ALGEBRA COMPREHENSIVE EXAMINATION

Fall 2014

Brookfield, Shaheen*, Webster

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; $\mathbb{Z}_n$ denotes the integers modulo n; $\mathbb{N}$ denotes the natural numbers.

Groups

G1 (a) Suppose that H is a subgroup of the group G with the property that ghg^{-1} is in H for all $g \in G$ and $h \in H$. Let a, b, and c be elements of G with $aH = bH$. Prove that $acH = bcH$.

(b) Suppose H is a subgroup of the group G and that a, b, and c be elements of G with $aH = bH$. Must $acH = bcH$? Prove or give a counterexample.

`Answer:`

(a) Suppose that $x \in acH$. Then $x = ach_1$ for some $h_1 \in H$. Since $a \in aH = bH$, we have $a = bh_2$ for some $h_2 \in H$. Since $c^{-1}h_2c \in H$ we have $c^{-1}h_2c = h_3$ for some $h_3 \in H$. Putting all this together:

$$x = ach_1 = bh_2ch_1 = bc(c^{-1}h_2c)h_1 = bch_3h_1 \in bcH.$$

Thus $acH \subseteq bcH$. Similarly $bcH \subseteq acH$.

(b) Counterexample: Let $G = S_3$, $H = \{1, (1\,2)\}$, $a = 1$, $b = (1\,2)$ and $c = (1\,3)$. Then $aH = bH = H$, but $acH = (1\,3)H = \{(1\,3), (1\,2\,3)\}$ and $bcH = (3\,2\,1)H = \{(3\,2\,1), (2\,3)\}$.

G2 Let N and H be subgroups of a group G with N normal. Suppose that the natural homomorphism $\pi : G \to G/N$ given by $\pi(g) = gN$ restricts to an isomorphism from H to G/N. (When this happens, G is called the **internal semidirect product** of N and H.) Prove the following:

(a) $H \cap N = \{1\}$.

(b) Each element $g \in G$ can be written in the form nh with uniquely determined $n \in N$ and $h \in H$.

`Answer:`

(a) *The kernel of π restricted to H is*

$$\{h \in H \mid \pi(h) = 1\} = \{h \in H \mid h \in N\} = H \cap N.$$

Since π restricted to H is injective, this kernel is trivial, that is, $H \cap N = \{1\}$.

(b) *Let $g \in G$. Since π is a bijection from H to G/N, there is a unique element $h \in H$ such that $\pi(h) = \pi(g)$. Then $\pi(gh^{-1}) = \pi(g)(\pi(h))^{-1} = 1$ and so $gh^{-1} \in \ker\pi = N$. Thus there is some $n \in N$ such that $g = nh$. The uniqueness of n follows from the uniqueness of h.*

G3 Suppose G is a group of order 56. Prove that G has a normal Sylow p subgroup for some prime p dividing 56.

`Answer:` *[See S11] Note that $56 = 2^3 \cdot 7$, so G has Sylow 2-subgroup(s) of order 8 and Sylow 7-subgroup(s) of order 7. By the Sylow Theorems, $n_7 \equiv 1 \mod 7$ and $n_7 | 8$, so n_7 is 1 or 8. If $n_7 = 1$, then the unique Sylow 7-subgroup is normal.*

Otherwise, G has 8 Sylow 7-subgroups. The intersection of any pair of these subgroups is trivial. Since each subgroup contains 6 elements of order 7, G has a total of $6 \cdot 8 = 48$ elements of order 6. This leaves room for only 8 other elements and these other elements must form a unique Sylow 2-subgroup which is therefore normal.

Rings

R1 For each $n \in \mathbb{N}$, let I_n be an ideal of a commutative ring R with $1 \neq 0$. Suppose that the ideals form an ascending chain, that is

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq I_4 \subseteq \cdots$$

and let $I = \bigcup_{n\in\mathbb{N}} I_n$.

(a) Show that I is an ideal of R.

(b) Suppose, in addition, that I_n is a proper ideal for all $n \in \mathbb{N}$. Show that I is a proper ideal.

