Problem 3.10 Give an example of a ring having identity but a subring of this having a different identity.

Solution Let

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

Then S is a ring with respect to usual addition and multiplication. Note S has the identity

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Consider the set

$$T = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}.$$

Clearly T is a subring of S having

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

as the identity.

Problem 3.3 Show that in a ring containing at least two elements including identity 1, the zero element must be different from the identity element.

Solution If possible, let $0 = 1$ and let a be any element of R. Then $a = 1 \cdot a = 0 \cdot a = 0$. Hence there is no element other than 0, contrary to the fact that R has at least two elements.

Problem 3.11 Show that the set $\{a + b\omega : \omega^3 = 1;\ a, b \in \mathbb{R}\}$ is a field with respect to usual addition and multiplication.

Solution Let $F = \{a + b\omega : a, b \in \mathbb{R}\}$, where $\omega^3 = 1$, then clearly $(F, +)$ is a commutative group. Next, let $a + b\omega \in F$, $c + d\omega \in F$. Then

$$\begin{aligned}(a + b\omega)(c + d\omega) &= ac + (bc + ad)\omega + bd\omega^2 \\ &= ac + (bc + ad)\omega - bd\,(1 + \omega) \\ &= (ac - bd) + (bc + ad - bd)\,\omega \in F \\ &\qquad\qquad [\text{since } 1 + \omega + \omega^2 = 0]\end{aligned}$$

So, $(F, +)$ is closed. Associativity of multiplication follows easily. The two distributive properties also follow easily. Hence $(F, +, \cdot)$ is a ring. Now, the element $1 = 1 + 0\omega \in F$ and satisfies the condition

$$(a + b\omega)\,1 = (a + b\omega) \quad \text{for all } a + b\omega \in F$$

Hence 1 is the multiplicative inverse of F. Finally, if $a + b\omega \neq 0$, i.e. if $a \neq 0$, $b \neq 0$, then

$$(a + b\omega)^{-1} = \frac{a - b}{a^2 - ab + b^2} - \frac{b}{a^2 - ab + b^2}\,\omega \in F$$

since

$$\frac{a - b}{a^2 - ab + b^2},\ \frac{b}{a^2 - ab + b^2} \in \mathbb{R} \qquad \text{when } a, b \in \mathbb{R}.$$

The commutativity of multiplication follows trivially. Hence F is a field.

Problem 3.9 Show that the set M of all matrices of the form

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}; \qquad a, b \in \mathbb{Z}$$

forms a left ideal of the ring R of all 2×2 matrices with integral elements, but it is not a right ideal.

Solution Let

$$A = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in M, \qquad B = \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} \in M$$

where $a, b, c, d \in \mathbb{Z}$. Then

$$A - B = \begin{pmatrix} a - c & 0 \\ b - d & 0 \end{pmatrix}$$

since $a - c, b - d \in \mathbb{Z}$. Again

$$AB = \begin{pmatrix} ac & 0 \\ bd & 0 \end{pmatrix}$$

since $ac, bd \in \mathbb{Z}$. So M is a subring. Further, if

$$S = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in R, \quad SA = \begin{pmatrix} pa + bq & 0 \\ ra + sb & 0 \end{pmatrix} \in M,$$

since $pa + bq, ra + sb \in \mathbb{Z}$. Hence M is a left ideal. Clearly,

$$P = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \in M, \qquad Q = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in R$$

Then

$$PQ = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \notin M$$

Hence M is not a right ideal.

Problem 3.4 Prove that the set $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5}: a, b \in \mathbb{Q}\}$ is a commutative ring with identity. Is this a field? Justify your answer.

Solution Let $a + b\sqrt{5}, c + d\sqrt{5} \in \mathbb{Q}(\sqrt{5})$. Then

$$(a + b\sqrt{5}) + (c + d\sqrt{5}) = (a + c) + (b + d)\sqrt{5} \in \mathbb{Q}(\sqrt{5})$$

since $a + c \in \mathbb{Q}$, $b + d \in \mathbb{Q}$. Again

$$(a + b\sqrt{5})\,(c + d\sqrt{5}) = (ac + 5bd) + (ad + bc)\sqrt{5} \in \mathbb{Q}(\sqrt{5})$$

since $ac + 5bd \in \mathbb{Q}$, $ad + bc \in \mathbb{Q}$. So the closure properties of addition and multiplication hold.

The associative properties of addition and multiplication follow trivially as $\mathbb{Q}$ is associative and commutative with respect to both addition and multiplication. Obviously the element $0 + 0\sqrt{5}$, i.e. 0 is the additive identity and 1, i.e. $1 + 0\sqrt{5}$ is the multiplicative identity.

Clearly the additive inverse (i.e. negative) of the element $(a + b\sqrt{5})$ is $(-a) + (-b)\sqrt{5}$, since

$$(a + b\sqrt{5}) + [(-a) + (-b)\sqrt{5}] = 0$$

The commutativity of addition is obvious.

Finally, for $a + b\sqrt{5}, c + d\sqrt{5}$ and $e + f\sqrt{5} \in \mathbb{Q}(\sqrt{5})$, we see

$$\begin{aligned}(a + b\sqrt{5})\,[(c + d\sqrt{5}) + (e + f\sqrt{5})] &= (a + b\sqrt{5})[(c + e) + (d + f)\sqrt{5}] \\ &= a(c + e) + 5b(d + f) + [a(d + f) + b(c + e)]\sqrt{5}\end{aligned}$$

and

$$\begin{aligned}(a + b\sqrt{5})\,(c + d\sqrt{5}) + (a + b\sqrt{5})\,(e + f\sqrt{5}) &= (ac + 5bd) + (ad + bc)\sqrt{5} + (ae + 5bf) + (af + be)\sqrt{5} \\ &= a(c + e) + 5b(d + f) + [a(d + f) + b(c + e)]\sqrt{5}\end{aligned}$$

Hence

$$(a + b\sqrt{5})[(c + d\sqrt{5}) + (e + f\sqrt{5})] = (a + b\sqrt{5})\,(c + d\sqrt{5}) + (a + b\sqrt{5})\,(e + f\sqrt{5})$$

Therefore the left distributive property holds in $\mathbb{Q}(\sqrt{5})$.

