Algebra Comprehensive Exam

— Spring 2008 —

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

(1) (a) Prove that a finite abelian group is a direct product of its Sylow subgroups.
(b) How many finite abelian groups of order 135 are there, up to isomorphism?

Solution. (a) Let G be a finite abelian group. Since G is abelian, every Sylow subgroup is normal. Moreover, every two Sylow subgroups commute. It follows that G is the direct product of its Sylow subgroups.

(b) Since $135 = 27 \cdot 5$, and every finite abelian p-group is a direct sum of cyclic subgroups, there are exactly 3 abelian groups of order 135: $\mathbb{Z}/135\mathbb{Z}$, $\mathbb{Z}/45\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. □

(2) Let k be a field and $G = \mathrm{G}l_n(k)$ be the group of $n \times n$ invertible matrices with entries in k. Let $U \subset G$ be the set of upper triangular matrices with all diagonal entries equal to 1.
(a) Prove that U is a subgroup of G.
(b) Now let p be a prime, $k = \mathbb{Z}/p\mathbb{Z}$ and G and U as above. Prove that U is a p-Sylow subgroup of G.
(c) Describe a non-abelian group of order 27.

Solution. (a)Let $X, Y \in U$. We prove that XY as well as $X^{-1} \in U$. This will show that U is a subgroup of G, since clearly the identity matrix is in U.

We have that

$$(XY)_{ij} = \sum_{k=1}^{n} X_{ik} Y_{kj}.$$

Since $X, Y \in U$, we have that $X_{ij} = Y_{ij} = 0$ if $j < i$, and $X_{ii} = Y_{ii} = 1$. If $j < i$ then, for all $k \geq i$, $Y_{kj} = 0$ and for all $k < i$ $X_{ik} = 0$, implying that $(XY)_{ij} = 0$. If $i = j$, then for all $k > i$, $Y_{kj} = 0$ and for all $k < i$ $X_{ik} = 0$, implying that $(XY)_{ii} = X_{ii} Y_{ii} = 1$. This shows that $XY \in U$.

Alternatively, we can write X and Y as

$$X = I + N_1$$
$$Y = I + N_2$$

where N_1, N_2 are strictly upper-triangular matrices. Then,

$$XY = (I + N_1)(I + N_2) = I + N_2 + N_1 + N_1 N_2.$$

Since the sum and the product of two strictly upper-triangular matrices is again upper triangular we have that $XY \in U$.

To show that $X^{-1} \in U$ notice that $X = I - N$ where N is a strictly upper triangular and hence nilpotent matrix. Then,

$$X^{-1} = I + N + N^2 + \cdots + N^m,$$

for some $m \geq 0$. Moreover, all positive powers of N are strictly upper triangular, and hence $X^{-1} \in U$.

(b) We first prove that the order of the group $\mathrm{G}l_n(\mathbb{Z}/p\mathbb{Z})$ is $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$. To see this observe that the number of ways to choose the first row of a matrix in $\mathrm{G}l_n(\mathbb{Z}/p\mathbb{Z})$

is $p^n - 1$ (only the all 0 row is disallowed). More generally, having chosen the first $i-1$ rows the number of ways to choose the i-th row is $p^n - p^{i-1}$ (one has to avoid picking a linear combination of the first $i-1$ rows and there are p^{i-1} such combinations which are all distinct since the first $i-1$ rows are linearly independent). The highest power of p dividing $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$ is clearly $p^{n-1}\cdot p^{n-2}\cdots 1$ which is also the order of U. Hence, U is a p-Sylow subgroup of G.

(c) Let $n = 3$ and $p = 3$. The corresponding group U has order 27 and is non-abelian. □

(3) Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group, i.e., $(-1)^2 = 1$ is the identity element, $i^2 = j^2 = k^2 = -1$, and

$$ij = k = -ji, \qquad jk = i = -kj, \qquad ki = j = -ik.$$

(a) Determine all subgroups of Q and prove that they are normal.
(b) What is the order of $\mathrm{Aut}(Q)$?

