George M. Bergman Spring 1999, Math 113, Section 2 22 May, 1999

102 Stanley Hall **Final Examination** 12:30-3:30 PM

1. (20 points, 4 points apiece) Find the following. Correct answers will get full credit whether or not work is shown.

(a) The expression for the element $(1,2,3,4)(2,4,6)$ of the group S_7 as a product of disjoint cycles

(b) The order of a^6, where a is any element of order 100 in any group

(c) An expression for the element $(2[x]+1)([x]+3)$ of the field $\mathbf{Q}[x]/<x^2+x+1>$ as a linear combination of $[x]$ and 1 with coefficients in $\mathbf{Q}$.

(d) A list of all the elements $[n]_7 \in \mathbf{Z}_7$ such that the ring $\mathbf{Z}_7[x]/<x^2-[n]_7>$ is a field.

(e) The characteristic of F, if F is a field with 27 elements.

2. Short proofs. (24 points, 8 points each)

(a) Let m and n be positive integers, and a, b integers. Show that if $am \equiv bm \pmod{mn}$, then $a \equiv b \pmod{n}$.

(b) Let G be a group and H a subgroup of G. Show that if H is cyclic (i.e., if there exists an element $a \in G$ such that $H = <a>$), then there exists a group homomorphism $\varphi: \mathbf{Z} \to G$ whose image $\varphi(\mathbf{Z})$ is H.

(c) Suppose F is an extension of a field K, of finite degree $[F:K] = n$. Show that every element of F is algebraic over K. (This is a result in the text, so in your proof you may only assume results proved before this one.)

3. Give each of the following. No proofs are required. (21 points; 7 points each.)

(a) A subfield of $\mathbf{R}$ that is isomorphic to $\mathbf{Q}[x]/<x^2-x-1>$. (Suggestion: write it as $\mathbf{Q}(\alpha)$ for an appropriate real number α.)

(b) An example of a Euclidean domain D, and a Euclidean norm function δ for D.

(c) The statement of Eisenstein's criterion for a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbf{Z}[x]$ to be irreducible.

4. (13 points.) A result is stated and proved below. Several steps in the proof are shown in boldface, with numbers before them. In each case, on the corresponding lines at the bottom of the page, you should give a brief *reason* why the assertion is true. Do not worry about giving additional reasons to support your reasons; one key fact or calculation is what is wanted in each case.

(Recall that an *inner automorphism* of a group means an automorphism of the form i_x for some $x\in G$, where $i_x(y) = xyx^{-1}$.)

Lemma. Every automorphism of the symmetric group S_3 is inner.

Proof. In S_3, let $a = (1,2,3)$ and $b = (1,2)$. We know that the six elements of S_3 can be written $a^i b^j$ with $i\in\{0,1,2\}$ and $j\in\{0,1,\}$. **(i) Consideration of orders of elements shows that every automorphism of S_3 must send a to one of the two elements $(1,2,3)$ or $(1,3,2)$**, and similarly must send b to one of the three elements $(1,2)$, $(1,3)$, or $(2,3)$. Moreover, an automorphism of S_3 is determined by what it does on a and b, that is **(ii) if φ and θ are automorphisms of S_3 such that $\varphi(a) = \theta(a)$ and $\varphi(b) = \theta(b)$, then $\varphi = \theta$.** Hence by our preceding observation there can be at most $2\times 3 = 6$ automorphisms of S_3.

On the other hand, **(iii) the homomorphism $S_3 \to \mathrm{Aut}(S_3)$ taking each $x\in S_3$ to i_x is one-to-one**. Hence S_3 has *at least six* inner automorphisms. So every automorphism of S_3 must be inner. □

5. (i) (7 points.) Let $\varphi\colon\ R \to S$ be a ring homomorphism, and recall that $\ker(\varphi)$ is defined as $\{r\in R \mid \varphi(r) = 0\}$. Show that $\ker(\varphi)$ is an *ideal* of R.

(ii) (5 points.) Conversely, if I is an ideal of a ring R, then we know from our reading that there is a homomorphism from R to another ring S whose kernel is I. State briefly what this ring is, and what the homomorphism is. (You do not have to describe how they are constructed; it is enough to identify them by the names and/or symbols used for them in the text. But if you can't remember these, explicit descriptions will be accepted.)

6. (10 points.) Find the greatest common divisor of 1,001 and 2,030, and express it as a linear combination of those two numbers, with integer coefficients.