The proof of the right distributive property is similar. Hence $\mathbb{Q}(\sqrt{5})$ is a ring. Since the element $1 + 0\sqrt{5} = 1 \in \mathbb{Q}(\sqrt{5})$ and it satisfies the condition that

$$(a + b\sqrt{5})1 = a + b\sqrt{5} = 1(a + b\sqrt{5})$$

Therefore $\mathbb{Q}(\sqrt{5})$ is a ring with identity.

$\mathbb{Q}(\sqrt{5})$ is a field, since every $a + b\sqrt{5} \in \mathbb{Q}(\sqrt{5})$, $a \neq 0$, $b \neq 0$ has the inverse

$$\frac{a}{a^2 - 5b^2} + \frac{-b}{a^2 - 5b^2}\sqrt{5}$$

(Note $a^2 - 5b^2 \neq 0$ since there exist no rationals a and b so that $a/b = \sqrt{5}$). Hence $\mathbb{Q}(\sqrt{5})$ is a field.

Problem 3.2 If in a ring R, $a^2 = a$ for each $a \in R$, prove that R is commutative.

Solution Since $a \in R$, $a + a \in R$. We note that,

$$(a + a)^2 = a + a$$

By distributive property, we get

$$a^2 + a^2 + a^2 + a^2 = a + a$$

or

$$a + a + a + a = a + a \qquad (\text{as } a^2 = a)$$

Now using cancellation property, we have

$$a + a = 0 \tag{1}$$

Hence $a = -a$, for all $a \in R$.

Next, let $a, b \in R$ be arbitrary. Then

$$(a + b)^2 = a + b$$

By distribution property, we have

$$a^2 + ab + ba + b^2 = a + b$$

or

$$a + ab + ba + b = a + b \qquad (\text{as } a^2 = a,\ b^2 = b)$$

Now using cancellation properties of addition, we get

$$ab + ba = 0$$

Therefore, $ab = -ba$. From Eq. (1), $ab = ba$. So, R is commutative.

Problem 3.8 If F is a field of characteristic m, prove that

$$(a + b)^m = a^m + b^m$$

for $a, b \in F$.

Solution Since m is the characteristic of F, $ma = 0$ for any $a \in F$. Now

$$\begin{aligned}(a + b)^m &= a^m + ma^{m-1}b + \frac{m(m-1)}{2!}a^{m-2}b^2 + \cdots + b^m \\ &= a^m + 0 + \ldots + 0 + b^m \\ &= a^m + b^m\end{aligned}$$

5. Let G be a group. Show that if $G/Z(G)$ is cyclic, then G is abelian.

Proof. To show G is abelian, we must show that given $g_1, g_2 \in G$, then

$$g_1 g_2 = g_2 g_1.$$

To begin, since the group $G/Z(G)$ is cyclic, it has a generator $[g] \in G/Z(G)$ for some $g \in G$. It follows that there are integers n_1, n_2 such that

$$[g_1] = [g]^{n_1} \text{ and } [g_2] = [g]^{n_2}.$$

We can rewrite this by saying that there exists $z_1, z_2 \in Z(G)$ such that $g_1 = g^{n_1} z_1$ and $g_2 = g^{n_2} z_2$. Then

$$g_1 g_2 = g^{n_1} z_1 g^{n_2} z_2 = g^{n_2} z_2 g^{n_1} z_1 = g_2 g_1$$

since by definition z_1, z_2 commute with all elements of G, and g commutes with itself. □

Example 3. *Consider* $Z_7 = [0, 1, 2, 3, \ldots\ldots 6, +_7, \times_7]$. *Show that* Z_7 *is a field.*

Sol. Consider the addition modulo 7 table as shown in Table I.

Table I

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

We first show that Z_7 is a ring under addition modulo 7 and multiplication modulo 7.

From Table I, we observe that each element inside the table is also in Z_7. It means that Z is closed under $+_7$.

Addition modulo is always associative

The first row inside the table coincides with the top most row of Table I. It means 0 is the additive identity.

Each element of Z_7 has additive inverse.

For example, Inverse of 1 is 6. Inverse of 2 is 5 etc. $\quad | 1 +_7 6 = 7 = 0$

$\quad | 2 +_7 5 = 7 = 0$

Also Table I is symmetrical w.r.t. $+_7$. It means Z_7 is additive w.r.t. $+_7$ *i.e.*,

For $\quad a, b \in Z_7, a +_7 b = b +_7 a \ \forall\ a, b \in Z_7$.

$\therefore$ Z_7 is an additive group w.r.t $+_7$.

Now consider the multiplication modulo 7 table as shown in Table II.

Table II

$\times_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

From Table II, we observe that each element inside the table is also in Z_7. It means Z_7 is closed w.r.t. $\times_7$. *i.e.*, for $a, b \in Z_7 \ \Rightarrow \ a \times_7 b \in Z_7 \ \forall\ a, b \in Z_7$

Finally, For $a, b, c \in Z_7$,

$$a \times_7 (b +_7 c) = a \times_7 b +_7 a \times_7 c$$

$(a +_7 b) \times_7 c = a \times_7 c +_7 6 \times_7 c$ is true for all $a, b, c \in Z_7$.

Hence Z_7 is a ring w.r.t. addition modulo 7 and multiplication modulo 7.

Also the Table II is symmetrical w.r.t. $\times_7$. It means that Z_7 is commutative *i.e.*,

$$a \times_7 b = b \times_7 a \ \forall\ a, b \in Z_7$$

Further, the second row inside the table coincides with the topmost row of Table II. It means 1 is the multiplicative identity of Z_7.

Hence, we have shown that Z_7 is a commutative ring with unity. To show Z_7 is a field, we show each non-zero element of Z_7 has multiplicative inverse.

The units of Z_7 are those elements which are relative primes to 7. (See Topic on 'units')

The elements which are prime to 7 are 1, 2, 3, 4, 5, 6. Hence the units of Z_7 are 1, 2, 3, 4, 5, 6. We can also check the elements which are units as below.

$$1 \times_7 1 = 1\ ;\ 2 \times_7 4 = 1\ ;\ 3 \times_7 5 = 1\ ;$$

$$4 \times_7 2 = 1\ ;\ 5 \times_7 3 = 1\ ;\ 6 \times_7 6 = 1.$$

Hence, each non-zero element of Z_7 has multiplicative inverse. Therefore Z_7 is a field.

