ALGEBRA COMPREHENSIVE EXAMINATION

Spring 2019

Brookfield*, Demeke, 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: $\mathbb{Q}$ 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 finite group with subgroup H.

(a) Prove that, if $[G : H] = 2$, then H is normal.

(b) Disprove that, if $[G : H] = 3$, then H is normal.

`Answer:`

(a) *Since $[G : H] = 2$, there are two left cosets of H, each of the same size. One of the left cosets is H itself, so the other left coset is $G \setminus H$. By the same argument, the right cosets of H are H and $G \setminus H$. Because the left and right cosets coincide, H is normal.*

(b) *Counterexample: S_3 has three subgroups of index 3: $H_1 = \{e, (1\,2)\}$, $H_2 = \{e, (1\,3)\}$ and $H_3 = \{e, (2\,3)\}$. None of these subgroups is normal. For example, $(1\,2)H_2(1\,2)^{-1} = H_3$.*

(G2) Let $\mathbb{R}^\times$ be the set of nonzero real numbers, an abelian group under multiplication. Let $\mathbb{R}^+$ be the set of positive real numbers and $H = \{-1, 1\}$. You may assume without proof that $\mathbb{R}^+$ and H are subgroups of $\mathbb{R}^\times$. Use the First Isomorphism Theorem to prove that $\mathbb{R}^\times/H$ is isomorphic to $\mathbb{R}^+$.

`Answer:` *Consider the absolute value function $\phi : \mathbb{R}^\times \to \mathbb{R}^+$ defined by $\phi(a) = |a|$. Since $\phi(ab) = |ab| = |a||b| = \phi(a)\phi(b)$ for all $a, b \in \mathbb{R}^\times$, ϕ is a homomorphism. The kernel of ϕ is $\ker\phi = \{a \in \mathbb{R}^\times \mid \phi(a) = 1\} = H$ and the image of ϕ is $\operatorname{im}\phi = \mathbb{R}^+$, so by the first isomorphism theorem, $\mathbb{R}^\times/\ker\phi \cong \operatorname{im}\phi$, that is, $\mathbb{R}^\times/H \cong \mathbb{R}^+$.*

Aside 1: The squaring function $\phi(a) = a^2$ for $a \in \mathbb{R}^\times$ works just as well the absolute value function in this proof.

Aside 2: Define $\psi : H \times \mathbb{R}^+ \to \mathbb{R}^\times$ by $\psi(h, r) = hr$ for all $(h, r) \in H \times \mathbb{R}^+$. Then it's easy to check that ψ is an isomorphism and so we get the stronger result that $H \times \mathbb{R}^+ \cong \mathbb{R}^\times$.

(G3) Recall that the dihedral group of order 12 can be written as

$$D_{12} = \{1, r, r^2, r^3, r^4, r^5, s, sr, sr^2, sr^3, sr^4, sr^5\}$$

with $|r| = 6$, $|s| = 2$ and $rs = sr^{-1}$. Find all Sylow 2-subgroups of D_{12}.

`Answer:` *[See F16] Sylow 2-subgroups of D_{12} have order 4. Since there are no elements of order 4 in D_{12}, each Sylow 2-subgroup must be isomorphic to the Klein group and be generated by two commuting elements of order 2. Since s and r^3 have order 2 and commute, $H = \{1, r^3, s, sr^3\}$ is a Sylow 2-subgroup. All other Sylow 2-subgroups are conjugates of H: $rHr^{-1} = \{1, r^3, sr, sr^4\}$, $r^2H(r^2)^{-1} = \{1, r^3, sr^2, sr^5\}$. This gives*

3 *Sylow 2-subgroups, which is consistent with the Sylow theorems that predict that the number of Sylow 2-subgroups should be* 1 *or* 3.

Rings

(R1) Let R be a commutative ring with $1 \neq 0$. Suppose that every proper ideal of R is prime. Prove that R is a field. Hint: For an element t in R, consider the ideal $I = (t^2) = Rt^2$ generated by t^2.

