Swarthmore College
Department of Mathematics and Statistics
Honors Examination: Algebra
Spring, 2004

Pick six questions which you would like to address in detail. If you have more time you might like to respond to the remaining questions. You may treat any challenge which begins "Can you ..." as "extra credit"; some of these could be dangerously time-consuming!

1. The *Gram-Schmidt* process is an algorithm which begins with an arbitrary basis of an inner-product space and produces an orthonormal basis. It's very general, but we will apply it here only in Euclidean space ($\mathbf{R}^n$, with the standard inner product).

(a) Use the Gram-Schmidt process to construct an orthonormal basis from the basis consisting of the columns of the matrix

$$M = \begin{pmatrix} 1 & 8 & 3 \\ -2 & -7 & 12 \\ 2 & -2 & 6 \end{pmatrix}.$$

(b) How can you characterize those square matrices whose columns form a basis for $\mathbf{R}^n$?

(c) How can you characterize those square matrices whose columns form an *orthonormal* basis for $\mathbf{R}^n$?

(d) Let Q be the matrix whose columns are the basis vectors you computed in (a). Compute the matrix R for which $M = Q\,R$. (*Hint:* View the steps taken in (a) as column operations on the matrix M; each column operation can be accomplished by multiplying on the right by an "elementary" matrix. This gives you an equation of the form $Q = M\,S$.)

Your observations in this problem have essentially proven a theorem! Can you fill in the blanks here? Can you complete the proof? "Theorem: Every _____ matrix can be written as the product of a _____ matrix and a _____ matrix."

2. Recall that in a group G, two elements x and y are said to be *conjugate* (to each other) if there is a group element g making $g^{-1}xg = y$.

(a) Show that for every pair of group elements a and b, the elements $x = ab$ and $y = ba$ are conjugate.

(b) Show that if x and y are conjugate, then they must have the same order.

(c) Give an example of an element x in a group G which is conjugate to a proper power of itself, that is, x is conjugate to an element y which is different from x but which is equal to x^k for some integer k.

(d) Suppose $G = S_n$, the symmetric group of permutations on n letters. Show that if x and y are conjugate permutations then they fix the same number of letters.

(e) Suppose $G = GL_n(\mathbf{R})$, the group of invertible $n \times n$ real matrices. Show that if x and y are conjugate matrices then they have equal sets of eigenvalues.

(f) Suppose again that $G = GL_n(\mathbf{R})$. With part (e) in mind, it's tempting to conjecture that two matrices x and y in G with the same sets of eigenvalues are indeed conjugate. That's false. Find (with proof) some additional conditions which *would* allow you to conclude that x and y are conjugate.

Can you find an example of two matrices with identical sets of eigenvalues which are not conjugate?

3. The *Hamilton-Cayley Theorem* states that if $A \in M_n(\mathbf{R})$ (the ring of $n \times n$ real matrices) and if $f(X) = \det(XI - A)$ is the characteristic polynomial of A, then $f(A) = 0$.

(a) Show that there can be infinitely many elements of $M_n(\mathbf{R})$ with the same characteristic polynomial (for $n > 1$).

(b) Show that the polynomial $f(X) = X^2 - 1$ has four roots in the ring $\mathbf{Z}/(8)$.

(c) Recall the *Polynomial Roots Theorem* — the one that assures you that a polynomial of degree n has at most n roots. Why do the examples in parts (a) and (b) not contradict this? Indicate a hypothesis for, or a step in the proof of the Polynomial Roots theorem which does not apply to the ring $\mathbf{Z}/(8)$.

4. The Postal Service receives many ordinary flat rectangular envelopes with a stamp neatly in the corner. These are fed into machine which taps the envelopes just as you would do by hand, to make them all lie in parallel planes in a stack, with two edges of each envelope pressing against the sides of a chute. These must be fed into a second machine which will turn each envelope around, looking to make sure there is a postage stamp on the envelope, and will use the location of the stamp as an indicator to know when the envelope is turned the right way so that a scanner can attempt to read the address.

Use the language of group theory to address this question: is it possible for that second machine to use a single simple motion repeatedly (as necessary) to check all the possible corners of the envelope and find the one with the stamp? (It is for you to decide what "simple motion" means; obviously the Postal Service would like to minimize the number and complexity of the devices it uses!) If you would like, you may assume all envelopes are congruent squares.

5. In this question we discuss only commutative rings (with identity element).

(a) Define carefully what a *prime ideal* is. How do prime ideals relate to ordinary prime numbers?

(b) State and prove a theorem connecting between prime ideals and integral domains.

(c) Give an example of a ring with a unique nonzero prime ideal.

It is a theorem that every maximal ideal is prime, but the converse does not hold. Can you find a ring which contains distinct nonzero prime ideals $\mathcal{P}_1$ and $\mathcal{P}_2$ with $\mathcal{P}_1 \subset \mathcal{P}_2$?

