ALGEBRA COMPREHENSIVE EXAMINATION

Fall 2018

Brookfield, Demeke, 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 G be a cyclic group. Let H be a subgroup of G. Prove that H is cyclic.
`Answer:` *[See S08 and S13] Fraleigh, Theorem 6.6. Dummit and Foote, Theorem 7, p. 58.*

(G2) Let G be a finite group and H be a subgroup of G.
(a) Prove that for any $g \in G$, that gH and H have the same size.
(b) Prove for any $a, b \in G$, that either $aH \cap bH = \emptyset$ or $aH = bH$.
(c) Use (a) and (b) to prove Lagrange's theorem.
`Answer:` *Fraleigh, Theorem 10.10. Dummit and Foote, Theorem 8, p. 89.*

(G3) Let G be a group of order 10. Show that $G \cong \mathbb{Z}_{10}$ or $G \cong D_{10}$. Here $D_{10} = \langle r, s \mid r^5 = s^2 = 1, rsrs = 1 \rangle$ is the dihedral group of order 10.
`Answer:` *[Compare S13 and S17] The only divisors of $|G|$ are $\{1, 2, 5, 10\}$. If G has an element of order 10, then G is cyclic and $G \cong \mathbb{Z}_{10}$. Otherwise, all nonidentity elements of G have order 5 or 2.*

By the Sylow theorems, n_5 divides $|G|$ and $n_5 \equiv 1 \mod 5$, so $n_5 = 1$. Thus G has a unique normal subgroup N of order 5 and all elements of order 5 are in N. Since $N \cong \mathbb{Z}_5$, there are 4 elements of order 5 in G. The other 5 elements of G must have order 2.

Let $r \in G$ be any element of order 5 and $s \in G$ an element of order 2. Then $rs \in G$, so $|rs| \in \{1, 2, 5\}$. But if $|rs| = 1$ or $|rs| = 5$, then $rs \in N$ which implies $s = r^{-1}(rs) \in N$, contradicting $|s| = 2$. This means that $|rs| = 2$, and $rsrs = 1$ which can be rewritten as $rs = sr^{-1}$, showing that $G \cong D_{10}$.

Rings

(R1) Let R and S be commutative rings with multiplicative identities. Show that I is an ideal of $R \times S$ if and only if $I = A \times B$ where A is an ideal of R and B is an ideal of S. [Hint: Consider the sets $\{x \in R \mid (x, 0) \in I\}$ and $\{y \in S \mid (0, y) \in I\}$.]
`Answer:` *See S13.*

(R2) Let R be a commutative ring with identity $1 \neq 0$. Let M be an ideal of R with $M \neq R$. Prove that if M is a maximal ideal of R, then R/M is a field. `Answer:` *See S08 and F14. Fraleigh, Theorem 27.9 Dummit and Foote, Proposition12, p. 254.*

(R3) Suppose that D is a domain with $2 \neq 0$ and $0 \neq a \in D$. Show that the equation $x^2 = a$ has either no solutions or exactly two solutions in D. In the second case, if we denote one of the solutions by v, then the other solution is $-v$.

`Answer:` *If $x^2 = a$ has no solutions, then we are done. Otherwise, suppose that $v \in D$ is a solution of $x^2 = a$. We need to show that v and $-v$ are distinct and that these elements are the only solutions of $x^2 = a$.*

Suppose first that $v = -v$. Then $2v = 0$ and, since D is a domain and $2 \neq 0$, we have $v = 0$. But $v = 0$ would imply $a = v^2 = 0$, contrary to assumption. Hence v and $-v$ are distinct solutions of $x^2 = a$.

Now suppose that u is some (perhaps third) solution of $x^2 = a$, then $u^2 = v^2$ and so $(u - v)(u + v) = 0$. Since D is a domain, we have $u - v = 0$ or $u + v = 0$, that is, $u = v$ or $u = -v$. Therefore there are exactly two solutions of $x^2 = a$.

Fields

(F1) Let E be the splitting field of $f(x) = x^3 - 5$ over $\mathbb{Q}$. Is $\mathrm{Gal}(E/\mathbb{Q})$ abelian? Find a familiar group (like $\mathbb{Z}_n$, S_n, D_n, ...) that is isomorphic to $\mathrm{Gal}(E/\mathbb{Q})$.
`Answer:` *[See F10 and S17] The roots of $x^3 - 5$ are $\sqrt[3]{5}$, $\omega\sqrt[3]{5}$ and $\omega^2\sqrt[3]{5}$ where $\omega = e^{2\pi i/3}$. So $E = \mathbb{Q}(\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5})$. Since $\omega = (\omega\sqrt[3]{5})/\sqrt[3]{5} \in E$, it follows that $E = \mathbb{Q}(\omega, \sqrt[3]{5})$. Consider*

