ALGEBRA COMPREHENSIVE EXAMINATION

Fall 2019

Brookfield, Demeke, 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: $\mathbb{R}$ denotes the set of real numbers; $\mathbb{Q}$ denotes the set of 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. All of these should be thought of as groups under ordinary addition, and as rings under ordinary addition and multiplication.

Groups

(G1) Let G be a group of order 99. Show that G is isomorphic to either $\mathbb{Z}_{99}$ or $\mathbb{Z}_{33} \times \mathbb{Z}_3$. (Note: You can quote, without proof, your favorite theorem about groups of order p^2 where p is prime.)

`Answer:` *This is the same as G1 from Spring 08 and G3 from Fall 13 with the prime 5 replaced by the prime 11. See also Fall 08 and Fall 11 exams regarding groups of order* 15.

By Sylow, $n_3 \equiv 1 \mod 3$ *and* n_3 *divides* 11, *so* $n_3 = 1$ *and* G *has a unique normal subgroup* K *of order* 9. *Also,* $n_{11} \equiv 1 \mod 11$ *and* n_{11} *divides* 3, *so* $n_{11} = 1$ *and* G *has a unique normal subgroup* H *of order* 11.

By the usual argument, $H \cap K = \{1\}$ *and* $H \times K \cong HK \leq G$. *Since* $|H \times K| = |H||K| = |G|$ *we have* $H \times K \cong G$.

We know that all groups of prime order and prime square order are abelian, and we know that direct products of abelian groups are abelian, so $H \times K \cong G$ *is abelian. Because* H *and* K *are abelian,* G *is abelian.*

By the Classification Theorem of Finite Abelian Groups, G *is isomorphic to either* $\mathbb{Z}_{99}$ *or* $\mathbb{Z}_{33} \times \mathbb{Z}_3$.

(G2) Let $\mathbb{R}$ be the set of real numbers, and let $\mathbb{Z}_2$ be the set of integers mod 2. Define an operation $*$ on $\mathbb{R} \times \mathbb{Z}_2$ by

$$(x, n) * (y, m) := (x + (-1)^n y, n + m).$$

(You may assume without proof that $*$ is a well-defined operation.)

(a) Prove that $\mathbb{R} \times \mathbb{Z}_2$ is a group under $*$.

(b) Is this group abelian? Prove that your answer is correct.

`Answer:` (a) *Associativity: A direct calculation shows that* $((x, n) * (y, m)) * (z, k)$ *and* $(x, n) * ((y, m) * (z, k))$ *are equal to*

$$(x + (-1)^n y + (-1)^{m+n} z, m + n + k).$$

Identity: $(0, 0)$ *is a left and right identity for* $\mathbb{R} \times \mathbb{Z}_2$.

Existence of inverses: The inverse of $(x, 0)$ *is* $(-x, 0)$. *The inverse of* $(x, 1)$ *is* $(x, 1)$.

(b) *This group is not abelian since, for example,* $(1, 1) * (0, 1) = (1, 0)$ *and* $(0, 1) * (1, 1) = (-1, 0)$.

(G3) Let G be a finite group. Provide a proof or a counterexample for the following statements:

(a) The number of elements of order 3 in G is even.
`Answer:` *If a has order 3, then a^{-1} also has order 3 and is not a. Since $(a^{-1})^{-1} = a$, elements of order 3 come in disjoint pairs of the form $\{a, a^{-1}\}$. Hence there must be an even number of elements of order 3.*

(b) If $a, b \in G$ such that $|a| = |b| = 3$, then $|ab| = 3$.
`Answer:` *Counterexample: Let a be an element of order 3 and $b = a^{-1}$. Then $|b| = 3$ and $|ab| = |e| = 1$.*
(Here $|x|$ means the order of x.)

Rings

(R1) Let R be a ring and let X and Y be ideals of R. Prove that

$$X + Y = \{a + b \mid a \in X, b \in Y\}$$

is an ideal of R.
`Answer:` *See Fraleigh, Chapter 27, Exercise 34*

(R2) Let $B = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid n \geq 0, n \in \mathbb{Z}, a_0, \ldots, a_n \in \mathbb{R}, a_1 = 0\}$. In other words, B is the set of all polynomials with real coefficients such that the coefficient of x is 0.

