ALGEBRA COMPREHENSIVE EXAMINATION

Fall 2009

Brookfield*, Krebs, 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) Prove that $\mathbb{Q}$ is not a cyclic group.
`Answer:` *Of course,* $\langle 0\rangle = \{0\} \neq \mathbb{Q}$*. And if* $0 \neq q \in \mathbb{Q}$*, Then* $\langle q\rangle = \{nq \mid n \in \mathbb{Z}\}$ *is the set of all integer multiples of* q*. But not all rational numbers are integer multiples of* q*, for example,* $q/2$ *is not. (If* $q/2 = nq$ *for some* $n \in \mathbb{Z}$*, then* $q = 0$ *contrary to assumption.) Thus* $\mathbb{Q}$ *is not equal to any of its cyclic subgroups, that is,* $\mathbb{Q}$ *is not cyclic.*

(2) Let G be a group of order 30. Show that G is not simple.
`Answer:` *By Sylow,* $n_3 \in \{1, 10\}$ *and* $n_5 \in \{1, 6\}$*. But if* $n_3 = 10$ *and* $n_5 = 6$*, then* G *would have* 20 *elements of order* 3 *and* 24 *elements of order* 5*—clearly impossible. Thus, either* $n_3 = 1$ *and* G *contains a unique normal subgroup of order* 3*, or* $n_5 = 1$ *and* G *contains a unique normal subgroup of order* 5*. Either way,* G *is not simple.*

(3) Suppose that G is a nonabelian group of order p^3 where p is a prime number. In the problems below you may use the following facts: (A) If G is a group with center Z and G/Z is cyclic, then G is abelian; (B) If a group G has order p^2 then G is abelian.

(a) Let Z be the center of G. Prove that $|Z| = p$.
`Answer:` *By Lagrange,* $|Z| = 1$*,* p*,* p^2 *or* p^3*. Using the class equation in the standard way we know that* $|Z| \neq 1$*. And* $|Z| = p^3$ *would imply* $Z = G$ *and hence* G *is abelian, contrary to assumption. And if* $|Z| = p^2$ *then* $|G/Z| = p$ *and so* G/Z *is cyclic which, by (A), implies* G *is abelian, contrary to assumption.*

(b) Let G' be the commutator subgroup of G. Prove that $G' = Z$.
`Answer:` $|G/Z|$ *has order* p^2 *so is an abelian group by (B). This implies* $G' \leq Z$ *and also* $|G'| = 1$ *or* $|G'| = p$*. But* $G' = \{1\}$ *would imply that* G *is abelian, contrary to assumption. So we are left with* $|G'| = p$ *and so* $G' = Z$*.*

Rings

(1) Let R be a commutative ring with identity 1. For each $n \in \mathbb{N}$, let I_i be a proper ideal of R such that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ Show that $J = \bigcup_{n\in\mathbb{N}} I_n$ is a proper ideal of R.
`Answer:` *[See F02] Let* $x \in J$ *and* $r \in R$*. Then* $x \in I_n$ *for some* $n \in \mathbb{N}$*, and so* $rx \in I_n \subseteq J$*. Thus* J *is closed under multiplication by elements of* R*.*

Let $x, y \in J$*. Then* $x \in I_n$ *and* $y \in I_m$ *for some* $n, m \in \mathbb{N}$*, and so* $x, y \in I_{\max(m,n)}$*. Hence* $x - y \in I_{\max(m,n)} \subseteq J$*. Thus* J *is closed under subtraction.*

These two closure conditions imply that J *is an ideal of* R*. If* J *is not proper, then* $J = R$ *and* $1 \in J$*. But then* $1 \in I_n$ *for some* $n \in \mathbb{N}$*, which means that* $I_n = R$*, contradicting the properness of* I_n*. Thus* J *must be proper.*

(2) Let $R = M_2(F)$ be the ring of 2×2 matrices over a field F with the usual operations. Show that the only (two-sided) ideals of R are $\{0\}$ and R itself (that is, R is a simple ring).
`Answer:` *Let J be a two-sided ideal of R. Suppose that $J \neq \{0\}$ and contains a nonzero matrix $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in J$. At least one of the entries of A must be nonzero. If $a_{11} \neq 0$, then*

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_{11} & 0 \\ 0 & a_{11} \end{bmatrix} \in J$$

and so $I \in J$ and $J = R$. Similar arguments work if $a_{12} \neq 0$, $a_{21} \neq 0$ or $a_{22} \neq 0$.