Example 2. *Consider the set M of all 2 × 2 matrices of the type* $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ *where* $\bar{a}$, $\bar{b}$ *are the conjugates of a and b. Is M a field ? Justify your answer.*

Sol. Consider A, B ∈ M where $A = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$

Then $$AB = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 5 \\ 1 & 5 \end{pmatrix}$$

Also $$BA = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 5 \\ 1 & -1 \end{pmatrix} \neq AB$$

Hence M is not commutative and therefore cannot be field.

Any number of the form $a + ib$, $a, b \in Z$ is called a Gaussian integer.

Example 4. *Show that the set J[i] of Gaussian integers form a ring under addition and multiplication. Is it an integral domain ? Is it field ?*

Sol. Let X = [$a + ib$, $a, b \in Z$] be the set of Gaussian integers. Then X is a ring.

We check X for integral domain.

Let $a + ib$, $c + id \in X$ such that a, b, c, d are non-zero integers.

Consider $(a + ib)(c + id) = 0$

$\Rightarrow \quad ac - bd + i(ad + bc) = 0 = 0 + 0i$

$\Rightarrow \quad ac - bd = 0, \quad ad + bc = 0,$

which is possible if either $a = 0 = b$ or $c = 0 = d$ *i.e.,* if either $a + ib = 0$ or $c + id = 0$

Hence X is without zero divisor. Therefore, X is an integral domain.

Further, if $0 \neq a + ib \in X$ be any non-zero element of X where $a, b \in Z$, then the multiplicative inverse of $a + ib$ is

$$\frac{1}{a+ib} = \frac{1}{a+ib} \times \frac{a-ib}{a-ib} = \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} - i\,\frac{b}{a^2+b^2} \notin J[i]$$

Since $\dfrac{a}{a^2+b^2}$ is not necessary an integer.

$\therefore$ X cannot be a field.

Example 1. *The ring of integers is a Euclidean domain.*

Sol. For $0 \neq a \in \mathbb{Z}$, define $d(a) = |a|$ (non-negative integer)

Let $0 \neq a, 0 \neq b \in \mathbb{Z}$. consider

$$d(ab) = |ab| = |a||b| \geq |a| = d(a)$$

$$\Rightarrow \quad d(ab) \geq d(a)$$

Also for $0 \neq a, b \in \mathbb{Z}$, we can find $q, r \in \mathbb{Z}$ such that $b = qb + r$, where $r = 0$ or $d(r) < d(a)$.

Hence $\mathbb{Z}$ is a Euclidean domain.

Example 2. *Every field is a Euclidean domain.*

Sol. For $0 \neq 0 \in F$, define $d(a) = 1$

| Since if $0 \neq a \in F$ and F is a field, we can find $a^{-1} \in F$ such that $aa^{-1} = 1 = d(a) \in F$

Let $0 \neq a, 0 \neq b \in F \Rightarrow ab \in F$

Now $d(ab) = 1 \geq d(a) \Rightarrow d(ab) \geq d(a)$

Also for $0 \neq b \in F$, we can write

$$a = (ab^{-1})\, b + 0 = qb + r \quad \text{where} \quad q = ab^{-1}, r = 0$$

Hence every field is an integral domain.

2. Factor $x^6 + 6 \in \mathbb{Z}_7[x]$ into linear terms in $\mathbb{Z}_7[x]$.

Solution. Let $f(x) = x^6 + 6 \in \mathbb{Z}_7[x]$. By Fermat's Theorem we have $\alpha^6 \equiv 1 \pmod 7$ for all $0 \neq \alpha \in \mathbb{Z}_7$. Thus $f(\alpha) = 0$ for all $0 \neq \alpha \in \mathbb{Z}_7$ (note that this also follows easily by inspection). It follows that $(x - \alpha)$ divides $f(x)$ for all $0 \neq \alpha \in \mathbb{Z}_7$. Consequently

$$x^6 + 6 = (x-1)(x-2)(x-3)(x-4)(x-5)(x-6)q(x) \in \mathbb{Z}_7[x],$$

for some $q(x) \in \mathbb{Z}_7[x]$. For reasons of degree, $\deg q(x) = 1$. By considering the coefficient of x^6, it is clear that $q(x) = 1$. Thus

$$x^6 + 6 = (x-1)(x-2)(x-3)(x-4)(x-5)(x-6) \in \mathbb{Z}_7[x].$$

1. Let $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$. Show that $\mathbb{Z}[\sqrt{3}]$ is a ring under the ordinary addition and multiplication of real numbers.

Solution. $\mathbb{Z}[\sqrt{3}]$ is a subset of the ring $(\mathbb{R}, +, \cdot)$. Let us first show that $\mathbb{Z}[\sqrt{3}]$ is closed under both $+$ and $\cdot$. Indeed, we have

$$a + b\sqrt{3} + a' + b'\sqrt{3} = (a + a') + (b + b')\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$

and

$$(a + b\sqrt{3}) \cdot (a' + b'\sqrt{3}) = (aa' + 3bb') + (ab' + a'b)\sqrt{3} \in \mathbb{Z}[\sqrt{3}].$$

Moreover, since $(a + b\sqrt{3}) + (-a' - b'\sqrt{3}) = (a - a') + (b - b')\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, it follows that $(Z[\sqrt{3}], +)$ is a subgroup of $(\mathbb{R}, +)$, and is thus an abelian group. (We are using the fact that if G is a group, and $S \subseteq G$ is a subset, then S is a subgroup if and only if $ab^{-1} \in S$ for all $a, b \in S$.)

