ALGEBRA COMPREHENSIVE EXAMINATION

Fall 2008

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.

Groups

(1) Show that any group of order 15 is cyclic.
`Answer:` *[See F11] Let G be a group of order 15. By Sylow, n_3 divides 15 and is congruent to 1 modulo 3. Thus $n_3 = 1$, and G has a unique normal subgroup H of order 3. Similarly, n_5 divides 15 and is congruent to 1 modulo 5. Thus $n_5 = 1$, and G has a unique normal subgroup K of order 5. $H \cap K$ is a subgroup of H and a subgroup of K, so its order divides both 3 and 5, and so $H \cap K = \{1\}$ and $H \times K \cong HK \leq G$. But $|H \times K| = 15 = |G|$ and so $H \times K \cong G$. Now we recall that groups of order 3 and 5 are isomorphic to $\mathbb{Z}_3$ and $\mathbb{Z}_5$ respectively and so $G \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$.*

(2) Let N and H be subgroups of a group G with N normal. Show that $NH = \{nh \mid n \in N \text{ and } h \in H\}$ is a subgroup of G.
`Answer:` *Of course, $N \neq \emptyset$ and $H \neq \emptyset$, so $NH \neq \emptyset$. Suppose $x_1, x_2 \in NH$. Then $x_1 = n_1h_1$ and $x_2 = n_2h_2$, with $n_1, n_2 \in N$ and $h_1, h_2 \in H$. Since N is normal, $h_1h_2^{-1}n_2^{-1} \in h_1h_2^{-1}N = Nh_1h_2^{-1}$ and so $h_1h_2^{-1}n_2^{-1} = n_3h_1h_2^{-1}$ for some $n_3 \in N$. This implies*

$$x_1x_2^{-1} = n_1h_1h_2^{-1}n_2^{-1} = n_1n_3h_1h_2^{-1} \in NH.$$

By the subgroup criterion, $NH \leq G$.

(3) Let p be a prime number and G a nontrivial finite p-group with center $Z(G)$.
  (a) Show that $Z(G)$ is nontrivial.
  `Answer:` *Fraleigh, Theorem 37.4, p. 329 and Dummit and Foote, Theorem 8, p. 125*
  (b) Let N be a nontrivial normal subgroup of G. Show that $N \cap Z(G)$ is nontrivial.
  `Answer:` *Since N is normal, it is a union of conjugacy classes of G. Such a conjugacy class has either one element, in which case the element is in $N \cap Z$, or has a multiple of p elements. Since the order of N is also a multiple of p, this implies that there must be at least p one element conjugacy classes in N. Hence $N \cap Z$ has at least p elements.*

Rings

(1) Let R be a finite commutative ring (not necessarily with a multiplicative identity) with more than one element and no zero divisors.
  (a) Show that R has a multiplicative identity and so is a domain.
  (b) Show that R is a field.
`Answer:` *[See F07]*
  (a) *For each nonzero $a \in R$, define a function $\phi_a : R \to R$ by $\phi_a(x) = ax$ for all $x \in R$. We show that ϕ_a is injective. Suppose that $\phi_a(x) = \phi_a(y)$ for*

some $x, y \in R$. Then $ax = ay$ and so $a(x-y) = 0$. Since $a \neq 0$ and R has no zero divisors, this can only happen if $x - y = 0$, that is, $x = y$. Because R is finite and ϕ_a is injective, ϕ_a is also surjective. In particular, there is some $e \in R$ such that $\phi_a(e) = a$ that is $ae = a$.
We show that e is the multiplicative identity element of R. Indeed, if $x \in R$, then $a(x - ex) = ax - aex = ax - ax = 0$, and, once again since a is not a zero divisor, we get $x = ex$. This shows that e is the multiplicative identity element of R, and so R is an integral domain.

(b) *Since ϕ_a is surjective, there is some element $b \in R$ such that $ab = e$, thus a has a multiplicative inverse. Since this is true of any nonzero element of R, R is a field.*

(2) Let R be the set of all matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ with $a, b \in \mathbb{R}$ together with the usual matrix addition and multiplication operations. Show that R is isomorphic to $\mathbb{C}$.
`Answer:` *We know that every element of $\mathbb{C}$ can be written uniquely in the form $a + ib$ with $a, b \in \mathbb{R}$. So the function $\phi : R \to \mathbb{C}$ defined by*

$$\phi\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a + ib$$

for $a, b \in \mathbb{R}$ is a bijection. It remains to show that ϕ is a homomorphism. The additive property is easy, so we confirm just the multiplicative property:

$$\begin{aligned}
\phi\left(\begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix}\right) &= \phi\left(\begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + b_1a_2 \\ -(a_1b_2 + b_1a_2) & a_1a_2 - b_1b_2 \end{bmatrix}\right) \\
&= (a_1a_2 - b_1b_2) + i(a_1b_2 + b_1a_2) \\
&= (a_1 + ib_1)(a_2 + ib_2) \\
&= \phi\left(\begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix}\right)\phi\left(\begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix}\right)
\end{aligned}$$

for all $a_1, a_2, b_1, b_2 \in \mathbb{Q}$.

