ALGEBRA COMPREHENSIVE EXAMINATION

Spring 2013

Brookfield*, Krebs, Shaheen, Webster

Directions: Answer 5 questions only. If you answer more than five questions, your exam score will be based on the five lowest scoring questions.You must answer *at least one* from each of groups, rings, and fields. Be sure to show enough work so that your answers are adequately supported.

Groups

(1) Show that, if G is a cyclic group, then every subgroup of G is cyclic.

`Answer:` *[See also S08] Suppose that* $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$. *Let* H *be a subgroup of* G. *If* $H = \{1\}$ *then* $H = \langle 1 \rangle$ *and so* H *is cyclic. Otherwise,* H *contains at least one element of the form* a^k *with* $k \in \mathbb{N}$.

Let $n \in \mathbb{N}$ *be the least natural number such that* $a^n \in H$. *Then* $\langle a^n \rangle \leq H$ *is automatic. We prove the opposite inclusion: Suppose that* $a^k \in H$. *Since* $n \in \mathbb{N}$, *there are* $q, r \in \mathbb{Z}$ *such that* $k = qn + r$ *and* $0 \leq r < n$. *Then* $a^r = a^{k-qn} = a^k(a^n)^{-q}$. *Because* a^n *and* a^k *are in* H, *so is* a^r. *But, by the choice of* n, *this is only possible if* $r = 0$. *Thus* $k = qn$ *and* $a^k = (a^n)^q \in \langle a^n \rangle$. *This shows that* $H = \langle a^n \rangle$ *and that* H *is cyclic.*

(2) (a) Let a and b be elements of a group G such that $|a| = 3$, $|b| = 2$ and $ab = ba$. Show that $|ab| = 6$.

(b) Find a group G and elements $a, b \in G$ such that $|a| = 3$, $|b| = 2$ and $|ab| \neq 6$.

`Answer:`

(a) *On one hand* $(ab)^6 = a^6b^6 = 1$ *and so* $|ab|$ *divides* 6. *On the other hand,* $\langle ab \rangle$ *contains an element of order* 2, *namely* $(ab)^3 = a^3b^3 = b$, *and an element of order* 3, *namely* $(ab)^4 = a^4b^4 = a$, *and so* $|\langle ab \rangle|$ *is a multiple of* $2 \cdot 3$. *Thus* $|ab| = \langle ab \rangle = 6$.

(b) *For example,* $a = (1, 2, 3)$, *and* $b = (1, 2)$ *in* S_3.

(3) Prove that any nonabelian group G of order 6 contains elements r and s such that $|r| = 3$, $|s| = 2$ and $|sr| = 2$. Do not use the fact that such a group is isomorphic to S_3. Hint: How many Sylow-3 subgroups are there?

`Answer:` *No element of* G *can have order* 6 *because otherwise* G *is cyclic and abelian. Thus all elements of* G *have order* 1, 2 *or* 3.

By the Sylow Theorems, the number of Sylow-3 *subgroups,* n_3, *satisfies* $n_3 | 6$ *and* $n_3 \equiv 1 \mod 3$. *These conditions imply that* $n_3 = 1$ *and there is a unique normal Sylow-*3 *subgroup* H. *This subgroup has order* 3, *so is cyclic, generated by an element* r *such that* $|r| = 3$ *and* $H = \{1, r, r^2\}$. *All other nonidentity elements of* G *must have order* 2. *Let* s *be such an element.*

To prove $|sr| = 2$ *it suffices to show that* sr *does not have order* 1 *or* 3, *that is,* $sr \neq 1$, $sr \neq r$ *and* $sr \neq r^2$. *But if* $sr = 1$, *then* $s = s(sr) = s^2r = r$ *which is impossible because* $|s| \neq |r|$. *If* $sr = r$, *then cancellation gives* $s = 1$ *which is impossible because* $|s| \neq |1|$. *And, if* $sr = r^2$, *then cancellation gives* $s = r$, *which is impossible. Thus* $|sr| = 2$.

Rings

(1) (a) Suppose that $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Q}[x]$ is irreducible over the rationals. Show that $g(x) = a_n + a_{n-1}x + a_{n-1}x^2 + \cdots + a_0x^n \in \mathbb{Q}[x]$ is irreducible over the rationals.
`Answer:` *Since $g(x) = x^n f(1/x)$, if f is reducible then so is g. Specifically, if $f(x) = h(x)k(x)$, with $\deg h = a$ and $\deg k = b$, then $a + b = n$ and $g(x) = (x^a h(1/x))(x^b k(1/x)$ with $\deg x^a h(1/x) = a$ and $\deg x^b k(1/x) = b$.*

(b) Prove that the polynomial $2x^5 - 4x^2 - 3$ is irreducible in $\mathbb{Z}[x]$.
`Answer:` *By Gauss's Lemma and (a), $2x^5 - 4x^2 - 3$ is irreducible over $\mathbb{Z}$ iff it is irreducible over $\mathbb{Q}$ iff $-3x^5 - 4x^3 + 2$ is irreducible over $\mathbb{Q}$. But $-3x^5 - 4x^3 + 2$ is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$.*

(2) Let R and S be commutative rings with unity.