Solution. (a) Aside from e, the group Q consists of six elements of order 4 and one element of order 2, namely -1. Consequently the only subgroups of Q are

$$Q, \quad \langle i\rangle, \quad \langle j\rangle, \quad \langle k\rangle, \quad \langle -1\rangle, \quad \{e\}.$$

(b) Any two elements of order four, which are not powers of each other, constitute a generating set for Q. Any automorphism $\varphi \in \mathrm{Aut}(Q)$ is determined by its behavior on a generating set, and must take a generating set to a generating set. Consider the generating set $\{i, j\}$. Then

$$\varphi(i) \in \{\pm i, \pm j, \pm k\} \qquad \text{and} \qquad \varphi(j) \in \{\pm i, \pm j, \pm k\} \setminus \{\pm\varphi(i)\}.$$

Consequently $|\mathrm{Aut}(Q)| = 24$. □

(4) Let A be a commutative ring and M a finitely generated A module. For $m \in M$ let $\mathrm{Ann}(m) = \{a \in A \mid am = 0\}$.
(a) Prove that for each $m \in M$, $\mathrm{Ann}(m)$ is an ideal of A.
(b) Let $P = \{\mathrm{Ann}(m) \mid m \in M, m \neq 0\}$. Prove that a maximal element of P is a prime ideal.

Solution. (a) Clearly, if $a, b \in \mathrm{Ann}(m)$ then so is $a+b$ and $-a$. Moreover, $0 \in \mathrm{Ann}(m)$. Finally, if $a \in \mathrm{Ann}(m)$ and $c \in A$, $ca \in \mathrm{Ann}(m)$ showing that $\mathrm{Ann}(m)$ is an ideal.

(b) Let $m \in M$ be an element such that $\mathrm{Ann}(m)$ is a maximal element of P. Let $xy \in \mathrm{Ann}(m)$, but $x \notin \mathrm{Ann}(m)$. Then, $xm \neq 0$. But $\mathrm{Ann}(xm)$ contains $\mathrm{Ann}(m)$ and hence must be equal to $\mathrm{Ann}(m)$ since $\mathrm{Ann}(m)$ is maximal in P. Since, $y \in \mathrm{Ann}(xm)$ it follows that $y \in \mathrm{Ann}(m)$, proving that $\mathrm{Ann}(m)$ is prime. □

(5) Recall that a commutative ring A is called Noetherian if every ideal of A is finitely generated.
(a) Prove that A is Noetherian if and only if every ascending sequence of ideals of A eventually stabilize.
(b) Let k be a field. Show that the ring $A = k[T^2, T^3]$ is Noetherian.
(c) Let $C[-1,1]$ denote the ring of continuous functions on the interval $[-1,1]$. Prove that $C[-1,1]$ is not Noetherian.

Solution. (a) Suppose every ascending sequence of ideals of A stabilize. Let $I \subset A$ be an ideal. Let $a_0 \in I$ and let $I_0 = (a_0)$. If $I = I_0$ then I is finitely generated. Otherwise, choose $a_1 \in I \setminus I_0$ and let $I_1 = (a_0, a_1)$ and so on. The sequence $I_0 \subset I_1 \subset I_2 \cdots$ must terminate by at some I_n by hypothesis. Then $I = I_n = (a_0, \ldots, a_n)$ is finitely generated.

Conversely, if every ideal of A is finitely generated and we have an ascending sequence, $I_0 \subset I_1 \subset \cdots \subset I_n \subset \cdots$ of ideals, then consider the ideal $I = \cup_{0 \leq j} I_j$. Then I is finitely generated. Let $I = (a_0, \ldots, a_m)$. There must exist some n such that $a_i \in I_n, 0 \leq i \leq m$. Then, $I_n = I_{n+1} = \cdots = I$, proving that the sequence $I_0 \subset I_1 \subset \cdots \subset I_n \subset \cdots$ stabilizes.

(b) The ring $k[T^2, T^3] \cong k[X, Y]/(X^3 - Y^2)$. By Hilbert's theorem we know that $k[X, Y]$ is Noetherian, and quotients of Noetherian rings are again Noetherian.