`Answer:` *Because the zero ideal* $\{0\}$ *is prime, if* $ab = 0$*, then* $ab \in \{0\}$ *so either* $a \in \{0\}$ *or* $b \in \{0\}$*, that is,* $a = 0$ *or* $b = 0$*. Thus* R *is an integral domain.*

Suppose that $t \in R$ *is nonzero and not a unit. Then* $I = (t^2) = Rt^2$ *is a proper ideal and hence prime. Since* $t^2 \in I$*, and* I *is prime, we have* $t \in I$*. This means that* $t = rt^2$ *for some* $r \in R$*. Since* R *is a domain, and* t *is nonzero, we can cancel* t *from this to get* $1 = rt$*. But this means that* t *is a unit, a contradiction.*

Hence all nonzero elements of R *are units and* R *is a field.*

(R2) Let $I = (x^3-1, x^4-1)$, an ideal in $\mathbb{Q}[x]$. Find some $h(x) \in \mathbb{Q}[x]$ such that $I = (h(x))$. Prove this equality.

`Answer:` *Let* $f(x) = x^3 - 1$ *and* $g(x) = x^4 - 1$*. Since* $x - 1$ *divides* $f(x)$ *and* $g(x)$*, and* $x - 1 = (-x)g(x) + f(x)$*,* $h(x) = x - 1$ *is the greatest common divisor of* $f(x)$ *and* $g(x)$*. (Of course the gcd can also be calculated (in one step!) using the Euclidean algorithm.) We show that* $I = (h(x))$*.*

Let $k(x) \in I$*, then for some* $a(x), b(x) \in \mathbb{Q}[x]$*,*

$$\begin{aligned} k(x) &= a(x)f(x) + b(x)g(x) \\ &= a(x)(x^3 + x^2 + x + 1)h(x) + b(x)(x^2 + x + 1)h(x) \\ &= (a(x)(x^3 + x^2 + x + 1) + b(x)(x^2 + x + 1))h(x) \in (h(x)). \end{aligned}$$

Now suppose that $k(x) \in (h(x))$*. Then, for some* $a(x) \in \mathbb{Q}[x]$*,*

$$k(x) = a(x)h(x) = a(x)((-x)g(x) + f(x)) = a(x)(-x)g(x) + a(x)f(x) \in I.$$

(R3) Let $\mathbb{Q}[x^2]$ be the smallest subring of $\mathbb{Q}[x]$ that contains $\mathbb{Q}$ and x^2. Show that $\mathbb{Q}[x^2]$ is isomorphic to $\mathbb{Q}[x]$.

`Answer:` *Let* $\phi : \mathbb{Q}[x] \to \mathbb{Q}[x^2]$ *be the evaluation homomorphism at* $x^2 \in \mathbb{Q}[x]$ *defined by* $\phi(f(x)) = f(x^2)$ *for all* $f \in \mathbb{Q}[x]$*. In more detail*

$$\phi(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0 + a_1x^2 + a_2x^4 + \cdots + a_nx^{2n}.$$

Then $\operatorname{im}\phi$ *is a subring of* $\mathbb{Q}[x]$ *that contains* $\mathbb{Q}$ *(since* $\phi(a_0) = a_0$ *for all* $a_0 \in \mathbb{Q}$*), and* x^2 *(since* $\phi(x) = x^2$*). This implies* $\mathbb{Q}[x^2] \subseteq \operatorname{im}\phi$*.*

On the other hand, every polynomial in $\operatorname{im}\phi$ *is obtained using ring operations from* x^2 *and* $\mathbb{Q}$*, so is in* $\mathbb{Q}[x^2]$*. This shows that* $\mathbb{Q}[x^2] = \operatorname{im}\phi$*.*

Because of the linear independence of $\{1, x^2, x^4, \dots\}$ *over* $\mathbb{Q}$*, if* $\phi(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = 0$*, then* $a_0 = a_1 = \cdots = a_n = 0$*. This implies that* $\ker\phi = \{0\}$*.*

By the first isomorphism theorem, $\mathbb{Q}[x^2] = \operatorname{im}\phi \cong \mathbb{Q}[x]/\ker\phi \cong \mathbb{Q}[x]$*.*

Fields

(F1) Let E be the splitting field of $(x^2-2)(x^2-3)$ over $\mathbb{Q}$. Let G be the Galois group of E over $\mathbb{Q}$. Find a familiar group isomorphic to G. By "familiar group" we mean a cyclic

group, symmetric group, alternating group, or dihedral group, or direct products of such groups.