(a) If A is an ideal of R and B is an ideal of S, show that $A \times B$ is an ideal of $R \times S$.
`Answer:`
(i) *Let $(a_1, b_1), (a_2, b_2) \in A \times B$. Since $a_1 - a_2 \in A$ and $b_1 - b_2 \in B$, we have $(a_1, b_1) - (a_2, b_2) = (a_1 - a_2, b_1 - b_2) \in A \times B$.*
(ii) *Let $(a, b) \in A \times B$ and $(r, s) \in R \times S$. Since $ra \in A$ and $sb \in B$ we have $(r, s)(a, b) = (ra, sb) \in A \times B$.*
(iii) *Since $A \times B$ is nonempty, (i) and (ii) imply that $A \times B$ is an ideal.*

(b) Show that every ideal I of $R \times S$ has the form $I = A \times B$ where A is an ideal of R and B is an ideal of S. Hint: $A = \{a \in R \mid (a, 0) \in I\}$.
`Answer:` *Given the ideal I, let $A = \{a \in R \mid (a, 0) \in I\}$ and $B = \{b \in S \mid (0, b) \in I\}$. We need to show that A, B are ideals and $I = A \times B$.*
(i) *Let $a_1, a_2 \in A$. Then $(a_1, 0), (a_2, 0) \in I$ and so $(a_1 - a_2, 0) = (a_1, 0) - (a_2, 0) \in I$. This means that $a_1 - a_2 \in A$.*
(ii) *Let $a \in A$ and $r \in R$. Then $(a, 0) \in I$ and $(r, 0) \in R \times S$ and so $(ra, 0) = (r, 0)(a, 0) \in I$. This implies that $ra \in A$.*
(iii) *Since A is non empty, (i) and (ii) imply that A is an ideal of R. Similarly, B is an ideal of S.*
(iv) *Suppose that $(a, b) \in I$. Because $(1, 0) \in R \times S$ and I is an ideal, $(a, 0) = (1, 0)(a, b)$ is in I. This means $a \in A$. Similarly, $b \in B$ and consequently $(a, b) \in A \times B$. This shows that $I \subseteq A \times B$.*
(v) *Suppose that $(a, b) \in A \times B$. Then $(a, 0), (0, b) \in I$ and so $(a, b) = (a, 0) + (0, b) \in I$. This shows that $A \times B \subseteq I$.*
(vi) *(iv) and (v) imply that $I = A \times B$.*

(3) Let p be a prime and let R be the ring of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ pb & a \end{bmatrix}$, where $a, b \in \mathbb{Z}$. Prove that R is isomorphic to $\mathbb{Z}(\sqrt{p})$.
`Answer:` *Note: The claim is true for any p that is not a square in $\mathbb{Z}$. If we can assume without proof that every element of $\mathbb{Z}(\sqrt{p})$ has the form $a + b\sqrt{p}$ for uniquely determined $a, b \in \mathbb{Z}$, then the function $\phi : R \to \mathbb{Z}(\sqrt{p})$ defined by $\phi\left(\begin{bmatrix} a & b \\ pb & a \end{bmatrix}\right) = a + b\sqrt{p}$ is a bijection. It remains to show only that ϕ is a*

homomorphism. And this is just confirmation of the equations

$$\phi\left(\begin{bmatrix} a_1 & b_1 \\ pb_1 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ pb_2 & a_2 \end{bmatrix}\right) = (a_1 + b_1\sqrt{p}) + (a_2 + b_2\sqrt{p})$$

$$\phi\left(\begin{bmatrix} a_1 & b_1 \\ pb_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ pb_2 & a_2 \end{bmatrix}\right) = (a_1 + b_1\sqrt{p})(a_2 + b_2\sqrt{p})$$

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

Fields

(1) Here's a fact from trigonometry that you may use without proof in this problem: Let n be a positive integer. Then there exists a polynomial $f \in \mathbb{Z}[x]$ such that $\cos nx = f(\cos x)$. [For example, when $n = 2$, the polynomial is $f(x) = 2x^2 - 1$; this is the double-angle formula $\cos 2x = 2\cos^2 x - 1$.]

Prove that if q is a rational number, then $\tan q\pi$ is algebraic over $\mathbb{Q}$.

