ALGEBRA COMPREHENSIVE EXAMINATION

Spring 2009

Brookfield, Chabot, Shaheen*

Directions: Answer 5 questions only. You must answer *at least one* from each of groups, rings, and fields. Be sure to show enough work that your answers are adequately supported.

Notation: Let $\mathbb{Q}$ denote the rational numbers.

Groups

(1) Show that all groups of order 275 are solvable.

`Answer:` *Let G be a group of order $275 = 5^2 \cdot 11$. By Sylow, n_{11} divides 275 and n_{11} is congruent to 1 modulo 11. The only number satisfying these conditions is $n_{11} = 1$, and so G has a normal subgroup N of order 11. Since N has prime order, N is abelian (cyclic even), and G/N has order 5^2 so is abelian. This means that G is solvable.*

(2) Let a, b and c be elements of a group G with identity element e. For each of the following statements, give either a proof or a concrete counterexample.

(a) If a has order 5 and $a^3b = ba^3$, then $ab = ba$.

(b) If $abc = e$, then $cab = e$.

(c) If $abc = e$, then $bac = e$.

`Answer:`

(a) $ab = a^6b = a^3a^3b = a^3ba^3 = ba^3a^3 = ba^6 = ba$.

(b) $cab = ceab = c(abc)ab = (cab)^2$, *so by cancellation,* $cab = e$.

(c) *If both $abc = e$ and $bac = e$ are true, then $ab = ba = c^{-1}$. For a counterexample we need two noncommuting group elements a and b and then we set $c = (ab)^{-1}$. For example, $a = (1, 2)$, $b = (1, 3)$ and $c = (1, 2, 3)$ in S_3.*

(3) Suppose that $\phi : G \to G'$ is a group homomorphism.

(a) Prove that $\ker(\phi)$ is a normal subgroup of G. (Prove both the normality and subgroup claims.)

(b) Prove that $G/\ker(\phi)$ is isomorphic to $\phi[G]$, where $\phi[G]$ is the image of G under the map ϕ.

`Answer:` *Fraleigh: Corollary 13.20, p. 132 and Theorem 14.1, p. 137*

Rings

(1) Suppose that R is a Principal Ideal Domain and I is a prime ideal of R. Prove that R/I is a Principal Ideal Domain.

`Answer:` *We have two things to prove:*

(a) *R/I is a domain: Suppose that $a + I, b + I \in R/I$ for some $a, b \in R$ satisfy $(a+I)(b+I) = (0+I)$. Then $ab+I = (a+I)(b+I) = (0+I) = I$ and so $ab \in I$. Since I is prime we have $a \in I$ or $b \in I$. If $a \in I$, then $(a + I) = (0 + I)$, and, if $b \in I$. then $(b + I) = (0 + I)$. Thus R/I is a domain.*

(b) *R/I is a PID: Let $\phi : R \to R/I$ be the natural homomorphism. Let K be an ideal of R/I. Then the inverse image of K in R, namely,*

$$\phi^{-1}(K) = \{r \in R \mid \phi(r) \in K\}$$

is an ideal of R. (Easy to check this.). Since R is a PID, $\phi^{-1}(K) = \langle r \rangle$ for some $r \in R$. Then $K = \langle \phi(r) \rangle$ is principal.

(2) Prove that every Euclidean Domain is a Principal Ideal Domain.
`Answer:` *Fraleigh: Theorem 46.4, p. 402. Dummit and Foote, p. 273.*

(3) For this question, all rings are commutative with $1 \neq 0$ and ring homomorphisms map 1 to 1. Let R be a ring. Show that R is a field if and only if every ring homomorphism $\phi : R \to S$ is injective (one-to-one).
`Answer:` *Suppose that R is a field, and $\phi : R \to S$ is a ring homomorphism. We show that ϕ is injective, equivalently, $\ker \phi = \{0\}$. Suppose that $\phi(r) = 0$ for some $r \in R$. If $r \neq 0$, then r has an inverse and so*

$$1 = \phi(1) = \phi(rr^{-1}) = \phi(r)\phi(r^{-1}) = 0\phi(r^{-1}) = 0.$$

This contradiction means that r must be zero. Hence $\ker \phi = \{0\}$ and ϕ is injective.

