

1. Use the First Isomorphism Theorem to show that  $\mathbb{Z}_{30}/(5) \cong \mathbb{Z}_5$ .

Consider the map  $\varphi : \mathbb{Z}_{30} \rightarrow \mathbb{Z}_5$  defined by  $\varphi([a]_{30}) = [a]_5$  for  $a \in \mathbb{Z}$ . It was shown in class that this map is well-defined and that it is a homomorphism. Moreover,  $\varphi$  is surjective, since every element in  $\mathbb{Z}_5$  is of the form  $[a]_5$  for some  $a \in \mathbb{Z}$  (so  $[a]_5 = \varphi([a]_{30})$ ). Note that  $[a]_5 = [0]_5$  iff  $5 \mid a$ . Hence,  $K_\varphi$ , the kernel of  $\varphi$ , consists of all  $[a]_{30}$  for which  $5 \mid a$ , that is,

$$K_\varphi = \{0, 5, 10, 15, 20, 25\} = (5) \subseteq \mathbb{Z}_{30}.$$

It follows by the First Isomorphism Theorem that  $\mathbb{Z}_{30}/(5) = \mathbb{Z}_{20}/K_\varphi \cong \mathbb{Z}_5$ . ◆

2. Let  $I$  be an ideal in  $\mathbb{R}[x]$  and suppose that  $f(x) \in I$  is a nonzero polynomial with minimal degree (that is, if  $g(x) \in I$  is nonzero, then  $\deg f(x) \leq \deg g(x)$ ). Prove that  $I = (f(x))$ .

Let  $h(x) \in (f(x))$ ; then  $h(x) = g(x)f(x)$  for some  $g(x) \in \mathbb{R}[x]$ . Since  $f(x) \in I$  and  $I$  is an ideal,  $g(x)f(x) \in I$ . Hence,  $(f(x)) \subseteq I$ .

For the reverse inclusion, let  $h(x) \in I$ . Then since  $\mathbb{R}$  is a field, the Division Algorithm applies; so there are  $q(x), r(x) \in \mathbb{R}[x]$  such that  $h(x) = f(x)q(x) + r(x)$  and either  $r(x) = 0$  or  $\deg r(x) < \deg f(x)$ . Since  $r(x) = h(x) - f(x)q(x)$  and  $h(x), f(x)q(x) \in I$ , we must have  $r(x) \in I$ . It follows that  $r(x) = 0$ , for if  $r(x) \neq 0$  then  $\deg r(x) < \deg f(x)$  contradicts the requirement that  $f(x)$  have minimal degree. Hence,  $h(x) = f(x)q(x)$  and thus  $h(x) \in (f(x))$ . It follows that  $I = (f(x))$ . ◆

3. Show that  $F = \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$  is a field. Is  $F$  finite? If so, find  $|F|$ .

To show that  $F = \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$  is a field it suffices to establish that  $p(x) = x^3 + x^2 + 1$  is irreducible in  $\mathbb{Z}_2[x]$  (since  $\mathbb{Z}_2$  is a field). Since  $\deg p(x) = 3$ ,  $p(x)$  is irreducible iff it has no roots in  $\mathbb{Z}_2$ . Since  $p(0) = 1 = p(1)$ ,  $p(x)$  has no roots and is thus irreducible. Therefore,  $F$  is a field as required. Since  $\mathbb{Z}_2$  is finite, so is  $F$ . The (distinct) congruence classes are all of the form

$$(x^3 + x^2 + 1) + a_0 + a_1x + a_2x^2$$

with  $a_i = 0, 1$ . Hence, there are  $2^3 = 8$  distinct congruence classes; thus,  $|F| = 8$ . ◆

4. Prove that  $\mathbb{Z}_3 \times \mathbb{Z}_4$  is cyclic by finding a generator. Show that  $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$ . Is  $\mathbb{Z}_6 \times \mathbb{Z}_8$  cyclic?