`Answer:` *First we prove that* $\cos q\pi$ *is algebraic over* $\mathbb{Q}$. *Let* $q = m/n$ *with* $m \in \mathbb{Z}$ *and* $n \in \mathbb{N}$. *Then there is a polynomial* $f \in \mathbb{Z}[x]$ *such that* $f(\cos q\pi) = \cos(nq\pi) = \cos m\pi$. *Since* $\cos m\pi$ *is an integer,* $\cos q\pi$ *is a root of the polynomial* $f(x) - \cos m\pi \in \mathbb{Z}[x]$ *and so* $\cos q\pi$ *is algebraic over* $\mathbb{Q}$.

Now we prove the same for the sine function: $\sin q\pi = \cos(\pi/2 - q\pi) = \cos((1/2 - q)\pi)$, *and so, because* $1/2 - q \in \mathbb{Q}$, $\sin q\pi$ *is also algebraic over* $\mathbb{Q}$.

Finally, because, the set of algebraic numbers is a field, $\tan q\pi = (\sin qx)/(\cos qx)$ *is algebraic over* $\mathbb{Q}$.

(2) Let $\alpha = \sqrt{3 + \sqrt{5}}$. Show that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Hint: $(x^2 - 3)^2 - 5 = (x^2 + 2)^2 - 10x^2$.

`Answer:` $\sqrt{5} = \alpha^2 - 3$ *and so* $\sqrt{5} \in \mathbb{Q}(\alpha)$. *Using the hint we get*

$$0 = (\alpha^2 - 3)^2 - 5 = (\alpha^2 + 2)^2 - 10\alpha^2$$

and so $\alpha^2 + 2 = \pm\sqrt{10}\alpha$. *This implies that* $\sqrt{10} = \pm(\alpha^2 + 2)/\alpha \in \mathbb{Q}(\alpha)$. *Also* $\sqrt{2} = \sqrt{10}/\sqrt{5}$ *is in* $\mathbb{Q}(\alpha)$. *This implies* $\mathbb{Q}(\sqrt{2}, \sqrt{5}) \subseteq \mathbb{Q}(\alpha)$.

For the opposite inclusion, a bit of playing around yields $(1 + \sqrt{5})^2 = 6 + 2\sqrt{5} = 2\alpha^2$ *and so*

$$\alpha^2 = \left(\frac{1 + \sqrt{5}}{\sqrt{2}}\right)^2.$$

Consequently, $\alpha = \pm(1 + \sqrt{5})/\sqrt{2} \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$ *and* $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

(3) Let E be the splitting field of $f(x) = x^4 - 2x^2 - 3$ over $\mathbb{Q}$.

(a) Calculate $[E : \mathbb{Q}]$.

`Answer:` *The roots of* f *are* $\pm i$ *and* $\pm\sqrt{3}$. *So* $E = \mathbb{Q}(i, \sqrt{3})$. *Since* $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ *and* $[E : \mathbb{Q}(\sqrt{3})] = 2$, *we have* $[E : \mathbb{Q}] = 4$.

(b) Classify the Galois group G of E over $\mathbb{Q}$.

`Answer:` *Since* E *is a Galois extension of* $\mathbb{Q}$, *the order of* G *is* $[E : \mathbb{Q}] = 4$. *Each automorphism in* G *sends* $\sqrt{3}$ *to a conjugate of* $\sqrt{3}$ *over* $\mathbb{Q}$, *and sends* i *to a conjugate of* i *over* $\mathbb{Q}$. *Moreover, the automorphism is determined by where it sends* $\sqrt{3}$ *and* i. *Thus* $G = \{\phi_0, \phi_1, \phi_2, \phi_3\}$ *is given by the table:*

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

ϕ_0 is the identity function. The other elements of G have order 2, so G is isomorphic to the Klein group $V = \mathbb{Z}_2 \times \mathbb{Z}_2$.

(c) Find all intermediate fields. That is, find all fields F with $\mathbb{Q} \subseteq F \subseteq E$.
`Answer:` *Each intermediate field is the fixed field of a subgroup of G. The subgroups and corresponding fields are as below:*

Group	*Field*
$\{\phi_0\}$	E
$\{\phi_0, \phi_1\}$	$\mathbb{Q}(i)$
$\{\phi_0, \phi_2\}$	$\mathbb{Q}(\sqrt{3})$
$\{\phi_0, \phi_3\}$	$\mathbb{Q}(i\sqrt{3})$
G	$\mathbb{Q}$

For example, the fixed field of $\{\phi_0, \phi_1\} \leq G$ has degree 2 over $\mathbb{Q}$ and contains i. Hence the fixed field is $\mathbb{Q}(i)$.