

Math 113 Midterm Exam Solutions  
July 16th, 2009

# 1 Computations

**Problem 1.1.** (2 points) Let  $\sigma \in S_7$  be the element  $\sigma = (1235)(237)(45)$ . Write  $\sigma$  as a product of disjoint cycles, and compute the order of  $\sigma$ .

**Solution 1.1.1.**  $\sigma = (1254)(37)$ . The order of  $\sigma$  is  $\text{lcm}(4, 2) = 4$ .

**Problem 1.2.** (3 points) Find all possible cycle types of permutations in  $S_6$ . For each cycle type, state whether permutations of that cycle type are even or odd. Circle the cycle types which correspond to elements of  $A_6$ .

**Solution 1.2.1.**

Cycle Type	Even/Odd	In $A_6$ ?
(6)	Odd	No
(1, 5)	Even	Yes
(1, 1, 4)	Odd	No
(2, 4)	Even	Yes
(1, 1, 1, 3)	Even	Yes
(1, 2, 3)	Odd	No
(3, 3)	Even	Yes
(1, 1, 1, 1, 2)	Odd	No
(1, 1, 2, 2)	Even	Yes
(2, 2, 2)	Odd	No
(1, 1, 1, 1, 1, 1)	Even	Yes

**Problem 1.3.** Let  $G = (\mathbb{Z}/11\mathbb{Z})^\times$ . Do the following:

1. (1 point) Show that  $G$  is cyclic by finding a generator.
2. (3 points) List all subgroups of  $G$ , and for each subgroup of  $G$ , give a generator for that subgroup.

**Solution 1.3.1** (Part 1). I claim that  $[2]$  is a generator. We have:

$x$	$[2]^x$
1	$[2]$
2	$[4]$
3	$[8]$
4	$[5]$
5	$[10]$
6	$[9]$
7	$[7]$
8	$[3]$
9	$[6]$
10	$[1]$

Hence every element of  $G$  is a power of  $[2]$ , so  $[2]$  is a generator for this group.

**Solution 1.3.2** (Part 2).  $G$  is a cyclic group of order 10 with generator  $[2]$ , and so has exactly one subgroup of order  $d$  for each  $d$  dividing 10, namely the subgroup generated by  $[2]^{10/d}$ . So the subgroups of  $G$  are:

- $G = \langle [2] \rangle$ ,
- $\langle [2]^2 \rangle = \langle [4] \rangle = \{[4], [5], [9], [3], [1]\}$ ,
- $\langle [2]^5 \rangle = \langle [10] \rangle = \{[10], [1]\}$ , and
- $\langle [2]^{10} \rangle = \{[1]\} = \{e\}$ .

**Problem 1.4.** (3 points) Show that  $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  by writing down an explicit isomorphism  $f : \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ . (You must prove that your function  $f$  is in fact an isomorphism).

**Solution 1.4.1** (Solution the First). Define  $f : \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  by  $f(n(\bmod 6)) = (n(\bmod 2), n(\bmod 3))$ . I claim  $f$  is an isomorphism. First we must check  $f$  is well-defined; suppose that  $n \equiv n'(\bmod 6)$ . Then  $6|(n - n')$ , hence also  $2|(n - n')$  and  $3|(n - n')$ , so  $n \equiv n'(\bmod 2)$  and  $n \equiv n'(\bmod 3)$ . Hence  $f(n(\bmod 6)) = f(n'(\bmod 6))$ , so  $f$  is well-defined.

From this point on I'll stop writing the “(mod 6)” stuff since it's hard to read and we really only needed it for well-definition. Now, I claim  $f$  is an isomorphism. We first check that  $f$  is a homomorphism; we have:

$$\begin{aligned} f(n + n') &= (n + n', n + n') \\ &= (n, n) + (n', n') \\ &= f(n) + f(n'). \end{aligned}$$

Hence  $f$  is a homomorphism. Now we have to check that  $f$  is a bijection. There are several ways to do this:

**Method 1** We use the nice criterion for checking that a homomorphism is injective: suppose  $f(n) = 0$ , i.e.  $(n, n) = (0, 0)$ . Then  $2|n$  and  $3|n$ . Since 2 and 3 are relatively prime,  $6|n$ , so  $n \equiv 0(\bmod 6)$ , i.e.  $n$  was 0 in  $\mathbb{Z}/6\mathbb{Z}$  to begin with. This shows that  $\ker(f) = \{0\}$ , so  $f$  is injective (since it's a homomorphism). Since  $|\mathbb{Z}/6\mathbb{Z}| = 6 = |\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}|$ , we have that  $f$  is an injective function between two finite sets with the same number of elements, so  $f$  is surjective.

**Method 2** We check  $f$  is injective directly. Suppose that  $f(n) = f(n')$ ; then  $(n, n) = (n', n')$ , so  $(n - n', n - n') = (0, 0)$ , hence  $2|(n - n')$  and  $3|(n - n')$ , so as above,  $6|(n - n')$ , hence  $n = n'$  in  $\mathbb{Z}/6\mathbb{Z}$ . Thus  $f$  is injective. As in Method 1, it follows that  $f$  is surjective.