Let  $a = (1, 1) \in \mathbb{Z}_3 \times \mathbb{Z}_4$ , then since  $3 \mid 12$  and  $4 \mid 12$ ,  $12a = (0, 0)$  so the order of  $a$  divides 12. We show that the order of  $a$  is 12 by tabulating the values of  $na$  for  $1 \leq n \leq 12$ :

$a$	1	2	3	4	5	6	7	8	9	10	11	12
$n(a)$	(1,1)	(2,2)	(0,3)	(1,0)	(2,1)	(0,2)	(1,3)	(2,0)	(0,1)	(1,2)	(2,3)	(0,0)

Alternatively, we may argue that  $na = (0, 0)$  iff  $3 \in n$  and  $4 \mid n$  and since  $n = 12$  is the smallest positive integer with this property, the order of  $a = (1, 1)$  is 12. Since  $\mathbb{Z}_3 \times \mathbb{Z}_4 = \langle (1, 1) \rangle$ ,  $\mathbb{Z}_3 \times \mathbb{Z}_4$  is cyclic with generator  $a = (1, 1)$ . Since the order of  $\mathbb{Z}_3 \times \mathbb{Z}_4$  is 12, we have  $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$ .

But  $\mathbb{Z}_6 \times \mathbb{Z}_8$  is not cyclic, since there is no element of order  $48 = 6 \cdot 8$ . Indeed, let  $(x, y) \in \mathbb{Z}_6 \times \mathbb{Z}_8$ , then since  $6x = 0$  and  $8y = 0$ , we have  $24(x, y) = (4(6x), 3(8y)) = (0, 0)$ . Hence, the order of  $(x, y)$  divides 24; therefore, there is no element of order 48 and so  $\mathbb{Z}_6 \times \mathbb{Z}_8$  is not cyclic. ◆

5. Let  $G$  be a group of order 21. Prove that every proper subgroup is cyclic.

Let  $H$  be a proper subgroup of  $G$ . Then by Lagrange's Theorem  $|H|$  divides  $|G| = 21$ . Since  $H$  is proper,  $|H| < 21$  so we must have  $|H| = 1, 3, 7$ . If  $|H| = 1$ , then  $H = \{e\}$ , which is cyclic. Otherwise,  $|H| = p$  is a prime where  $p = 3, 7$ . But since every group of prime order is cyclic  $H$  is cyclic. ◆

6. Show that  $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{R} \text{ and } a > 0 \right\}$  is a subgroup of  $GL(2, \mathbb{R})$ . Prove that the map  $f : G \rightarrow \mathbb{R}^*$  given by  $f\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\right) = a$  is a group homomorphism. Is  $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$  a normal subgroup of  $G$ ?

Note first that  $G \neq \emptyset$  since  $G$  contains the identity element. Let  $A \in G$ ; then  $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$  for some  $a, b \in \mathbb{R}$  with  $a > 0$  and  $\det(A) = a \neq 0$ . So  $A \in GL(2, \mathbb{R})$ . To show it is a subgroup we must show that it is closed under multiplication and taking inverses. Let  $A, C \in G$ , then  $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$  and  $C = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$  for some  $a, b, c, d \in \mathbb{R}$  with  $a, c > 0$  and

$$AC = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix} \in G \quad \text{and} \quad A^{-1} = \begin{pmatrix} 1/a & -b/a \\ 0 & 1 \end{pmatrix} \in G$$

since  $ac > 0$  and  $1/a > 0$ . Hence,  $G$  is closed under multiplication and taking inverses and is therefore a subgroup.

To show that  $f$  as defined above is a homomorphism, let  $A, C \in G$ , then  $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$  and  $C = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$  for some  $a, b, c, d \in \mathbb{R}$  with  $a, c > 0$ . Then

$$f(AC) = f\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}\right) = f\left(\begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix}\right) = ac = f\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\right) f\left(\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}\right) = f(A)f(C).$$

Hence,  $f$  is a homomorphism. Note that

$$K_f = \{A \in G \mid f(A) = 1\} = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\} = N.$$

By a recent homework exercise, the kernel of a homomorphism is a normal subgroup. Hence,  $N = K_f$  is a normal subgroup of  $G$ .