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{Q}(\omega, \sqrt[3]{5}) = E$$

$$\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{5})}_{3} \quad \underbrace{\mathbb{Q}(\sqrt[3]{5}) \subseteq E}_{2} \qquad \underbrace{\mathbb{Q} \subseteq E}_{6}$$

By Eisenstein, $x^3 - 5$ is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$. Because, ω is a root of $x^2 + x + 1 \in \mathbb{Q}(\sqrt[3]{5})[x]$, the degree of ω over $\mathbb{Q}(\sqrt[3]{5})$ is at most 2. But $\mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{R}$ and $\omega \notin \mathbb{R}$, so ω has degree 2 over $\mathbb{Q}(\sqrt[3]{5})$. This implies $[E : \mathbb{Q}(\sqrt[3]{5})] = 2$ and $[E : \mathbb{Q}] = 6$.

Since E is a splitting field, $\mathrm{Gal}(E, \mathbb{Q})$ is a group of order 6 and is isomorphic to $\mathbb{Z}_6$ or S_3. Each automorphism in $\mathrm{Gal}(E, \mathbb{Q})$ sends $\sqrt[3]{5}$ to one of its three conjugates $\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}$, and sends ω to one of its two conjugates ω, ω^2. Moreover, since $\sqrt[3]{5}$ and ω generate E over $\mathbb{Q}$, each automorphism is determined by where it sends these generators. Hence $\mathrm{Gal}(E, \mathbb{Q}) = \{\phi_0, \phi_1, \phi_2, \phi_3, \phi_4, \phi_5\}$ where

x	$\sqrt[3]{5}$	ω	$\sqrt[3]{5}$	$\omega\sqrt[3]{5}$	$\omega^2\sqrt[3]{5}$
$\phi_0(x)$	$\sqrt[3]{5}$	ω	$\sqrt[3]{5}$	$\omega\sqrt[3]{5}$	$\omega^2\sqrt[3]{5}$
$\phi_1(x)$	$\omega\sqrt[3]{5}$	ω	$\omega\sqrt[3]{5}$	$\omega^2\sqrt[3]{5}$	$\sqrt[3]{5}$
$\phi_2(x)$	$\omega^2\sqrt[3]{5}$	ω	$\omega^2\sqrt[3]{5}$	$\sqrt[3]{5}$	$\omega\sqrt[3]{5}$
$\phi_3(x)$	$\sqrt[3]{5}$	ω^2	$\sqrt[3]{5}$	$\omega^2\sqrt[3]{5}$	$\omega\sqrt[3]{5}$
$\phi_4(x)$	$\omega\sqrt[3]{5}$	ω^2	$\omega\sqrt[3]{5}$	$\sqrt[3]{5}$	$\omega^2\sqrt[3]{5}$
$\phi_5(x)$	$\omega^2\sqrt[3]{5}$	ω^2	$\omega^2\sqrt[3]{5}$	$\omega\sqrt[3]{5}$	$\sqrt[3]{5}$

This group is isomorphic to S_3, for example, because it is not abelian: $\phi_1(\phi_3(\sqrt[3]{5})) = \phi_1(\sqrt[3]{5}) = \omega\sqrt[3]{5}$, whereas, $\phi_3(\phi_1(\sqrt[3]{5}) = \phi_3(\omega\sqrt[3]{5})) = \omega^2\sqrt[3]{5}$. In addition, from the table we see that the Galois group acts as the set of all permutations of $\{\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}\}$, which shows explicitly that $\mathrm{Gal}(E, \mathbb{Q}) \cong S_3$.

(F2) Prove that every finite integral domain is field. `Answer:` *Fraleigh, Theorem 19.11. Dummit and Foote, Corollary 3, p. 228.*

(F3) Show that the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic. Hint: You need to use the irrationality of $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{6}$.

`Answer:` *[Fall 14] Since* $\mathbb{Q}(\sqrt{3})$ *obviously contains a cube root of* 3*, it suffices to show that* $\mathbb{Q}(\sqrt{2})$ *does not contain a cube root of* 3*.*

Suppose to the contrary that $(a + b\sqrt{2})^2 = 3$ *for some* $a, b \in \mathbb{Q}$*. Then* $a^2 + 2b^2 + 2ab\sqrt{2} = 3$*. We consider three cases: If both* a *and* b *are nonzero, then this equation can be rewritten as* $\sqrt{2} = (3 - a^2 - 2b^2)/2ab$*. If* $a = 0$*, then* $2b^2 = 3$ *and hence* $2b = \pm\sqrt{6}$*. Similarly, if* $b = 0$*, we have* $a^2 = 3$ *and hence* $a = \pm\sqrt{3}$*. None of these cases are possible since each shows that a known irrational number,* $\sqrt{2}$*,* $\sqrt{3}$ *or* $\sqrt{6}$*, is rational. That leaves only the case* $a = b = 0$*, which can easily be eliminated since* $0^2 \neq 3$*.*