First Midterm: Answers

MA441: Algebraic Structures I

12 October 2003

1) Definitions

1. Define what it means for a subset of a group to be a **subgroup**.

   A subset H of G that is itself a group under the operation of G is a subgroup.

2. Define what it means for a group to be **cyclic**.

   A group G is cyclic if there is an element a such that G is generated by a, that is, $G = \langle a \rangle$. (Alternatively, G is cyclic if there is an element a with the same order as G.)

2) Give an example of

1. a nonabelian group of order 10.

   The dihedral group D_5.

2. a group with exactly five subgroups (including the trivial subgroup and itself). List the subgroups.

   The additive group of integers modulo 16, denoted $\mathbb{Z}/16\mathbb{Z}$ or Z_{16}. The subgroups are $\langle 1 \rangle$, $\langle 2 \rangle$, $\langle 4 \rangle$, $\langle 8 \rangle$, $\langle 0 \rangle = \langle 16 \rangle$.

3) Fill in the blanks.

1. The order of 3 in $U(11)$ is 5.

2. The order of the group $U(15)$, which equals $\phi(15)$, is 8.

   $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

3. If $x \in G$, $x \neq e$, and $x^{18} = x^{33} = e$, then $|x| = 3$.

   The GCD of 18 and 33 is 3.

4. In the group D_4, let R denote rotation by 90 degrees counterclockwise, and let F denote a flip about the vertical. Written in the form $R^i F^j$, the element FR equals $R^3 F$.

5. A complete list of all generators of $\mathbb{Z}/10\mathbb{Z}$ is $\{1, 3, 7, 9\}$.

4) Euclidean algorithm

1. Use the Euclidean Algorithm to express $\gcd(57, 5)$ as an integer linear combination of 57 and 5. Show your work.

   We calculate the GCD by the Euclidean Algorithm:

$$\begin{aligned} 57 &= 11 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1, \\ 1 &= 1 \cdot 5 - 2 \cdot 2 \\ 2 &= 57 - 11 \cdot 5 \\ 1 &= 1 \cdot 5 - 2(57 - 11 \cdot 5) \\ &= 23 \cdot 5 - 2 \cdot 57. \end{aligned}$$

2. Find the multiplicative inverse of 5 in $U(57)$. Show your work.

   Since $23 \cdot 5 - 2 \cdot 57 = 1$, we have $23 \cdot 5 \equiv 1 \pmod{57}$, therefore $23 = 5^{-1}$ in $U(57)$.

5) Permutations
Consider permutations of the set $\{1, 2, 3, 4, 5, 6, 7\}$.

1. Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 2 & 6 & 5 & 1 \end{pmatrix}, \ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 3 & 1 & 4 & 6 \end{pmatrix}.$$

   Write α and β in cycle notation.

   $\alpha = (13427)(56)$, $\beta = (125)(3764)$.

2. Compute the composition $\alpha\beta$ and write it in cycle notation. Write α^{-1} in cycle notation. (Note: we compose permutations from left to right, so $(123)(12) = (23)$, not (13).)

   $\alpha\beta = (1726)(45)$, $\alpha^{-1} = (17243)(56)$.

The next two questions ask for proofs. Be sure to write carefully and explain your arguments with clear and coherent sentences.

6) Let a be an element of a group G. Define $\langle a \rangle$, the cyclic subgroup generated by a, and prove that it is a subgroup of G.

The cyclic group generated by a, denoted $\langle a \rangle$, is $\{a^n : \forall n \in \mathbb{Z}\}$.

To show that $\langle a \rangle$ is a subgroup of G, we can apply the Two-step Subgroup Test. First, we show that that $\langle a \rangle$ is closed under the operation of the group. Let a^m and a^n be two arbitrary elements of $\langle a \rangle$. Their composition a^{m+n} is again in $\langle a \rangle$ since $m+n$ is an integer. Next, we show that $\langle a \rangle$ is closed under inversion, that is, for any element in $\langle a \rangle$, its inverse is also in $\langle a \rangle$. Let a^n be any element of $\langle a \rangle$. Then its inverse a^{-n} is also in $\langle a \rangle$ because $-n$ is an integer.

You could also apply the One-Step Subgroup test by noting that $a^n(a^m)^{-1}$ in again in $\langle a \rangle$ because $n - m$ is an integer.

7) Let G be a group. Show that

$$Z(G) = \bigcap_{a \in G} C(a),$$

that is, the center of a group is the intersection of the centralizers of every element in the group.

Note that this is Gallian's Exercise 15 of Chapter 3 (page 68), assigned in Homework 2.

The center $Z(G)$ is $\{x \in G : \forall a \in G, xa = ax\}$, that is, the elements of G that commute with all elements. The center $C(a)$ is $\{x \in G : xa = ax\}$, that is the elements of G that commute with a.

Suppose x is any element in the center $Z(G)$. Then for any a in G, $xa = ax$. This implies that $x \in C(a)$. Since this is true for any $a \in G$, x is in $C(a)$ for every $a \in G$, hence is in their intersection. This shows that

$$Z(G) \subseteq \bigcap_{a \in G} C(a).$$

Conversely, suppose x is in $\bigcap_{a \in G} C(a)$. Then for any $a \in G$, we know $xa = ax$. This means that x commutes with every element of G, so $x \in Z(G)$. This shows that

$$Z(G) \supseteq \bigcap_{a \in G} C(a).$$

You could also prove the result more concisely by noting that all the steps in the above argument are reversible. Choose any $x \in Z(G)$. Now $x \in Z(G)$ iff $xa = ax$ for any $a \in G$, iff for any $a \in G$, $x \in C(a)$, iff $x \in \bigcap_{a \in G} C(a)$.