

Math 317 C1  
HOUR EXAM II  
15 July 2002

**SOLUTIONS**

1. Let  $G$  be an abelian group and let  $H = \{a \in G \mid a^2 = e\}$ . Show that  $H$  is a subgroup of  $G$ .

SOLUTION: Let  $a, b \in H$ . We must show that  $ab^{-1} \in H$ . Thus since  $G$  is abelian,

$$(ab^{-1})^2 = a^2(b^{-1})^2 = a^2(b^2)^{-1} = ee^{-1} = e.$$

Therefore  $H$  is a subgroup of  $G$ .

2. Let  $\alpha = (235)(146)(78)$  be a permutation in  $S_8$ . Find a permutation  $\beta \in S_8$  which satisfies  $\beta\alpha\beta^{-1} = (148)(375)(26)$ .

SOLUTION: The effect of a conjugation on  $(235)(146)(78)$  is another permutation with the same cycle structure whose entries are the images of the entries of the original permutation under  $\beta$ . Therefore, if  $\beta = \begin{pmatrix} 2 & 3 & 5 & 1 & 4 & 6 & 7 & 8 \\ 1 & 4 & 8 & 3 & 7 & 5 & 2 & 6 \end{pmatrix}$  we get the desired effect. Therefore  $\beta = (13472)(586)$ .

There are many other solutions depending on how we write the original permutation.

3. Let  $f : G \rightarrow H$  be a surjective homomorphism and let  $Z(G)$  be the center of  $G$ . Show that  $f(z)$  commutes with every element of  $H$ , for each  $z \in Z(G)$ .

SOLUTION: Let  $h \in H$ . Then since  $f$  is surjective, there is  $g \in G$  such that  $f(g) = h$ . Now if  $z \in Z(G)$ , then

$$f(z)h = f(z)f(g) = f(zg) = f(gz) = f(g)f(z) = hf(z).$$

4. Let  $(R^\times, \cdot)$  be the group of nonzero real numbers under multiplication and let  $(R^+, \cdot)$  be the group of positive real numbers under multiplication. If  $T$  is the subgroup of  $R^\times$  consisting of  $\{1, -1\}$ . Show that  $R^\times/T \simeq R^+$ .

(Hint: Consider the mapping  $f : R^\times \rightarrow R^+$  defined by  $f(x) = |x|$ , the absolute value of  $x$ , and use the First Isomorphism Theorem.)

SOLUTION: Let  $f : R^\times \rightarrow R^+$  defined by  $f(x) = |x|$ . We first show that  $f$  is a homomorphism. If  $a, b \in R^\times$ , then  $f(ab) = |ab| = |a||b| = f(a)f(b)$ .

If  $a \in \ker f$ , then  $f(a) = |a| = 1$ , since 1 is the identity of  $(R^+, \cdot)$ . But if  $a$  is a real number and  $|a| = 1$ , then either  $a = 1$  or  $a = -1$ . Hence  $\ker f = \{1, -1\} = T$ .

$f$  is surjective, since every positive real number is the absolute value of itself and so  $\text{im } f = R^+$ . The First Isomorphism Theorem says  $R^\times/\ker f \simeq \text{im } f$ . Thus

$$R^\times/T \simeq R^+.$$

5. Let  $p$  be a prime.

a) What is the order of the multiplicative group  $U(\mathbb{Z}_p)$ ?

b) Suppose  $p = 4d + 3$  for some integer  $d$ . Show that  $U(\mathbb{Z}_p)$  doesn't contain an element of order 4.

c) Deduce from b) above that the congruence

$$x^2 \equiv -1 \pmod{p}$$

has no solution when the prime  $p = 4d + 3$ .

SOLUTION: a) Since  $U(\mathbb{Z}_p)$  is the multiplicative group of all congruence classes  $[r] \pmod{p}$  with  $0 \leq r < p$  and  $(r, p) = 1$ , it follows from the fact that  $p$  is a prime, that  $U(\mathbb{Z}_p)$  has  $p - 1$  elements.

b) Since  $p = 4d + 3$ , the order of  $U(\mathbb{Z}_p)$  is  $p - 1 = 4d + 2$ . If  $U(\mathbb{Z}_p)$  had an element of order 4, then 4 would divide  $4d + 2$ , by Lagrange's Theorem. That is clearly false and so  $U(\mathbb{Z}_p)$  has no element of order 4.

c) If the congruence  $x^2 \equiv -1 \pmod{p}$  had a solution, then  $x^4 \equiv 1 \pmod{p}$ . Then  $[x]^4 = [1]$ , and  $[x]^2 \neq [1]$ . Hence the order of  $[x]$  is 4 or a divisor of 4, namely 2. But since  $[x]^2 \neq [1]$ , its order is not 2 and so  $U(\mathbb{Z}_p)$  has an element of order 4, a contradiction. Therefore  $x^2 \equiv -1 \pmod{p}$  has no solution when  $p$  is a prime with  $p = 4d + 3$ .