To check that $(Z[\sqrt{3}], +, \cdot)$ is a ring, we must check that $(Z[\sqrt{3}], +)$ is an abelian group (which we have done above), that $\cdot$ is associative (this is true since it is true for $\mathbb{R}$), and that the distributive laws hold (this is also true since it is true for $\mathbb{R}$). Thus $(Z[\sqrt{3}], +, \cdot)$ is a ring. □

6. If G is a group and $|G : Z(G)| = 4$, prove that $G/Z(G)$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Solution. Every four element subgroup is either isomorphic to $\mathbb{Z}_4$ (a cyclic group) or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (the Klein 4-Group). Because there are only two options, assume the opposite, that $G/Z(G) \cong \mathbb{Z}_4$. We then know that $G/Z(G)$ is cyclic because $\mathbb{Z}_4$ is. From a previously proved theorem, if a factor group is cyclic then the overall group is Abelian so G must be Abelian. However, if this were the case, then the center $Z(G) = G$, and $|G/Z(G)| = |G/G| = |G|/|G| = 1$ which contradicts our assumption that is is four. Our factor group must then be isomorphic to the Klein 4-Group.

3. (a) What is the order of the element $14 + \langle 8 \rangle$ in $\mathbb{Z}_{24}/\langle 8 \rangle$?

Solution. We must find the smallest m such that $14m \in \langle 8 \rangle = \{8k, k \in \mathbb{Z}\}$. The number $14m$ will then be the least common multiple of 8 and 14, and $m = \text{lcm}(8, 14)/14 = 56/14 = 4$.

(b) What is the order of $4U_5(105)$ in the factor group $U(105)/U_5(105)$.

Solution. We must find the smallest m such that $4^m \in U_5(105)$, so 4^m must be relatively prime to 105 and $4^m = 5k + 1, 0 \leq k \leq 20$. $105 = 3 * 5 * 7$, and $4^m = 2^{2m}$, so 4^m will always be relatively prime to 105 because they share no common factors. We must then find the smallest m such that $4^m = 5k + 1$. For $m = 1$ we $4 \neq 1 \mod 5$, but for $m = 2$ we have $4^2 = 16 = 5(3) + 1 \in U_5(105)$, so $|4U_5(105)| = 2$.

4. Let $G = \mathbb{Z}_4 \oplus U(4)$, $H = \langle (2, 3) \rangle$ and $K = \langle (2, 1) \rangle$. Show that $G/H \ncong G/K$.

Solution. Note that $G = \{(0, 1), (0, 3), (1, 1), (1, 3), (2, 1), (2, 3), (3, 1), (3, 3)\}$. G/K and G/H will both have four elements. We can label the cosets of H as: $G/H = \{H, (1, 1)H, (2, 1)H, (3, 1)H\}$, and it is easy to see that the coset $(1, 1)H$ has order 4 and will generate the factor group, so G/H is cyclic. On the other hand, we can label the cosets of K as $G/K = \{K, (0, 3)K, (1, 1)K, (1, 3)K\}$, yet all the elements except the identity have order two, so none of them can generate the group and G/K is not cyclic. Therefore $G/H \ncong G/K$.

5. (a) (15 points) How many homomorphisms are there from $\mathbb{Z}_{15}$ to $\mathbb{Z}_{10}$?

(b)(15 points) Let $\varphi : \mathbb{Z}_{20} \to \mathbb{Z}_{10}$ be a homomorphism such that $\varphi(4) = 2$ and $\varphi(5) = 5$. Determine φ, $\text{im}(\varphi)$ and $\ker(\varphi)$.

Solution:
(a) Since $\mathbb{Z}_{15}$ is cyclic, the image of 1 completely determines φ. If $\varphi(1) = a$ then the order of a in $\mathbb{Z}_{10}$ must divide both 10 and 15, so it must be 1 or 5.
If $|a| = 1$ then $a = 0$ is the only possibility.
If $|a| = 5$, then a can have 4 values (the Euler function of 5).

So there are 5 such homomorphisms.

(b) Since $5 - 4 = 1$, therefore $\phi(1) = \phi(5) - \phi(4) = 3$. Thus $\varphi(x) = 3x \mod 10$. Then $\text{im}(\varphi) = \langle 3 \rangle = \mathbb{Z}_10$ and $\ker(\varphi) = \langle 10 \rangle \subset \mathbb{Z}_{20}$.

1. (15 points) Let G be a group of order 21, which has exactly one subgroup of order 3 and exactly one subgroup of order 7. Show that G is cyclic.

Solution:
Assume G is not cyclic. Then all elements in G have order 1, 3 or 7. Since there is only one subgroup of order 7, there are 6 elements of order 7. Since there is only one subgroup of order 3, there are 2 elements of order 3. There is one element of order 1. Thus the group only has $6 + 2 + 1 = 9$ elements, not 21, a contradiction.

 # 4.14: Suppose that a cyclic group G has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 7. What is $|\ G\ |$? What can you say if 7 is replaced with p where p is a prime?

- Since G is cyclic, there is some element a in G such that $\langle a\rangle = G$. Since G has a subgroup of order 7, and G is cyclic, we know that 7 divides the order of G. That is, $|\ \langle a\rangle\ | = |\ G\ | = 7n$ for some positive integer n. We now test a few possible values of n:
  - Suppose $n = 1$. Then G and one of its subgroups both have order 7. By the Fundamental Theorem of Cyclic Groups (FTCG), G and its subgroup of order 7 are the same, contradicting the condition that G has 3 distinct subgroups.
  - Suppose n is 2, 3, 4, 5, or 6. Then, by FTCG, $G = \langle a\rangle$ has a subgroup of order n. Thus, G has at least 4 subgroups: $\{e\}$, the subgroup of order 7, the subgroup of order n, and G itself. This contradicts the fact that G has exactly three subgroups.
  - Suppose $n = 7$. Then $|\ G\ | = 7 \cdot 7 = 49$. Since 7 is the only positive divisor of 49 between 1 and 49, it is the only possible order of a subgroup other than $\{e\}$ or G. FTCG also tells us that there is *exactly* one subgroup of order 7. This fits the supposed criteria.
  - In general, if we suppose that n is any positive integer besides 7, we see that G is guaranteed a subgroup of order n by the FTCG, which means that G will have *at least* 4 distinct subgroups.

  We therefore conclude that the order of G must be $7^2 = 49$.
- More generally, if 7 is replaced by any prime p under the supposed conditions, the the order of G must be p^2.

