1. Say whether the following statements are true or false. (You do not need to provide justification.)
(a) The ring $\mathbf{Z}[x]$ of polynomials with integer coefficients is euclidean.
(b) The ring $\mathbf{R}[x]$ of polynomials with real coefficients is a principal ideal domain.
(c) The ring $\mathbf{Q}[x, y]$ of polynomials in two variables with rational coefficients is a euclidean domain.
(d) The ring $\mathbf{Z}[i]$ of Gaussian integers is a principal ideal domain.
(e) The group S_4 of permutations of $\{1, 2, 3, 4\}$ has an element of order 5.
(f) Every group of order 8 contains an element of order 8.
(g) Every group of order 7 contains an element of order 7.
(h) The ring $\mathbf{Q}[x]/(x^2 - 2)$ is a field.
(i) The ring $\mathbf{R}[x]/(x^2 - 2)$ is a field.
(j) If G_1 and G_2 are two groups of the same cardinality, and this cardinality is prime, then G_1 and G_2 are isomorphic.
(k) The equation $x^2 + 1 = 0$ has two roots in the ring $\mathbf{Z}_p$ when p is a prime and $p \equiv 1 \pmod 4$.
(l) Let G_1 and G_2 be two groups, and let $H_1 \subset G_1$ and $H_2 \subset G_2$ be normal subgroups. If H_1 is isomorphic to H_2, and G_1/H_1 is isomorphic to G_2/H_2, then G_1 is isomorphic to G_2.

2. (a) Give the definition of a Euclidean ring.
(b) Show that a Euclidean ring is a principal ideal domain.
(c) Show that the ring $\mathbf{Z}[\sqrt{-5}]$ is not a Euclidean ring (for any choice of "size function" δ.)

3. Let G be a finite group. Define its *exponent*, n, to be the least common multiple of the orders of all the elements of G.
(a) Show that n divides the cardinality of G.
(b) Give an example of a group G where n is strictly less than the cardinality of G.
(c) Let F be a field, and let $F^\times$ be the group of non-zero elements of F, where the group law is given by multiplication. If G is a subgroup of $F^\times$, show that n is equal to the cardinalty of G, *without* invoking the theorem that G is cyclic.

4. Let $R = \mathbf{Z}[\sqrt{-2}]$ be the ring of elements of the form $a + b\sqrt{-2}$, with $a, b \in \mathbf{Z}$. Define $\delta : R \longrightarrow \{0, 1, 2, \ldots\}$ by $\delta(a + b\sqrt{-2}) = a^2 + 2b^2$.
(a) Show that R, equipped with this function δ, is a Euclidean ring.
(b) Let p be an odd prime. If there is an integer n such that p^2 divides $n^2 + 2$, show that there exists another integer m such that p divides $m^2 + 2$ but p^2 does not divide $m^2 + 2$.
(c) If p is a prime which divides $n^2 + 2$ for some integer n, show that there exist integers a and b such that $p = a^2 + 2b^2$.

5. Let $G = \mathbf{GL}_2(\mathbf{Z}_p)$ be the multiplicative group of invertible 2×2 matrices with entries in the field $\mathbf{Z}_p$ with p elements, where p is a prime.
(a) Show that the set of matrices of the form $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ with $a \in \mathbf{Z}_p$ is a subgroup of G, and is isomorphic to $\mathbf{Z}_p$ (where the group law is addition).
(b) Show that the set of matrices of the form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ with $ab \neq 0$ is a subgroup of G, and is isomorphic to $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$ (where the group law comes from multiplication in $\mathbf{Z}_p$).
(c) Using (a) and (b), show that the cardinality of G is divisible by $p(p-1)^2$.
(d) (For extra credit): What is the cardinality of G?

6. Let $n = ab$ be a product of two integers which are *relatively prime*: $\gcd(a,b) = 1$. Let R_1 be the ring $\mathbf{Z}_n$, and R_2 be the Cartesian product of $\mathbf{Z}_a$ and $\mathbf{Z}_b$.
(a) Let $\phi : R_1 \longrightarrow R_2$ be the function which sends x to (x_a, x_b), where x_a (resp. x_b) denotes the congruence class of x modulo a (resp. modulo b). Show that ϕ is a homomorphism.
(b) Show that ϕ is injective.
(c) Show that ϕ is surjective.
(d) Show that, if $n = pq$ is a product of two odd primes, then the multiplicative group of $\mathbf{Z}_n$ (i.e, the group $\mathbf{Z}_n^\times$ of all elements in $\mathbf{Z}_n$ which have a multiplicative inverse) is *not* cyclic.
(e) Show that if p is prime then the multiplicative group $\mathbf{Z}_p^\times$ is cyclic.

7. Let S_n be the group of permutations on the set $X = \{1, 2, \ldots, n\}$, and let G be a subgroup of S_n. Let $G_1 \subset G$ be the set of all permutations in G which fix 1.
(a) Show that G_1 is a subgroup of G.
(b) Define a function f from the coset space G/G_1 to X by the rule $f(aG_1) = a(1)$. Show that f is *well defined*, and that it is an injection (of sets).
(c) We say that G is a *transitive* subgroup of S_n if for all $i, j \in X$, there is a permutation $a \in G$ such that $a(i) = j$. If G is transitive, show that the coset space G/G_1 has cardinality n.
(d) If G is a transitive subgroup of S_n, show that n divides the cardinality of G.
(e) Using the result of (c), show that $\#S_n = n(\#S_{n-1})$, where $\#H$ is used to denote the cardinality of the set H.
(f) Use the formula of part (e) to prove that $\#S_n = n!$.

8. (a) If G is any group such that $x^2 = 1$ for all $x \in G$, show that G must be abelian.
(b) Let R be a ring, and let $G(R)$ be the set of all three by three matrices of the form $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, with $a, b, c \in R$. Show that $G(R)$ is a subgroup of $\mathbf{GL}_3(R)$, and that $G(R)$ is non-commutative for any ring R in which $1 \neq 0$.
(c) Show that

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & ka & kb + \frac{k(k-1)}{2}ac \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix}.$$

(d) Give an example of a non-abelian group G of order 27 in which $x^3 = 1$ for all $x \in G$.

FACULTY OF SCIENCE

FINAL EXAMINATION

MATHEMATICS 189-235A

BASIC ALGEBRA I

Examiner: Professor H. Darmon
Associate Examiner: Professor S.W. Drury

Date: Tuesday, December 17, 1996
Time: 9:00 A.M. - 12:00 Noon

INSTRUCTIONS

You have 3 hours. It is good strategy to attempt all questions. Each question is worth 15 points, for a maximum total of 120 points. If you are stuck on a question for too long, move on to the next one.

This exam comprises the cover and 3 pages of questions.