Now suppose that every ring homomorphism $\phi : R \to S$ is injective. Suppose that $r \in R$ is not zero. Consider the natural homomorphism $\pi : R \to R/(r)$ with $\ker \pi = (r)$. Since r is a nonzero element of $\ker \pi$, π is not injective, and, by hypothesis, π must be the zero homomorphism. Hence $\ker \pi = (r) = R$. In particular, since $1 \in R$, there is some element $s \in R$ such that $rs = 1$ and so r is a unit.

We have proved that all nonzero elements of R are units, and so R is a field.

OR

Since every ideal of R is the kernel of a homomorphism, there are exactly two ideals: The kernel of the zero homomorphism, namely R, and the kernel of any injective homomorphism, namely $\{0\}$. Since R has only two ideals, it is a field.

Fields

(1) Let E be the splitting field of $p(x) = x^8 - 2$ over $\mathbb{Q}$, and assume $p(\alpha) = 0$. Let $\omega = e^{2\pi i/8}$ be a primitive 8th root of unity. FACT: $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$.
(a) Explain why $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$.
(b) Prove that $[E : \mathbb{Q}] = 16$.
`Answer:`
(a) *p is irreducible over $\mathbb{Q}$ by Eisenstein with prime 2. So $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\alpha, \mathbb{Q}) = \deg p = 8$.*
(b) *By (I hope) a familiar argument, $E = \mathbb{Q}(\sqrt[8]{2}, \omega)$ and*

$$[E : \mathbb{Q}] = [\mathbb{Q}(\sqrt[8]{2}, \omega) : \mathbb{Q}(\sqrt[8]{2})]\, [\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}].$$

By (a), $[\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = 8$. Since $\mathbb{Q}(\sqrt[8]{2})$ is contained in the reals and ω is not real, $[\mathbb{Q}(\sqrt[8]{2}, \omega) : \mathbb{Q}(\sqrt[8]{2})] > 1$.
Since ω is a primitive 8th root of unity, it is a root of $x^4 + 1$ (the 8th cyclotomic polynomial), or $\omega = e^{2\pi i k/8}$ for some $k \in \{1, 3, 5, 7\}$, or $\omega = (\pm 1 \pm i)/\sqrt{2}$. From any of these descriptions of ω its is possible to show that $(\omega^2 + 1)^2 = 2\omega^2$. Thus $\omega^2 \pm \sqrt{2}\,\omega + 1 = 0$ for some choice of sign. In particular, ω is a root of a degree 2 polynomial, $x^2 \pm \sqrt{2}\,x + 1$, with coefficients in $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[8]{2})$. This implies $[\mathbb{Q}(\sqrt[8]{2}, \omega) : \mathbb{Q}(\sqrt[8]{2})] \leq 2$.

Combining the inequalities we get $[\mathbb{Q}(\sqrt[8]{2}, \omega) : \mathbb{Q}(\sqrt[8]{2})] = 2$ and $[E : \mathbb{Q}] = [\mathbb{Q}(\sqrt[8]{2}, \omega) : \mathbb{Q}(\sqrt[8]{2})]\,[\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = 2 \cdot 8 = 16$.

(2) Let $E = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.
  (a) Show that $[E : \mathbb{Q}] = 6$.
  (b) If K is a field with $\mathbb{Q} \subseteq K \subseteq E$, show that K is one of $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$), or E.
  (c) Prove that $E = \mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$).

`Answer:`

(a) *By Eisenstein's criterion, the polynomials $x^2 - 2$ and $x^3 - 2$ are irreducible over $\mathbb{Q}$, and so $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. In particular, since E contains $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$ and since 2 and 3 are relatively prime, it follows that $[E : \mathbb{Q}]$ is divisible by $2 \cdot 3 = 6$. On the other hand, $E = \mathbb{Q}(\sqrt[3]{2})(\sqrt{2})$, so $[E : \mathbb{Q}(\sqrt[3]{2})] \leq 2$ and hence $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \leq 6$. Thus $[E : \mathbb{Q}] = 6$.*

