MATH E-105, SUMMER 2001
GROUPS, GRAPHS, AND ALGEBRAIC STRUCTURES FOR COMPUTING
Homework Assignment # 3
Due: July 9, 2001

Reading

- Hand-outs
- Section 9.4 (pp. 380–385).
- Section 9.5 (pp. 389–390).

Required Problems

1. Do exercise #5 from p. 392, section 9.5.
2. Do exercise #10 from p. 392, section 9.5.
3. In class, we have discussed the following five groups, all of which have six elements:
   - the symmetry group of the equilateral triangle (D_3),
   - the permutation group on the set of three letters (S_3)
   - the group of additive congruences modulo 6 ($\mathbb{Z}_6$)
   - the multiplicative group of non-zero elements modulo 7 ($\mathbb{Z}_7^\times$)
   - the six rotations of a regular hexagon about an axis perpendicular to the hexagon (C_6)

   Are these different manifestations of the same group? Which of them are abelian? Which are cyclic? Find a natural identification between the ones that are the "same." Show that this identification is an isomorphism.
4. We can create a finite field $\mathbb{F}_9$ with 9 elements by considering polynomials with coefficients in $\mathbb{Z}_3$ and reducing modulo the irreducible polynomial x^2+1. (This leads to the replacement rule $x^2+1=0$ or $x^2=2$.) Write out the addition and multiplication tables for $\mathbb{F}_9$. *(Hint: Let the elements of $\mathbb{Z}_3$ be 0, 1, and 2, and you will get polynomials like $2x+1$, where all the coefficients are non-negative.)*

5. Consider arithmetic modulo 12 (the additive group $\mathbb{Z}_{12}$ with its multiplicative structure as well). Find all the zero divisors, and for each element that is not a zero divisor, find its multiplicative inverse.

6. Show that 3 is a generator for the multiplicative group $\mathbb{Z}_7$, and find any other generators.

7. Find subgroups of the symmetry group of the icosahedron isomorphic to D_3, D_5, and A_5, and for each, find two permutations which generate the subgroup. (Note that you can check your answer using Groups.exe.)

8. For the symmetry groups of the Platonic solids, list all possible orders of subgroups, and for any such subgroup, indicate the number of elements in a left-coset.

Exploratory Problems

9. When we constructed $\mathbb{F}_9$ in exercise # 4, we used the irreducible polynomial x^2+1, but this was not the only possible choice of such an irreducible polynomial. Construct $\mathbb{F}_9$ using the irreducible polynomial $y^2 + 2y + 2$.

10. Find an irreducible polynomial of degree 3 with coefficients in $\mathbb{Z}_2$, and use it to construct the finite field $\mathbb{F}_8$. *(Hint: Note that if a polynomial of degree 3 were to factor, then at least one of its factors would be linear, which means that it must have a root.)*

11. Let G be a finite group, and let H be a subgroup. Suppose that all of the conjugate subgroups of H (subgroups of the form $g^{-1}Hg$ for some $g \in G$) are equal to H. Show that every left-coset of H is also a right-coset of H.

12. Let G be a finite group (that is, $|G| < \infty$), and let $g \in G$. Prove that the order of g is finite.