

**IMMERSE 2005**  
**Algebra Problems June 28th, 2005**

3. Prove that every commutative ring (with identity) is symmetric.

**Solution:** Let  $R$  be a commutative ring with identity. Suppose that  $abc = 0$  for some  $a, b, c \in R$ . Since  $R$  is commutative,  $bc = cb$ . Therefore,  $acb = abc = 0$ . That is, whenever  $abc = 0$  we have  $acb = 0$ . So  $R$  is symmetric.

4. Prove that every symmetric ring is reversible.

**Solution:** Let  $R$  be a symmetric ring. Then, by definition,  $1 \in R$  (That is,  $R$  has an identity, call it 1.) Suppose  $ab = 0$  for some  $a, b \in R$ . Then  $1 \cdot ab = 0$ , so, since  $R$  is symmetric,  $1 \cdot ba = 0$ . Therefore, whenever  $ab = 0$  we have  $ba = 0$ , so  $R$  is reversible.

5. A ring with identity which has no non-zero zero divisors is reversible and symmetric.

**Solution:** Let  $R$  be a ring with identity which has no non-zero zero divisors. Suppose  $abc = 0$  for some  $a, b, c \in R$ . Since  $R$  has no non-zero zero divisors and  $(ab)c = 0$ , either  $ab = 0$  or  $c = 0$ . If  $c = 0$  then any product involving  $c$  is 0, in particular,  $acb = 0$ . If  $ab = 0$ , then since  $R$  has no non-zero zero divisors, either  $a = 0$  or  $b = 0$ . In both cases, we have  $acb = 0$ . Therefore, whenever  $abc = 0$  we also have  $acb = 0$ . Therefore,  $R$  is symmetric. By problem 4.,  $R$  must also be reversible.

6. Suppose that  $R$  is a subring (with identity) of  $S$ . Prove that if  $S$  is reversible then  $R$  is reversible.

**Solution:** Let  $a, b \in R \subseteq S$  such that  $ab = 0$ . Since  $S$  is reversible, we have  $ba = 0$ . Therefore, whenever  $ab = 0$  in  $R$  we have  $ba = 0$ . Since  $R$  has an identity,  $R$  is reversible.

7. Suppose that  $R$  is a subring (with identity) of  $S$ . Prove that if  $S$  is symmetric then  $R$  is symmetric.

**Solution:** Let  $a, b, c \in R \subseteq S$  such that  $abc = 0$ . Since  $S$  is symmetric, we have  $acb = 0$ . Therefore, whenever  $abc = 0$  in  $R$ , we also have  $acb = 0$ . Since  $R$  has an identity,  $R$  is symmetric.

8. If  $R$  is a reversible ring and  $a, b, c \in R$  such that  $abc = 0$ , what other products of three elements must be zero? Form a conjecture and prove your claim.

**Solution:** Let  $R$  be a reversible ring and  $a, b, c \in R$  such that  $abc = 0$ . Then we also have that  $bca = 0$  and  $cab = 0$ . Furthermore, there are reversible rings for which  $abc = 0$  and  $acb \neq 0, bac \neq 0$ , and  $cba \neq 0$ .

**Proof:** Since  $R$  is reversible and  $(ab)c = 0$  we have  $c(ab) = 0$ . Similarly, we can group  $b$  and  $c$  yielding  $a(bc) = 0$ , so  $(bc)a = 0$ . Thus, whenever  $abc = 0$  in a reversible ring, we also have  $bca = 0$  and  $cab = 0$ . If  $abc = 0$  implies  $bac = 0$  or  $cba = 0$  in a reversible ring, then by grouping elements and applying the reversible property, we have  $acb = 0$  and therefore the ring is symmetric. Since there are reversible rings which are not symmetric, there are reversible rings for which  $abc = 0$  and  $acb \neq 0, bac \neq 0$ , and  $cba \neq 0$ .

9. If  $R$  is a symmetric ring and  $a, b, c \in R$  such that  $abc = 0$ , what other products of three elements must be zero? Form a conjecture and prove your claim.

**Solution:** Let  $R$  be a symmetric ring and  $a, b, c \in R$  such that  $abc = 0$ , then all six products of  $a, b, c$  must be zero.

**Proof:** Whenever  $abc = 0$ , by definition of a symmetric ring,  $acb = 0$ . Since a symmetric ring is reversible, we also have  $bca = 0$  and  $cab = 0$ . Finally, applying the symmetric property to the last two equations, we have  $bca = 0$  implies  $bac = 0$  and  $cab = 0$  implies  $cba = 0$ .

10. Express each of the following as a product of disjoint cycles:

$$(a) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 2 & 1 & 4 & 5 & 6 & 3 & 8 & 9 \end{pmatrix}$$

$$(b) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 1 & 7 & 5 & 2 & 6 & 3 & 9 \end{pmatrix}$$

**Solution:**

$$(a) (173)$$

$$(a) (1476283)$$

11. Verify the following:

$$(a) (12)(23)(34) = (1432)$$

$$(b) (1234)(2345) = (13524)$$

$$(c) (12)(53214)(23) = (245)$$

$$(d) (7236)(85)(571)(1537)(486) = (1348)(27)(56)$$

**Solution:**

$$(a) \begin{array}{l} 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \\ 2 \rightarrow 1 \rightarrow 1 \rightarrow 1 \\ 3 \rightarrow 3 \rightarrow 2 \rightarrow 2 \\ 4 \rightarrow 4 \rightarrow 4 \rightarrow 3 \end{array}$$

$$(b) \begin{array}{l} 1 \rightarrow 2 \rightarrow 3 \\ 2 \rightarrow 3 \rightarrow 4 \\ 3 \rightarrow 4 \rightarrow 5 \\ 4 \rightarrow 1 \rightarrow 1 \\ 5 \rightarrow 5 \rightarrow 2 \end{array}$$

$$(c) \begin{array}{l} 1 \rightarrow 2 \rightarrow 1 \rightarrow 1 \\ 2 \rightarrow 1 \rightarrow 4 \rightarrow 4 \\ 3 \rightarrow 3 \rightarrow 2 \rightarrow 3 \\ 4 \rightarrow 4 \rightarrow 5 \rightarrow 5 \\ 5 \rightarrow 5 \rightarrow 3 \rightarrow 2 \end{array}$$

$$(d) \begin{array}{l} 1 \rightarrow 1 \rightarrow 1 \rightarrow 5 \rightarrow 3 \rightarrow 3 \\ 2 \rightarrow 3 \rightarrow 3 \rightarrow 3 \rightarrow 7 \rightarrow 7 \\ 3 \rightarrow 6 \rightarrow 6 \rightarrow 6 \rightarrow 6 \rightarrow 4 \\ 4 \rightarrow 4 \rightarrow 4 \rightarrow 4 \rightarrow 4 \rightarrow 8 \\ 5 \rightarrow 5 \rightarrow 8 \rightarrow 8 \rightarrow 8 \rightarrow 6 \\ 6 \rightarrow 7 \rightarrow 7 \rightarrow 1 \rightarrow 5 \rightarrow 5 \\ 7 \rightarrow 2 \rightarrow 2 \rightarrow 2 \rightarrow 2 \rightarrow 2 \\ 8 \rightarrow 8 \rightarrow 5 \rightarrow 7 \rightarrow 1 \rightarrow 1 \end{array}$$

12. Show that the inverse of  $(a_1 a_2 \cdots a_k)$  in  $\Sigma_n$  is  $(a_1 a_k a_{k-1} \cdots a_3 a_2)$ .

**Solution:**

We multiply ...

$$\begin{array}{cccc} a_1 & \rightarrow & a_2 & \rightarrow & a_1 \\ a_2 & \rightarrow & a_3 & \rightarrow & a_2 \\ a_3 & \rightarrow & a_4 & \rightarrow & a_3 \\ & & \vdots & & \\ a_{k-1} & \rightarrow & a_k & \rightarrow & a_{k-1} \\ a_k & \rightarrow & a_1 & \rightarrow & a_k \end{array}$$

Where  $a_1 \rightarrow a_2$  means  $a_1$  maps to  $a_2$ .

Therefore,  $(a_1 a_2 a_3 \cdots a_{k-1} a_k)(a_1 a_k a_{k-1} \cdots a_3 a_2) = (a_1)(a_2)(a_3) \cdots (a_{k-1})(a_k) = (1)$

13. Let  $\tau$  be a transposition and let  $\sigma \in \Sigma_n$ . Prove that  $\sigma\tau\sigma^{-1}$  is a transposition.

**Solution:** Write  $\tau = (ij)$  where  $i, j \in \{1, 2, \dots, n\}, i \neq j$ . Let  $l, k \in \{1, 2, \dots, n\}$  such that  $\sigma(l) = i$  and  $\sigma(k) = j$ . Then  $l \neq k$  and  $\sigma^{-1}(i) = l, \sigma^{-1}(j) = k$ . Consider  $\sigma\tau\sigma^{-1}$ . We have

$$(\sigma\tau\sigma^{-1})(l) = \sigma^{-1}(\tau(\sigma(l))) = \sigma^{-1}(\tau(i)) = \sigma^{-1}(j) = k,$$

and

$$(\sigma\tau\sigma^{-1})(k) = \sigma^{-1}(\tau(\sigma(k))) = \sigma^{-1}(\tau(j)) = \sigma^{-1}(i) = l.$$

Furthermore, for any  $t \in \{1, 2, \dots, n\}, t \neq l, k$  we have  $\sigma(t) \neq i, j$  so  $\tau(\sigma(t)) = \sigma(t)$ . Therefore,

$$(\sigma\tau\sigma^{-1})(t) = \sigma^{-1}(\tau(\sigma(t))) = \sigma^{-1}(\sigma(t)) = t.$$

Thus,  $\sigma\tau\sigma^{-1} = (kl)$ .

14. Let  $\sigma$  and  $\tau$  be disjoint cycles in  $\Sigma_n$ . Prove that  $\sigma\tau = \tau\sigma$ .

**Solution:** We will look at how  $\sigma$  and  $\tau$  act on each  $m \in \{1, \dots, n\}$  separately, and deduce the desired result.

Since  $\sigma, \tau$  are disjoint, at most one of  $\sigma, \tau$  acts nontrivially on  $m$ . Without loss of generality, assume that  $\tau$  fixes  $m$ . Because  $\sigma, \tau$  are disjoint, we know that  $\tau$  must also fix  $\sigma(m)$  which means

$$\tau \circ \sigma(m) = \sigma(m) = \sigma \circ \tau(m)$$

This holds for every  $m \in \{1, \dots, n\}$ , so we conclude that  $\tau\sigma = \sigma\tau$ .

15. (a) Let  $\sigma$  and  $\tau$  be disjoint cycles in  $\Sigma_n$  with  $\sigma^k = \tau^m = (1)$ . Prove  $(\sigma\tau)^{\text{lcm}(k,m)} = (1)$ .  
 (b) Find an example which shows that the disjoint condition above is necessary, i.e., find  $\sigma, \tau \in \Sigma_n$  with  $\sigma^k = \tau^m = (1)$  but  $(\sigma\tau)^{\text{lcm}(k,m)} \neq 1$ .

**Solution:**

- (a) Given that  $\sigma$  and  $\tau$  are disjoint, we can use the fact that we can commute these cycles, which was proven in the last problem. Thus we can see that for  $l = \text{lcm}(k, m)$ , we have the following equalities.

$$\begin{aligned}
 (\sigma\tau)^l &= (\sigma\tau)(\sigma\tau) \cdots (\sigma\tau) \\
 &= \sigma\tau\sigma\tau \cdots \sigma\tau \\
 &= \sigma\sigma\tau\tau\sigma\sigma \cdots \tau\tau \\
 &= \sigma\sigma\tau\sigma\tau\sigma \cdots \tau\tau \\
 &= \sigma\sigma\sigma\tau\tau\tau \cdots \tau\tau \\
 &\vdots \\
 &= \sigma^l \tau^l \\
 &= (\sigma^k)^a (\tau^m)^b, \text{ for } a, b \in \mathbf{R} \text{ such that } ka = mb = l \\
 &= (1)^a (1)^b \\
 &= (1)
 \end{aligned}$$

Thus we have shown that  $(\sigma\tau)^{\text{lcm}(k,m)} = (1)$ .

- (b) Take  $\sigma = (123)$  and  $\tau = (124)$ . Since these are three cycles, we know  $\sigma^3 = \tau^3 = (1)$ , which can be verified by the reader. We also know that  $\text{lcm}(3, 3) = 3$ . Now we will consider  $((123)(124))^3$ .

$$\begin{aligned}
 ((123)(124))^3 &= ((13)(24))^3 \\
 &= (13)(24)(13)(24)(13)(24) \\
 &= (13)(24)(24)(13)(13)(24) \\
 &= (13)(1)(1)(24) \\
 &= (13)(24) \\
 &\neq (1)
 \end{aligned}$$

Thus we have found  $\sigma, \tau \in \Sigma_n$  with  $\sigma^k = \tau^m = (1)$  but  $(\sigma\tau)^{\text{lcm}(k,m)} \neq (1)$ .

16. If  $R$  is any ring, then the center of the ring  $R$  is the set  $C = \{c \in R \mid cr = rc \forall r \in R\}$ .

- (a) Show  $C$  is a subring of  $R$ .  
 (b) A subring  $I$  of  $R$  is a left ideal provided  $r \in R$  and  $x \in I \implies rx \in I$ . A subring  $I$  of  $R$  is a right ideal provided  $r \in R$  and  $x \in I \implies xr \in I$ .  $I$  is an ideal if it is both a left and right ideal. Show that  $C$  may not be an ideal.

**Solution:**

- (a) Notice that  $1r = r1$  for all  $r \in R$ , so  $1 \in C$ . Therefore  $C \neq \emptyset$ . Let  $a \in C$ . Then  $ar = ra$  for all  $r \in R$ . So  $ra^{-1} = a^{-1}(ar)a^{-1} = a^{-1}(ra)a^{-1} = a^{-1}r$  for all  $r \in R$ . So  $a^{-1} \in C$ . Let  $b \in C$  and consider the element  $ab$ . Then  $abr = arb = rab$ , so  $ab \in C$ . Also,  $(a+b)r = ar + br = ra + rb = r(a+b)$ , so  $a+b \in C$ . Thus,  $C$  is a subring of  $R$ .

(b) In #41 we show that the center of the ring of quaternions is  $\mathbb{R}$ . Since  $i = i \cdot 1 \notin \mathbb{R}$  even though  $1 \in \mathbb{R}$  and  $i$  is in the ring of quaternions, we have that the center of the ring of quaternions is not an ideal.

17. An element  $r$  in a ring  $R$  is idempotent if  $r^2 = r$ . If  $r \in R$  is an idempotent element and  $x \in R$  then  $(xr - rrx)^2 = 0_R$ .

**Solution:** Since  $R$  may not be commutative, we must be careful to 'foil' everything out. Then

$$\begin{aligned} (xr - rrx)^2 &= (xr - rrx)(xr - rrx) \\ &= xrxr - rrrxr - rrxrx + rrrrx \\ &= xrxr - rrxr - rrxrx + rrxrx \\ &= 0_R \end{aligned}$$

18. An element  $a$  of a ring  $R$  is nilpotent if  $a^n = 0$  for some positive integer  $n$ .

(a) Prove that in a commutative ring  $a + b$  is nilpotent if  $a$  and  $b$  are.

(b) Show that this result may be false if  $R$  is not commutative.

(c) Prove that  $R$  has no nonzero nilpotent elements if and only if  $0_R$  is the unique solution of the equation  $x^2 = 0_R$ .

**Solution:**

(a) Let  $a$  and  $b$  be nilpotent, say  $a^{n_a} = 0$  and  $b^{n_b} = 0$ . Consider  $(a + b)^{n_a + n_b} = \sum_{i=0}^{n_a + n_b} \binom{n_a + n_b}{i} a^{n_a + n_b - i} b^i$  since  $R$  is commutative. Notice that when  $i \leq n_b$ ,  $n_a + n_b - i \geq n_a$ , so  $a^{n_a + n_b - i} = 0$ . When  $i > n_b$ ,  $b^i = 0$ . Thus, for all  $i$ ,  $a^{n_a + n_b - i} b^i = 0$ . Therefore,  $(a + b)^{n_a + n_b} = 0$ . So  $a + b$  is nilpotent.

(b) Let  $R$  be the ring of  $2 \times 2$  matrices over  $\mathbb{R}$  and consider the elements  $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ,  $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ . Then  $a^2 = b^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ . However,  $a + b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  and  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^n \in \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$  for all  $n$ . So  $a + b$  is not nilpotent.