`Answer:` *Clearly* $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. *Since* $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ *(see Fall 2018), we have* $[E, \mathbb{Q}] = 4$*:*

$$\begin{array}{ccccc} \mathbb{Q} & \subseteq & \mathbb{Q}(\sqrt{2}) & \subseteq & E \\ & {\scriptstyle 2}\llcorner\!\!\lrcorner{\scriptstyle 2} & & & \\ & {\scriptstyle 4}\llcorner\!\!\lrcorner & & & \end{array}$$

Since E *is a Galois extension of* $\mathbb{Q}$, $\mathrm{Gal}(E, \mathbb{Q})$ *has order* 4. *Each automorphism in* $\mathrm{Gal}(E, \mathbb{Q})$ *permutes* $\{\sqrt{2}, -\sqrt{2}\}$ *and* $\{\sqrt{3}, -\sqrt{3}\}$ *and is determined by those permutations. There are four such permutations and and so each must give an element of* $\mathrm{Gal}(E, \mathbb{Q})$. *So* $\mathrm{Gal}(E, \mathbb{Q}) = \{\phi_0, \phi_1, \phi_2, \phi_3\}$ *as in the table:*

x	$\sqrt{2}$	$\sqrt{3}$
$\phi_0(x)$	$\sqrt{2}$	$\sqrt{3}$
$\phi_1(x)$	$-\sqrt{2}$	$\sqrt{3}$
$\phi_2(x)$	$\sqrt{2}$	$-\sqrt{3}$
$\phi_3(x)$	$-\sqrt{2}$	$-\sqrt{3}$

ϕ_0 *is the identity function. The other elements of* $\mathrm{Gal}(E, \mathbb{Q})$ *have order* 2, *so* $\mathrm{Gal}(E, \mathbb{Q})$ *is isomorphic to the Klein group* $V = \mathbb{Z}_2 \times \mathbb{Z}_2$.

(F2) Let F be a field with characteristic not equal to 2 or 3. Show that $x^2 + 3 \in F[x]$ has a zero in F if and only if $x^2 + x + 1 \in F[x]$ has a zero in F. Hint: Complete the square.

`Answer:` *Suppose that* $f = x^2 + x + 1$ *has a zero* $a \in F$. *Then* $a^2 + a + 1 = 0$. *Set* $b = 2a + 1 \in F$. *Then*

$$b^2 + 3 = (2a + 1)^2 + 3 = 4a^2 + 4a + 4 = 4(a^2 + a + 1) = 0.$$

Hence b *is a zero of* $g = x^2 + 3$. *Conversely, suppose that* b *is a zero of* $g = x^2 + 3$. *Then* $b^2 + 3 = 0$. *Set* $a = (b - 1)/2 \in F$. *Note that this make sense because* $2 \neq 0$ *so has a multiplicative inverse* $2^{-1} = 1/2$ *in the field* F. *Then*

$$\begin{aligned} a^2 + a + 1 &= \frac{1}{4}(b^2 - 2b + 1) + \frac{1}{2}(b - 1) + 1 \\ &= \frac{1}{4}(b^2 - 2b + 1 + 2(b - 1) + 4) = \frac{1}{4}(b^2 + 3) = 0, \end{aligned}$$

and so a *is a zero of* f.

(F3) Let α and β be complex numbers such that $\alpha = \beta^2 - 1$ and $\beta = \alpha^2 - 1$. Show that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 2$.

`Answer:` *Since* $\alpha = \beta^2 - 1 \in \mathbb{Q}(\beta)$, *we have* $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta)$. *Similarly* $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$.

Plugging $\alpha = \beta^2 - 1$ *into* $\beta = \alpha^2 - 1$, *we get* $\alpha = (\alpha^2 - 1)^2 - 1$, *that is,* α *is a zero of* $f(x) = x^4 - 2x^2 - x$. *This polynomial has zeros* 0 *and* -1, *so factors:* $f(x) = x(x+1)(x^2 - x - 1)$. *Since* α *is a zero of one of the factors of* $f(x)$, *the degree of* α *over* $\mathbb{Q}$ *is at most* 2. *(In fact,* $\alpha, \beta \in \{0, -1, \frac{1}{2}(1 \pm \sqrt{5})\}$.*)*

Aside: The claim is true when $\alpha, \beta \in \mathbb{C}$ *satisfy* $\alpha = \beta^2 - A$ *and* $\beta = \alpha^2 - A$ *where* A *is any rational number. Plugging either of these equations into the other, shows*

that α *and* β *are zeros of* $f(x) = (x^2 - x + A)(x^2 + x + A + 1)$, *so* α *and* β *have a most degree* 2 *over* $\mathbb{Q}$.