(b) *If $\mathbb{Q} \subseteq K \subseteq E$, then $[K : \mathbb{Q}]$ divides $[E : \mathbb{Q}] = 6$ and thus $[K : \mathbb{Q}] = 1, 2, 3$ or 6. If $[K : \mathbb{Q}] = 1$, then $K = \mathbb{Q}$ and if $[K : \mathbb{Q}] = 6$, then $K = E$.*

Suppose $[K : \mathbb{Q}] = 2$. Then $\mathbb{Q} \subseteq K \subseteq K(\sqrt{2}) \subseteq E$ as in the diagram:

$$\mathbb{Q} \subseteq K \subseteq K(\sqrt{2}) \subseteq E$$

└─ 2 ─┴── ? ──┴── ? ──┘
└─ 2 ─┴────── 3 ──────┘

Since $\sqrt{2}$ is a root of $x^2 - 2 \in K[x]$, we have $[K(\sqrt{2}) : K] \leq 2$. But $[K(\sqrt{2}) : K]$ also divides $[E : K] = 3$. Hence $[K(\sqrt{2}) : K] = 1$, $K(\sqrt{2}) = K$ and $\sqrt{2} \in K$ and $K \subseteq \mathbb{Q}(\sqrt{2})$. In particular, since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [K : \mathbb{Q}] = 2$ we have $K = \mathbb{Q}(\sqrt{2})$.

Finally, suppose that $[K : \mathbb{Q}] = 3$. Then $\mathbb{Q} \subseteq K \subseteq K(\sqrt[3]{2}) \subseteq E$ as in the diagram:

$$\mathbb{Q} \subseteq K \subseteq K(\sqrt[3]{2}) \subseteq E$$

└─ 3 ─┴── ? ──┴── ? ──┘
└─ 3 ─┴────── 2 ──────┘

Then $[E : K] = 2$, and because $\sqrt[3]{2} \in E$, the degree of $\sqrt[3]{2}$ is 1 or 2 over K. This means that the polynomial $x^3 - 2 \in K[x]$ is reducible over K which in turn means that this polynomial has a root in K. But $K \subseteq E \subseteq \mathbb{R}$, and the only real root of $x^3 - 2$ is $\sqrt[3]{2}$, so we must have $\sqrt[3]{2} \in K$. This means that $\mathbb{Q}(\sqrt[3]{2}) \subseteq K$, and since $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [K : \mathbb{Q}] = 3$, we conclude that $K = \mathbb{Q}(\sqrt[3]{2})$.

Aside: This claim can also be proved by applying Galois theory to the splitting field of $x^6 - 2$, a field that contains E.

(c) *Let $L = \mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$ so that $\mathbb{Q} \subseteq L \subseteq E$ and note that there are only four possibilities for L. If $L = \mathbb{Q}(\sqrt{2})$, then $\sqrt{2}$ and $\sqrt{2} + \sqrt[3]{2}$ are in $\mathbb{Q}(\sqrt{2})$, so $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = E$, a contradiction. Similarly, L cannot be contained in $\mathbb{Q}(\sqrt[3]{2})$. Thus, by (b), $L = E$.*

OR

Let $\alpha = \sqrt{2}+\sqrt[3]{2}$. *Then cubing both sides of* $\alpha-\sqrt{2} = \sqrt[3]{2}$ *and solving for* $\sqrt{2}$ *we get* $\sqrt{2} = (\alpha^3 + 6\alpha - 2)/(3\alpha^2 + 2) \in \mathbb{Q}(\alpha)$. *Note that* $3\alpha^2 + 2 \neq 0$ *because* $\alpha \in \mathbb{R}$. *Since* $\sqrt{2} \in \mathbb{Q}(\alpha)$, *we have* $\sqrt[3]{2} = \alpha - \sqrt{2}$ *is in* $\mathbb{Q}(\alpha)$ *too. This implies* $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$. *The opposite inclusion is clear so we have proven that* $E = \mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$.

(3) Let p be a prime and $n \geq 1$. Prove that there exists a finite field of size p^n.
`Answer:` *[See S14 and S10] Fraleigh Lemma 33.10, p. 303.*