(c) If  $R$  has no nonzero nilpotent elements, then  $0_R$  is the only solution to  $x^2 = 0_R$  (as any other solution would be a nonzero nilpotent of  $R$ ). Suppose the unique solution of the equation  $x^2 = 0_R$  is  $0_R$ . Suppose, by way of contradiction, that  $a$  is a nonzero nilpotent of  $R$ . Then  $a^n = 0_R$  for some  $n > 0$ . We may assume  $n$  is minimal, that is,  $a^m \neq 0_R$  for any  $m < n$ . Then  $(a^{n-1})^2 = a^{2n-2} = a^n a^{n-2} = 0_R$  and  $a^{n-1} \neq 0_R$ , contradicting that  $0_R$  is the unique solution.

19. Let  $R$  be a ring in which  $x^3 = x \forall x \in R$ . Prove that  $R$  is commutative.

**Solution:** Let  $R$  be a ring such that  $x^3 = x$  for all  $x \in R$ .

**Claim 1** If  $y^2 = 0$  for some  $y \in R$ , then  $y = 0$ . **Pf:**  $y = y^3 = yy^2 = y0 = 0$ .

**Claim 2**  $y^2$  is idempotent ( $(y^2)^2 = y^2$ ) for all  $y \in R$ . **Pf:**  $(y^2)^2 = y^4 = yy^3 = yy = y^2$ .

**Claim 3**  $xy^2 = y^2x$  for all  $x, y \in R$ . **Pf:** By claim 2 and #17,  $(xy^2 - y^2xy^2)^2 = 0$  and by a similar proof,  $(y^2x - y^2xy^2)^2 = 0$ . Then by Claim 1,  $xy^2 - y^2xy^2 = 0 = y^2x - y^2xy^2$ .

Let  $x, z \in R$ . Then  $x(z + z^2) = (z + z^2)x$  by Claim 3. So  $x(2z^2 + 2z) = (2z^2 + 2z)x$  (multiplying out and simplifying with claim 2 and the assumption on  $R$ ). Since  $z^2x = xz^2$ ,  $2z^2x = 2xz^2 = x(2z^2)$ . Therefore,  $x(2z) = 2xz = (2z)x = 2zx$ . Also, since  $(z + z^2)^3 = z + z^2$  by the assumption on  $R$ , multiplying out and simplifying, yields  $3z^2 + 3z = 0$ . So  $x(3z^2 + 3z) = x0 = 0x = (3z^2 + 3z)x$ . And again,  $x$  commutes with  $z^2$ , so  $3xz = 3zx$ . Therefore,  $xz = 3xz - 2xz = 3zx - 2zx = zx$ . Therefore,  $x$  and  $z$  commute for all  $x, z \in R$ , so  $R$  is commutative.

20. Let  $G$  be a group. If  $a, b, c \in G$ , prove that there is a unique element  $x \in G$  such that  $axb = c$ .

**Solution:** Let  $x = a^{-1}cb^{-1}$ . Then  $axb = a(a^{-1}cb^{-1})b = c$ . Suppose  $y$  is such that  $ayb = c = axb$ . Then  $y = a^{-1}(ayb)b^{-1} = a^{-1}cb^{-1} = a^{-1}(axb)b^{-1} = x$ . Thus,  $x$  is unique.

21. Let  $G$  be a group. If  $a, b \in G$  with  $b^6 = e$  and  $ab = b^4a$ , prove that  $b^3 = e$  and  $ab = ba$ .

**Solution:**

$$\begin{aligned}
 a &= ae \\
 &= ab^6 \\
 &= b^4ab^5 \\
 &= b^8ab^4 \\
 &= b^{12}ab^3 \\
 &= (b^6)^2ab^3 \\
 &= ab^3
 \end{aligned}$$

Thus,  $e = a^{-1}a = a^{-1}(ab^3) = b^3$  and  $ab = b^4a = b^3(ba) = e(ba) = ba$ .

22. Let  $G$  be a group. If  $(ab)^n = a^n b^n$  for three consecutive integers  $n$  and for all  $a, b \in G$ , prove that  $G$  is abelian.

**Solution:** Let  $n \in \mathbb{Z}$  such that  $(ab)^n = a^n b^n$ ,  $(ab)^{n+1} = a^{n+1} b^{n+1}$ , and  $(ab)^{n+2} = a^{n+2} b^{n+2}$  for all  $a, b \in G$ . Then,

$$\begin{aligned}
 ab &= (ab)^n (ab)^{-(n-1)} = a^n b^n (ab)^{-n+1} \\
 &= (ab)^{n+1} (ab)^{-n} = a^{n+1} b^{n+1} (ab)^{-n} \\
 &= (ab)^{n+2} (ab)^{-n-1} = a^{n+2} b^{n+2} (ab)^{-n-1}
 \end{aligned}$$

Then

$$\begin{aligned}
 b^n &= a^{-n} a^n b^n (ab)^{-n+1} (ab)^{n-1} \\
 &= a^{-n} a^{n+1} b^{n+1} (ab)^{-n} (ab)^{n-1} \\
 &= ab^{n+1} (ab)^{-1} \\
 &= ab^n a^{-1}
 \end{aligned}$$

Similarly,

$$\begin{aligned}
 b^{n+1} &= a^{-(n+1)} (a^{n+1} b^{n+1} (ab)^{-n}) (ab)^n \\
 &= a^{-(n+1)} (a^{n+2} b^{n+2} (ab)^{-n-1}) (ab)^n \\
 &= ab^{n+2} (ab)^{-1} \\
 &= ab^{n+1} a^{-1}
 \end{aligned}$$

So  $ab^n = b^n a$  and  $ab^{n+1} = b^{n+1} a$ . Then  $ab^{n+1} = b^n ab = b^{n+1} a$ , so  $ab = ba$ .

23. Let  $G$  be a nonempty set equipped with an associative operation with the properties

- i. There is an element  $e \in G$  such that  $ea = a$  for all  $a \in G$ .
- ii. For each  $a \in G$  there exists  $d \in G$  such that  $da = e$ .

Show that  $G$  is a group.

**Solution:** To show that  $G$  is a group, we will show that the  $e$  in i. is the identity (also on the right side), and that the assumed left inverses from ii. are also right inverses. Let  $a \in G$ . Then by ii., there is some  $d \in G$  so that  $da = e$ . Also by ii., there is some  $f \in G$  so that  $fd = e$ . Notice that  $(da)e = ee = e = da$ , so  $f(dae) = (fd)ae = eae = ae = f(da) = (fd)a = ea = a$ . Therefore,  $e$  is also the right identity. Then  $a = ea = (fd)a = f(da) = fe = f$  (since  $e$  is also the right identity). So  $a = f$  and  $ad = fd = a$ . Thus,  $d$  which is the left inverse of  $a$  is also the right inverse. Therefore,  $G$  is a nonempty set with an associative property, an identity (left and right), and each element has an inverse (left and right). Thus,  $G$  is a group.

24. Let  $G$  be a cyclic group. Prove that every subgroup of  $G$  is cyclic.

**Solution:** We show in #26 that a cyclic group  $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ . Let  $H$  be a subgroup of  $G$ . If  $H = \{1\}$ , then  $H = \langle 1 \rangle$  and is cyclic, so suppose  $H$  is nontrivial. Let  $N = \{n \in \mathbb{N} \mid a^n \in H\}$ . Since  $H$  is nontrivial, there is some  $a^n \in H$  where  $n \neq 0$ . Then, since  $H$  is a subgroup of  $G$ ,  $a^{-n} \in H$ . Then one of  $n, -n > 0$ , so  $N$  is nonempty. Since every nonempty set of the natural numbers has a least element, there is some  $m \in N$  minimal. We claim  $H = \langle a^m \rangle$ . Since  $a^m \in H$ ,  $\langle a^m \rangle \subseteq H$ . Let  $1 \neq x \in H$ . Then  $x \in G$ , so  $x = a^n$  for some  $n \neq 0$ . By replacing  $x$  with  $x^{-1}$  if need be, we may assume  $n > 0$ . Write  $n = km + r$  where  $k \in \mathbb{Z}$  and  $0 \leq r < m$ . Then  $a^n = (a^m)^k a^r \in H$ . Since  $a^m \in H$ ,  $a^{-km} \in H$ . So  $a^r = a^{-km} a^n \in H$ . If  $r \neq 0$ , then  $r \in N$  and  $r < m$ , contradicting the minimality of  $m$ . Thus,  $r = 0$ . So  $a^n = (a^m)^k \in \langle a^m \rangle$ . Therefore,  $x, x^{-1} \in \langle a^m \rangle$ . So  $H = \langle a^m \rangle$  is cyclic.

25. Prove that if  $G$  is a cyclic group, then  $G$  is abelian.

**Solution:** Again, we prove this problem assuming #26. Let  $G = \langle a \rangle$  be cyclic and let  $x, y \in G$ . Since  $G = \{a^n \mid n \in \mathbb{Z}\}$ ,  $x = a^n, y = a^m$  for some  $n, m \in \mathbb{Z}$ . Then  $xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx$ . Therefore,  $G$  is abelian.

26. Prove that if  $G = \langle a \rangle$  is a cyclic group then  $G = \{a^n \mid n \in \mathbb{Z}\}$ .

**Solution:** Let  $G = \langle a \rangle$  be a cyclic group and let  $H = \{a^n \mid n \in \mathbb{Z}\}$ . Since  $G$  contains  $a$ ,  $G$  must contain all the elements of  $H$  since  $G$  is closed under the operation. In fact, any group containing  $a$  must contain  $H$ . Since  $a \in H$ ,  $H \neq \emptyset$ . For any  $a^n, a^m \in H$ ,  $a^n a^m = a^{n+m} \in H$  and  $a^{-n} \in H$ , so  $H$  is a subgroup of any group containing  $a$ . Since  $G$  is the smallest subgroup containing  $a$ ,  $G \subseteq H$ . Therefore,  $G = H$ .

In the following (#27 – #35), let  $R$  be a commutative ring with identity and the notation is that that is used on the second page of the paper.

27. Let  $n \geq 4$ . Determine the number of permutations in  $\Sigma_n$  which are the product of two disjoint transpositions.

**Solution:** In order to get the product of two disjoint transposition, you must first choose four of the  $n$  elements to permute, and there are  $\binom{n}{4}$  ways of doing this. In order to make these four elements into two disjoint transpositions, it is enough to choose two of the four elements to put into the first transposition, so there are  $\binom{4}{2}$  ways of doing that. However, since disjoint cycles commute, we can permute our disjoint transpositions and still have the same group element, so we have two ways of writing each distinct product. Hence there are

$$\frac{\binom{n}{4} \binom{4}{2}}{2} = \frac{n(n-1)(n-2)(n-3)}{8}$$

permutations in  $\Sigma_n$  which are the product of two disjoint transpositions.

28. Determine all subgroups of

- (a)  $\Sigma_2$
- (b)  $\Sigma_3$

**Solution:**

- (a) Since subgroups must contain the identity, and  $\Sigma_2 = \{(1), (1, 2)\}$ , the only other possibilities for subgroups are the identity by itself or with  $(1, 2)$ . As  $\{(1)\}$  is the trivial subgroup, and  $\{(1), (1, 2)\}$  is all of  $\Sigma_2$ , which we know is a subgroup, both of these possibilities are indeed subgroups. Thus, the subgroups of  $\Sigma_2$  are

$$H_1 = \{(1)\} \quad \text{and} \quad H_2 = \{(1), (1, 2)\}.$$

- (b) The trivial group is a subgroup of every group. Also, if we look at cyclic subgroups generated by single elements, we get the subgroups  $\langle(1, 2)\rangle, \langle(1, 3)\rangle, \langle(2, 3)\rangle, \langle(1, 2, 3)\rangle$ . Now, if  $K$  is a subgroup containing two distinct transpositions, then  $K$  must contain a three-cycle, because  $(1, 2)((1, 3) = (1, 2, 3), (1, 2)(2, 3) = (1, 3, 2), (1, 3)(2, 3) = (1, 3, 2)$ , and hence  $K$  contains  $\langle(1, 2, 3)\rangle$ , so  $|K| > 3$ . Since the order of a subgroup must divide the order of a group, we know that  $|K| = 6$ , and hence  $K = \Sigma_3$ . Similarly, if  $K$  contains a transposition and a three cycle,  $|K| > 3$  implies that  $K = \Sigma_3$ . Since the only options for subgroups of  $\Sigma_3$  must contain no transpositions, one transposition, or more than one transposition, and either no three-cycles or two three cycles, we must have exhausted all possible subgroups above.

Hence, the subgroups of  $\Sigma_3$  are

$$\begin{aligned} H_1 &= \{(1)\}, & H_2 &= \langle(1, 2)\rangle = \{(1), (1, 2)\}, & H_3 &= \langle(1, 3)\rangle = \{(1), (1, 3)\}, \\ H_4 &= \langle(2, 3)\rangle = \{(1), (2, 3)\}, & H_5 &= \langle(1, 2, 3)\rangle = \{(1), (1, 2, 3), (1, 3, 2)\}, \\ H_6 &= \Sigma_3 = \{(1), (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}. \end{aligned}$$

29. Prove that  $\Sigma_n$  is not cyclic for  $n \geq 3$ .

**Solution:** Suppose that  $\Sigma_n$  is cyclic for some  $n \geq 3$ . Then there is an element  $\sigma \in \Sigma_n$  such that  $\Sigma_n = \langle\sigma\rangle$ . Then we know that we can find natural numbers  $r$  and  $s$  so that  $\sigma^r = (1, 2)$  and  $\sigma^s = (1, 3)$ . Thus,  $\sigma^{r+s} = \sigma^r \sigma^s = (1, 2)(1, 3) = (1, 2, 3)$ , but  $\sigma^{r+s} = \sigma^{s+r} = \sigma^s \sigma^r = (1, 3)(1, 2) = (1, 3, 2)$ . This says that  $(1, 2, 3) = (1, 3, 2)$ , which is a contradiction. Hence, the assumption that  $\Sigma_n$  is cyclic must be a bad one, so  $\Sigma_n$  is not cyclic for any  $n \geq 3$ .

30. For  $n \geq 2$ , prove  $n = 2 \Leftrightarrow C_n = \Sigma_n$ .

**Solution:**

( $\Leftarrow$ ) Suppose that  $n = 2$ . Then  $C_n = \langle(1, 2)\rangle = \{(1), (1, 2)\} = \Sigma_n$ .

( $\Rightarrow$ ) Suppose that  $C_n = \Sigma_n$ . Then  $|C_n| = |\Sigma_n|$ , which means that  $n = n!$ , so  $1 = (n - 1)!$ . However, this means that  $n - 1$  is either zero or one, so  $n$  is either 1 or two. As we are given that  $n \geq 2$ , it must be that  $n = 2$ .

31. Prove  $P_n(R)$  is a subgroup of  $\Sigma_n$ .

**Solution:** In order to see that  $P_n(R)$  is a subgroup, we need to show that it contains the identity, and that it is closed under multiplication and inverses.

Suppose that  $x_1 x_2 \dots x_n = 0$ , for  $x_i \in R$ . If  $\sigma = (1)$ , then  $x_{\sigma(1)} x_{\sigma(2)} \dots x_{\sigma(n)} = x_1 x_2 \dots x_n = 0$ , so  $\sigma$  is in  $P_n(R)$ .

Suppose that  $\sigma_1$  and  $\sigma_2$  are in  $P_n(R)$ . Then if  $x_1 x_2 \dots x_n = 0$ , we have that  $x_{\sigma_1(1)} x_{\sigma_1(2)} \dots x_{\sigma_1(n)} = 0$ , since  $\sigma_1 \in P_n(R)$ . Also, if we write  $x_{\sigma_1(1)} x_{\sigma_1(2)} \dots x_{\sigma_1(n)}$  as  $y_1 \dots y_n$ , then we have that  $y_1 \dots y_n = 0$ , and since  $\sigma_2 \in P_n(R)$ , we have that  $y_{\sigma_2(1)} \dots y_{\sigma_2(n)} = 0$ . Plugging back in for  $y_i$  yields that  $x_{\sigma_2(\sigma_1(1))} x_{\sigma_2(\sigma_1(2))} \dots x_{\sigma_2(\sigma_1(n))} = 0$ . Thus,  $\sigma_2 \sigma_1 \in P_n(R)$ , so  $P_n(R)$  is closed under multiplication.