(a) Prove that B is a subring of $\mathbb{R}[x]$.
(b) Let $I = \{a_2 x^2 + \cdots + a_n x^n \mid n \geq 0, n \in \mathbb{Z}, a_2, \ldots, a_n \in \mathbb{R}\}$. Prove that I is an ideal of B.
(c) Prove that I is not a principal ideal. Hint: x^2 and x^3 are both elements of I.
(d) Prove that B is not a Euclidean domain. Hint: Use the other parts of this problem.

`Answer:` (a) *It is straightforward to check that B is closed under subtraction and multiplication. Compare Fraleigh Exercise 48, Section 18.*

(b) *It is straightforward to check that I is closed under subtraction and multiplication by elements of B. Compare Fraleigh Definition 26.10, Section 26.*

(c) *Suppose to the contrary that $I = (f)$ for some nonzero $f \in I$. Since $x^2, x^3 \in I$, there is some nonzero $g, h \in B$ such that $x^2 = gf$ and $x^3 = hf$. In particular this implies $\deg f + \deg g = 2$ and $\deg f + \deg h = 3$. Since there are no nonzero elements of I with degree 0 or 1, the first of these equations implies $\deg f = 2$. Then the second equation implies that $\deg h = 1$. This is a contradiction since B contains no elements of degree 1.*

(d) *By Fraleigh, Theorem 46.4, all Euclidean domains are PIDs. Because of* (c), *B is not a PID, so it can't be a Euclidean domain either.*

(R3) Let R be a commutative ring with identity 1_R. Prove that an ideal $M \neq R$ is maximal if and only if for every $r \in R$ with $r \notin M$, there exists $x \in R$ such that $1_R - xr \in M$.
`Answer:` *See Fall 08 and Fall 12.*

Fields

(F1) Let K be a field and F be a subfield of K. Prove that if $[K : F] = n$ and F has q elements, then K has q^n elements.
`Answer:` *Fraleigh, Theorem 33.1*

(F2) Suppose that E is the splitting field of a separable polynomial in $\mathbb{Q}[x]$ with $[E : \mathbb{Q}] = 6$. Show that there exists $\alpha \in E$ such that the minimal polynomial of α over $\mathbb{Q}$ has degree 3.

`Answer:` *E is a Galois extension of $\mathbb{Q}$ of degree 6, so the Galois group $\mathrm{Gal}(E, \mathbb{Q})$ has order 6. This group could be isomorphic to $\mathbb{Z}_6$ or to S_3. Either way, $\mathrm{Gal}(E, \mathbb{Q})$ has a subgroup of index 3. By the Galois theorems, there is an intermediate field K such that $\mathbb{Q} \subseteq K \subseteq E$ and $[K : \mathbb{Q}] = 3$. Let α be in K but not in $\mathbb{Q}$. Since the degree of α over $\mathbb{Q}$ divides $[K : \mathbb{Q}]$ and can't be 1 (since otherwise $\alpha \in \mathbb{Q}$), we have $\deg_{\mathbb{Q}} \alpha = 3$, that is, the minimal polynomial of α over $\mathbb{Q}$ has degree 3.*

(F3) Let F be a finite field of order n. Prove that the polynomial $x^2 + x + 1$ has a root in F if and only if $n - 1$ is divisible by 3. Hint: $(x^2 + x + 1)(x - 1) = x^3 - 1$.

Correction: For this claim to be true we have to assume that the characteristic of F is not 3.

`Answer:` *For a finite field F of order n, the group of units F^* has order $n - 1$.*

If 3 divides $n - 1$ then, by Cauchy's Theorem, F^* contains an element a of order 3. This means $a^3 = 1$ but $a \neq 1$. Equivalently, a is a root of $x^3 - 1$ but not of $x - 1$. Because of the factorization, $(x^2 + x + 1)(x - 1) = x^3 - 1$, a must be a root of $x^2 + x + 1$.

Conversely, if a is a root of $x^2 + x + 1$, then a is a root of $x^3 - 1$ and $a^3 = 1$. If the characteristic of F is not 3 then $1^2 + 1 + 1 = 3 \neq 0$ so 1 is not a root of $x^2 + x + 1$. Hence $a \neq 1$ and so a has order 3 in F^*. By Lagrange, 3 divides the order of F^*.

Example: In the field $\mathbb{Z}_3$, 1 is a root of $x^2 + x + 1$, even though 3 does not divide $|\mathbb{Z}_3| - 1 = 2$.