Master's Exam and Ph.D. Qualifying Exam
Algebra: Math 817-818, June 1, 2000

Do 6 problems, 2 from each of the three sections. If you work on more than six problems, or on more than 2 from any section, clearly indicate which you want graded. For problems with more than one part, do not assume that all parts count equally. There are 15 problems on three pages.

If you have doubts about the wording of a problem, please ask for clarification. In no case should you interpret a problem in such a way that it becomes trivial.

Note: $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ denote the fields of rational, real and complex numbers respectively, and $\mathbb{Z}$ denotes the ring of integers. Problems marked with an "o" deal with old stuff not covered during the 1999–2000 academic year. Problems marked with an "n" deal with new stuff not usually covered in previous editions of the course. These markings are purely advisory; you may choose any problems you want, subject to the rules in the first paragraph.

Section I: Groups

(o1) Let G be a simple group of order 60. Prove that G has 10 Sylow 3-subgroups. (Do not assume that $G \cong \mathrm{A}_5$.)

(o2) Prove that there are no simple groups of order n for $212 \leq n \leq 222$. (Hints: $212 = 2^2 \cdot 53$; $213 = 3 \cdot 71$; $214 = 2 \cdot 107$; $215 = 5 \cdot 43$; $216 = 2^3 \cdot 3^3$; $217 = 7 \cdot 31$; $218 = 2 \cdot 109$; $219 = 3 \cdot 73$; $220 = 2^2 \cdot 5 \cdot 11$; $221 = 13 \cdot 17$; $222 = 2 \cdot 3 \cdot 37$. You might start by proving that there are no simple groups of order pq, where p and q are distinct primes. The eleven parts of the problem do *not* count equally!)

(3) Let G be a group of odd order, and let N be a normal subgroup of G with $|N| = 5$. Prove that N is contained in the center of G. Show by example that this can fail if N is not assumed to be normal.

(n4) Let L be a plane lattice (a discrete subgroup of $\mathbb{R}^2$ generated by two linearly independent vectors), and let G be a group of rotational symmetries of L fixing the origin.

(a) If ρ_θ (rotation through angle θ about the origin) is a non-trivial element of G, prove that $|\theta| \geq \pi/3$. (You may assume without proof that L contains a shortest non-zero vector.)

(b) Prove that G is finite.

(c) Prove that $|G| \leq 6$.

(n5) Let $\mathrm{t}_{\mathbf{a}} : \mathbb{R}^2 \to \mathbb{R}^2$ be the translation along the vector $\mathbf{a}$. (Thus $\mathrm{t}_{\mathbf{a}}(\mathbf{b}) = \mathbf{a} + \mathbf{b}$ for every vector $\mathbf{b} \in \mathbb{R}^2$.) Let $\rho_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ be the rotation about the origin through an angle θ, where $0 < \theta < 2\pi$. (Thus ρ is left multiplication by the matrix $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$.) Prove directly that the composition $\mathrm{t}_{\mathbf{a}}\rho_\theta$ (first the rotation, followed by the translation) has a fixed point, and deduce that $\mathrm{t}_{\mathbf{a}}\rho_\theta$ is a rotation about that point.

Section II: Rings and Fields

(6) Let $f(x) = x^4 + \frac{1}{3}x^3 + \frac{2}{3}x^2 + 2x + \frac{1}{5}$.

(a) Prove that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(b) Deduce that $f(x)$ is irreducible in $\mathbb{Q}(\sqrt[3]{2})[x]$. (Hint: Let $\alpha \in \mathbb{C}$ be a root of $f(x)$, and think about degrees of various field extensions.)

(7) Let R be an integral domain (commutative with identity).

(a) Define precisely the greatest common divisor of two elements a and b in R, and prove that it is unique up to multiplication by a unit (if it exists).

(b) Using the factorizations $2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ in the ring $R := \mathbb{Z}[\sqrt{-5}]$, find two elements of R that do not have a greatest common divisor, and justify completely.

(8) For a prime power q, let $\mathbb{F}_q$ denote the field with q elements.

(a) Draw a diagram showing all of the subfields of $\mathbb{F}_{2^{20}}$, indicating inclusion relations among the various subfields.

(b) Use your diagram to find the number of elements of $\mathbb{F}_{2^{20}}$ that are not in any proper subfield of $\mathbb{F}_{2^{20}}$.

(c) Using your answer to (b), compute, with some explanation, the number of irreducible polynomials of degree 20 over $\mathbb{F}_2$. (Since there are more than $50,000$ of them, you do not need to list them!)

(9) Use the First Isomorphism Theorem to prove that $\mathbb{Z}[x]/(x^2 + 2x + 2)$ is isomorphic to $\mathbb{Z}[i]$, the ring of Gaussian integers. Justify everything carefully.

Section III: Linear Algebra

(10) Find the Jordan canonical form J and the rational canonical form R of the real matrix $A := \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 3 & 1 \end{bmatrix}$. Find an invertible matrix P such that $PAP^{-1} = J$. (Or, if you prefer, find an invertible matrix P such that $P^{-1}AP = J$.)

(n11) Let α be an $n \times n$ matrix with entries in $\mathbb{Z}$, and let G be the abelian group presented by α. (Thus $G = \mathbb{Z}^n/(\text{column space of } \alpha)$, otherwise known as the *cokernel* of α.) Prove that G is finite if and only if $\det(\alpha) \neq 0$.

(n12) Let $\langle\ ,\ \rangle$ and $||\ \ ||$ denote the usual inner product and norm on $\mathbb{R}^n$. (Thus $\langle X, Y \rangle = X^{\mathrm{t}}Y$ for column vectors $X, Y \in \mathbb{R}^n$, and $||X|| = \sqrt{\langle X, X \rangle}$.) Using basic properties of matrix operations, prove that the following conditions on an $n \times n$ real matrix A are equivalent:

(a) $||AX|| = ||X||$ for every $X \in \mathbb{R}^n$.

(b) $\langle AX, AY \rangle = \langle X, Y \rangle$ for every $X, Y \in \mathbb{R}^n$.

(c) $A^{\mathrm{t}}A = \mathrm{I}_n$ (the $n \times n$ identity matrix).

(13) Let α be an $n \times n$ real matrix. Prove that $\text{rank}(\alpha) \leq 1$ if and only if α can be factored as the product of a column vector and a row vector (that is, if and only if $\alpha = \gamma\rho$, where γ is $m \times 1$ and ρ is $1 \times n$).

(14) You are given the following information about the real matrix A:

(i) A is 7×7.

(ii) The minimal polynomial of A is $(x-1)^3(x-2)^2$.

(iii) $\det(A) \leq 10$.

Find all possible lists of elementary divisors for A, and the corresponding lists of invariant factors. (Since nobody can remember which is which, you will not lose points if you confuse elementary divisors with invariant factors.) For each possibility, give the Jordan canonical form J and the rational canonical form R of A.