Lastly, if  $\sigma \in P_n(R) \subseteq \Sigma_n$  is not  $(1)$ , then  $\Sigma_n$  has finite order, which means that  $\sigma$  has finite order, so there is some integer  $m \geq 2$  (since  $\sigma \neq (1)$ ) such that  $\sigma^m = (1)$ . Then  $\sigma^{m-1} = \sigma^{-1}$ . Since  $\sigma$  is in  $P_n(R)$ , we showed above that  $P_n(R)$  is closed under multiplication, and  $m \geq 2$ , we know that  $m-1 \geq 1$ , and hence  $\sigma^{m-1} \in P_n(R)$ . Thus,  $\sigma^{-1} = \sigma^{m-1} \in P_n(R)$ , and so  $P_n(R)$  is closed under inverses.

32. Show that if  $(1, 2) \in P_3(R)$ , then  $P_3(R) = \Sigma_3$ .

**Solution:** Suppose that  $x_1 x_2 x_3 = 0$  for  $x_i \in R$ . Since  $1 \in R$ , we have  $(x_1 x_2) x_3 1 = 0$ . Moreover, since  $(1, 2) \in P_3(R)$ ,  $x_3 (x_1 x_2) 1 = 0$ , so  $x_3 x_1 x_2 = 0$ . Therefore,  $x_1 x_2 x_3 = 0$  implies that  $x_3 x_1 x_2 = 0$ , and so  $(1, 3, 2) \in P_3(R)$ . From 28.b), we know that the only subgroup of  $\Sigma_3$  containing  $(1, 2)$  and  $(1, 3, 2)$  is  $\Sigma_3$ , so  $P_3(R) = \Sigma_3$ .

33. Show that  $P_3(R) \in \{I_3, \Sigma_3, C_3\}$ .

**Solution:** Suppose that  $P_3(R) \notin \{I_3, \Sigma_3\}$ .

Generalizing 32., we can prove that if  $P_3(R)$  contains any transposition, then  $P_3(R) = \Sigma_3$ : If  $(1, 3) \in P_3(R)$ , then

$$x_1x_2x_3 = 0 \Leftarrow (x_1x_2)1x_3 = 0 \Leftarrow x_31(x_1x_2) = 0 \Leftarrow x_3x_1x_2 = 0,$$

so  $(1, 3, 2) \in P_3(R)$ ; If  $(2, 3) \in P_3(R)$ , then

$$x_1x_2x_3 = 0 \Leftarrow 1x_1(x_2x_3) = 0 \Leftarrow 1(x_2x_3)x_1 = 0 \Leftarrow x_2x_3x_1 = 0 \Leftarrow (1, 2, 3) \in P_3(R).$$

Again, by 28 b), both of these cases mean that  $P_3(R) = \Sigma_3$ .

Now, by the assumption that  $P_3(R) \notin \{I_3, \Sigma_3\}$ , we know that  $P_3(R)$  contains no transpositions. However,  $P_3(R) \neq I_3$  implies that there is non-identity element in  $P_3(R)$ . By 28 b), we know that there is only one subgroup of  $\Sigma_3$  that is not trivial and contains no transpositions, and it is  $\{(1), (1, 2, 3), (1, 3, 2)\} = \langle (1, 2, 3) \rangle$ , the cyclic subgroup generated by  $(1, 2, 3)$ . Thus,  $P_3(R) = C_3$ .

Therefore,  $P_3(R) \in \{I_3, \Sigma_3, C_3\}$ .

36. Let  $G$  be the subgroup  $M_2(\mathbb{C})$  generated by  $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  and  $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ .

- (a) Show  $G$  is a non-abelian group of order 8.
- (b) Show that  $G$  is isomorphic to the quaternion group.

**Solution:**

- (a) We construct the Cayley Table for  $G$  below. To do so, we begin with a table with three rows labelled  $I, A$ , and  $B$  and three columns labelled  $I, A$ , and  $B$ . We begin filling in the table, introducing a new letter for each element which doesn't already appear. Each time a new letter is introduced, a new row and column is added to the table with this label. In this way we ensure that  $G$  is a non-abelian group of order 8 (notice that  $AB \neq BA$ ).

	$I$	$A$	$B$	$C$	$D$	$E$	$F$	$G$
$I$	$I$	$A$	$B$	$C$	$D$	$E$	$F$	$G$
$A$	$A$	$C$	$D$	$E$	$F$	$I$	$G$	$B$
$B$	$B$	$G$	$C$	$F$	$A$	$D$	$I$	$E$
$C$	$C$	$E$	$F$	$I$	$G$	$A$	$B$	$D$
$D$	$D$	$B$	$E$	$G$	$C$	$F$	$A$	$I$
$E$	$E$	$I$	$G$	$A$	$B$	$C$	$D$	$F$
$F$	$F$	$D$	$I$	$B$	$E$	$G$	$C$	$A$
$G$	$G$	$F$	$A$	$D$	$I$	$B$	$E$	$C$

Where  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ,  $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ,  $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ ,  $C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ ,  $D = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ ,  $E = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ,  $F = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$ ,  $G = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$ .

- (b) Consider the map,  $\varphi : G \rightarrow Q_8$ , given by:

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &\mapsto 1, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \mapsto -1, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \mapsto i, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \mapsto -i, \\ \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} &\mapsto j, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \mapsto -j, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \mapsto k, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \mapsto -k. \end{aligned}$$

Applying this identification to the Cayley table for  $G$  above yields the Cayley table for  $Q_8$ . Therefore,  $\varphi$  is a group isomorphism between  $G$  and  $Q_8$ .

37. Let  $G$  be the subgroup  $M_2(\mathbb{C})$  generated by  $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  and  $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ .

- (a) Show  $G$  is a non-abelian group of order 8.  
 (b) Show that  $G$  is not isomorphic to the quaternion group.

**Solution:**

- (a) As in #36, we construct the Cayley table for  $G$  which demonstrates that  $G$  is a non-abelian group of order 8.

	$I$	$A$	$B$	$C$	$D$	$E$	$F$	$G$
$I$	$I$	$A$	$B$	$C$	$D$	$E$	$F$	$G$
$A$	$A$	$C$	$D$	$E$	$F$	$I$	$G$	$B$
$B$	$B$	$G$	$I$	$F$	$E$	$D$	$C$	$A$
$C$	$C$	$E$	$F$	$I$	$G$	$A$	$B$	$D$
$D$	$D$	$B$	$A$	$G$	$I$	$F$	$E$	$C$
$E$	$E$	$I$	$G$	$A$	$B$	$C$	$D$	$F$
$F$	$F$	$D$	$C$	$B$	$A$	$G$	$I$	$E$
$G$	$G$	$F$	$E$	$D$	$C$	$B$	$A$	$I$

Where  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ,  $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ,  $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ,  $C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ ,  $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ,  $E = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ,  $F = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$ ,  $G = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ .

- (b) There are numerous ways to demonstrate this. One way is to note that the elements  $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$  and  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  in  $G$  are distinct elements of order 2. Since  $Q_8$  contains only one element of order 2, namely  $-1$ , it must be that  $G \not\cong Q_8$ .

38. Determine all subgroups of  $Q_8$ .

**Solution:** Since  $Q_8$  has order 8, the only possible orders for its subgroups are 1, 2, 4, and 8. The unique subgroups of order 1 and 8 are  $\{1\}$  and  $Q_8$ , respectively. Since  $-1$  is the only element in  $Q_8$  of order 2,  $\{1, -1\}$  is the unique subgroup of order 2. Again since  $-1$  is the only element of order 2, all subgroups of order 4 must be cyclic. So the remaining subgroups of  $Q_8$  are  $\{1, -1, i, -i\}$ ,  $\{1, -1, j, -j\}$ , and  $\{1, -1, k, -k\}$ .

39. If  $G$  is a group, then  $C = \{a \in G \mid ax = xa, \forall x \in G\}$  is called the center of  $G$ .

- (a) Show  $C$  is an abelian subgroup of  $G$ .  
 (b) What is the center of  $Q_8$ ?

**Solution:**

- (a) Since  $1 \cdot x = x \cdot 1, \forall x \in G$ , we have that  $1 \in C$ , hence  $C \neq \phi$ .  
 Let  $a, b \in C$ . So for all  $x \in G$ , we have

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$$

Thus  $ab \in C$ , hence  $C$  is closed under multiplication.

Let  $a \in C$ . So for all  $x \in G$ , we have

$$a^{-1}x = a^{-1}x(a \cdot a^{-1}) = a^{-1}(xa)a^{-1} = a^{-1}(ax)a^{-1} = (a^{-1} \cdot a)xa^{-1} = xa^{-1}.$$

Thus  $a^{-1} \in C$ , hence  $C$  is closed under inverses. Therefore  $C$  is a subgroup of  $G$ .

(b) The center of  $Q_8$  is  $\{1, -1\}$ . To see this, we first note that  $1 \cdot x = x \cdot 1$  and  $-1 \cdot x = x \cdot -1$  for all  $x \in Q_8$ , so  $\{1, -1\}$  is contained in the center. To see that these are all the elements of the center, we consider each remaining element of  $Q_8$  separately. Since  $ij \neq ji$ , neither  $i$  nor  $j$  can be in the center. Similarly,  $(-i)j \neq j(-i)$ ,  $i(-j) \neq (-j)i$ ,  $ik \neq ki$ ,  $i(-k) \neq (-k)i$ . So no other elements of  $Q_8$  commute with every element of  $Q_8$ .

40. Let  $q \in \mathbb{H}$ . Prove that  $qi = iq \Leftrightarrow q \in \mathbb{C}$ .

**Solution:** Suppose  $qi = iq$ . Write  $q = a + bi + cj + dk$ , where  $a, b, c, d \in \mathbb{R}$ . So we have

$$\begin{aligned} qi &= iq \\ (a + bi + cj + dk)i &= i(a + bi + cj + dk) \\ -b + ai + dj - ck &= -b + ai - dj + ck \end{aligned}$$

From this we get that  $c = -c$  and  $d = -d$ , hence  $c = d = 0$ . Thus  $q = a + bi \in \mathbb{C}$ .

Suppose  $q \in \mathbb{C}$ . Write  $q = a + bi$ , where  $a, b \in \mathbb{R}$ . So we have

$$qi = (a + bi)i = -b + ai = i(a + bi) = iq.$$

This completes the proof.

41. Determine the center of  $\mathbb{H}$ .

**Solution:** Denote the center of  $\mathbb{H}$  by  $C$ . First note that for all  $r \in \mathbb{R}$ ,  $rx = xr$ ,  $\forall x \in \mathbb{H}$ . Thus  $\mathbb{R} \subseteq C$ . From #40, we get that  $C \subseteq \mathbb{C}$ , since elements in  $C$  must commute with  $i$ . By an argument similar to #40 (replacing  $i$  with  $j$ ), we get that  $Cj = jC \Leftrightarrow C \subseteq \mathbb{R}[j]$ . Thus  $C \subseteq \mathbb{R}[j]$ , hence  $C \subseteq \mathbb{R}[j] \cap \mathbb{C} = \mathbb{R}$ . Thus  $C = \mathbb{R}$ .

42. Determine conditions on  $a, b, c, d \in \mathbb{R}$  so that  $q^2 = -1$  where  $q = a + bi + cj + dk$ .

**Solution: Claim:**  $q^2 = -1 \Leftrightarrow a = 0$  and  $b^2 + c^2 + d^2 = 1$ .

**Proof:** Suppose  $q^2 = -1$ . Since computation yields

$$q^2 = (a + bi + cj + dk)^2 = (a^2 - b^2 - c^2 - d^2) + 2abi + 2acj + 2adk,$$

we get that  $a^2 - b^2 - c^2 - d^2 = -1$  and that  $ab = ac = ad = 0$ . If  $a \neq 0$ , then  $b = c = d = 0$ , hence  $a^2 = -1$ . Since  $a \in \mathbb{R}$ , this is a contradiction. Thus  $a = 0$ , so  $b^2 + c^2 + d^2 = 1$ .

Suppose  $a = 0$  and  $b^2 + c^2 + d^2 = 1$ . So we have that

$$q^2 = (bi + cj + dk)^2 = -b^2 - c^2 - d^2 = -1.$$

This completes the proof of the claim.

43. Show that the equation  $x^2 = -1$  has infinitely many solutions in  $\mathbb{H}$ .

**Solution:** From #42, we have that solutions to the equation  $x^2 = -1$  in  $\mathbb{H}$  are in one-to-one correspondence with points on the unit sphere. Since there are infinitely many points on the unit sphere, the result follows.

44. Prove that  $\mathbb{H}$  is a division ring.

**Solution:** Let  $q \in \mathbb{H} \setminus \{0\}$ . Write  $q = a + bi + cj + dk$ , where  $a, b, c, d \in \mathbb{R}$ . Consider the element  $q' := \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} \in \mathbb{H}$ . (Note: Since  $q \neq 0$ ,  $a^2 + b^2 + c^2 + d^2 \neq 0$ .) So we have that

$$q \cdot q' = (a + bi + cj + dk) \left( \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} \right) = 1 = \left( \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} \right) (a + bi + cj + dk) = q' \cdot q$$

Thus  $q$  has an inverse in  $\mathbb{H}$ . Therefore  $\mathbb{H}$  is a division ring.

45. Prove that  $R[x]$  is a commutative ring with identity whenever  $R$  is.

**Solution:** We know  $R[x]$  is a ring. Suppose  $R$  is commutative with identity. Let  $a, b \in R[x]$  and write  $a = (a_0, a_1, \dots, a_n, 0, \dots)$  and  $b = (b_0, b_1, \dots, b_m, 0, \dots)$ . Then  $ab = (c_0, c_1, c_2, \dots)$  where  $c_k = \sum_{i+j=k} a_i b_j$  and  $ba = (d_0, d_1, d_2, \dots)$  where  $d_k = \sum_{j+i=k} b_j a_i$ . Since  $a_i b_j = b_j a_i$  for all  $i, j$ ,  $c_k = d_k$  for all  $k$ . So  $ab = ba$  and therefore  $R[x]$  is commutative. Consider the element  $(1, 0, 0, \dots) \in R[x]$ . Then  $(1, 0, 0, \dots)(b_0, b_1, \dots, b_m, 0, \dots) = (b_0, b_1, \dots, b_m, 0, \dots) = (b_0, b_1, \dots, b_m, 0, \dots)(1, 0, 0, \dots)$ . Thus,  $(1, 0, 0, \dots)$  is the identity element of  $R[x]$ .

46. If  $R$  is an integral domain, prove that for  $f(x), g(x) \in R[x]$ ,

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)).$$

**Solution:** Let  $R$  be an integral domain and let  $f(x), g(x) \in R[x]$ . Let  $n = \deg(f(x))$  and  $m = \deg(g(x))$ . Write  $f(x) = (f_0, f_1, \dots, f_n, 0, \dots)$  and  $g(x) = (g_0, g_1, \dots, g_m, 0, \dots)$ . Then  $f(x)g(x) = (h_0, h_1, h_2, 0, \dots)$  where  $h_k = \sum_{i+j=k} f_i g_j$ . Notice that if  $i > n$  or  $j > m$  then  $f_i = 0$  or  $g_j = 0$  so  $f_i g_j = 0$ . In particular, if  $k > n + m$  and  $i + j = k$  then  $i > n$  or  $j > m$ , so  $f_i g_j = 0$ . Therefore,  $\deg(f(x)g(x)) \leq n + m$ . Let  $k = n + m$ . Then the only contribution to the sum is when  $i \leq n$  and  $j \leq m$ . If  $i + j = n + m$  and  $i \leq n$  and  $j \leq m$ , then  $i = n$  and  $j = m$ . Therefore,  $h_{n+m} = f_n g_m$ . Since  $f_n \neq 0, g_m \neq 0$  and  $R$  has no nonzero zero-divisors,  $f_n g_m \neq 0$ . Therefore,  $\deg(f(x)g(x)) = n + m = \deg(f(x)) + \deg(g(x))$ .

47. If  $R$  is an integral domain with identity, prove that any unit in  $R[x]$  must already be a unit in  $R$ .

**Solution:** Let  $R$  be an integral domain with identity. Suppose  $f(x) \in R[x]$  is a unit. We seek to show that  $f(x) = (f_0, 0, 0, \dots)$  for some unit  $f_0 \in R$ . There is some  $g(x) \in R[x]$  such that  $f(x)g(x) = (1, 0, 0, \dots)$ . By 46,  $0 = \deg((1, 0, 0, \dots)) = \deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$ . Since degrees are nonnegative,  $\deg(f(x)) = \deg(g(x)) = 0$ . Thus,  $f(x) = (f_0, 0, 0, \dots)$  and  $g(x) = (g_0, 0, 0, \dots)$  and  $f_0 g_0 = 1$ .