 # 5.34: Let $H = \{\beta \in S_5 \mid \beta(1) = 1 \text{ and } \beta(3) = 3\}$. Prove that H is a subgroup of S_5. Is your argument valid when 5 is replaced by any $n \geq 3$?

- We use the Two-Step Subgroup Test. Let α, γ be elements of H. Then:

$$\begin{aligned}\alpha\gamma(1) &= \alpha(\gamma(1)) \\ &= \alpha(1) = 1,\end{aligned}$$

  and

$$\begin{aligned}\alpha\gamma(3) &= \alpha(\gamma(3)) \\ &= \alpha(3) = 3,\end{aligned}$$

  so $\alpha\gamma$ is in H. Also, since $1 = \alpha^{-1}(\alpha(1)) = \alpha^{-1}(1)$ and $3 = \alpha^{-1}(\alpha(3)) = \alpha^{-1}(3)$, we see that α^{-1} is in H. This gives the desired result.
- Replacing S_5 with S_n for any $n \geq 3$ does not affect the argument.

 # 5.36: In S_4, find a cyclic subgroup of order 4 and a noncyclic subgroup of order 4.

- The subgroup of S_4 generated by (1234) is cyclic, since $(1234)^4 = e$, and the set $\{e, (1234), (1234)^2, (1234)^3\}$ is closed under composition.
- Referencing the table given for A_4 in chapter 5 (note that A_4 is a subgroup of S_4), we can see readily that $\{(1), (12)(34), (13)(24), (14)(23)\}$ gives a non-cyclic subgroup of S_4 that has order 4.

 # 5.28: Let $\beta = (123)(145)$. Write β^{99} in disjoint cycle form.

- In disjoint cycle form, $\beta = (14523)$. Thus, the permutation has order 5, and $\beta^5 = e$. Therefore,

$$\begin{aligned}\beta^{99} &= \beta^{5\cdot 19+4}\\ &= (\beta^{5\cdot 19})\beta^4\\ &= (\beta^5)^{19}\beta^4\\ &= e^{19}\beta^4\\ &= \beta^4\end{aligned}$$

- Now we compute $\beta^4 = (14523)(14523)(14523)(14523) = (13254)$. Thus, $\beta^{99} = (13254)$.

 # 5.18: Let $\alpha = \begin{bmatrix}1&2&3&4&5&6&7&8\\2&3&4&5&1&7&8&6\end{bmatrix}$ and $\beta = \begin{bmatrix}1&2&3&4&5&6&7&8\\1&3&8&7&6&5&2&4\end{bmatrix}$. Write α, β, and $\alpha\beta$ as

- products of disjoint cycles,
  - $\alpha = (12345)(678)$
  - $\beta = (23847)(56)$
  - $\alpha\beta = (12345)(678)(23847)(56) = (12485736)$
- products of 2-cycles.
  - $\alpha = (15)(14)(13)(12)(68)(67)$
  - $\beta = (27)(24)(28)(23)(56)$
  - $\alpha\beta = (16)(13)(17)(15)(18)(14)(12)$

 # 5.9: Determine whether the following permutations are even or odd.

- (135): Written as a product of 2-cycles, we get (15)(13), so this is even.
- (1356): Written as a product of 2-cycles, we get (16)(15)(13), so this is odd.
- (13567): Written as a product of 2-cycles, we get (17)(16)(15)(13), so this is even.
- (12)(134)(152): Written as a product of disjoint cycles, we get (15)(234). Rewritten as a product of 2-cycles, we get (15)(24)(23), so this is odd.
- (1243)(3521): Written as a product of disjoint cycles, we get (354). Rewritten as a product of 2-cycles, we get (34)(35), so this is even.

 # 5.3: What is the order of each of the following permutations?

- (124)(357): disjoint, both of length 3, so the order of the permutation is $lcm(3,3) = 3$
- (124)(3567): disjoint and of lengths 3 and 4, so the order of the permutation is $lcm(3,4) = 12$
- (124)(35): disjoint and of lengths 3 and 2, so the order of the permutation is $lcm(3,2) = 6$
- (124)(357869): disjoint and of lengths 3 and 6, so the order of the permutation is $lcm(3,6) = 6$
- (1235)(24567): not disjoint, so we rewrite this permutation as a product of disjoint cycles. The result is (124)(3567), with cycles of orders 3 and 4, so the order of the permutation is $lcm(3,4) = 12$
- (345)(245): not disjoint, so we rewrite this permutation as a product of disjoint cycles. The result is (25)(34), so the order of the permutation is $lcm(2,2) = 2$

 # 4.22: Prove that a group of order 3 must be cyclic.

- Seeking a contradiction, let G be a group of order 3 that is not cyclic. Thus G has an identity element e, and two additional elements, call them a and b. Since $\langle a \rangle$ and $\langle b \rangle$ are both subgroups of G, they both contain e. Since G is not cyclic, b is not in $\langle a \rangle$ and a is not in $\langle b \rangle$. Thus, it must be true that $a^2 = e$ and $b^2 = e$, or else we would have that $ea = aa = a$ and $eb = bb = b$, which would mean that not G is not a group (see HW#2, Question 5). Putting all of this into a multiplication table, we see:

$G =$

	e	a	b
e	e	a	b
a	a	e	
b	b		e

Thus we now only need to determine the products ab and ba. But notice that ab and ba cannot be e, a, or b (by HW#2, Question 5). Thus, G is not closed, which contradicts the fact that G is a group. Since the assumption that G is not cyclic leads to this absurdity, we conclude that G must be cyclic.

 # 4.8: Let a be an element of a group and let $| a | = 15$. Compute the orders of the following elements of G:

- a^3, a^6, a^9, a^{12}
  - For each a^k above, $\gcd(15, k) = 3$. Thus, the order of each is $15/3 = 5$.
- a^5, a^{10}
  - For each a^k above, $\gcd(15, k) = 5$. Thus, the order of each is $15/5 = 3$.
- a^2, a^4, a^8, a^{14}
  - For each a^k above, $\gcd(15, k) = 1$. Thus, the order of each is $15/1 = 15$.

