield of F. Since K is finite, it is isomorphic to the field $\mathbb{Z}_p$ for some prime p. Because F can be considered as a finite dimensional vector space over K, if $\dim_K F = n$, then each element of F can be written uniquely in the form $a_1b_1 + a_2b_2 + \cdots + a_nb_n$ where $\{b_1, b_2, \ldots, b_n\}$ is a basis for F over K, and $a_1, a_2, \ldots, a_n \in K$. Since there are p choices for each of $a_1, a_2, \ldots, a_n$, there are a total of p^n elements of F.