48. Let  $R$  be a commutative ring with no nonzero nilpotent elements. If  $f(x) = (a_0, a_1, \dots, a_m, 0, \dots) \in R[x]$  is a zero divisor, prove there is a  $b \neq 0$  in  $R$  so that  $ba_0 = ba_1 = \dots = ba_m = 0$ .

**Solution:** Let  $R$  be a commutative ring with no nonzero nilpotent elements and suppose  $f(x) = (a_0, a_1, \dots, a_m, 0, \dots) \in R[x]$  is a zero divisor. Then there is some  $0 \neq g(x) = (b_0, b_1, \dots, b_n, 0, \dots) \in R[x]$  such that  $f(x)g(x) = (0, 0, 0, \dots)$ . Then we have the equations:

$$\begin{aligned} a_0 b_0 &= 0 \\ a_0 b_1 + a_1 b_0 &= 0 \\ &\vdots \\ a_{m-1} b_n + a_m b_{n-1} &= 0 \\ a_m b_n &= 0 \end{aligned}$$

Let  $k = \min\{i \mid b_i \neq 0\}$ . Notice that  $0 \leq k \leq n$  since  $g(x) \neq 0$ . The equations reduce to:

$$\begin{aligned} a_0 b_k &= 0 \\ a_0 b_{k+1} + a_1 b_k &= 0 \\ &\vdots \\ a_{m-1} b_n + a_m b_{n-1} &= 0 \\ a_m b_n &= 0 \end{aligned}$$

Notice that, by multiplying the second reduced equation by  $b_k$  and using commutivity of  $R$ , we have  $a_0 b_k b_{k+1} + a_1 b_k^2 = a_1 b_k^2 = 0$ . This leads us to claim that  $a_i b_k^{i+1} = 0$  for all  $0 \leq i \leq n$  which we prove by induction. Suppose the statement holds for all  $i \leq j$  and consider the  $(j+1)$ st reduced equation:

$$\begin{aligned} a_{j+1} b_k + a_j b_{k+1} + \dots + a_0 b_{k+j+1} &= 0 \text{ if } j+1 \leq n-k \\ a_{j+1} b_k + a_j b_{k+1} + \dots + a_{j+k+1-n} b_n &= 0 \text{ if } j+1 > n-k \end{aligned}$$

In either case, multiplying by  $b_k^j$  and using commutivity of  $R$  and the inductive hypothesis, the equation reduces to  $a_{j+1} b_k^{j+1} = 0$ , proving the claim. Therefore, in particular,  $a_i b_k^m = 0$  for all  $0 \leq i \leq m$ . Since  $b_k \neq 0$  by choice of  $k$  and  $R$  has no nonzero nilpotent elements,  $b_k^m \neq 0$ .

For the following (#49 – #51), let  $R$  be a commutative ring with identity.

49. If  $R$  is a subring of  $S$ , then  $R[G]$  is a subring of  $S[G]$  for any group  $G$ .

**Solution:** We first show that  $R[G]$  is a subset of  $S[G]$ . Then, since the ring operations in  $R[G]$  are compatible with those in  $S[G]$  (the operations are the same whether considered in  $R[G]$  or  $S[G]$ ), we have that  $R[G]$  is a subring of  $S[G]$ . Let  $\alpha \in R[G]$ . Then  $\alpha = \sum_{g \in G} a_g \cdot g$ , where  $a_g \in R \forall g \in G$ . Since  $R \subseteq S$ ,  $\alpha \in S[G]$ . So  $R[G] \subseteq S[G]$ .

50. Let  $H < G$ . Show that  $R[H]$  is a subring of  $R[G]$ .

**Solution:** Let  $\alpha \in R[H]$  and write  $\alpha = \sum_{h \in H} a_h \cdot h$ ,  $a_h \in R$ . We can rewrite  $\alpha$  as  $\alpha = \sum_{g \in G} b_g \cdot g$  where  $b_g = a_h$  if  $g = h \in H$  and  $b_g = 0$  if  $g \notin H$ . Thus,  $\alpha \in R[G]$ . Again, since the ring operations on  $R[H]$  are compatible with those of  $R[G]$ ,  $R[H]$  is a subring of  $R[G]$ .

51. Show that the set of all elements of  $R[G]$  whose coefficients sum to zero is a subring of  $R[G]$ .

**Solution:** Let  $S = \{a = \sum_{g \in G} a_g g \in R[G] \mid \sum_{g \in G} a_g = 0\} \subseteq R[G]$ . Then  $0 \in S$  so  $S \neq \emptyset$ . Suppose  $a = \sum_{g \in G} a_g g, b = \sum_{g \in G} b_g g \in S$  and consider the element  $a - b = \sum (a_g - b_g)g$ . The sum of coefficients of  $a - b$  is  $\sum (a_g - b_g) = \sum a_g - \sum b_g = 0$  (since the sums are finite). Thus,  $a - b \in S$ . Consider the element  $ab = \sum_{g \in G} c_g g$  where  $c_g = \sum_{h \in G} a_h b_{h^{-1}g}$ . The sum of coefficients of  $ab$  is  $\sum_{g \in G} \sum_{h \in G} a_h b_{h^{-1}g} = \sum_{g \in G} (\sum_{h \in G} a_h b_{h^{-1}g}) = 0$  since the sums are finite and  $\sum_{h \in G} a_h b_{h^{-1}g} = \sum_{g \in G} b_g = 0$ . Thus,  $ab \in S$  and so  $S$  is a subring of  $R[G]$ .

52. In  $\mathbb{Z}[\Sigma_3]$  let

$$\alpha = 3(12) - 5(23) + 14(123),$$

$$\beta = 6(1) + 2(23) - 7(123).$$

Compute the following:

- (a)  $\alpha + \beta$
- (b)  $2\alpha - 3\beta$
- (c)  $\alpha\beta$
- (d)  $\beta\alpha$
- (e)  $\alpha^2$

**Solution:**

$$\begin{aligned} \alpha + \beta &= [3(12) - 5(23) + 14(123)] + [6(1) + 2(23) - 7(123)] \\ \text{(a)} \quad &= 6(1) + 3(12) + [-5 + 2](23) + [14 - 7](123) \\ &= 6(1) + 3(12) - 3(23) + 7(123) \end{aligned}$$

$$\begin{aligned} 2\alpha - 3\beta &= 2[3(12) - 5(23) + 14(123)] - 3[6(1) + 2(23) - 7(123)] \\ \text{(b)} \quad &= 6(12) - 10(23) + 28(123) - 18(1) - 6(23) + 21(123) \\ &= 18(1) + 6(12) - 16(23) + 49(123) \end{aligned}$$

$$\begin{aligned} \alpha\beta &= [3(12) - 5(23) + 14(123)][6(1) + 2(23) - 7(123)] \\ &= 18(12)(1) + 6(12)(23) - 21(12)(123) - 30(23)(1) - 10(23)(23) \\ \text{(c)} \quad &+ 35(23)(123) + 84(123)(1) + 28(123)(23) - 98(123)(123) \\ &= 18(12) + 6(132) - 21(13) - 30(23) - 10(1) + 35(12) + 84(123) + 28(13) - 98(132) \\ &= -10(1) + 53(12) + 7(13) + 30(23) + 84(123) - 92(132) \end{aligned}$$

$$\begin{aligned} \beta\alpha &= [6(1) + 2(23) - 7(123)][3(12) - 5(23) + 14(123)] \\ &= 18(1)(12) - 30(1)(23) + 84(1)(123) + 6(23)(12) - 10(23)(23) \\ \text{(d)} \quad &+ 28(23)(123) - 21(123)(12) + 35(123)(23) + 98(123)(123) \\ &= 18(12) - 30(23) + 84(123) + 6(123) - 10(1) + 28(12) - 21(23) + 35(13) + 98(132) \\ &= -10(1) + 46(12) + 35(13) - 51(23) + 90(123) + 98(132) \\ &\neq \alpha\beta \end{aligned}$$

$$\begin{aligned}
\alpha^2 &= [3(12) - 5(23) + 14(123)][3(12) - 5(23) + 14(123)] \\
&= 9(12)(12) - 15(12)(23) + 42(12)(123) - 15(23)(12) + 25(23)(23) \\
\text{(e)} \quad &- 70(23)(123) + 42(123)(12) - 70(123)(23) + 196(123)(123) \\
&= 9(1) - 15(132) + 42(13) - 15(123) + 25(1) - 70(12) + 42(23) - 70(13) + 196(132) \\
&= 34(1) - 70(12) - 28(13) + 42(23) - 15(123) + 181(132)
\end{aligned}$$

53. Explain why  $\mathbb{R}[Q_8]$  is not the same ring as the ring of quaternions.

**Solution:** In exercise 44, we showed that the ring of quaternions is a division ring. In exercise 59, we showed that the ring  $\mathbb{R}[Q_8]$  is not a division ring. Therefore, the two rings cannot be the same.

54. (a) If  $H \cong G$  as groups, show that  $R[G] \cong R[H]$  as rings.

(b) Find an example to show that the converse is not necessarily true.

**Solution:**

(a) Suppose there exists a group isomorphism,  $\varphi : G \rightarrow H$ . Consider the map,  $\theta : R[G] \rightarrow R[H]$ , given by  $\theta(\sum_{g \in G} r_g g) = \sum_{g \in G} r_g \varphi(g)$ , for  $\sum_{g \in G} r_g g \in R[G]$ . We will first demonstrate that  $\theta$  is a ring homomorphism.

Let  $\sum_{g \in G} r_g g, \sum_{g \in G} s_g g \in R[G]$ . So

$$\begin{aligned}
\theta(\sum_{g \in G} r_g g + \sum_{g \in G} s_g g) &= \theta(\sum_{g \in G} (r_g + s_g)g) \\
&= \sum_{g \in G} (r_g + s_g)\varphi(g) \\
&= \sum_{g \in G} r_g \varphi(g) + \sum_{g \in G} s_g \varphi(g) \\
&= \theta(\sum_{g \in G} r_g g) + \theta(\sum_{g \in G} s_g g),
\end{aligned}$$

and also

$$\begin{aligned}
\theta((\sum_{g \in G} r_g g) \cdot (\sum_{g \in G} s_g g)) &= \theta(\sum_{g \in G} (\sum_{hk=g} r_h s_k)g) \\
&= \sum_{g \in G} (\sum_{hk=g} r_h s_k)\varphi(g) \\
&= (\sum_{g \in G} r_g \varphi(g)) \cdot (\sum_{g \in G} s_g \varphi(g)) \\
&= \theta(\sum_{g \in G} r_g g) \cdot \theta(\sum_{g \in G} s_g g).
\end{aligned}$$

Thus  $\theta$  is a ring homomorphism. Finally, we show that  $\theta$  is a bijection.

Suppose that for  $\sum_{g \in G} r_g g, \sum_{g \in G} s_g g \in R[G]$ ,  $\theta(\sum_{g \in G} r_g g) = \theta(\sum_{g \in G} s_g g)$ . Thus  $\sum_{g \in G} r_g \varphi(g) = \sum_{g \in G} s_g \varphi(g)$ , hence  $r_g = s_g$ , for all  $g \in G$ . Thus  $\sum_{g \in G} r_g g = \sum_{g \in G} s_g g$ .

Let  $\sum_{h \in H} r_h h \in R[H]$ . Since  $\varphi$  is a group isomorphism, for all  $h \in H$  there is a unique  $g_h \in G$  such that  $\varphi(g_h) = h$ . Thus we may write

$$\sum_{h \in H} r_h h = \sum_{h \in H} r_h \varphi(g_h) = \sum_{g_h \in G} r_h \varphi(g_h) = \sum_{g \in G} r_{\varphi(g)} \varphi(g) = \theta(\sum_{g \in G} r_{\varphi(g)} g).$$

Thus  $\theta$  is a bijection, hence a ring isomorphism, i.e.  $R[G] \cong R[H]$ .

(b) PENDING

55. Let  $G$  be a group with  $g \in G$  and  $g^m = e$ . Let  $R$  be a commutative ring with identity 1. Show  $(1 - g)(1 + g + \dots + g^{m-1}) = 0$  in  $R[G]$ .

**Solution:** We have

$$\begin{aligned}
(1 - g)(1 + g + \dots + g^{m-1}) &= 1 + g + \dots + g^{m-1} - g(1 + g + \dots + g^{m-1}) \\
&= 1 + g + \dots + g^{m-1} - (g + g^2 + \dots + g^m) \\
&= 1 + g + \dots + g^{m-1} - (1 + g + \dots + g^{m-1}) \\
&= 0.
\end{aligned}$$

56. Let  $G = \{g_1, g_2, \dots, g_n\}$  be a finite group. Prove that  $N = g_1 + g_2 + \dots + g_n$  is in the center of  $R[G]$ .

**Solution:** Let  $g \in G$  and consider it as a ring element in  $R[G]$ . So

$$Ng = \left( \sum_{h \in G} h \right) g = \sum_{h \in G} hg = \sum_{h \in G} h = \sum_{h \in G} gh = g \left( \sum_{h \in G} h \right) = gN.$$

Thus for an element  $\sum_{h \in G} r_h h \in R[G]$ , we have

$$N \left( \sum_{g \in G} r_g g \right) = \sum_{g \in G} r_g Ng = \sum_{g \in G} r_g gN = \left( \sum_{g \in G} r_g g \right) N.$$

Thus  $N$  is in the center of  $R[G]$ .

58. Let  $R$  be a commutative ring with identity and let  $G$  be a finite group with  $|G| > 1$ . Show that  $R[G]$  contains zero-divisors.

**Solution:** Since  $|G| > 1$ , there is an element  $g \in G$  for which  $o(g) = m > 1$ . Thus  $1 - g \neq 0$  and  $1 + g + \dots + g^{m-1} \neq 0$  in  $R[G]$ . However by #55,  $(1 - g)(1 + g + \dots + g^{m-1}) = 0$ , hence  $R[G]$  contains zero-divisors.

59. Show that  $\mathbb{R}[Q_8]$  is not a division ring.

**Solution:** Since  $\mathbb{R}$  is a commutative ring with identity and  $Q_8$  is a finite group with  $|Q_8| > 1$ , we may use #58. So the group ring contains a zero-divisor  $x \in \mathbb{R}[Q_8]$  (say,  $y \neq 0$  is such that  $xy = 0$ ). However  $x$  cannot have an inverse ( $x^{-1}$ , say) in  $\mathbb{R}[Q_8]$ , for then

$$y = 1 \cdot y = (x^{-1}x)y = x^{-1}(xy) = x^{-1} \cdot 0 = 0,$$

which contradicts the fact that  $y \neq 0$ . Since there are non-zero elements in  $\mathbb{R}[Q_8]$  which don't have an inverse,  $\mathbb{R}[Q_8]$  is not a division ring.

60. Verify some of the equations in (S) on the fifth page (p. 284) of the paper.

**Solution:** Suppose that  $aa' = b = \sum_{q \in Q_8} b_q q$ , where  $a = (t, u, v, w)$  and  $a' = (t', u', v', w')$ . Then using the notation in the paper

$$\begin{aligned} b_1 &= t_1 t'_1 + t_2 t'_2 + u_1 u'_1 + u_2 u'_2 + v_1 v'_1 + v_2 v'_2 + w_1 w'_1 + w_2 w'_2 \\ &= t t' + u \cdot u' + v \cdot v' + w \cdot w' \end{aligned}$$

$$\begin{aligned} b_{-1} &= t_1 t'_2 + t_2 t'_1 + u_1 u'_1 + u_2 u'_2 + v_1 v'_1 + v_2 v'_2 + w_1 w'_1 + w_2 w'_2 \\ &= t \cdot t' + uu' + vv' + ww' \end{aligned}$$

The other equations follow similarly.

61. Verify  $aa' = 0$  while  $a'a \neq 0$  for  $a$  and  $a'$  as defined in the first displayed equations on the seventh page of the paper (p. 286).