 # 1:

- $\mathbb{Z}_{12}$:
  - $| \mathbb{Z}_{12} | = 12$;
  - $| 0 | = 1$; $| 1 | = 12$; $| 2 | = 6$; $| 3 | = 4$; $| 4 | = 3$; $| 5 | = 12$; $| 6 | = 2$; $| 7 | = 12$; $| 8 | = 3$; $| 9 | = 4$; $| 10 | = 6$; $| 11 | = 12$.
- $U(10)$:
  - $| U(10) | = \phi(10) = \phi(2 \cdot 5) = (1)(4) = 4$;
  - $| 1 | = 1$; $| 3 | = 4$; $| 7 | = 4$; $| 9 | = 2$.
- $U(12)$:
  - $| U(12) | = \phi(12) = \phi(2^2 \cdot 3) = (2)(2) = 4$;
  - $| 1 | = 1$; $| 5 | = 2$; $| 7 | = 2$; $| 11 | = 2$.
- $U(20)$:
  - $| U(20) | = \phi(20) = \phi(2^2 \cdot 5) = (2)(4) = 8$;
  - $| 1 | = 1$; $| 3 | = 4$; $| 7 | = 4$; $| 9 | = 2$; $| 11 | = 2$; $| 13 | = 4$; $| 17 | = 4$; $| 19 | = 2$.
- D_4:
  - $| D_4 | = 8$;
  - $| R_0 | = 1$; $| R_{90} | = 4$; $| R_{180} | = 2$; $| R_{270} | = 4$; $| H | = 2$; $| V | = 2$; $| D | = 2$; $| D' | = 2$.
- *Observations*: The order of every element divides the order of the group.

 # 4: Prove that in any group, an element and its inverse have the same order.

– Seeking a contradiction, suppose that this is not true. That is, suppose that there are elements a and a^{-1} such that $|\ a\ | = n$ and $|\ a^{-1}\ | = m$, with n and m positive integers such that $n \neq m$. Without loss of generality, suppose also that $m < n$. Then $e = e \cdot e = (a^n) \cdot ((a^{-1})^m) = a^{n-m}$. The consequence that $a^{n-m} = e$ implies that n is not the order of a, contradicting our assumption. We conclude that $n = m$.

 # 29: Let G be an Abelian group with identity e and let n be some fixed integer. Prove that the set of all elements of G that satisfy the equation $x^n = e$ is a subgroup of G.

– Let H denote the subset of G satisfying $x^n = e$. We use the Two-Step Subgroup Test.

1. Let x and y be in H. Thus $x^n = y^n = e$ and

$$\begin{aligned}(xy)^n &= \underbrace{xy \cdot xy \cdot \ldots \cdot xy}_{n \text{ times}} = x^n y^n \quad \text{(since } G \text{ is abelian)} \\ &= e \cdot e = e.\end{aligned}$$

   Therefore $xy \in H$ as desired.
2. Let $x \in H$. Then $x^n = e$ and thus $(x^{-1})^n = (x^n)^{-1} = e^{-1} = e$. Therefore $x^{-1} \in H$, and H is a subgroup of G.

– An example of a group G in which the set of all elements of G that satisfy $x^2 = e$ does not form a subgroup of G:

- Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.
  – Suppose that G is an Abelian group with $a, b \in G$. We have

$$\begin{aligned}(ab)^{-1} &= b^{-1}a^{-1} \quad \text{by the socks-shoes lemma} \\ &= a^{-1}b^{-1} \quad \text{since } G \text{ is Abelian.}\end{aligned}$$

  – Now suppose that $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$. Again, by the socks-shoes lemma, we have $(ab)^{-1} = b^{-1}a^{-1}$, and thus

$$a^{-1}b^{-1} = b^{-1}a^{-1}$$

  for all a, b in G. Multiplying by a on both the left and the right gives:

$$aa^{-1}b^{-1}a = ab^{-1}a^{-1}a$$

  and thus canceling the inverses gives

$$b^{-1}a = ab^{-1}.$$

  Now multiplying on both the right and the left by b gives

$$bb^{-1}ab = bab^{-1}b$$

  and canceling the inverses gives

$$ab = ba.$$

  Since this equation holds for all a and b in G, we have that G is Abelian.

1. Let $GL_2(\mathbb{Z}_2)$ denote the collection of 2×2 matrices with entries in $\mathbb{Z}_2$ which have *non-zero* determinant.(We listed these matrices out in class.)

   (a) Make a multiplication table for $GL_2(\mathbb{Z}_2)$.

   - Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $C = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, $D = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $E = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, and $F = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.
   - The multiplication table may be expressed as follows:

	A	B	C	D	E	F
A	A	B	C	D	E	F
B	B	C	A	F	D	E
C	C	A	B	E	F	D
D	D	E	F	A	B	C
E	E	F	D	C	A	B
F	F	D	E	B	C	A

   (b) Which pairs of matrices satisfy $a \cdot b = b \cdot a$?

   - For all $b \in GL_2(\mathbb{Z}_2)$, $A \cdot b = b \cdot A$. That is, every element commutes with the identity.
   - Every element also commutes with itself.
   - The only other pair that commutes is (B, C).

   (c) Are there any elements which commute with *every* other matrix? That is, find all elements a in $GL_2(\mathbb{Z}_2)$ such that $a \cdot b = b \cdot a$ for every b in $GL_2(\mathbb{Z}_2)$.

   - The only element which commutes with every other element in this table is the identity.

   (d) For each matrix a, compute a, a^2, a^3, and so on until the pattern is clear. Determine the length of the repeating cycle for each matrix.

   - Let a = A. Then we have A, A, A,.... Cycle length is 1.
   - Let a = B. Then we have B, C, A, B, C,.... Cycle length is 3.
   - Let a = C. Then we have C, B, A, C, B,.... Cycle length is 3.
   - Let a = D. Then we have D, A, D, A,.... Cycle length is 2.
   - Let a = E. Then we have E, A, E, A,.... Cycle length is 2.
   - Let a = F. Then we have F, A, F, A,.... Cycle length is 2.

4. Let $U(9)$ denote the collection of units in $\mathbb{Z}_9$ (see HW #1 question 2). There should be 6 such units.

(a) Make a multiplication table for $U(9)$.