**Method 3** We check by hand that  $f$  is surjective; we have

$$\begin{aligned} f(0) &= (0, 0) \\ f(1) &= (1, 1) \\ f(2) &= (0, 2) \\ f(3) &= (1, 0) \\ f(4) &= (0, 1) \\ f(5) &= (1, 2). \end{aligned}$$

Hence every element of  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  is in the image of  $f$ , so  $f$  is surjective. Since  $f$  is a surjection between finite sets of the same size,  $f$  is injective.

**Solution 1.4.1** (Solution the Second). Define  $f : \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  by

$$\begin{aligned} f(0) &= (0, 0) \\ f(1) &= (1, 1) \\ f(2) &= (0, 2) \\ f(3) &= (1, 0) \\ f(4) &= (0, 1) \\ f(5) &= (1, 2). \end{aligned}$$

Then  $f$  is clearly a bijection, and we have to check that  $f$  is a homomorphism.

Note first that for all  $a \in \mathbb{Z}/6\mathbb{Z}$ , we have

$$f(0 + a) = f(a) = (0, 0) + f(a) = f(0) + f(a),$$

so it remains to check that  $f(a + b) = f(a) + f(b)$  for all pairs of nonzero elements  $a$  and  $b$ . Note that since both  $\mathbb{Z}/6\mathbb{Z}$  and  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  are abelian, the order of  $a$  and  $b$  do not matter. We have:

$$\begin{aligned} f(1 + 1) &= f(2) = (0, 2) = (1, 1) + (1, 1) = f(1) + f(1) \\ f(1 + 2) &= f(3) = (1, 0) = (1, 1) + (0, 2) = f(1) + f(2) \\ f(1 + 3) &= f(4) = (0, 1) = (1, 1) + (1, 0) = f(1) + f(3) \\ f(1 + 4) &= f(5) = (1, 2) = (1, 1) + (0, 1) = f(1) + f(4) \\ f(1 + 5) &= f(0) = (0, 0) = (1, 1) + (1, 2) = f(1) + f(5) \\ f(2 + 2) &= f(4) = (0, 1) = (0, 2) + (0, 2) = f(2) + f(2) \\ f(2 + 3) &= f(5) = (1, 2) = (0, 2) + (1, 0) = f(2) + f(3) \\ f(2 + 4) &= f(0) = (0, 0) = (0, 2) + (0, 1) = f(2) + f(4) \\ f(2 + 5) &= f(1) = (1, 1) = (0, 2) + (1, 2) = f(2) + f(5) \\ f(3 + 3) &= f(0) = (0, 0) = (1, 0) + (1, 0) = f(3) + f(3) \\ f(3 + 4) &= f(1) = (1, 1) = (1, 0) + (0, 1) = f(3) + f(4) \\ f(3 + 5) &= f(2) = (0, 2) = (1, 0) + (1, 2) = f(3) + f(5) \\ f(4 + 4) &= f(2) = (0, 2) = (0, 1) + (0, 1) = f(4) + f(4) \\ f(4 + 5) &= f(3) = (1, 0) = (0, 1) + (1, 2) = f(4) + f(5) \\ f(5 + 5) &= f(4) = (0, 1) = (1, 2) + (1, 2) = f(5) + f(5). \end{aligned}$$

Thus  $f$  is a homomorphism.

## 2 Theory

**Problem 2.1.** (3 points) Show that  $D_n$  has a subgroup of order  $k$  for every  $k$  dividing  $n$ .

**Solution 2.1.1** (Solution the First). The element  $r \in D_n$  has order  $n$ , hence  $\langle r \rangle \leq D_n$  is a cyclic subgroup of order  $n$ . A cyclic group of order  $n$  has a (unique) subgroup of order  $k$  for every  $k$  dividing  $n$ , i.e.  $\langle r \rangle$  has a subgroup of order  $k$  for every  $k$  dividing  $n$ . Since subgroups of  $\langle r \rangle$  are also subgroups of  $D_n$ , we are done.

**Solution 2.1.2** (Solution the Second). Let  $k$  be a natural number dividing  $n$ . Since  $r \in D_n$  has order  $n$ , the element  $r^{n/k}$  has order  $\frac{n}{\gcd(n, n/k)} = \frac{n}{n/k} = k$ , hence  $\langle r^{n/k} \rangle$  is a subgroup of  $D_n$  of order  $k$ . (This is essentially the same as the first solution).

**Remark** It is actually true that  $D_n$  has a subgroup of order  $k$  for every  $k$  dividing  $2n$ ; the desired subgroup of order  $2k$  is the subgroup consisting of all products of  $r^{n/k}$  with  $s$ . (For example, in  $D_{12}$ , one subgroup of order 6 is given by  $\{e, r^2, r^4, r^6, r^8, r^{10}\}$ , while another is given by  $\{e, r^4, r^8, s, r^4s, r^8s\}$ ).