**Solution:** So we have

$$\begin{aligned} a &= (1 + (x + y)i + (y - x)j + k)f \\ &= (1 + (x + y)i + (y - x)j + k)\left(\frac{1}{2}(1 - (-1))\right) \\ &= \frac{1}{2} - \frac{1}{2}(-1) + \frac{1}{2}(x + y)i - \frac{1}{2}(x + y)(-i) + \frac{1}{2}(y - x)j - \frac{1}{2}(y - x)(-j) + \frac{1}{2}k - \frac{1}{2}(-k) \\ a' &= (1 - yi + xj)f \\ &= (1 - yi + xj)\left(\frac{1}{2}(1 - (-1))\right) \\ &= \frac{1}{2} - \frac{1}{2}(-1) - \frac{1}{2}yi + \frac{1}{2}y(-i) + \frac{1}{2}xj - \frac{1}{2}x(-j). \end{aligned}$$

So for  $aa' = b = \sum_{q \in Q_8} b_q q$ , and using the above formulas, we have

$$\begin{aligned} b_1 &= \frac{1}{4} + \frac{1}{4} + \frac{1}{4}(xy + y^2) + \frac{1}{4}(xy + y^2) - \frac{1}{4}(xy - x^2) - \frac{1}{4}(xy - x^2) \\ &= \frac{1}{2} + \frac{1}{2}y^2 + \frac{1}{2}x^2 \\ &= 0, \\ b_{-1} &= -\frac{1}{4} - \frac{1}{4} - \frac{1}{4}(xy + y^2) - \frac{1}{4}(xy + y^2) + \frac{1}{4}(xy - x^2) + \frac{1}{4}(xy - x^2) \\ &= -\frac{1}{2} - \frac{1}{2}y^2 - \frac{1}{2}x^2 \\ &= 0, \\ b_i &= -\frac{1}{4}y - \frac{1}{4}y + \frac{1}{4}(x + y) + \frac{1}{4}(x + y) - \frac{1}{4}x - \frac{1}{4}x \\ &= 0, \\ b_{-i} &= \frac{1}{4}y + \frac{1}{4}y - \frac{1}{4}(x + y) - \frac{1}{4}(x + y) + \frac{1}{4}x + \frac{1}{4}x \\ &= 0, \\ b_j &= \frac{1}{4}x + \frac{1}{4}x + \frac{1}{4}(y - x) + \frac{1}{4}(y - x) - \frac{1}{4}y - \frac{1}{4}y \\ &= 0, \\ b_{-j} &= -\frac{1}{4}x - \frac{1}{4}x - \frac{1}{4}(y - x) - \frac{1}{4}(y - x) + \frac{1}{4}y + \frac{1}{4}y \\ &= 0, \\ b_k &= \frac{1}{4}(x^2 + xy) + \frac{1}{4}(x^2 + xy) + \frac{1}{4}(y^2 - xy) + \frac{1}{4}(y^2 - xy) + \frac{1}{4} + \frac{1}{4} \\ &= \frac{1}{2}x^2 + \frac{1}{2}y^2 + \frac{1}{2} \\ &= 0, \\ b_{-k} &= -\frac{1}{4}(x^2 + xy) - \frac{1}{4}(x^2 + xy) - \frac{1}{4}(y^2 - xy) - \frac{1}{4}(y^2 - xy) - \frac{1}{4} - \frac{1}{4} \\ &= -\frac{1}{2}x^2 - \frac{1}{2}y^2 - \frac{1}{2} \\ &= 0. \end{aligned}$$

Thus  $aa' = 0$ .

Now consider  $a'a = b' = \sum_{q \in Q_8} b'_q q$ . Since

$$\begin{aligned} b'_j &= \frac{1}{4}(y - x) + \frac{1}{4}(y - x) + \frac{1}{4}y + \frac{1}{4}y + \frac{1}{4}x + \frac{1}{4}x \\ &= y \neq 0, \end{aligned}$$

we have that  $a'a \neq 0$ , as desired.

62. Let  $G$  be a group with  $H < G$ .

- Prove that the relation on  $G$  defined by  $a \sim b \iff b^{-1}a \in H$  is an equivalence relation on  $H$ .
- Show that for any element  $a \in H$ , the equivalence class of  $a$ , under the relation given above is  $aH = \{ah \mid h \in H\}$ .

**Solution:**

- Let  $a \in H$ . Then since  $a^{-1}a = e \in H$ , we have that  $a \sim a$ . Thus  $\sim$  is reflexive.

Let  $a, b \in H$  and suppose that  $a \sim b$ . Since  $b^{-1}a \in H$  by assumption, we have that  $a^{-1}b = (b^{-1}a)^{-1} \in H$ , since  $H$  is closed under inverses. Hence  $b \sim a$ . Thus  $\sim$  is symmetric.

Let  $a, b, c \in H$  and suppose that  $a \sim b$  and  $b \sim c$ . Thus  $b^{-1}a, c^{-1}b \in H$ . Hence  $c^{-1}a = c^{-1}(b^{-1}b)a = (c^{-1}b)(b^{-1}a) \in H$ , since  $H$  is closed under multiplication. Hence  $a \sim c$ . Thus  $\sim$  is transitive. Therefore  $\sim$  is an equivalence relation.

(b) Suppose first that  $b \in H$  is in the equivalence class of  $a$ . Thus  $a^{-1}b = h$  for some  $h \in H$ . Hence  $b = ah \in aH$ .

Next let  $b \in aH$ . So  $b = ah$  for some  $h \in H$ . So we have  $a^{-1}b = a^{-1}(ah) = (a^{-1}a)h = h \in H$ , thus  $b \sim a$ . This completes the proof.

63. In  $\Sigma_3$ , let  $a = (12)$ .

(a) Compute  $aC_3a^{-1}$ .

(b) Prove that there is an element  $h \in C_3$  such that  $aha^{-1} \neq h$ .

(c) Is  $C_3 \triangleleft \Sigma_3$ ? Prove or disprove.

**Solution:**

(a) So we have

$$aC_3a^{-1} = (12)\{(1), (123), (132)\}(12) = \{(12)(1)(12), (12)(123)(12), (12)(132)(12)\} = \{(1), (132), (123)\} = C_3.$$

(b) From the above calculation, we have that for  $h = (123) \in C_3$ ,  $aha^{-1} = (12)(123)(12) = (132) \neq h$ .

(c) Since  $(1), (123), (132) \in C_3$ ,  $(1)C_3(1)^{-1} = (123)C_3(123)^{-1} = (132)C_3(132)^{-1} = C_3$ . We also have that

$$(12)C_3(12)^{-1} = C_3,$$

$$(23)C_3(23)^{-1} = \{(23)(1)(23), (23)(123)(23), (23)(132)(23)\} = \{(1), (132), (123)\} = C_3,$$

$$(13)C_3(13)^{-1} = \{(13)(1)(13), (13)(123)(13), (13)(132)(13)\} = \{(1), (132), (123)\} = C_3.$$

Thus since  $gC_3g^{-1} = C_3$ , for all  $g \in \Sigma_3$ ,  $C_3 \triangleleft \Sigma_3$ .

64. Let  $H < G$ . Prove  $|aH| = |H|$ ,  $\forall a \in G$ .

**Solution:** Consider the map  $\varphi : H \rightarrow aH$ , given by  $h \mapsto ah$ . We need to show that this is a bijection. For  $h, h' \in H$ , if  $ah = ah'$ , we have  $h = h'$  (by multiplying both sides by  $a^{-1}$ ). Thus  $\varphi$  is injective.

Let  $b \in aH$ . Hence  $b = ah$  for some  $h \in H$ . Thus  $\varphi(h) = ah = b$ . So  $\varphi$  is surjective, hence a bijection.

65. Give an example of a group  $G$ , a subgroup  $H$  and an element  $a \in G$  such that  $aHa^{-1} \subset H$ , but  $aHa^{-1} \neq H$ .

**Solution:** Let  $G = F(a, b)$ , the free group on two (non-commuting) elements  $a$  and  $b$ . Consider the subgroup

$$H = \langle a^k b^n a^{-k} \mid n \in \mathbb{Z}, k \geq 0 \rangle.$$

Notice that conjugating by  $a$  yields

$$aHa^{-1} = a \langle a^k b^n a^{-k} \mid n \in \mathbb{Z}, k \geq 0 \rangle a^{-1} = \langle a^{k+1} b^n a^{-k-1} \mid n \in \mathbb{Z}, k \geq 0 \rangle = \langle a^k b^n a^{-k} \mid n \in \mathbb{Z}, k \geq 1 \rangle < H.$$

However  $b \in H \setminus aHa^{-1}$ . That  $b \in H$  is clear, as it is included in the set of generators. To see that  $b \notin aHa^{-1}$ , suppose instead that it is an element in that subgroup. Thus  $b = a^{k_1} b^{n_1} a^{-k_1} \cdots a^{k_r} b^{n_r} a^{-k_r}$ , where  $k_i \geq 1$  and  $n_i \in \mathbb{Z} \setminus \{0\}$ . It must be that  $k_1 = k_i$ , for all  $i$ . (If this were not the case then there would be an  $i$  such that  $k_i \neq k_{i+1}$ . Hence the “word,”  $a^{k_1} b^{n_1} a^{-k_1} \cdots a^{k_r} b^{n_r} a^{-k_r}$ , would contain a reduced string  $\cdots b^{k_i} a^{k_{i+1}-k_i} b^{k_{i+1}} \cdots$ . Thus there would be an uncancellable “ $a$ ”-term, so the word could not equal  $b$ .) Thus we can write  $b = a^{k_1} b^n a^{-k_1}$ , where  $k_1 \geq 1$  and  $n \in \mathbb{Z} \setminus \{0\}$ . But since  $a^{k_1} b^n a^{-k_1}$  contains uncancellable “ $a$ ”-terms, the word could not possibly equal  $b$ . Hence it must be that  $b \notin aHa^{-1}$ . Thus  $aHa^{-1} \subsetneq H$ .

66. Find an example of a group  $G$  and a subgroup  $H$  where the natural “multiplication” on  $\overline{G} = \{aH | a \in G\}$  is not well-defined.

**Solution:** We need only pick our favorite non-normal subgroup. Consider  $G = \Sigma_3$  and  $H = \{(1), (12)\}$ . So we have that  $(23)H = \{(23), (123)\} = (123)H$  and  $(13)H = \{(13), (132)\} = (132)H$ . Supposing that multiplication is well-defined, we have that

$$(1)H = (123)(132)H = (123)H \cdot (132)H = (23)H \cdot (13)H = (23)(13)H = (132)H,$$

which is a contradiction, since  $(1)H \neq (132)H$ .

67. Prove or Disprove: If  $M \triangleleft N$  and  $N \triangleleft G$ , then  $M \triangleleft G$ .

**Solution:** Consider  $G = \Sigma_4$ ,  $N = \{(1), (12)(34), (13)(24), (14)(23)\}$ , and  $M = \{(1), (12)(34)\}$ .

**Claim:**  $N \triangleleft G$ .

Consider the alternating subgroup,  $A_4$ .

( $A_4 = \{(1), (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$ ; it is the set of all elements in  $\Sigma_4$  that can be represented as the product of an even number of transpositions.) Note that  $[\Sigma_4 : A_4] = 2$ , hence  $A_4 \triangleleft \Sigma_4$  by a future homework problem. Now let  $\sigma \in \Sigma_4$ . Clearly,  $\sigma(1)\sigma^{-1} = (1)$ . Consider  $(12)(34) \in N$ . Since  $(12)(34) \in A_4$ ,  $\sigma(12)(34)\sigma^{-1} \in A_4$ . But also note that  $(\sigma(12)(34)\sigma^{-1})^{-1} = \sigma(12)(34)\sigma^{-1}$ . The only elements in  $A_4$  that are their own inverses are elements in  $N$ , hence  $\sigma(12)(34)\sigma^{-1} \in N$ . Similarly,  $\sigma(13)(24)\sigma^{-1}, \sigma(14)(23)\sigma^{-1} \in N$ , thus  $\sigma N \sigma^{-1} \subset N$ . Thus  $N \triangleleft G$ .

Since  $[N : M] = 2$ , we have  $M \triangleleft N$ . However  $(14)(12)(34)(14) = (13)(24) \notin M$ , thus  $M \not\triangleleft G$ . This disproves the proposition.

68. Let  $N < \Sigma_4$  consist of all those permutations  $\sigma$  such that  $\sigma(4) = 4$ . Is  $N$  normal in  $\Sigma_4$ ? Prove or disprove.

**Solution:** First note that  $(12) \in N$ , as it fixes 4. By conjugating with  $(14)$ , we have  $(14)(12)(14) = (24) \notin N$ . Hence  $(14)N(14)^{-1} \not\subset N$ . Thus  $N \not\triangleleft G$ .

69. Let  $G$  be a group. A commutator in  $G$  is an element of the form  $aba^{-1}b^{-1}$  with  $a, b \in G$ . Let  $G^C$  be the subgroup generated by the commutators. Then  $G^C$  is called the commutator subgroup. Show that  $G^C$  is normal.

**Solution:** Let  $g \in G$ . We will show first that for a generator,  $aba^{-1}b^{-1} \in G^C$ , that  $g(aba^{-1}b^{-1})g^{-1} \in G^C$ . We have

$$g(aba^{-1}b^{-1})g^{-1} = ga(g^{-1}g)b(g^{-1}g)a^{-1}(g^{-1}g)b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \in G^C.$$

So for an arbitrary element  $g_1g_2 \cdots g_n \in G^C$ , where  $g_i = a_i b_i a_i^{-1} b_i^{-1}$ , we have

$$gg_1g_2 \cdots g_n g^{-1} = gg_1(g^{-1}g)g_2 \cdots (g^{-1}g)g_n g^{-1} = (gg_1g^{-1})(gg_2g^{-1}) \cdots (gg_n g^{-1}) \in G^C.$$

Thus  $gG^C g^{-1} \subset G^C$ , hence  $G^C \triangleleft G$ .

70. If a cyclic subgroup  $T$  of  $G$  is normal in  $G$ , then show that every subgroup of  $T$  is normal in  $G$ .

**Solution:** Let  $S < T = \langle a \rangle$ . If  $S = \{1\}$ , then we're done as  $\{1\} \triangleleft G$ . Suppose  $S \neq \{1\}$ . Let

$$d = \min\{n \in \mathbb{N} | a^n \in S\}.$$

**Claim:**  $S = \langle a^d \rangle$ .

Now  $\langle a^d \rangle \subset S$ , since  $a^d \in S$ . Suppose there is an element  $a^m \in S \setminus \langle a^d \rangle$  (say  $m > 1$ , without loss of generality). By definition,  $d < m$ , hence we may write  $m = qd + r$ , where  $0 < r < d$ , as  $m$  is not a multiple of  $d$ . Since  $a^m, a^{-qd} \in S$ ,  $(a^m)(a^{-qd}) = a^r \in S$ . But  $0 < r < d$ , which contradicts the minimality of  $d$ . Hence  $S = \langle a^d \rangle$ .

Now let  $g \in G$ . Since  $T \triangleleft G$ , we have  $gag^{-1} = a^l$  for some  $l$ . Hence

$$gSg^{-1} = g\langle a^d \rangle g^{-1} = \langle ga^d g^{-1} \rangle = \langle (gag^{-1})^d \rangle = \langle a^{ld} \rangle \subset S.$$

Thus  $S \triangleleft G$ .

71. Let  $H$  be a subgroup of  $G$ . If  $\langle a \rangle \triangleleft G, \forall a \in H$ , then  $H \triangleleft G$ .

**Solution:** Consider  $a \in H$  and let  $g \in G$ . Since  $\langle a \rangle \triangleleft G$ , we have  $gag^{-1} \in \langle a \rangle \subset H$ . Hence  $gHg^{-1} = \{ghg^{-1} | h \in H\} \subset H$ . Thus  $H \triangleleft G$ .

72. Let  $G$  be a finite group of even order, and let  $H < G$  with  $|H| = \frac{1}{2}|G|$ . Prove  $H \triangleleft G$ .

**Solution:** Since every coset of  $H$  has size  $|H|$ , and  $|G| = 2|H|$ , there must be only two left cosets of  $H$  in  $G$ , and two right cosets of  $H$  in  $G$ . Since  $eH = H = He$  is both a left coset and a right coset, and cosets partition the group  $G$ , the other coset must be  $G \setminus H$  when looking at both left and right cosets. Hence, the left cosets equal the right cosets, which means that  $H$  is normal in  $G$ .

73. Let  $H$  be a subgroup of order  $N$  in a group  $G$ . If  $H$  is the only subgroup of order  $n$  then  $H$  is normal in  $G$ .

**Solution:** Suppose that  $H$  were not normal in  $G$ . Then there is some  $g \in G$  such that  $gHg^{-1} \neq H$ . However,  $|gH| = |H|$ , and similarly,  $|gHg^{-1}| = |H|$ , which means that  $gHg^{-1}$  has the same order as  $H$ . As there is only one subgroup of order  $n$  in  $G$ , it must be that  $gHg^{-1} = H$ , which contradicts the supposition that  $H$  is not normal. Thus,  $H$  is normal in  $G$ .

