## Math 370 Fall, 2006 MidTerm 1

Solutions must be handed in by 3pm, Thursday, November 2. There is no particular order to the problems. Those with no stars are worth 10 points, with one star 15, with two stars 20. Grading: 90 = C, 120 = B, 150 = A. Staple the cover page supplied to your problem set. Display prominently the number of the problem you are solving at the beginning of every answer.

1. Prove that the group of symmetries of the regular tetrahedron is isomorphic to  $A_4$ .

 $2^*$ . Prove that the group of symmetries of the cube is isomorphic to  $S_4$ .

3<sup>\*\*</sup>. Prove that the center of  $SL_2(\mathbb{F}_5)$ , the group of all 2 × 2 matrices with coefficients in the field  $\mathbb{F}_5$  and having determinant equal to 1, consists of the two matrices ±1. ("SL" stands for "special linear group".) Now prove that  $SL_2(\mathbb{F}_5)/\{\pm 1\}$  has order 60 and that it is isomorphic to  $A_5$ .

4<sup>\*</sup>. Prove that all automorphisms of  $S_5$  are inner, i.e., of the form  $x \to axa^{-1}$  for some a.

5. Exhibit an outer autmorphism of  $S_6$ , i.e., one which is not inner.

6. The characteristic polynomial of a matrix A is  $det(x \cdot 1 - A)$ . Prove that the characteristic polynomial of the  $n \times n$  matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ -a_n & -a_{n-1} & -a_{n-2} & -a_{n-3} & \dots & -a_2 & -a_1 \end{pmatrix}$$

is  $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots a_n$ . The Cayley-Hamilton theorem asserts that every matrix in fact satisfies its characteristic polynomial. Now show that if  $a_1 = a_2 = \ldots a_n = 1$  then  $A^{n+1} = 1$ .

7. Let G be the group of invertible  $n \times n$  matrices with coefficients in the field  $\mathbb{F}_p$  of p elements. The order |G| of this group is  $(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$ . What is the highest power of p dividing |G|? Find a subgroup of G having this order. (This is a p-Sylow subgroup of G).

8. Let  $Z_n = \langle x \rangle$  be a cyclic group of order n and for each integer a let  $\sigma_a : Z_n \to Z_n$  by  $\sigma_a(x) = x^a$ . a) Prove that  $\sigma_a$  is an automorphism of  $Z_n$  if and only if a and n are relatively prime. b) Prove that  $\sigma_a = \sigma_b$  if and only if  $a \equiv b \pmod{n}$ . c) Prove that every automorphism of  $Z_n$  is equal to  $\sigma_a$  for some integer a. d) Prove that  $\sigma_a \circ \sigma_b = \sigma_{ab}$ . Deduce that the map  $\bar{a} \mapsto \sigma_a$  is an isomorphism of  $(\mathbb{Z}/n\mathbb{Z})^{\times}$  onto the automorphism group of  $Z_n$ .

9. Let  $\varphi$  be a linear transformation from the finite dimensional vector space V to itself such that  $\varphi^2 = \varphi$ . a) Prove that image  $\varphi \cap \ker \varphi = 0$ . b) Prove that  $V = \operatorname{image} \varphi \oplus \ker \varphi$ . c) Prove that there is a basis of V such that the matrix of  $\varphi$  with respect to this basis is a diagonal matrix whose entries are 0 or 1.

10. Let G be a finite Abelian group in which the number of solutions in G of

the equation  $x^n = 1$  is at most *n* for every positive integer *n*. Prove that *G* must be a cyclic group.

11. Prove that any finite multiplicative subgroup of a field is cyclic, hence in particular that the multiplicative group of  $\mathbb{F}_q$  is a cyclic group of order q - 1. Find a generator in each of the following cases: q = 4, 5, 7, 9, 11, 25. (Generators are not unique, but there is a smallest one.)

12. Let F be the set of all  $2 \times 2$  real matrices of the form  $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ . Show that F is a field isomorphic to the complex numbers  $\mathbb{C}$ . Now find a set of  $2 \times 2$ 

matrices with complex entries which is isomorphic to the quaternions  $\mathbb{H}$  (under the usual addition and multiplication of matrices.

13<sup>\*</sup>. We have seen that every subgroup of an Abelian group is normal. Let G now be a group with the property that every subgroup is normal. Is it necessarily Abelian? (Give a proof or a counterexample.)

14<sup>\*</sup>. Determine *all* groups of order 8 up to isomorphism.

15\*. If G is a group (not necessarily finite) in which  $(ab)^2 = a^2b^2$  for all elements a, b in G then it is trivial that G is Abelian. (Why?) Now suppose that G is a finite group whose order is not divisible by 3. Prove that every element is then the cube of some other element. Now prove that if in addition  $(ab)^3 = a^3b^3$  then G is Abelian.

16. Prove that if A is an  $n \times n$  matrix (with coefficients in any field) such that  $A^m = 0$  for some m, then already  $A^n = 0$ . (A matrix such that  $A^m = 0$  for some m is called *nilpotent*.)

17\*\*. If A, B are real  $n \times n$  matrices then we can never have AB - BA = 1 because tr(AB) = tr(BA), so the trace of the left side is 0, while that of the right side is n. Show, however, that AB - BA = 1 is possible if the coefficients are in the field  $\mathbb{F}_p$  of p elements. (What can you say about the size of the matrices?) Now consider real matrices with an *infinite* number of rows and columns but in which each row has only a finite number of non-zero entries. (These matrices are called *row finite*.) One can still add, subtract, and form the product of any two. (Why?) Now show by example that AB - BA = 1 is possible for such matrices.

18<sup>\*\*</sup>. Let G be a finitely generated group. Show that for every integer n there exist only finitely many subgroups of index n. Now suppose that there exists a subgroup of finite index in G. Prove that G contains a characteristic subgroup of finite index. (A characteristic subgroup is one which is carried into itself by every automorphism.)

19\*. Show that the set of all non-zero matrices of the form  $\begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$  over the field  $\mathbb{F}_5$  of 5 elements is a cyclic group under matrix multiplication. What is the order of this group?

20\*\*. Let V be a vector space over the complex numbers (possibly of infinite dimension) and  $T: V \to V$  be a linear map such that  $T^n = \mathbf{1}$  for some positive integer n. Prove that V is then a direct sum of subspaces  $V = V_0 \oplus V_1 \cdots \oplus V_{n-1}$  such that  $T|V_k = e^{2k\pi i/n} \cdot \mathbf{1}$ .