(c) Let $I_n \subset C[-1, 1]$ be the ideal of functions vanishing on the interval $[-1/n, 1/n]$. Then the sequence $I_1 \subset I_2 \subset I_3 \cdots$ is a strictly ascending sequence of ideals that does not stabilize. □

(6) Let k be an infinite field, V a k-vector space and $A \in \mathrm{End}(V)$. For $v \in V$, the minimal polynomial of v (with respect to the the endomorphism A) is the monic polynomial p of smallest possible degree such that $p(A)v = 0$. Prove that for any endomorphism A there exists an element $v \in V$ whose minimal polynomial (with respect to A) coincides with that of A.

Solution. For any $v \in V$, let $I_v \subset k[X]$ be the ideal defined by $I_v = \{P \in k[X] \mid P(A) \cdot v = 0\}$. Let $I_v = (P_v)$ for some monic polynomial P_v since $k[X]$ is a PID. Let P_A be the minimal polynomial of A. Since $P_A \in I_v$, $P_v | P_A$. Hence, as v runs over the whole of V, we have a finite number of choices for P_v. Let these be $P_1, \ldots, P_k$. Then, V is contained in the union of subspaces, $V_i = \{v \in V \mid P_i(A) \cdot v = 0\}, 1 \leq i \leq k$, and hence $V = V_i$ for some i (say i_0). Then, $P_{i_0}(A) \cdot V = 0$. Hence, $P_A | P_{i_0}$ and hence $P_A = P_{i_0}$. □

(7) (a) Prove that the sum of two algebraic numbers is an algebraic number.
(b) Compute the degree of the extension $\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}$.
(c) What is the degree of the minimal polynomial of $2^{1/2} + 2^{1/3}$ over $\mathbb{Q}$?

Solution. (a) α is an algebraic number iff the extension $\mathbb{Q}(\alpha) : \mathbb{Q}$ is finite. If α and β are algebraic numbers, then $\mathbb{Q}(\alpha) : \mathbb{Q}$ and $\mathbb{Q}(\beta) : \mathbb{Q}$ are finite. Therefore $\mathbb{Q}(\alpha, \beta) : \mathbb{Q}$ is finite, and since $\mathbb{Q} \subset \mathbb{Q}(\alpha + \beta) \subset \mathbb{Q}(\alpha, \beta)$, then $\mathbb{Q}(\alpha + \beta) : \mathbb{Q}$ is finite. The result follows.

(b) $\mathbb{Q}(2^{1/3}) : \mathbb{Q}$ and $\mathbb{Q}(2^{1/2}) : \mathbb{Q}$ are finite extensions of comprime degrees 3 and 2 respectively. Thus, $\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}$ is an extension of degree $2 \cdot 3 = 6$.

(c) By (a) and (b) it follows that the degree $\mathbb{Q}(2^{1/2} + 2^{1/3}) : \mathbb{Q}$ divides 6. Since it is strictly bigger than 1, it follows that it is 2,3 or 6. If the degree is 2, then look at the chain: $\mathbb{Q} \subset \mathbb{Q}(2^{1/2} + 2^{1/3}) \subset \mathbb{Q}(2^{1/2} + 2^{1/3}, 2^{1/2}) = \mathbb{Q}(2^{1/2}, 2^{1/3})$ where the degree of the extension $\mathbb{Q}(2^{1/2} + 2^{1/3}) \subset \mathbb{Q}(2^{1/2} + 2^{1/3}, 2^{1/2})$ is 1 or 2. It follows that the degree of $\mathbb{Q} \subset \mathbb{Q}(2^{1/2}, 2^{1/3})$ is 2 or 4 absurd. Likewise, if the degree of $\mathbb{Q}(2^{1/2} + 2^{1/3}) : \mathbb{Q}$ is 3 we reach a contradiction by looking at the chain $\mathbb{Q} \subset \mathbb{Q}(2^{1/2} + 2^{1/3}) \subset \mathbb{Q}(2^{1/2} + 2^{1/3}, 2^{1/3}) = \mathbb{Q}(2^{1/2}, 2^{1/3})$. It follows that the degree $\mathbb{Q}(2^{1/2} + 2^{1/3}) : \mathbb{Q}$ is 6, thus the minimal polynomial of $2^{1/2} + 2^{1/3}$ over $\mathbb{Q}$ has degree 6. □