74. Let  $G$  be a group,  $H < G, K < G$ . Define  $HK = \{hk | h \in H, k \in K\}$ .

- Show  $HK < G$  if and only if  $HK$  is closed under the binary operation of the group.
- Show that if  $H \triangleleft G$  or  $K \triangleleft G$ , then  $HK < G$ .
- Show

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

- Let  $H = \langle \sigma \rangle$  and  $K = \langle \tau \rangle$  where  $\sigma$  is a 3-cycle and  $\tau$  is a 2-cycle in  $\Sigma_3$ . Show  $HK = \Sigma_3$ .

**Solution:**

- Suppose that  $HK < G$ . Since subgroups are closed under the group operation,  $HK$  must be closed under the group operation.

Conversely, suppose that  $HK$  is closed under the binary operation of the group. Note that since  $H$  and  $K$  are both subgroups, the both contain the identity  $e$ , which means that  $e = e \cdot e \in HK$ , so  $HK$  contains the identity. Also, given an element  $hk \in HK$ , its inverse is  $k^{-1}h^{-1} = (ek^{-1})(h^{-1}e)$ , and since  $H$  and  $K$  are closed under inverses,  $ek^{-1}$  and  $h^{-1}e$  are in  $HK$ . By the closure of  $HK$  under the group operation,  $k^{-1}h^{-1}$  is also in  $HK$ , so  $HK$  is closed under inverses. Hence,  $HK$  is a subgroup of  $G$ .

- (b) Suppose that  $H \triangleleft G$ , and let  $h_1k_1, h_2k_2 \in HK$ . Then  $h_1k_1h_2k_2 = h_1k_1h_2k_1^{-1}k_1k_2$ . Since  $H$  is normal,  $k_1h_2k_1^{-1}$  is some  $h_3 \in H$ , so  $h_1k_1h_2k_2 = h_1h_3k_1k_2$  and since  $H$  and  $K$  are closed under multiplication,  $h_1h_3 \in H$  and  $k_1k_2 \in K$ , which means that  $h_1h_3k_1k_2 = h_1k_1h_2k_2 \in HK$ . Thus  $HK$  is closed under the group operation, which means that  $HK < G$  by part (a).

Now suppose that  $K \triangleleft G$ , and let  $h_1k_1, h_2k_2 \in HK$ . Then  $h_1k_1h_2k_2 = h_1h_2h_2^{-1}k_1h_2k_2$ , and since  $K$  is normal in  $G$ ,  $h_2^{-1}k_1h_2$  is in  $K$ , call it  $k_3$ . Then  $h_1h_2k_3k_2 = h_1k_1h_2k_2$ . As  $h_1h_2 \in H$ , and  $k_3k_2 \in K$ ,  $h_1k_1h_2k_2 \in HK$ . Hence,  $HK$  is closed under the group operation, and so by part (a),  $HK$  is a subgroup of  $G$ .

- (c) We can write  $HK$  as

$$HK = \cup_{k \in K} Hk,$$

where any two cosets  $Hk$  are either disjoint or equal. Thus, if  $a$  is the number of distinct cosets  $Hk$ ,  $|HK| = |H|a$ .

We now claim that  $a$  equals the number of cosets of  $H \cap K$  in  $K$ , which is just  $\frac{|K|}{|H \cap K|}$ . In other words, we claim that  $Hk_1 = Hk_2$  if and only if  $(H \cap K)k_1 = (H \cap K)k_2$ .

( $\Rightarrow$ ) Suppose that  $Hk_1 = Hk_2$ , so  $k_1k_2^{-1} \in H$ . Then  $k_1k_2^{-1} \in H \cap K$ , so

$$(H \cap K)k_2 = (H \cap K)(k_1k_2^{-1})k_2 = (H \cap K)k_1.$$

( $\Leftarrow$ ) Suppose that  $(H \cap K)k_1 = (H \cap K)k_2$ . This means that  $(H \cap K)k_1$  and  $(H \cap K)k_2$  are both nonempty and contained in  $Hk_1 \cap Hk_2$ . Hence,  $Hk_1 \cap Hk_2 \neq \emptyset$ , and since these cosets are not distinct, they must be equal. Therefore,  $Hk_1 = Hk_2$ .

- (d) Since  $|H| = 3$  and  $|K| = 2$  and  $H \cap K = \{e\}$ , by part (c),  $|HK| = 6$ . Since  $HK \subseteq \Sigma_3$ , and  $\Sigma_3$  has order six,  $HK$  must equal  $\Sigma_3$ .

75. Suppose  $H$  and  $K$  are normal subgroups of a group  $G$  with  $H \cap K = \langle e \rangle$ . Prove that  $hk = kh$  for all  $h \in H, k \in K$ .

**Solution:** Suppose that  $h \in H$  and  $k \in K$ , and consider the element  $hkh^{-1}k^{-1}$ . Since  $K$  is normal,  $hkh^{-1} \in K$ , and since  $K$  is closed under multiplication,  $hkh^{-1}k^{-1} \in K$ . Similarly,  $H$  is normal, and so  $kh^{-1}k^{-1} \in H$ , and  $H$  is closed under multiplication, which means that  $hkh^{-1}k^{-1} \in H$ . Thus,  $hkh^{-1}k^{-1} \in H \cap K = \{e\}$ . Therefore,  $hkh^{-1}k^{-1} = e$ , and so  $hk = kh$ .

76. Let  $\mathbb{C}^*$  be the group of non-zero complex numbers under multiplication. Geometrically, we can identify  $a + bi \in \mathbb{C}^*$  with the point  $(a, b)$  in the cartesian coordinate plane. Let  $H = \{a + bi \mid a^2 + b^2 = 1\} < \mathbb{C}^*$ . Give a geometric description of the cosets of  $H$ .

**Solution:** Write  $H$  using exponential notation as  $H = \{e^{i\theta} \mid 0 \leq \theta < 2\pi\}$ . Then, given any  $z \in \mathbb{C}^*$ , write  $z = re^{i\theta_0}$ ,  $zH = \{re^{i(\theta+\theta_0)} \mid 0 \leq \theta < 2\pi\}$ . Since  $\theta$  still goes from zero to  $2\pi$ ,  $zH$  is a circle centered at the origin with radius  $r$ .

Hence, the cosets of  $H$  are circles centered at the origin of various radii.

77. Show that every Abelian group satisfies the hamiltonian group property (i.e. every subgroup is normal).

**Solution:** Let  $H$  be a subgroup of an abelian group  $G$ , and let  $g \in G, h \in H$ . Then  $ghg^{-1} = gg^{-1}h$ , since  $G$  is abelian, so  $ghg^{-1} = h \in H$ , and hence  $H$  is normal in  $G$ . Thus every subgroup of  $G$  is normal.

78. Show that the group of quaternions is a hamiltonian group.

**Solution:** By # 38 the subgroups of the quaternions are

$$\begin{aligned} &\{1\}, \quad \{\pm 1\}, \quad \{\pm 1, \pm i\}, \\ &\{\pm 1, \pm j\}, \quad \{\pm 1, \pm k\}, \quad Q_8. \end{aligned}$$

The trivial subgroups are always normal, and by # 39, the center is  $\{\pm 1\}$ , which means that  $\pm 1$  commute with everything in the group, and hence  $\{\pm 1\}$  is normal in  $Q_8$ . The remaining three subgroups each have order four, which means that they are normal in  $Q_8$  by # 72. Hence every subgroup of  $Q_8$  is normal, and hence  $Q_8$  is hamiltonian.

79. Show that if  $G$  is a non-abelian group such that every cyclic subgroup of  $G$  is normal in  $G$ , then  $G$  is hamiltonian.

**Solution:** Suppose that  $H$  is a subgroup of  $G$ , and let  $h \in H$  and  $g \in G$ . Let  $K = \langle h \rangle$ . Since  $K$  is a cyclic subgroup of  $G$ ,  $K$  is normal in  $G$ , which means that  $ghg^{-1} \in K$ . However, since  $H$  is a subgroup, and hence closed under the group operation,  $h \in H$  implies that  $\langle h \rangle \subseteq H$ , and hence  $ghg^{-1} \in K \subseteq H$ . Therefore,  $H$  is normal in  $G$ . Since this holds for all subgroups  $H$  of  $G$ ,  $G$  is hamiltonian.

80. A group that has only a finite number of subgroups must be finite.

**Solution:** We will prove the contrapositive - that all infinite groups have an infinite number of subgroups. Let  $G$  be an infinite group. Suppose there is some  $a \in G$  such that  $o(a) = \infty$ . Consider the subgroups generated by powers of  $a$ :  $H_1 = \langle a \rangle, H_2 = \langle a^2 \rangle, \dots, H_n = \langle a^n \rangle, \dots$ . We claim that these subgroups are all distinct. Suppose, by way of contradiction, that  $H_i = H_j$  for some  $i < j$ . Then  $a^i \in H_j$ , so there is some  $k$  such that  $(a^j)^k = a^i$ , which implies  $a^{jk-i} = 1$ . Since  $i < j, i < jk$  so  $jk - i > 0$ . But this contradicts that the order of  $a$  is infinite. Therefore, each of the subgroups above are distinct and so  $G$  has an infinite number of subgroups. Otherwise, suppose every element of  $G$  has some finite order. Consider the collection of subgroups of  $G$  generated by a single element (that is, all cyclic subgroups). We claim that this collection contains an infinite number of distinct subgroups of  $G$ . Suppose, by way of contradiction, that  $G$  has only a finite number of subgroups. Then an infinite number of subgroups generated by distinct elements of  $G$  must all be equal. That is, there is an infinite collection  $\{g_i \in G \mid i \in \mathbb{N}, g_i \neq g_j \forall i \neq j\}$  such that  $\langle g_1 \rangle = \langle g_2 \rangle = \langle g_3 \rangle = \dots$ . Since every element of  $G$  has a finite order, there is some  $n$  such that  $o(g_1) = n$ . Then  $\langle g_1 \rangle = \{g_1^k \mid k \in \mathbb{Z}\}$  contains  $n$  distinct elements. In particular,  $\langle g_1 \rangle$  does not contain an infinite number of distinct elements, a contradiction. Thus,  $G$  has infinitely many distinct subgroups.

81. An infinite group is cyclic if and only if it is isomorphic to each of its nontrivial proper subgroups.

**Solution:** Let  $G$  be an infinite cyclic group, say  $G = \langle a \rangle$ . Let  $H$  be a nontrivial proper subgroup. The  $H$  is cyclic (exercise 24, supplemental problems). Say  $H = \langle b \rangle$ . Since  $H$  is a subgroup of  $G$ ,  $b \in G$ . So  $b = a^k$  for some  $k$ . If  $b^n = 1$  for some  $n > 0$ , then  $a^{kn} = 1$ , contradicting that  $G$  is infinite. Therefore,  $b$  must have infinite order. Consider the map  $\varphi : G \rightarrow H$  defined by  $a \mapsto b$ . That is,  $\varphi(a^t) = b^t$  for all  $a \in G$ . We claim that  $\varphi$  is an isomorphism. We first note that since  $b$  has infinite order, the kernel of  $\varphi$  is trivial. (If  $\varphi(a^t) = 1$  then  $b^t = 1$ , so  $t = 0$ .) For any  $b^t \in H$  we have  $a^t \in G$  such that  $\varphi(a^t) = b^t$ , so  $\varphi$  is surjective and thus a bijection.  $\varphi(1) = \varphi(a^0) = b^0 = 1$  and  $\varphi(a^t a^{-k}) = \varphi(a^{t-k}) = b^{t-k} = b^t b^{-k} = \varphi(a^t) \varphi(a^{-k})$ . Thus  $\varphi$  is an isomorphism of groups. So  $G$  is isomorphic to each of its nontrivial proper subgroups. Conversely, suppose  $G$  is an infinite group isomorphic to each of its nontrivial proper subgroups. Let  $1 \neq a \in G$  and consider the subgroup  $H = \langle a \rangle$ . Then  $G$  is isomorphic to  $H$ , say  $\varphi : G \rightarrow H$  is such an isomorphism. Let  $x \in G$  such that  $\varphi(x) = a$ . Let  $y \in G$ . Then  $\varphi(y) = a^t$  for some  $t$ . Since  $\varphi$  is a homomorphism,  $\varphi(x^t) = \varphi(x)^t = a^t$ . Since  $\varphi$  has trivial kernel,  $x^t = y$ . Thus,  $G = \langle x \rangle$ . So  $G$  is cyclic.

82. Let  $G$  be a group.

- Suppose  $G = \langle a, b \rangle$ , that is,  $G$  is a group containing the elements  $a$  and  $b$  and all other elements required by the definition of a group. You can think of this as though  $H$  is a group which contains the elements  $a$  and  $b$  and  $G$  is the smallest subgroup of  $H$  which contains  $a$  and  $b$ .  $G$  is called the *free group on*  $\{a, b\}$ . What do the elements of  $G$  look like?
- Suppose  $G = \langle a, b \rangle$  is Abelian. Can you improve upon your answer above for this case? Note: We often describe groups like this using a technique often referred to as "generators and relations". This group would be  $\langle a, b : aba^{-1}b^{-1} = e \rangle$  or  $\langle a, b : ab = ba \rangle$ .
- Suppose  $G = \langle a, b \rangle$  is Abelian with  $o(a) = n < \infty$  and  $o(b) = m < \infty$ . Can you improve your answer above? Note: Using generators and relations, this group is  $\langle a, b : aba^{-1}b^{-1} = a^n = b^m = e \rangle$ .
- Suppose  $G = \langle a, b : aba^{-1}b^{-1} = a^n = b^m = e \rangle$ . What can you say about  $|G|$ ?

**Solution:**

- Since  $G$  is a group containing  $a$  and  $b$ ,  $G$  must contain  $a^2, ab, ba$ , and  $b^2$  since  $G$  must be closed. Then  $G$  must also contain  $a^3, a^2b, aba, ab^2, ba^2, bab, b^2a$ , and  $b^3$ . Etc. That is, any combination of  $a$ 's and  $b$ 's must be in  $G$ . We can write such combinations as  $a^{n_1}b^{m_1}a^{n_2}b^{m_2} \dots a^{n_k}b^{m_k}$  where  $n_i, m_i \in \mathbb{Z}$ . To see this, note that negative powers are necessary for  $G$  to have inverses and whenever two powers of  $a$  appear consecutively their powers may be combined. Thus, an element in  $G$  (often called a 'word') will have powers of  $a$  alternating with powers of  $b$ .  $G$  need not contain any other elements as the set  $\{a^{n_1}b^{m_1}a^{n_2}b^{m_2} \dots a^{n_k}b^{m_k} \mid k \in \mathbb{N}, n_i, m_i \in \mathbb{Z}\}$  forms a group containing  $a$  and  $b$  and is therefore the smallest such group.
- The elements described above must all still be in  $G$ , but when  $a$  and  $b$  commute the word  $a^{n_1}b^{m_1}a^{n_2}b^{m_2} \dots a^{n_k}b^{m_k}$  reduces to  $a^N b^M$  where  $N = \sum_{i=1}^k n_i, M = \sum_{i=1}^k m_i$ . Thus,  $G = \{a^N b^M \mid N, M \in \mathbb{Z}\}$ .
- Whenever  $N$  is greater than or equal to  $n$ , the word  $a^N b^M$  reduces to  $a^{(N-n)} b^M$ . Similarly, whenever  $M$  is greater than or equal to  $m$ , the word  $a^N b^M$  reduces to  $a^N b^{(M-m)}$ . Therefore, the elements of  $G$  are of the form  $a^i b^j$  where  $0 \leq i < n$  and  $0 \leq j < m$ .
- From part (c), we have that any element in  $G$  can be written in the form  $a^i b^j$  where  $0 \leq i < n$  and  $0 \leq j < m$  (and any element of this form is in  $G$ ). Thus, there are  $nm$  elements in  $G$ . So  $|G| = nm$ .

83. In  $\Sigma_3$  determine

- $o((12)), o((13))$
- $\langle (12), (13) \rangle$
- Does your answer contradict what you saw in problem #82? Explain.

**Solution:**

- Notice that  $(12)(12) = (1)$ . Since  $(12) \neq (1)$ ,  $o((12)) = 2$ . Also,  $(13)(13) = (1)$  and  $(13) \neq (1)$ , so  $o((13)) = 2$ .
- We have  $\langle (12), (13) \rangle = \{(1), (12), (13), (12)(13) = (123), (13)(12) = (132), (13)(12)(13) = (13)(123) = (23) = (12)(13)(12)\}$ .
- Let  $a = (12), b = (13)$ . Notice that although  $o(a) = o(b) = 2$ , we have  $|G| = |\langle a, b \rangle| = 6 \neq o(a)o(b) = 4$ . However, in #82 we assumed  $a$  and  $b$  commute whereas in this case  $a$  and  $b$  do not commute. Therefore this does not contradict what we found above.