(3) Let I be the ideal of $\mathbb{Z}[x]$ generated by 2 and x. Show that I is not a principal ideal.
`Answer:` *First we notice that any polynomial in I has the form $f(x) = 2g(x) + xh(x)$ for some $g, h \in \mathbb{Z}[x]$. In particular, $f(0) = 2g(0)$ is an even integer.*

Now suppose that I is principal, that is, $I = (f)$ for some $f \in \mathbb{Z}[x]$. Then, in particular, $2 \in I = (f)$ and so $2 = g(x)f(x)$ for some $g \in \mathbb{Z}[x]$. But $\deg g + \deg f = \deg 2 = 0$, *so* $\deg g = \deg f = 0$ *and g and f are constant polynomials, that is $g, f \in \mathbb{Z}$. From above, f must be ± 2, and so $I = (f) = (2) = \{2h(x) \mid h(x) \in \mathbb{Z}[x]\}$, that is, I is the set of polynomials whose coefficients are all even. But then $x \notin I$, a contradiction. Thus we have shown that I is not a principal ideal.*

Fields

(1) Consider $f(x) = x^3 + 3x^2 + 3x + 2 \in \mathbb{Z}_5[x]$. Is f irreducible over $\mathbb{Z}_5$? Let K be the splitting field of f over $\mathbb{Z}_5$. Factor f completely over $K[x]$.
`Answer:` *[See F08] $f(3) = 0$ and so $f(x) = (x+2)(x^2+x+1)$. Since x^2+x+1 has no roots in $\mathbb{Z}_5$, this polynomial is irreducible. Then $K = \mathbb{Z}_5(\alpha)$ where $\alpha^2 + \alpha + 1 = 0$. The other root of $x^2 + x + 1$ in K is $-1 - \alpha$ and so $f(x) = (x + 2)(x - \alpha)(x + 1 + \alpha)$ in $K[x]$.*

(2) Find the Galois group of $f(x) = x^4 - 2$ over $\mathbb{Q}$. Show that it is not abelian.
`Answer:` *Let $\alpha = \sqrt[4]{4}$. Then the other roots of f are $i\alpha$, $-\alpha$ and $-i\alpha$. The splitting field of f is $F = \mathbb{Q}(\alpha, i)$. Since f is irreducible over $\mathbb{Q}$ (by Eisenstein with $p = 2$, for example), α has degree 4 over $\mathbb{Q}$, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Since $i \notin \mathbb{Q}(\alpha) \subseteq \mathbb{R}$, i has degree 2 over $\mathbb{Q}(\alpha)$, and hence $[F : \mathbb{Q}] = 8$. By Galois Theory, the Galois group of f has order 8 and it is isomorphic to a subgroup of S_4. But all such subgroups of S_4 are isomorphic to the dihedral group of order 8, D_8, a nonabelian group.*

(3) Let p be a prime number, and let $\mathbb{Z}_p$ be the field of integers modulo p. Let E be a finite extension field of $\mathbb{Z}_p$. Let n be a positive integer. Let

$$S = \sum_{x \in E} x^n.$$

(a) Let $\sigma \in \mathrm{Gal}(E/\mathbb{Z}_p)$. Show that $\sigma(S) = S$.
`Answer:` *σ is, among other things, a bijection from E to E. So it simply permutes the terms of the sum defining S. Thus $\sigma(S) = S$.*

(b) Show that $S \in \mathbb{Z}_p$.

`Answer:` *Every finite extension of a finite field is Galois, and so by definition of a Galois extension, the fixed field of* $\mathrm{Gal}(E/\mathbb{Z}_p)$ *is* $\mathbb{Z}_p$. *By* (a), S *is in this fixed field.*