6. The *Freshman's Dream* is the "theorem" that all functions f are linear: $f(x + y) = f(x) + f(y)$ for all x and y. Sadly, it's not true.

(a) Prove however that it *is* true when p is a prime number and f is the p^2-th power function $f(x) = x^{p^2}$, defined on the polynomial ring $\mathbf{Z}/(p)\,[t]$.

(b) Find a value of $k > 1$ so that $x^k \equiv x \pmod{35}$ for all integers x

(c) Why is there no value of $k > 1$ such that $x^k \equiv x \pmod{25}$ for all integers x?

7. A classic result in field theory states that the multiplicative group of a finite field is a cyclic group.

(a) The number $p = 127$ is prime. Show that exactly half the nonzero elements of the field $\mathbf{Z}/(127)$ are squares.

(b) If x is an element of $\mathbf{Z}/(127)$ and $y = x^2$, show that $z = y^{32}$ must equal either x or $-x$. (*Hint:* What is z^2?).

(c) Generalize (b) to give an algorithm for extracting square roots mod p when p is a prime number which is one less than a multiple of 4.

(d) The *Fermat number* $n = 2^{32} + 1$ happens to be composite. Let q be a prime divisor of n. Show that 2 is an element of the multiplicative group of $\mathbf{Z}/(q)$ having order exactly 64. Conclude that $q - 1$ is a multiple of 64.

(Actually, since this means $q \equiv 1 \pmod 8$, one may use a result called *Quadratic Reciprocity* to show that 2 is itself a square, meaning that $q - 1$ is a multiple of 128. Euler used this sort of reasoning to quickly find a prime divisor of n; can you?)

8. The techniques of geometric construction used in ancient Greece required the use of an *unmarked* straightedge. But Archimedes knew that if we allow ourselves to mark the straightedge, it is possible to trisect an arbitrary angle using this tool and a compass. Other tools (called *trisectrices*) have been developed for this purpose as well. So suppose you are permitted to perform the classical constructions *and* to trisect arbitrary angles.

(a) Show that it is possible to construct a perfect enneagon (a polygon with nine sides).

(b) Is it possible to construct a perfect hendecagon (an eleven-sided figure)?

Can you decide whether or not it is possible to construct a perfect heptagon with the same tools?

9. Consider the curves in the plane defined by the equations

$$C_1 : y^2 = x(x^2 + 1) \qquad\qquad C_2 : v^2 = u(u^2 - 4)$$

You may accept the following facts without proof: Each of these defines an elliptic curve over the rational field $\mathbf{Q}$, and if the function

$$f(u, v) = \left(\frac{u^2 - 4}{4u}, \frac{v(u^2 + 4)}{8u^2} \right)$$

is applied to a point (u, v) lying in C_2 then the resulting point $(x, y) = f(u, v)$ lies in C_1. Moreover, the function $f : C_2 \longrightarrow C_1$ is a group homomorphism between these two (finitely-generated abelian) groups. (As is typical, we take the point at infinity to be the identity element for the groups.)

(a) Find all points of order 2 on these curves.

(b) Show that if (x, y) is a point on C_1 with rational coordinates, then x is a rational square. (*Hint:* Count how many times a prime can divide the numerator or denominator of x.)

(c) Show that if (x, y) is a point on C_1 with rational coordinates, and x is a square, then $x^2 + 1$ is a square.

(d) Show that if x is a rational number such that $x^2 + 1$ is a square, then $x = \dfrac{u}{4} - \dfrac{1}{u}$ for some rational number u.

(e) Show that the claims in (b)–(d) imply that the map $f : C_2 \longrightarrow C_1$ is a surjection.

(f) Suppose that A_1 and A_2 are finitely-generated abelian groups without elements of finite order, and that there are homomorphisms $f : A_2 \longrightarrow A_1$ and $g : A_1 \longrightarrow A_2$ which are both surjections, such that $f \circ g$ is the doubling map on A_1, that is, $(f \circ g)(a) = a + a$ for every element $a \in A_1$. Prove that A_1 must be the trivial group (i.e. it has order 1).

You may wonder why question (f) is here. Well, it turns out there is also a group homomorphism $g : C_1 \longrightarrow C_2$ which one can show to be almost a surjection on rational points: g induces a surjection onto $C_2/T(C_2)$ where $T(C_2)$ is the *torsion subgroup* of C_2, which is the set of elements of finite order. The composite $f \circ g$ does indeed turn out to be the doubling map.

So by applying (f) to the groups $A_i = C_i/T(C_i)$, one concludes that the curves C_i consist only of torsion elements. By this process, known as *descent*, we can obtain a complete (finite) list of the rational points on these curves! Can you supply all the missing details?