`Answer:` *[See F02 and F09]*

(a) *$\underline{\text{ I closed under addition}}$: Let $i, j \in I$. Then there are $m, n \in \mathbb{N}$ such that $i \in I_m$ and $j \in I_n$. Without loss of generality, $m \leq n$ and then $i \in I_m \subseteq I_n$. Since $i, j \in I_n$ and I_n is an ideal, $i + j \in I_n \subseteq I$.*

$\underline{\text{ I closed under multiplication by ring elements:}}$ Let $i \in I$ and $r \in R$. Then $i \in I_n$ for some $n \in \mathbb{N}$. Since I_n is an ideal, $ri \in I_n \subseteq I$.

(b) *We prove the contrapositive, namely, if I is not proper, then I_n is not proper for some $n \in \mathbb{N}$.*

If I is not proper, then $I = R$. In particular, $1 \in I$. Then $1 \in I_n$ for some $n \in \mathbb{N}$. But this means $I_n = R$. Indeed, for any $r \in R$, we have $r = r1 \in I_n$ because I_n is an ideal.

R2 Given a prime number p and an integer $n \geq 2$, prove that the ring $\mathbb{Z}/\langle p^n \rangle$ does not contain an integral domain. You may assume that any subring of $\mathbb{Z}/\langle p^n \rangle$ contains the multiplicative identity of $\mathbb{Z}/\langle p^n \rangle$.

`Answer:` *[See S10] It is notationally convenient to replace $\mathbb{Z}/\langle p^n \rangle$ by $\mathbb{Z}_{p^n}$ (These rings are isomorphic). Let R be any subring of $\mathbb{Z}_{p^n}$. We are allowed to assume that the multiplicative identity element of $\mathbb{Z}_{p^n}$ is in R, that is, $1 \in R$. But $\mathbb{Z}_{p^n}$ is a cyclic group under addition and 1 is a generator. Since R is also an abelian group under addition, $\mathbb{Z}_{p^n} = \langle 1 \rangle \subseteq R \subseteq \mathbb{Z}_{p^n}$. Hence $R = \mathbb{Z}_{p^n}$. It remains only to show that $\mathbb{Z}_{p^n}$ is not an integral domain. Since $p^n = 0$ in $\mathbb{Z}_{p^n}$ and $n \geq 2$, we get $p \cdot (p^{n-1}) = 0$ with p and p^{n-1} both nonzero. Therefore $\mathbb{Z}_{p^n}$ is not an integral domain.*

R3 Let R be a commutative ring with identity 1. Prove that an ideal M is maximal if and only if R/M is a field.

`Answer:` *See Fraleigh, Theorem 27.9.*

Fields

F1 Let $\alpha \in \mathbb{C}$ be one zero of $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$.

(a) Show that f is irreducible over $\mathbb{Q}$.

(b) Show that $\beta = \alpha^2 - 2$ is another zero of f.

(c) Show that $\mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{Q}$.

`Answer:`

(a) By the Rational Zeros Theorem, f has no rational zeros and so is irreducible over $\mathbb{Q}$. Note that this implies that α has degree 3 over $\mathbb{Q}$.

(b) From $\alpha^3 - 3\alpha + 1 = 0$ we get,

$$\alpha^3 = 3\alpha - 1 \qquad \alpha^4 = 3\alpha^2 - \alpha \qquad \alpha^6 = (3\alpha - 1)^2 = 9\alpha^2 - 6\alpha + 1.$$

With these formulas at hand we can now calculate $f(\beta)$:

$$\begin{aligned} f(\beta) &= (\alpha^2 - 2)^3 - 3(\alpha^2 - 2) + 1 \\ &= (\alpha^6 - 6\alpha^4 + 12\alpha^2 - 8) - 3\alpha^2 + 6 + 1 \\ &= 9\alpha^2 - 6\alpha + 1 - 6(3\alpha^2 - \alpha) + 12\alpha^2 - 8 - 3\alpha^2 + 6 + 1 \\ &= 0 \end{aligned}$$

Thus β is a zero of f. But β cannot be α since otherwise we would have $\alpha = \alpha^2 - 2$, α would be a zero of $x^2 - x - 2 \in \mathbb{Q}[x]$, and α would have degree 2 over $\mathbb{Q}$.