84. Prove every finitely generated Abelian torsion group is finite.

**Solution:** Let  $G$  be a finitely generated Abelian torsion group. Say  $G$  is generated by  $a_1, a_2, \dots, a_k$ . Since  $G$  is torsion, each of these generators has a finite order, say  $n_1, n_2, \dots, n_k$  respectively. Then every element of  $G$  is of the form  $a_1^{x_1} a_2^{x_2} \dots a_k^{x_k}$  where  $0 \leq x_i < n_i$ . Therefore  $|G| = \prod_{i=1}^k n_i$ .

85. Let  $G$  be an Abelian group with  $a, b \in G$  and  $o(a) = n < \infty$  and  $o(b) = m < \infty$ . Prove there is an element  $c \in G$  such that  $o(c) = \text{lcm}(m, n)$ .

**Solution:** We first consider the case when  $m$  and  $n$  are relatively prime. Then  $\text{lcm}(mn) = mn$ . Let  $c = ab$ . Notice that  $c^{mn} = (ab)^{mn} = (a^n)^m(b^m)^n = 1$  since  $G$  is commutative. Thus,  $o(c) \leq \text{lcm}(m, n)$ . Suppose  $c^x = 1$  for some  $x > 0$ . Then  $a^x b^x = 1$ . Raising both sides of this equation by  $o(a) = n$  yields  $b^{nx} = 1$ . Thus,  $o(b) = m|nx$ . Since  $m$  and  $n$  are relatively prime, this means  $m|x$ . Similarly, raising both sides of the equation by  $o(b) = m$  yields  $a^{mx} = 1$ . So  $o(a) = n|mx$  and therefore  $n|x$ . Thus,  $x$  is a common multiple of  $m$  and  $n$ . So  $x \geq \text{lcm}(m, n)$ . Therefore,  $o(c) = mn = \text{lcm}(m, n)$ . Now suppose  $m$  and  $n$  are not relatively prime and let  $d = \text{gcd}(m, n)$ . Consider the elements  $a_2 = a, b_2 = b^d$ . Notice that  $o(a_2) = o(a) = n$  and that  $o(b_2) = \frac{o(b)}{d} = \frac{m}{d}$ . Since  $d$  is the greatest common divisor of  $n$  and  $m$ , we now have that the orders of  $a_2$  and  $b_2$  are relatively prime and  $\text{lcm}(o(a_2), o(b_2)) = o(a_2)o(b_2) = n\frac{m}{d} = \text{lcm}(m, n)$ . Thus, by the first case,  $c = a_2 b_2$  has the desired order.

86. Let  $G$  be a finite abelian group in which the number of solutions in  $G$  of the equation  $x^n = e$  is at most  $n$  for every positive integer  $n$ . Prove that  $G$  must be a cyclic group.

**Solution:** Suppose the size of  $G$  is  $N$ . If there is an element of  $G$  of order  $N$ , then we must have that  $G$  is cyclic and generated by that element. Suppose, to the contrary, that there is no element of order  $N$ . Let  $m = \max\{o(x) \mid x \in G\}$ . Since  $G$  is finite, there is an element  $a$  of order  $m$  and  $m < N$ . We claim that  $x^m = 1$  for all  $x \in G$ . Suppose there is some  $b \in G$  such that  $b^m \neq 1$ . Then it must mean that  $m$  is not a multiple of  $o(b)$ . Therefore,  $\text{lcm}(m, o(b)) > m$ . However, from #85 we have that there is an element  $c \in G$  with order  $\text{lcm}(o(a), o(b)) > m$ , contradicting maximality of  $m$ . Therefore, it must be that  $x^m = 1$  for all  $x \in G$ . Thus,  $x^m = 1$  has  $|G| = N > m$  solutions, contradicting our assumption on  $G$ . Thus, it must be that there is an element of order  $N$  in  $G$  and so  $G$  is cyclic.

87. Let  $p$  be a prime and  $R$  a commutative ring with identity of characteristic  $p$ .

- (a) Then for every  $a, b \in R$  and every positive integer  $n$ ,  $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ .  
 (b) Show that this may be false if the characteristic  $p$  is not prime or if  $R$  is not commutative.

**Solution:**

- (a) The proof is by mathematical induction on  $n$ :  
 Suppose that  $n = 1$ . Then the binomial theorem tells us that

$$(a + b)^p = \sum_{i=0}^p \binom{p}{i} a^i b^{p-i}.$$

For  $0 < i < p$ ,  $\binom{p}{i} = \frac{p!}{i!(p-i)!}$  and since  $0 < p - i < p$ . Since  $p$  is prime, the  $p$  in  $p!$  cannot be cancelled by anything in the denominator, which means that  $p$  divides  $\binom{p}{i}$ . Since the characteristic of the ring is  $p$ , this means that  $\binom{p}{i} = 0$  in  $R$ , and hence

$$(a + b)^p = \binom{p}{0} a^0 b^p + \binom{p}{p} a^p b^0 = a^p + b^p.$$

Thus, the basis case of  $n = 1$  holds, so let the inductive hypothesis be that  $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ . Then  $(a + b)^{p^{n+1}} = [(a + b)^{p^n}]^p$ , and by the inductive hypothesis, this equals  $[a^{p^n} + b^{p^n}]^p$ . As  $a^{p^n}$  and  $b^{p^n}$  are both in  $R$ , the basis case applies to get that  $[a^{p^n} + b^{p^n}]^p = (a^{p^n})^p + (b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}}$ .

Therefore,  $(a + b)^{p^{n+1}} = a^{p^{n+1}} + b^{p^{n+1}}$ .

Therefore,  $(a + b)^{p^n} = a^{p^n} + b^{p^n}$  for all integers  $n \geq 1$ .

- (b) Consider the ring  $\mathbb{Z}_4$ , which has characteristic four. Then  $(1 + 1)^4 = 2^4 = 16 = 0 \pmod{4}$ , but  $1^4 + 1^4 = 1 + 1 = 2$ . Hence  $(1 + 1)^4 \neq 1^4 + 1^4$ , and so in the case where  $p$  is not prime, the statement may not hold. Now consider the group ring  $\mathbb{Z}_2[Q_8]$ , which has characteristic two. Then  $(1(i) + 1(j))^2 = 1(i^2) + 1(ij) + 1(ji) + 1(j^2) = 2(-1) + 1(k) + 1(-k)$  and since the ring has characteristic two, this simplifies to  $1(k) + 1(-k)$ . On the contrary,  $(1(i))^2 + (1(j))^2 = 1(i^2) + 1(j^2) = 2(-1) = 0$ , and hence  $(1(i) + 1(j))^2 \neq (1(i))^2 + (1(j))^2$ . Thus the statement may not hold when the ring is not commutative.

88. Let  $R$  be a commutative ring with identity of prime characteristic  $p$ . If  $a, b \in R$  and  $n \geq 1$ , prove that  $(a - b)^{p^n} = a^{p^n} - b^{p^n}$ .

**Solution:** If  $p = 2$ , then  $-1 = 1$ , which means that  $(a - b)^{p^n} = (a + b)^{p^n}$ , and by #87, this equals  $a^{p^n} + b^{p^n}$ . Using that  $-1 = 1$  again, this becomes  $a^{p^n} - b^{p^n}$ . Therefore,  $(a - b)^{p^n} = a^{p^n} - b^{p^n}$ .

If  $p > 2$ , then  $p$  is odd (since  $p$  is prime). Hence  $(a - b)^{p^n} = (a + (-b))^{p^n} = a^{p^n} + (-1 \cdot b)^{p^n}$  by # 87. Since  $R$  is commutative,  $(-1 \cdot b)^{p^n} = (-1)^{p^n} b^{p^n}$  and since  $p$  is odd,  $p^n$  is odd, which means that  $(-1)^{p^n} = -1$ . Therefore,  $a^{p^n} + (-1 \cdot b)^{p^n} = a^{p^n} - b^{p^n}$ , which means that  $(a - b)^{p^n} = a^{p^n} - b^{p^n}$ .

89. Let  $R = \{(a, b, c) | a \in \mathbb{Z}_2, b \in \mathbb{Z}_3, c \in \mathbb{Z}\}$ . Define addition and multiplication coordinate-wise. What is the characteristic of  $R$ ?

**Solution:** The characteristic is zero, because there is no positive integer  $n$  such that  $(0, 0, 1)^n = (0, 0, 0)$  since  $(0, 0, 1)^n = (0, 0, n)$  and  $n \neq 0$  in  $\mathbb{Z}$  for any  $n \neq 0$ .

90. Give an example of an integral domain which has an infinite number of elements, yet is of nonzero characteristic.

**Solution:** Let  $\mathbb{Z}_p$  be the field with  $p$  elements, and let  $R = \mathbb{Z}_p[x]$ . Then  $R$  has characteristic  $p$ , and  $R$  is an integral domain because it is a  $\mathbb{Z}_p$  is a field. However, there are an infinite number of elements, since the set  $\{1, x, x^2, \dots\}$  is infinite and none of its elements are equal to each other.

91. Show that  $e = \frac{1}{2}(1 + (-1))$  is a central idempotent of  $K[Q_8]$  where  $K$  is a field of characteristic different from 2.

**Solution:** As  $\{\pm 1\}$  is the center of  $Q_8$  and multiplication in  $K$  is commutative, since  $K$  is a field,  $e$  commutes with everything in the group ring. Also,

$$e^2 = \frac{1}{4}(1^2 + (1)(-1) + (-1)(1) + (-1)^2) = \frac{1}{4}(2(1) + 2(-1)) = \frac{1}{2}(1 + (-1)) = e.$$

Thus  $e$  is an idempotent that commutes with everything in the group ring, so  $e$  is a central idempotent.

92. If  $R$  is a ring with unity, 1, then  $\text{char}(R) = \circ(1)$  if  $\circ(1)$  is finite and  $\text{char}(R) = 0$  if  $\circ(1)$  is infinite.

**Solution:** Suppose that  $\circ(1) = n < \infty$ . Then certainly  $\text{char}(R) \geq n$ , since  $\text{char}(R)$  is the smallest integer,  $m$ , such that  $m \cdot a = 0$ , so in particular  $m \cdot 1 = 0$ , and so  $m \geq \circ(1)$ .

Moreover,  $n \cdot 1 = 0$  implies that  $0 = a(n \cdot 1) = n(a \cdot 1) = n \cdot a$  for any  $a \in R$ . Thus,  $\text{char}(R) \leq n$ . Therefore,  $\text{char}(R) = n = \circ(1)$ .

If  $\circ(1)$  is not finite, then there is no integer  $n \in \mathbb{N}$  so that  $n \cdot a = 0$  for all  $a \in R$ , because if there were, in particular,  $n \cdot 1 = 0$ , so  $n$  would be at least the order of 1, which we've already said is not finite. Thus,  $R$  must have characteristic zero.

93. Let  $F$  be a field of characteristic  $p$ . Prove that the mapping  $\phi : \mathbb{Z} \rightarrow F$  given by  $\phi(n) = n \cdot 1_F$  is a ring homomorphism and that  $\ker \phi = p\mathbb{Z}$ .

**Solution:** Suppose that  $n, m \in \mathbb{Z}$ . Then  $\phi(nm) = (nm) \cdot 1_F = 1_F + 1_F + \dots + 1_F$  where there are  $nm$   $1_F$ 's. Using the distributive property of rings,  $(nm) \cdot 1_F = (n \cdot 1_F)(m \cdot 1_F)$ . As this equals  $\phi(n)\phi(m)$ ,  $\phi$  preserves multiplication. Also,  $\phi(n + m) = n \cdot 1_F + m \cdot 1_F = (1_F + \dots + 1_F) + (1_F + \dots + 1_F) = 1_F + \dots + 1_F = (n + m)1_F$ . Thus,  $\phi$  is a homomorphism, because it preserves addition and multiplication.

94. Let  $R$  be a commutative ring with no nonzero zero divisors.

- (a) Let  $a$  and  $b$  be nonzero elements of  $R$ . Prove that for any integer  $k$ ,  $k \cdot a = 0$  if and only if  $k \cdot b = 0$ .
- (b) Let  $a$  and  $b$  be nonzero elements of  $R$ . Prove  $\circ(a) = \circ(b)$ .
- (c) Suppose  $\text{char}(R) \neq 0$ . Let  $a$  be a nonzero element of  $R$ . Prove  $\text{char}(R) = \circ(a)$ .
- (d) Show  $\text{char}(R)$  is zero or prime.
- (e) If  $R$  is an integral domain and if  $na = 0_R$  for some  $a \neq 0$  in  $R$  and some integer  $n \neq 0$ , prove that  $\text{char}(R)$  is finite.

**Solution:**

- (a) Suppose that  $k \cdot a = 0$ . Then  $0 = k \cdot a = (k \cdot a)b = a(k \cdot b)$ . Since  $a \neq 0$  and  $R$  has no nonzero zero divisors, it must be that  $k \cdot b = 0$ .

The reverse direction holds by symmetry. Thus,  $0 = k \cdot a$  if and only if  $0 = k \cdot b$ .

- (b) Let  $k = \circ(a)$ . Then  $k$  is the smallest positive integer such that  $k \cdot a = 0$ . By part (a),  $k \cdot b = 0$ , which means that  $k \geq \circ(b)$ . By symmetry, if  $j = \circ(b)$ , then  $j \geq k$ . Hence,  $j = k$ , so  $\circ(a) = \circ(b)$ .
- (c) Let  $n = \circ(a)$ . By part (b),  $n = \circ(b)$  for every  $b \in R$ , which means that  $\text{char}(R) \leq n$ . Suppose that  $m = \text{char}(R)$ . Then  $m \geq n$ , since  $n$  is the order of  $a$ , and the order of an element is the *smallest* integer  $n$  such that  $na = 0$ . Hence if  $ma = 0$ ,  $m$  must be at least  $n$ .

Since we have  $n \leq m \leq n$ , it must be true that  $n = m$ , and hence  $\circ(a) = \text{char}(R)$ .

- (d) Suppose that  $R$  has nonzero characteristic  $mn$ , where  $m, n \in \mathbb{N}$  are both greater than one. Then  $mn = \circ(a)$  for all  $a \in R$  from part (c), which means that  $mn$  is the smallest integer such that  $(mn)a = 0$ . Thus,  $(mn)(ab) = 0$  for all  $a, b \in R$ , and since  $(mn)(ab) = (ma)(nb)$ , we have that  $(ma)(nb) = 0$ .

By assumption, we know that  $R$  has no nonzero zero divisors, which means that either  $ma = 0$  or  $nb = 0$ . Since both  $m, n > 1$ , we have that  $m, n < mn$ . Since  $mn = \circ(a) = \circ(b)$ , this is a contradiction, because if  $ma = 0$ , then  $a$  has order less than  $mn$ , and if  $nb = 0$ , then  $b$  has order less than  $mn$ .

- (e) Since  $R$  is an integral domain, it contains a unity,  $1$ . If  $na = 0$  for some  $a \neq 0$  in  $R$  and  $n \in \mathbb{N}$ , then  $0 = n \cdot a = a(n \cdot 1)$ , and since  $R$  has no nonzero zero divisors and  $a \neq 0$ , it must be that  $n \cdot 1 = 0$ . Hence,  $b(n \cdot 1) = 0$  for every  $b \in R$  and redistributing yields that  $n \cdot b = 0$  for every  $b \in R$ . Thus,  $\text{char}(R) \leq n$ , and so the characteristic is nonzero.

97. Let  $G'$  be the smallest subgroup of  $G$  containing  $\{xyx^{-1}y^{-1} | x, y \in G\}$ , called the commutator subgroup of  $G$ . Show that

- (a)  $G' \triangleleft G$ .
- (b)  $G/G'$  is abelian.
- (c) If  $G/N$  is abelian, then  $G' \subset N$ .
- (d) If  $H < G$  and  $G' \subset H$ , then  $H \triangleleft G$ .

**Solution:**

- (a) This was done previously in problem #69.
- (b) Let  $aG', bG' \in G/G'$ . So we have that

$$aG' \cdot bG' = abG' = ab(b^{-1}a^{-1}baG') = baG' = bG' \cdot aG'.$$

Thus  $G/G'$  is abelian.

