# FALL 2012 ALGEBRA COMPREHENSIVE EXAM

**Instructions:** Complete 5 of the 8 problems below. If you attempt more than five questions, then clearly indicate which five should be graded.

(1) (a) Over a field of characteristic 0, prove that you cannot find two matrices $A$ and $B$ such that $AB - BA = I$, where $I$ denotes the identity matrix.
    (b) Show that the statement is false in characteristic 2.

(2) Let $G$ be a group of order $p^2q$ where $p$ and $q$ are distinct primes. Prove that $G$ has a non-trivial normal subgroup.

(3) For $n \geq 3$, prove that the alternating group $A_n$ is generated by 3-cycles.

(4) Find five nonabelian groups of order 24 that are pairwise non-isomorphic. Prove that your answer is correct.

(5) Let $R$ be a commutative ring and $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ be a zero divisor in the polynomial ring $R[x]$. Show that there is a nonzero element $b \in R$ such that $ba_0 = ba_1 = \cdots = ba_n = 0$.

(6) Let $f(x) \in \mathbb{Q}[x]$ be a rational polynomial irreducible over $\mathbb{Q}$. Prove that $f(x)$ has no multiple (repeated) roots in $\mathbb{C}$.

(7) Let $F$ be a finite field. Show that if $a, b \in F$ are both non-squares, then $ab$ is a square.

(8) Let $\alpha = \sqrt{5}$ and $\beta = \sqrt[3]{2}$.
    (a) Prove that the degree of the field extension $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ is 6.
    (b) Prove that the degree of the field extension $\mathbb{Q}(\alpha + \beta)/\mathbb{Q}$ is 6.
    (c) Find the minimal polynomial of $\alpha + \beta$ over $\mathbb{Q}$.

**Solution.**

(1) (a) Take trace of both sides. Suppose matrices are of size $n \times n$, then

$$0 = \mathrm{Tr}\,(AB) - \mathrm{Tr}\,(BA) = \mathrm{Tr}\,(I) = n.$$

This leads to a contradiction for characteristics not diving $n$.

(b) Over $\mathbb{Z}/2\mathbb{Z}$, take

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

(2) Let $n_p$ and $n_q$ be the number of $p$-Sylow subgroups and $q$-Sylow subgroups respectively. By Sylow's Theorems, the $p$-Sylow subgroups are conjugate to each other and $n_p = 1(\operatorname{mod} p)$. But $n_p | p^2q$, so $n_p$ is either 1 or $q$. Similarly, $n_q = 1(\operatorname{mod} q)$, and $n_q$ is 1 or $p$ or $p^2$. If $n_p = 1$ or $n_q = 1$, a Sylow subgroup is normal, and we are done. Otherwise, $q|(p \pm 1)$ and $p|(q-1)$, so the only possibility is $p = 2$ and $q = 3$. Then $G$ is a group of order 12. If $n_2 = 1$, we are done. Otherwise, $n_2 = 3$, and $G$ acts transitively on the three 2-Sylow subgroups by conjugation. Thus we get a non-trivial homomorphism from $G$ to $S_3$, whose kernel is a non-trivial normal subgroup.

(3) Let $n \geq 3$. Every element of $A_n$ can be written as the product of even number of transpositions. Note that $(ab)(ac) = (acb)$, and $(ab)(cd) = (ab)(bc)(bc)(cd) = (bca)(cdb)$ where $a, b, c, d$ are distinct elements in $\{1, 2, \ldots, n\}$. Hence $A_n$ is generated by 3-cycles.

(4) Let $S_n$ denote the symmetric group of order $n$ and $D_n$ denote the dihedral group consisting of symmetries of a regular $n$-gon.

(a) $S_4$
(b) $D_{12}$
(c) $S_3 \times C_4$
(d) $S_3 \times C_2 \times C_2$
(e) $D_6 \times C_2$

The last three groups have non-trivial and unique centers, so they're not isomorphic to any other on the list. The group $D_{12}$ has 11 elements of order 2 while $S_4$ has only 9, so they're not isomorphic to each other.

(5) Let $g(x) = b_0 + b_1x + \cdots + b_mx^m \in R[x]$ be a polynomial of minimal degree in $R[x]$ satisfying $g(x)f(x) = 0$. We will show that $b_ma_i = 0$ for $0 \leq i \leq n$. It is clear that $b_ma_n = 0$. Then $a_ng(x)f(x) = 0$, so $a_ng(x)$ must be identically 0; otherwise $a_ng(x)$ would have degree less than $g(x)$. Thus $(a_0 + \cdots + a_{n-1}x^{n-1})g(x) = 0$, which implies that $b_ma_{n-1} = 0$ and $a_{n-1}g(x) = 0$. By repeating this argument, we conclude that $a_ig(x) = 0$ and $b_ma_i = 0$ for all $0 \leq i \leq n$.

(6) Suppose $f$ has a repeated root $a$, then $a$ is a root of the derivative $f'$ and $g = \gcd(f, f') \in \mathbb{Q}[x]$, the greatest common divisor of $f$ and $f'$. In particular, $g$ is not a constant polynomial. Since it divides $f$

and is of lower degree, we have a contradiction to the irreducibility of $f$.

(7) Let $F^*$ be the multiplicative group of nonzero elements in $F$. It is a cyclic group. Let $c$ be a generator. Since $a$ and $b$ are non-squares, they are non-zero, and they are both odd powers of $c$. Thus $ab$ is an even power of $c$, so it is a square.

(8) (a) It is sufficient to show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 3$.

(b) Let $\gamma = \alpha + \beta$. Use linear algebra to show that $\{1, \gamma, \gamma^2, \gamma^3\}$ are linearly independent over $\mathbb{Q}$. Since $\mathbb{Q}(\gamma)$ is a subfield of $\mathbb{Q}(\alpha, \beta)$, the order $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ has to divide 6 and $1, 2, 3$ are ruled out.

(c) Cube $\sqrt[3]{2} = \gamma - \sqrt{5}$ to get

$$2 = \gamma^3 - 3\sqrt{5}\gamma^2 + 15\gamma - 5\sqrt{5}.$$

Squaring $\sqrt{5}(3\gamma^2 + 5) = \gamma^3 + 15\gamma - 2$ shows that $\gamma$ is a root of

$$f(x) = (x^3 + 15x - 2)^2 - 5(3x^2 + 5)^2.$$

Since $\deg f(x) = 6$, it is the minimal polynomial of $\gamma$ by part (b).