(c) The splitting field is, by definition, $\mathbb{Q}(\alpha, \beta, \gamma)$ where γ is the third zero of f. From (b) we have $\beta = \alpha^2 - 2 \in \mathbb{Q}(\alpha)$. Also, since $\alpha + \beta + \gamma = 0$ (or because $\gamma = \beta^2 - 2$), we have $\gamma \in \mathbb{Q}(\alpha)$. Thus $\mathbb{Q}(\alpha, \beta, \gamma) \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta, \gamma)$, which implies that $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\alpha)$.

F2 Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

`Answer:` *If $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are isomorphic, then $\mathbb{Q}(\sqrt{2})$ contains a square root of 3. We will show that this is impossible.*

Suppose that $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ with $a, b \in \mathbb{Q}$ satisfies $(a + b\sqrt{2})^2 = 3$. 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 $0^2 \neq 3$.

F3 Let E be the splitting field of $x^6 - 3$ over the rationals $\mathbb{Q}$.

(a) Find E and $[E : \mathbb{Q}]$. Explain with all the details.

(b) Prove that $\mathrm{Gal}(E/\mathbb{Q})$ is not abelian.

`Answer:` *[See F08]*

(a) The zeros of $x^6 - 3$ are $\sqrt[6]{3}$, $\lambda\sqrt[6]{3}$, $\lambda^2\sqrt[6]{3}$, $\lambda^3\sqrt[6]{3}$, $\lambda^4\sqrt[6]{3}$ and $\lambda^5\sqrt[6]{3}$ where $\lambda = e^{2\pi i/6}$. Since $\lambda = (\lambda\sqrt[6]{3})/\sqrt[6]{3} \in E$, it follows that $E = \mathbb{Q}(\lambda, \sqrt[6]{3})$. Consider

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[6]{3}) \subseteq \mathbb{Q}(\lambda, \sqrt[6]{3}) = E$$

$$\underbrace{\hspace{4em}}_{6}\underbrace{\hspace{6em}}_{2}$$

$$\underbrace{\hspace{10em}}_{12}$$

By Eisenstein, $x^6 - 3$ is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(\sqrt[6]{3}) : \mathbb{Q}] = 6$. Because, λ is a zero of $x^2 - x + 1 \in \mathbb{Q}(\sqrt[6]{3})[x]$, the degree of λ over $\mathbb{Q}(\sqrt[6]{3})$ is at most 2. But $\mathbb{Q}(\sqrt[6]{3}) \subseteq \mathbb{R}$ and $\lambda \notin \mathbb{R}$, so λ has degree 2 over $\mathbb{Q}(\sqrt[6]{3})$. This implies $[E : \mathbb{Q}(\sqrt[6]{3})] = 2$ and $[E : \mathbb{Q}] = 12$.

(b) Since E is a splitting field, $\mathrm{Gal}(E/\mathbb{Q})$ is a group of order 12. Each automorphism in $\mathrm{Gal}(E/\mathbb{Q})$ sends $\sqrt[6]{3}$ to one of its six conjugates $\sqrt[6]{3}$, $\lambda\sqrt[6]{3}$, $\lambda^2\sqrt[6]{3}$, $\lambda^3\sqrt[6]{3}$, $\lambda^4\sqrt[6]{3}$, $\lambda^5\sqrt[6]{3}$, and sends λ to one of its two conjugates λ, λ^5. Moreover, since $\sqrt[6]{3}$ and λ generate E over $\mathbb{Q}$, each automorphism is determined by where it sends these generators. In particular, there are automorphisms $r, s \in \mathrm{Gal}(E/\mathbb{Q})$ such that $r(\sqrt[6]{3}) = \lambda\sqrt[6]{3}$, $r(\lambda) = \lambda$, $s(\sqrt[6]{3}) = \sqrt[6]{3}$, $s(\lambda) = \lambda^5$. With a bit of calculation, one can show that $|r| = 6$, $|s| = 2$ and $rs = sr^{-1}$ and so $\mathrm{Gal}(E/\mathbb{Q}) \cong D_{12}$.

With less calculation, one finds that $r(s(\sqrt[6]{3})) = \lambda\sqrt[6]{3}$, whereas $s(r(\sqrt[6]{3})) = \lambda^5\sqrt[6]{3}$ which shows that $rs \neq sr$ and so $\mathrm{Gal}(E/\mathbb{Q})$ is not abelian.