ALGEBRA COMPREHENSIVE EXAM
SPRING 2014

Choose any five problems. If you attempt more than five, indicate clearly which five are to be graded.

(1) Suppose G is a group with $|G| = 60$ and $|Z(G)|$ is divisible by 4. Show that G has a normal subgroup of order 5.

Solution: By Sylow's theorem, G has at least one subgroup of order 5; fix one and call it H. The number n of such subgroups is congruent to 1 modulo 5 and divides $60/5 = 12$. Thus n is either 1 or 6. Also, G acts transitively by conjugation on the subgroups of order 5, and n is the index in G of the stabilizer of H. The stabilizer is the normalizer $N_G(H)$, so $n = [G : N_G(H)]$. We know $H \subset N_G(H)$ and $Z(G) \subset N_G(H)$, so 5 divides the order of $N_G(H)$ and 4 does too. This implies that the order of $N_G(H)$ is at least 20, so $n \leq 60/20 = 3$. Therefore $n = 1$ and H is normal.

(2) Let $GL(n, \mathbb{Q})$ denote the group of invertible $n \times n$ matrices with entries in the rational numbers. Let p be a prime satisfying $p > n+1$. Show that if $A \in GL(n, \mathbb{Q})$ satisfies $A^p = I$ then $A = I$ (here I denotes the $n \times n$ identity matrix).

Solution: Since $A^p = I$, the minimal polynomial $m(x)$ of A divides $x^p - 1$. Note that $m(x)$ has coefficients in $\mathbb{Q}$ and that the factorization of $x^p - 1$ into irreducible factors over $\mathbb{Q}$ is

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \cdots + 1).$$

Since $p - 1 > n$ and the degree of m is $\leq n$, the second factor above does not appear in $m(x)$. We conclude that $m(x) = (x - 1)$. This implies that $A = I$.

(3) Find the degree of the splitting field of the polynomial $x^6 - 7$ over:
(a) $\mathbb{Q}$
(b) $\mathbb{Q}(\zeta_3)$ where ζ_3 is a primitive 3rd root of unity.
(c) $\mathbb{F}_3$ (the field with 3 elements).

Solution: Let L be the splitting field in question. For (a) and (b), let $\sqrt[6]{7}$ be the positive real 6-th root of 7, and let $\zeta_3 = e^{2\pi i/3}$ be a primitive cube root of unity in $\mathbb{C}$. Then the roots of $x^6 - 7$ are the numbers $\pm\zeta_3^i \sqrt[6]{7}$ where $i = 0, 1, 2$. The field they generate is also generated by ζ_3 and $\sqrt[6]{7}$. Moreover, ζ_3 generates an imaginary quadratic extension, and $\sqrt[6]{7}$ generates a real extension of degree 6. Thus together they generate an extension of $\mathbb{Q}$ of degree 12 and an extension of $\mathbb{Q}(\zeta_3)$ of degree 6. For part (c), note that in $\mathbb{F}_3[x]$ we have

$$x^6 - 7 = x^6 - 1 = (x^2 - 1)^3.$$

The roots of this polynomial (± 1) lie in $\mathbb{F}_3$, so the splitting field is $\mathbb{F}_3$ itself.

(4) Let R be a principal ideal domain. Show that if $P \neq \langle 0 \rangle$ is a prime ideal then P is maximal.

Solution: Suppose $P = (a)$ (the principal ideal generated by $a \in R$) and suppose $P \subset Q = (b)$ and $P \neq Q$. Since $P \subset Q$ we have $a = bc$ and since $P \neq Q$, $b \notin P$. By the definition of a prime ideal, we must have $c \in P$, say $c = ad$. But then $a = bc = bad$ and $a \neq 0$ (since $P \neq 0$), which implies that b is a unit in R and $Q = R$. This shows that P is maximal.