(3) Let R be a commutative ring with identity and M an ideal of R. Show that M is maximal if and only if, for every $r \in R \setminus M$, there is an $x \in R$ such that $1 - rx \in M$. Note: $R \setminus M = \{r \in R \mid r \notin M\}$.
`Answer:` *[See F12] Suppose that M is maximal. If $r \in R \setminus M$, then the ideal containing M and r is strictly bigger than M so is the whole ring R. Specifically, $\langle r \rangle + M = R$. In particular, $1 \in \langle r \rangle + M$ and so there are $x \in R$ and $m \in M$ such that $1 = rx + m$. Consequently $1 - rx = m \in M$.*

Conversely, suppose that for every $r \in R \setminus M$ there is an $x \in R$ such that $1 - rx \in M$. Let I be an ideal such that $M \subseteq I \subseteq R$. If $I = M$ we are done. Otherwise, I contains an element r that is not in M. By assumption, there exists $x \in R$ and $m \in M$ such that $1 = rx + m$. This implies that $1 \in \langle r \rangle + M$ and so $\langle r \rangle + M = R$. Because $r \in I$ we also have $\langle r \rangle + M \subseteq I$, and so $I = R$. This shows that M is maximal.

Fields

(1) Let E be the splitting field of $x^6 - 3$ over the rational numbers $\mathbb{Q}$.

(a) Find $[E : \mathbb{Q}]$. Explain.
(b) Show that the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ is not abelian.

`Answer:` *[See F14]*

(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*

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[6]{3}) \subseteq \mathbb{Q}(\lambda, \sqrt[6]{3}) = E$$
$$\underbrace{\hphantom{\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[6]{3})}}_{6}\underbrace{\hphantom{\subseteq \mathbb{Q}(\lambda, \sqrt[6]{3})}}_{2}$$
$$\underbrace{\hphantom{\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[6]{3}) \subseteq \mathbb{Q}(\lambda, \sqrt[6]{3})}}_{12}$$

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.

(2) Let E be an extension field of F with $[E : F] = 5$.
(a) Show that $F(\alpha) = F(\alpha^3)$ for all $\alpha \in E$.
(b) Show that $F(\alpha) = F(\alpha^9)$ for all $\alpha \in E$.

`Answer:` *[See F07] Reminder: $\deg(\alpha, F) = [F(\alpha) : F]$ divides $[E : F] = 5$. So either $\deg(\alpha, F) = [F(\alpha) : F] = 1$ with $F(\alpha) = F$ and $\alpha \in F$, or $\deg(\alpha, F) = [F(\alpha) : F] = 5$ with $F(\alpha) = E$ and $\alpha \notin F$.*

(a) *If $\alpha \in F$, then $\alpha^3 \in F$ and $F(\alpha) = F(\alpha^3) = F$. Otherwise, α is not in F and so $\deg(\alpha, F) = 5$. Because of this, α^3 cannot be in F either. (If $\alpha^3 \in F$ then the degree of α would be three or less.) Thus $\deg(\alpha^3, F) = 5$ and $F(\alpha) = F(\alpha^3) = E$.*

(b) *By (a), $F(\alpha) = F(\alpha^3) = F((\alpha^3)^3) = F(\alpha^9)$.*

(3) Let K be the splitting field of $f(x) = x^3 + 3x^2 + 3x + 2 \in \mathbb{Z}_5[x]$ over $\mathbb{Z}_5$.
(a) Is f irreducible over $\mathbb{Z}_5$?
(b) How many elements does K have?
(c) Factor f completely in $K[x]$.

`Answer:`

(a) *No. $f(3) = 0$ and so $f(x) = (x - 3)(x^2 + x + 1)$.*

(b) *Since $3 \in \mathbb{Z}_5$, K is the splitting field for $x^2 + x + 1$. Because $x^2 + x + 1$ has no zeros in $\mathbb{Z}_5$ it is irreducible over $\mathbb{Z}_5$ and K has degree 2 over $\mathbb{Z}_5$. This means that $|K| = 5^2 = 25$.*

(c) *Let α be a zero of x^2+x+1 in K so that $K = \mathbb{Z}_5(\alpha)$. Since $x-\alpha$ is a factor of x^2+x+1, we can use long division to get the other factor: $x+\alpha+1$. The complete factorization of f is then $f(x) = (x-3)(x-\alpha)(x+\alpha+1)$.*