**Problem 2.2.** Let  $G$  be an abelian group, and let  $g, h \in G$  be elements.

1. (2 points) Let  $H$  be the set  $\{g^n h^m \mid n, m \in \mathbb{Z}\}$ . Show that  $H$  is a subgroup of  $G$ .
2. (3 points) Suppose that there exists some element  $a \in G$  and integers  $k, \ell \in \mathbb{Z}$  such that  $g = a^k$  and  $h = a^\ell$ . Show that the subgroup  $H$  defined in part (1) is cyclic.

**Solution 2.2.1** (Part 1). Note first that  $H \neq \emptyset$  since for example  $gh \in H$ . Now, let  $x, y \in H$  be arbitrary. Then  $x = g^n h^m$  and  $y = g^p h^q$  for some  $n, m, p, q \in \mathbb{Z}$ . Thus

$$x(y^{-1}) = g^n h^m h^{-q} g^{-p} = g^{n-p} h^{m-q} \in H.$$

Thus  $H$  is a subgroup of  $G$ . (Alternatively you can check that  $xy \in H$ ,  $e \in H$ , and  $x^{-1} \in H$ . All are done in the same way.)

**Solution 2.2.2** (Part 2, Super Slick Method). Since  $g = a^k$  and  $h = a^\ell$ , every element of  $H$  is of the form

$$g^n h^m = (a^k)^n (a^\ell)^m = a^{kn+\ell m} \in \langle a \rangle.$$

Hence  $H$  is a subgroup of the cyclic group  $\langle a \rangle$ , so  $H$  is cyclic.

**Solution 2.2.3** (Part 2, Normal Method). Let  $d = \gcd(k, \ell)$ . I claim that  $H = \langle a^d \rangle$ . We have that  $d = nk + m\ell$  for some  $n, m \in \mathbb{Z}$ , hence

$$a^d = a^{nk+m\ell} = (a^k)^n (a^\ell)^m = g^n h^m \in H,$$

thus  $\langle a^d \rangle \leq H$ .

On the other hand,  $d|k$  and  $d|\ell$ , so there exist  $p, q \in \mathbb{Z}$  such that  $k = dp$  and  $\ell = dq$ . Let  $x = g^n h^m$  be an arbitrary element of  $H$ . Then

$$x = g^n h^m = (a^k)^n (a^\ell)^m = a^{kn+\ell m} = a^{d(pn+qm)} = (a^d)^{pn+qm} \in \langle a^d \rangle,$$

hence  $H \leq \langle a^d \rangle$ , as desired.

**Problem 2.3.** (4 points) State and prove Lagrange's Theorem.

**Solution 2.3.1.** Let  $G$  be a group and let  $H$  be a subgroup. We prove two propositions first, then we will prove Lagrange's theorem.

**Proposition 2.4.** *The set of left cosets of  $H$  in  $G$  is a partition of  $G$ .*

*Proof.* We have to show that:

1. Every element of  $G$  is contained in some left coset of  $H$ , and
2. If  $g_1H$  and  $g_2H$  are two left cosets, either  $g_1H = g_2H$  or else  $g_1H \cap g_2H = \emptyset$ .

To prove (1), let  $g$  be an element of  $G$ ; then  $g = ge \in gH$ .

To prove (2), suppose that  $g_1H \cap g_2H \neq \emptyset$ . Then there exists some  $x \in g_1H \cap g_2H$ , so there exist  $h_1, h_2 \in H$  such that

$$g_1h_1 = x = g_2h_2,$$

hence  $g_2^{-1}g_1 = h_2h_1^{-1} \in H$ , so by our proposition about equality of cosets, we have  $g_1H = g_2H$ . (We can also prove this directly: let  $h \in H$  be arbitrary; since  $g_1 = g_2h_2h_1^{-1}$ , we have  $g_1h = g_2h_2h_1^{-1}h \in g_2H$ , so  $g_1H \subseteq g_2H$ . By symmetry of  $g_1$  and  $g_2$ , we also have  $g_2H \subseteq g_1H$ , hence  $g_1H = g_2H$ .  $\square$ )

**Proposition 2.5.** *Every left coset  $gH$  of  $H$  has  $|H|$  elements.*

*Proof.* Define a function  $f : H \rightarrow gH$  by  $f(h) = gh$ . Then  $f$  is clearly surjective by the definition of  $gH$ , and  $f$  is injective since if  $f(h_1) = f(h_2)$  then  $gh_1 = gh_2$ , so  $h_1 = h_2$  by left cancellation. Thus  $f$  is a bijection, so  $gH$  has the same number of elements as  $H$ , namely  $|H|$ .  $\square$

**Theorem 2.6** (Lagrange's Theorem). *Let  $G$  be a finite group and let  $H$  be a subgroup of  $G$ . Then  $|G| = |H|[G : H]$ .*

*Proof.* The left cosets of  $H$  partition  $G$  into  $[G : H]$  many pieces, each of which has  $|H|$  elements. Thus  $|G| = |H|[G : H]$ .  $\square$