(5) Let V be a finite dimensional vector space over a field $\mathbf{F}$ and let $\langle , \rangle : V \times V \to \mathbf{F}$ be a bilinear form. Prove that

$$\dim_{\mathbf{F}}\{v \in V \mid \langle v, w\rangle = 0 \text{ for all } w \in V\} = \dim_{\mathbf{F}}\{w \in V \mid \langle v, w\rangle = 0 \text{ for all } v \in V\}.$$

Solution: Fix a basis of V and let A be the matrix of the bilinear form with respect to this basis. For all $v, w \in V$ we have $\langle v, w\rangle = v^T A w$. Then $\langle v, w\rangle = v^T A w = 0$ for all $w \in V$ if and only if $v^T A = 0$, i.e. v is in the left kernel of A. It follows that $\{v \in V \mid \langle v, w\rangle = 0 \text{ for all } w \in V\}$ is the left kernel of A and similarly $\{w \in V \mid \langle v, w\rangle = 0 \text{ for all } v \in V\}$ is the right kernel of A. Therefore they have equal dimensions as desired.

(6) Let $\varphi : R_1 \to R_2$ be a homomorphism of commutative rings with identity. Suppose that for every prime ideal $I \subset R_2$, the induced homomorphism $R_1 \to R_2/I$ is surjective. Is it necessarily true that φ is surjective?

Solution: Such a homomorphism φ does not have to be surjective. Let F be a field and let $F[x]$ be the ring of polynomials over F. Let $R_1 = F$, $R_2 = F[x]/(x^2)$ and $\varphi : R_1 \to R_2$ be the inclusion map. Let $\bar{x} \in R_2$ be the image of x under the natural projection from $F[x]$. Observe that $\bar{x} \neq 0$ and since $\bar{x}^2 = 0$ in R_2 it follows that $\bar{x} \in I$ for every prime ideal I of R_2. It follows that the induced homomorphism $R_1 \to R_2/I$ is surjective for any prime ideal I. For a second example, take F a field, $R_1 = F$, $R_2 = F \oplus F$ and $\varphi : R_1 \to R_2$ the diagonal inclusion.

(7) Let $\mathbb{F}_q$ be the finite field of cardinality q. How many elements $x \in \mathbb{F}_{64}$ generate $\mathbb{F}_{64}$ as an extension of $\mathbb{F}_2$?

Solution: Recall that for any prime p, $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if m divides n. Let $\alpha \in \mathbb{F}_{64}$ and suppose that $\mathbb{F}_2(\alpha) \neq \mathbb{F}_{64}$. Then $\mathbb{F}_2(\alpha)$ is a subfield of $\mathbb{F}_{64} = \mathbb{F}_{2^6}$ and we see that $\mathbb{F}(\alpha)$ is isomorphic to $\mathbb{F}_2$, $\mathbb{F}_4$ or $\mathbb{F}_8$. It follows that $\mathbb{F}(\alpha) \neq \mathbb{F}_{64}$ if and only if $\alpha \in \mathbb{F}_2$, $\alpha \in \mathbb{F}_4$, or $\alpha \in \mathbb{F}_8$. Taking into account that $\mathbb{F}_2 \subset \mathbb{F}_4$, $\mathbb{F}_2 \subset \mathbb{F}_8$, and $\mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_2$,we see that there are 10 elements $\alpha \in \mathbb{F}_{64}$, such that $\mathbb{F}(\alpha) \neq \mathbb{F}_{64}$ and 54 elements $\alpha \in \mathbb{F}_{64}$, such that $\mathbb{F}(\alpha) = \mathbb{F}_{64}$.

(8) Let G be an abelian group with generators x, y, and z and relations

$$3x - 2y + 5z = 6x + 2y + 4z = -3x + 5y - 8z = 0.$$

Express G as a direct sum of cyclic groups and find the rank and the torsion subgroup of G.

Solution: Let H be the subgroup of $\mathbb{Z}^3$ generated by $\begin{pmatrix} 3 \\ -2 \\ 5 \end{pmatrix}$, $\begin{pmatrix} 6 \\ 2 \\ 4 \end{pmatrix}$ and $\begin{pmatrix} -3 \\ 5 \\ -8 \end{pmatrix}$. It follows that $G \cong \mathbb{Z}^3/H$. Consider the matrix

$$\begin{pmatrix} 3 & 6 & -3 \\ -2 & 2 & 5 \\ 5 & 4 & -8 \end{pmatrix}.$$

A sequence of elementary integer row and column operations (equivalently, changing basis in $\mathbb{Z}^3$ and H) yields the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

It follows that $G \cong \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}$ and therefore the rank of G is 1 and its torsion subgroup is isomorphic to $\mathbb{Z}/9\mathbb{Z}$.