Mathematics 113 Professor A. Ogus
March 14, 2008

Algebra Midterm Exam

Note: There are three problems. Write your answers on the exam, using both sides of the page if necessary. Use complete sentences and correct punctuation. You lose points for extraneous statements, especially if they are incorrect.

1. Cyclic groups

   (a) What is the definition of a *cyclic* group?

   A group G is cyclic if there exists an element $g \in G$ such that $G = \{g^i : i \in \mathbf{Z}\}$.

   (b) State the division algorithm for the integers.

   Let n be an integer and let d a positive integer. Then there exists a unique pair of integers (q, r) such that $n = qd + r$ and $0 \leq r < d$.

   (c) Use the division algorithm to prove that every subgroup of a cyclic group is cyclic.

   Suppose that H is a subgroup of $G = \{g^i : i \in \mathbf{Z}\}$. If $H = \{e\}$, then certainly H is cyclic: H is $\{e^i : i \in \mathbf{Z}\}$. If not, there is an integer $i \neq 0$ such that $g^i \in H$. Since H is a group $g^{-i} \in H$, and it follows that there at least one positive integer i such that $g^i \in H$. Then by the well-ordering principle, there is a smallest such integer, which we call d. Let $h := g^d$. We claim that $H = \{h^k : k \in \mathbf{Z}\}$. Indeed, suppose that $g^i \in H$. Write $i = qd + r$ as in the division algorithm. Then $g^r = g^i g^{d-q} = g^i h^{-q}$ belongs to h, since h and g^i belong to h. But $0 \leq r < d$, so by the minimality of d, $r = 0$ and $g^i = h^q$.

2. Permutations

(a) What is the definition of the group S_n? (Be sure to define the group law as well as the elements of S_n.)

The group S_n consists of the set of all bijections from the set $\{1, 2, \ldots, n\}$ to itself. The group law is composition of functions.

(b) What is the definition of an *even* (resp. *odd*) element of S_n? What are the two facts that make your definition "well-defined"?

A permutation is even if it can be written as a product of an even number of transpositions and it is odd if it can be written as a product of an odd number of transpositions. This works because

- Every permutation can be written as a product of transpositions.
- If a permutation is written as a product of n and also as a product of m transpositions, then $m \equiv n \pmod 2$.

(c) Write each of the following permutations as a product of disjoint cycles, say whether it is even or odd, and compute its order.

i. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$

This is (1 3 8)(2 7)(4 9 5 6). It is even, and its order is 12.

ii. (1 4 9 3)(4 3 7 2)(6 5)(2 8 1).

This is (1 9 3 7 2 8 4)(5 6). It is odd, and its order is 14.

3. Integers modulo n.

   In the following problems, work in the ring $\mathbf{Z}_{60}$ of integers modulo 60, with the operations of addition and multiplication. Show your work, but you do not need to write careful proofs.

   (a) Find all solutions to the equation $35x = 7$.

   This has no solutions. Indeed, multiplying both sides by 12 yields the equation $0x = 24$, which is not possible.

   (b) Find all solution solutions to the equation $35x = 10$.

   Consider first the stronger equation $7x = 2$. Since 7 and 60 are relatively prime, this has a unique solution, namely $x = 26$. (Note that $26 \cdot 7 = 182 \equiv 2 \pmod{60}$.) We can get other solutions by adding z to 26, provided that $5z = 0$. The possible such z are just the multiples of 12, so we get as our solution set $\{2, 14, 26, 38, 50, \}$

   (c) How many elements are there in the group $\mathbf{Z}_{60}^*$ of invertible elements of $\mathbf{Z}_{60}$?

   This is $\phi(60) = \phi(4)\phi(3)\phi(5) = 2 \cdot 2 \cdot 4 = 16$.

   (d) Find a number n between 0 and 60 such that $7^{100} \equiv n \pmod{60}$.

   Since 7 is relatively prime to 60, $7^{\phi(60)} \equiv 1 \pmod{60}$. Thus $7^{16} \equiv 1 \pmod{60}$, and it follows that $7^{n16} \equiv 1 \pmod{60}$ for every n. Taking $n = 6$, we see that $7^{100} = 7^{96+4} \equiv 7^4 \equiv (49)^2 \equiv (-11)^2 \equiv 121 \equiv 1$

   (e) Is the group $\mathbf{Z}_{60}^*$ cyclic? Explain.

   In fact $\mathbf{Z}_{60}^* \cong \mathbf{Z}_4^* \times \mathbf{Z}_3^* \times \mathbf{Z}_5^* \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_4$. Thus every element has exponent 4 and the group is not cyclic.