- (c) It's enough to show that  $N$  contains all the generators of  $G'$ . Let  $aba^{-1}b^{-1} \in G'$ . Since

$$a^{-1}b^{-1}N = a^{-1}N \cdot b^{-1}N = b^{-1}N \cdot a^{-1}N = b^{-1}a^{-1}N,$$

multiplying both sides by  $(b^{-1}a^{-1})^{-1} = ab$  yields  $aba^{-1}b^{-1}N = N$ . Thus  $aba^{-1}b^{-1} \in N$ . Hence  $G' \subset N$ , which completes the proof.

(d) Let  $g \in G$ . For  $h \in H$ , we have that  $ghg^{-1} = ghg^{-1}(h^{-1}h) = (ghg^{-1}h^{-1})h$ . Since  $G' \subset H$ ,  $ghg^{-1}h^{-1} \in H$ . Thus since  $H$  is closed under multiplication,  $ghg^{-1} = (ghg^{-1}h^{-1})h \in H$ . Thus  $gHg^{-1} \subset H$ . Therefore  $H \triangleleft G$ .

98. Let  $G$  be the group of real numbers under addition and let  $N$  be the subgroup of  $G$  consisting of all the integers. Prove that  $G/N$  is isomorphic to the group of all complex numbers of absolute value 1 under multiplication.

**Solution:** Denote  $T = \{e^{i\theta} \in \mathbb{C} \mid \theta \in \mathbb{R}\} =$  group of all complex numbers of absolute value 1. Consider the map  $\varphi : \mathbb{R}/\mathbb{Z} \rightarrow T$ , given by  $r + \mathbb{Z} \mapsto e^{i2\pi r}$ . We must show that this is an isomorphism.

Let  $r + \mathbb{Z}, s + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ . So

$$\varphi((r + \mathbb{Z}) + (s + \mathbb{Z})) = \varphi((r + s)\mathbb{Z}) = e^{i2\pi(r+s)} = e^{i2\pi r} \cdot e^{i2\pi s} = \varphi(r + \mathbb{Z}) \cdot \varphi(s + \mathbb{Z}).$$

Thus  $\varphi$  is a homomorphism.

Suppose  $r + \mathbb{Z}, s + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$  are such that  $\varphi(r + \mathbb{Z}) = \varphi(s + \mathbb{Z})$ . Thus  $e^{i2\pi r} = e^{i2\pi s}$ , hence  $e^{i2\pi(r-s)} = 1$ . So we have that  $r - s \in \mathbb{Z}$ , i.e. that  $r + \mathbb{Z} = s + \mathbb{Z}$ . Thus  $\varphi$  is injective.

Let  $e^{i\theta} \in T$ . So we have  $\varphi(\frac{\theta}{2\pi} + \mathbb{Z}) = e^{i2\pi \frac{\theta}{2\pi}} = e^{i\theta}$ . Thus  $\varphi$  is surjective.

Thus  $\varphi$  is an isomorphism and  $\mathbb{R}/\mathbb{Z} \cong T$ .

99. Let  $G$  be a group with  $H$  a subgroup of finite index. Show that there exists a normal subgroup  $N$  of  $G$  contained in  $H$  and also of finite index.

**Solution:** Denote  $N_H = \{g \in G \mid gHg^{-1} = H\}$ .

**Claim:**  $N_H$  is a subgroup of  $G$ .

Let  $a, b \in N_H$ . Thus  $(ab)N_H(ab)^{-1} = a(bN_Hb^{-1})a^{-1} = aN_Ha^{-1} = N_H$ , hence  $ab \in N_H$ .

Let  $a \in N_H$ . Then  $a^{-1}N_Ha = a^{-1}(aN_Ha^{-1})a = N_H$ , hence  $a^{-1} \in N_H$ . Thus  $N_H$  is a subgroup.

Note that  $H < N_H$ , as  $hN_Hh^{-1} = N_H$ , for all  $h \in H$ . Thus  $[G : N_H] \leq [G : H] < \infty$ .

**Claim:**  $\#\{gHg^{-1} \mid g \in G\} = [G : N_H]$ .

It's enough to show that  $gHg^{-1} = kHk^{-1}$  if and only if  $gN_H = kN_H$ , for  $g, k \in G$ . Suppose  $gHg^{-1} = kHk^{-1}$ . Thus  $k^{-1}gHg^{-1}k = H$ , so  $k^{-1}g \in N_H$ . Hence  $k^{-1}gN_H = N_H$ , and so  $gN_H = kN_H$ .

Suppose  $gN_H = kN_H$ . Thus  $k^{-1}g \in N_H$ . Hence  $k^{-1}gHg^{-1}k = H$ , and so  $gHg^{-1} = kHk^{-1}$ . This completes the proof of the claim.

So we now have that the number of conjugates of  $H$  must be finite. Take  $K = \{g \in G \mid g \in kHk^{-1}, \forall k \in G\} =$  intersection of all conjugates of  $H$ .

**Claim:**  $K \triangleleft G$ .

That  $K$  is a subgroup is clear as it's an intersection of subgroups. Let  $g \in G$  and  $k \in K$ . In order to show that  $gkg^{-1} \in K$ , consider an arbitrary conjugate of  $H$ , say  $aHa^{-1}$ . We want to show that  $gkg^{-1} \in aHa^{-1}$ . Now since  $k \in K$ , we have that  $k \in g^{-1}aHa^{-1}g$ . Thus  $gkg^{-1} \in g(g^{-1}aHa^{-1}g)g^{-1} = aHa^{-1}$ . Hence  $gKg^{-1} \subset K$ , and so  $K \triangleleft G$ .

In order to prove that  $[G : K] < \infty$ , we prove the following:

**Claim:** For subgroups  $S, T$  in  $G$ , if  $[G : S], [G : T] < \infty$ , then  $[G : S \cap T] < \infty$ .

Consider a map  $\theta : \{x(S \cap T) \mid x \in G\} \rightarrow \{(xS, xT) \mid x \in G\}$ , given by  $x(S \cap T) \mapsto (xS, xT)$ . First, we show that  $\theta$  is well-defined. Suppose  $x(S \cap T) = y(S \cap T)$ . Thus  $x^{-1}y \in S \cap T$ , hence  $x^{-1}y \in S, T$ . So  $x^{-1}yS = S$  and  $x^{-1}yT = T$ , i.e.  $yS = xS$  and  $yT = xT$ , which shows that the map is well-defined.

Next, we show that the map is injective. Suppose  $x(S \cap T)$  and  $y(S \cap T)$  are such that  $(xS, xT) = (yS, yT)$ . Thus  $x^{-1}y \in S, T$ , i.e.  $x^{-1}y \in S \cap T$ . So  $x(S \cap T) = y(S \cap T)$ . Thus  $\theta$  is injective.

So since this map is injective, we have that

$$[G : S \cap T] = \#\{x(S \cap T) \mid x \in G\} \leq \#\{(xS, xT) \mid x \in G\} \leq [G : S] \cdot [G : T] < \infty,$$

which completes the proof of the claim.

Finally, since  $H$  has only finitely many conjugates, we have that  $[G : K] < \infty$  by applying the above claim a finite number of times. This completes the proof.

100. If  $N$  is the ideal of all nilpotent elements in a commutative ring  $R$ , then  $R/N$  is a ring with no non-zero nilpotent elements.

**Solution:** Let  $a + N \in R/N$  be nilpotent. Thus there exists an  $n \geq 1$  such that  $(a + N)^n = a^n + N = 0 + N$ . Thus  $a^n \in N$ , hence there exists an  $m \geq 1$  such that  $a^{nm} = (a^n)^m = 0$ . Thus  $a \in N$ , so  $a + N = 0 + N$ . This completes the proof.

101. Let  $\phi : R \rightarrow S$  be a homomorphism of commutative rings with  $\ker \phi = K$ ,  $I \triangleleft R$  and  $J \triangleleft S$ .

- (a)  $\phi^{-1}(J)$  is an ideal in  $R$  that contains  $K$ .
- (b) If  $\phi$  is surjective, then  $\phi(I)$  is an ideal in  $S$ .
- (c) If  $\phi$  is not surjective,  $\phi(I)$  need not be an ideal in  $S$ .

For the following  $\phi$  is surjective.

- (d) If  $P$  is a prime ideal in  $R$  that contains  $K$ , then  $\phi(P)$  is a prime ideal in  $S$ .
- (e) If  $Q$  is a prime ideal in  $S$ , then  $\phi^{-1}(Q)$  is a prime ideal in  $R$  that contains  $K$ .
- (f) There is a one-to-one correspondence between the set of all prime ideals in  $R$  that contain  $K$  and the set of all prime ideals in  $S$  given by  $P \mapsto \phi(P)$ .
- (g) If  $I \triangleleft R$ , then every prime ideal in  $R/I$  is of the form  $P/I$ , where  $P \triangleleft R$  is a prime ideal that contains  $I$ .

**Solution:**

- (a) Let  $a, b \in \phi^{-1}(J)$ . So  $\phi(a + b) = \phi(a) + \phi(b) \in J$ , as  $J$  is closed under addition. Hence  $a + b \in \phi^{-1}(J)$ .  
Let  $a \in \phi^{-1}(J)$  and  $r \in R$ . So  $\phi(ra) = \phi(r) \cdot \phi(a) \in J$ . Hence  $ra \in \phi^{-1}(J)$ . Thus  $\phi^{-1}(J)$  is an ideal in  $R$ .  
Since  $\{0\} \subset J$ , we have that  $K = \phi^{-1}(\{0\}) \subset \phi^{-1}(J)$ . This completes the proof.
- (b) Let  $a, b \in \phi(I)$ . So  $a = \phi(\alpha)$ ,  $b = \phi(\beta)$  for some  $\alpha, \beta \in I$ . Hence  $a + b = \phi(\alpha) + \phi(\beta) = \phi(\alpha + \beta) \in \phi(I)$ , as  $I$  is closed under addition.  
Let  $a \in \phi(I)$  and  $s \in S$ . So  $a = \phi(\alpha)$  for some  $\alpha \in I$ , and since  $\phi$  is surjective, there is an element  $r \in R$  such that  $\phi(r) = s$ . Hence  $sa = \phi(r) \cdot \phi(\alpha) = \phi(r\alpha) \in \phi(I)$ . Thus  $\phi(I)$  is an ideal in  $S$ .
- (c) Consider the ring map,  $\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[x]$ , given by  $\phi(f) = f(0)$ .

**Claim:**  $\phi$  is a homomorphism.

Let  $f, g \in \mathbb{Z}[x]$ . So

$$\phi(f + g) = (f + g)(0) = f(0) + g(0) = \phi(f) + \phi(g),$$

and

$$\phi(f \cdot g) = (f \cdot g)(0) = f(0) \cdot g(0) = \phi(f) \cdot \phi(g).$$

Thus  $\phi$  is a ring homomorphism.

Now note that  $\phi(\mathbb{Z}[x]) = \mathbb{Z}$  (hence  $\phi$  is not surjective). Also note that  $\phi(\mathbb{Z}[x]) = \mathbb{Z}$  is not an ideal in  $\mathbb{Z}[x]$  (e.g.  $x\mathbb{Z} \not\subset \mathbb{Z}$ ). This completes the proof.

- (d) From the above, it is enough to show that  $\phi(P)$  is prime. Let  $a, b \in S$  and suppose that  $ab \in \phi(P)$ . We may write  $ab = \phi(u)$  for  $u \in P$ . Since  $\phi$  is surjective, there exist  $s, t \in R$  such that  $a = \phi(s)$  and  $b = \phi(t)$ . So  $\phi(u) = ab = \phi(s) \cdot \phi(t) = \phi(st)$ . Hence we have that  $u - st \in K \subset P$ , and since  $u \in P$ ,  $st \in P$ . Since  $P$  is prime, either  $s$  or  $t$  is contained in  $P$ , hence either  $a = \phi(s)$  or  $b = \phi(t)$  is contained in  $\phi(P)$ . Thus  $\phi(P)$  is prime.
- (e) Again, it is enough to show that  $\phi^{-1}(Q)$  is prime. Let  $a, b \in R$  and suppose that  $ab \in \phi^{-1}(Q)$ . Hence we have that  $\phi(a) \cdot \phi(b) = \phi(ab) \in Q$ . Since  $Q$  is prime, either  $\phi(a)$  or  $\phi(b)$  is contained in  $Q$ , hence either  $a$  or  $b$  is contained in  $\phi^{-1}(Q)$ . Thus  $\phi^{-1}(Q)$  is prime.

(f) We need to show that the map described is both injective and surjective.

**Claim:** For  $P \triangleleft R$  prime containing  $K$ ,  $P = \phi^{-1}\phi(P)$ .

Let  $x \in P$ . Thus  $\phi(x) \in \phi(P)$ , hence  $x \in \phi^{-1}\phi(P)$ . This establishes  $P \subset \phi^{-1}\phi(P)$ . Let  $y \in \phi^{-1}\phi(P)$ . So  $\phi(y) = \phi(a)$  for some  $a \in P$ . Thus  $y - a \in K \subset P$ . Since  $a \in P$ , we have that  $y \in P$ . This completes the proof of the claim.

**Claim:** For  $Q \triangleleft S$  prime,  $Q = \phi\phi^{-1}(Q)$ .

Let  $x \in Q$ . Since  $\phi$  is surjective, there is an element  $r \in R$  such that  $\phi(r) = x$ . Hence  $x \in \phi^{-1}(Q)$ , so  $x = \phi(r) \in \phi\phi^{-1}(Q)$ . This establishes  $Q \subset \phi\phi^{-1}(Q)$ . Let  $y \in \phi\phi^{-1}(Q)$ . So there exists an element  $b \in \phi^{-1}(Q)$  such that  $\phi(b) = y$ . But since  $b \in \phi^{-1}(Q)$ ,  $y = \phi(b) \in Q$ . This completes the proof of the claim.

Now suppose  $P, P' \triangleleft R$  are prime and contain  $K$ . If  $\phi(P) = \phi(P')$ , then  $P = \phi^{-1}\phi(P) = \phi^{-1}\phi(P') = P'$ . Thus the map is injective.

Suppose  $Q \triangleleft S$  is prime. Then  $\phi^{-1}(Q)$  is prime in  $R$  and contains  $K$ , where  $\phi\phi^{-1}(Q) = Q$ . Thus the map is surjective, which completes the proof.

(g) Consider the canonical surjective homomorphism,  $\phi : R \rightarrow R/I$ , given by  $r \mapsto r + I$ . For  $Q \triangleleft R/I$  prime, the above exercise gives that  $Q = \phi(P) = \{p + I \mid p \in P\} = P/I$ , where  $P \triangleleft R$  is prime and contains  $\ker \phi = I$ . This completes the proof.

102. If  $\text{char}(F) = p$ , then  $\mathbb{Z}_p$  is a subfield of  $F$ .

**Solution:** Note that since  $F$  is a field,  $F$  contains an identity element 1. Consider a “map”  $\phi : \mathbb{Z}_p \rightarrow F$ , given by  $\bar{n} \mapsto n \cdot 1$ . To see that this is a well-defined, suppose that  $\bar{n} = \bar{m}$ . Then  $m - n = kp$ . Hence in  $F$ ,  $n \cdot 1 = (m + kp) \cdot 1 = m \cdot 1 + kp \cdot 1 = m \cdot 1$ . Thus  $\phi$  is well-defined.

**Claim:**  $\phi$  is a ring homomorphism.

Let  $\bar{n}, \bar{m} \in \mathbb{Z}_p$ . Then

$$\phi(\bar{n} + \bar{m}) = \phi(\overline{n+m}) = (n+m) \cdot 1 = n \cdot 1 + m \cdot 1 = \phi(\bar{n}) + \phi(\bar{m}),$$

and

$$\phi(\bar{n} \cdot \bar{m}) = \phi(\overline{nm}) = nm \cdot 1 = (n \cdot 1)(m \cdot 1) = \phi(\bar{n}) \cdot \phi(\bar{m}).$$

Thus  $\phi$  is a ring homomorphism.

Finally, we need to show that  $\phi$  is injective. Let  $\bar{n}, \bar{m} \in \mathbb{Z}_p$  and suppose that  $n \cdot 1 = m \cdot 1$ . Thus  $(n - m) \cdot 1 = 0$ , so it must be that  $p \mid (n - m)$ , as  $\text{char}(F) = p$ . Thus  $\bar{n} = \bar{m}$ . So  $\phi$  is injective. Thus  $\mathbb{Z}_p$  embeds into  $F$ , hence it is (i.e. isomorphic to) a subfield of  $F$ .