- The multiplication table is as follows:

·	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

(b) Which pairs of elements of $U(9)$ satisfy $a \cdot b = b \cdot a$?

- All pairs of elements satisfy $a \cdot b = b \cdot a$.

(c) For each element a in $U(9)$, compute a, a^2, a^3, and so on until the pattern is clear. Determine the length of the repeating cycle for each matrix.

- Let a = 1. Then we have 1, 1, 1,.... Cycle length is 1.
- Let a = 2. Then we have 2, 4, 8, 7, 5, 1,.... Cycle length is 6.
- Let a = 4. Then we have 4, 7, 1, 4, 7, 1, ... Cycle length is 3.
- Let a = 5. Then we have 5, 7, 8, 4, 2, 1, ... Cycle length is 6.
- Let a = 7. Then we have 7, 4, 1, 7, 4, 1, ... Cycle length is 3.
- Let a = 8. Then we have 8, 1, 8, 1,.... Cycle length is 2.

(d) Any observations? How does the group $U(9)$ compare with the two other groups on this problem set of size 6?

- $U(9)$ is different from the other groups. For one, every element commutes with every other element, which is not true in the others. Also, $U(9)$ has elements that produce different cycle lengths than the others.

- #3 Show that (a) $\{1, 2, 3\}$ under multiplication modulo 4 is not a group, but that (b) $\{1, 2, 3, 4\}$ under multiplication modulo 5 is a group.

  (a) This is not a group, since it is not closed. Consider that $2 \cdot 2 \equiv 0 \pmod 4$, and that 0 is not in the set.

  (b) This is a group. A quick multiplication table shows that the operation is binary. By associativity of multiplication in the integers, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, so the operation is associative. Consider any element $a \in \mathbb{Z}_5 - \{0\}$. Then $1 \cdot a = a \cdot 1 = a$, so there is an identity, namely 1. Consider any element $a \in \mathbb{Z}_5 - \{0\}$. Then a has an inverse. The justification follows: $1 \cdot 1 = 1 \equiv 1 \pmod 5$; $2 \cdot 3 = 6 \equiv 1 \pmod 5$; $3 \cdot 2 = 6 \equiv 1 \pmod 5$; $4 \cdot 4 = 16 \equiv 1 \pmod 5$.

- #5 Find the inverse of the matrix $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $GL(2, \mathbb{Z}_{11})$.

  We have

$$\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}^{-1} = \frac{1}{2 \cdot 5 - 3 \cdot 6} \begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 5 & 5 \\ 8 & 2 \end{bmatrix} = 4 \begin{bmatrix} 5 & 5 \\ 8 & 2 \end{bmatrix} = \begin{bmatrix} 9 & 9 \\ 10 & 8 \end{bmatrix}.$$

2. Compute $2^{2047423023} \pmod{11}$.

- Fermat's Little Theorem tells us that $a^p \equiv a \pmod{p}$, where p is a prime. Or, if a and p are coprime, then $a^{p-1} \equiv 1 \pmod{p}$.

  Since 2 and 11 are coprime, we make use of the second part of Fermat's Little Theorem, which tells us that $2^{10} \equiv 1 \pmod{11}$. This also means that $2^{20} = 2^{10} \cdot 2^{10} \equiv 1 \cdot 1 = 1 \pmod{11}$, and in general that $2^{10b} \equiv 1 \pmod{11}$, where b is any positive integer. Thus, $2^{2047423023} = 2^{2047423020} \cdot 2^3 \equiv 1 \cdot 2^3 = 8 \pmod{11}$.

3. Find the multiplicative inverse of 7 in $\mathbb{Z}_{11}$. Find the multiplicative inverse of 7 in $\mathbb{Z}_{101}$.

- In $\mathbb{Z}_{11}$, the multiplicative inverse of 7 is 8, since $7 \cdot 8 = 56 \equiv 1 \pmod{11}$.
- In $\mathbb{Z}_{101}$, the multiplicative inverse of 7 is 29, since $7 \cdot 29 = 203 \equiv 1 \pmod{101}$.

5. Compute the order of $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ in $\mathrm{GL}_2(\mathbb{Z}_3)$ - that is, find the smallest positive integer d such that A^d is the identity matrix.

   - We do this problem with direct computation:
   - $A^1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
     $A^2 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$
     $A^3 = \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}$
     $A^4 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$
     $A^5 = \begin{bmatrix} 0 & 2 \\ 2 & 2 \end{bmatrix}$
     $A^6 = \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix}$
     $A^7 = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$
     $A^8 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
   - We conclude that the order of $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ is 8.

3. Compute the following values: $\phi(100)$, $\phi(40)$, $\phi(101)$.
   [Recall that we have formulas $\phi(p^n) = p^n - p^{n-1}$ and $\phi(mn) = \phi(m)\phi(n)$ if m and n are relatively prime.]

   - $\phi(100) = \phi(2^2 \cdot 5^2) = (2-1)(2^1)(5-1)(5^1) = (1)(2)(4)(5) = 20$
   - $\phi(40) = \phi(2^3 \cdot 5^1) = (2-1)(2^2)(5-1)(5^0) = (1)(4)(4)(1) = 16$
   - $\phi(101) = (101-1)(101^0) = 100$ (101 is a prime!)

4. Give 5 examples of groups with 8 elements. Do these groups have distinct multiplication tables up to reordering?

   - $(\mathbb{Z}_8, +)$, i.e. $\mathbb{Z}_8$ under addition
   - $U(15)$, since $\phi(15) = \phi(3 \cdot 5) = (3-1)(5-1) = (2)(4) = 8$.
   - $U(16)$, since $\phi(16) = \phi(2^4) = (2-1)(2^3) = (1)(8) = 8$.
   - $U(20)$, since $\phi(20) = \phi(2^2 \cdot 5) = (2-1)(2^1)(5-1) = (1)(2)(4) = 8$.
   - $U(24)$, since $\phi(24) = \phi(2^3 \cdot 3) = (2-1)(2^2)(3-1) = (1)(4)(2) = 8$.

52. Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} | a \in \mathbf{R}, a \neq 0 \right\}$. Show that G is a group under matrix multiplication. Explain why each element of G has an inverse even though the matrices have 0 determinants. (Compare with Example 10.)

$$G = \left\{ X_a = \begin{pmatrix} a & a \\ a & a \end{pmatrix} \middle| a \in \mathbf{R}, a \neq 0 \right\}$$

Let $X_a, X_b \in G \Rightarrow X_a \cdot X_b = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix} = X_{2ab} \in G$

We have $X_a = X_b \Leftrightarrow a = b$

Comutativity:

$X_a \cdot X_b = X_{2ab} = X_{2ba} = X_b \cdot X_a$

Asociativity:

$(X_a \cdot X_b) \cdot X_c = X_{2ab} \cdot X_c = X_{4abc}$

$X_a \cdot (X_b \cdot X_c) = X_a \cdot X_{2bc} = x_{4abc}$

Then $(X_a \cdot X_b) \cdot X_x = X_a \cdot (X_b \cdot X_c)$

Identity element:

Let X_e be the identity element:

Then $X_a \cdot X_e = X_e \cdot X_a = X_a$

We have $X_a \cdot X_e = X_a \Leftrightarrow X_{2ae} = X_a \Leftrightarrow 2ae = a \Leftrightarrow e = \frac{1}{2}$

So the identity element is $X_{\frac{1}{2}} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

Reciprocal element:

Let $X_a \in G$ and $X_{a'} \in G$ the reciprocal element.

Then $X_a \cdot X_{a'} = X_{a'} \cdot X_a = X_{\frac{1}{2}}$

$X_{2aa'} = X_{\frac{1}{2}} \Rightarrow 2aa' = \frac{1}{2} \Rightarrow a' = \frac{1}{4a}$

So, the reciprocal element of X_a is $X_{\frac{1}{4a}}$

Each element has an inverse because the identity element is not I_2 and we can't apply the same rule for an inverse of a matrix.

1. Determine whether each of the following subsets is a subgroup of the given group. If not, state which of the subgroup axioms fails.

(a) The set of real numbers $\mathbb{R}$, viewed as a subset of the complex numbers $\mathbb{C}$ (under addition).

(b) The set $\pi\mathbb{Q}$ of rational multiples of π, as a subset of $\mathbb{R}$ (under addition).

(c) The set of $n \times n$ matrices with determinant 2, as a subset of $\mathrm{GL_n}(\mathbb{R})$.

(d) The set $\{i, m_1, m_2, m_3\} \subset D_3$ of reflections of the equilateral triangle, along with the identity transformation.

Solution. (a) Yes, $\mathbb{R}$ is a subgroup of $\mathbb{C}$. The sum of any two real numbers is real, $0 \in \mathbb{R}$, and if $a \in \mathbb{R}$, then $-a \in \mathbb{R}$.

(b) Yes, $\pi\mathbb{Q}$ is a subgroup of $\mathbb{R}$ under addition. The verification is almost identical to the argument that we gave in class to show that $\mathbb{Q}$ is a subgroup of $\mathbb{R}$.

(c) No, this set is not a subgroup of $\mathrm{GL_n}(\mathbb{R})$, since it is not closed. If A and B both have determinant 2, then $\det(AB) = 4$, so $AB \in \mathrm{GL_n}(\mathbb{R})$. It is also easy to see that this set does not contain the identity matrix, and that none of its elements possess inverses within the set.

(d) No, this is not a subgroup of D_3. It contains the identity by definition, and each element is its own inverse, but the set is not closed. For example, we saw that $m_1 m_2 = r_1$.

5. Let r and s be positive integers, and define

$$H = \{nr + ms : n, m \in \mathbb{Z}\}.$$

(a) Show that H is a subgroup of $\mathbb{Z}$.

(b) We saw in class that every subgroup of $\mathbb{Z}$ is cyclic. Therefore, $H = \langle d \rangle$ for some $d \in \mathbb{Z}$. What is this integer d? Prove that the d you've found is in fact a generator for H.

Proof. (a) We can verify directly that $H \leq \mathbb{Z}$. If $nr + ms, nt + mu \in H$, then

$$(nr + ms) + (nt + mu) = n(r + t) + m(s + u),$$

which is again in H. Thus H is closed. Also, $0 = n \cdot 0 + m \cdot 0 \in H$, and if $nr + ms \in H$, then

$$-(nr + ms) = n(-r) + m(-s) \in H,$$

so H is indeed a subgroup of $\mathbb{Z}$.

(b) We claim that H is generated by $d = \gcd(n, m)$. To prove this, we need to check that $H = \langle d \rangle$. First, note that since $d \mid n$ and $d \mid m$, $d \mid nr + ms$ for any $r, s \in \mathbb{Z}$. That is, any element of H is a multiple of d, so

$$H \subset \langle d \rangle = d\mathbb{Z}.$$

We also need to check that $d\mathbb{Z} \subset H$, and it is enough to show that $d \in H$. (Remember that any subgroup containing d must also contain the cyclic subgroup that it generates.) For this, we just need to remember Bézout's lemma/Extended Euclidean algorithm, which says that there are integers $x, y \in \mathbb{Z}$ such that

$$nx + my = \gcd(n, m) = d.$$

Therefore, $d \in H$, so $H = d\mathbb{Z}$. □

7. [Saracino, #5.22] Let G be a group. Define

$$Z(G) = \{a \in G : ax = xa \text{ for all } x \in G\}.$$

In other words, the elements of $Z(G)$ are exactly those which commute with *every* element of G. Prove that $Z(G)$ is a subgroup of G, called the **center** of G.

Proof. Suppose that $a, b \in Z(G)$. Then $ax = xa$ and $bx = xb$ for all $x \in G$, and for any $x \in G$ we have

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

so $ab \in Z(G)$. Therefore, $Z(G)$ is closed. Also, we certainly have $ex = xe = x$ for all $x \in G$, so $e \in Z(G)$. Finally, if $a \in Z(G)$, then

$$a^{-1}x = ((a^{-1}x)^{-1})^{-1} = (x^{-1}a)^{-1} = (ax^{-1})^{-1},$$

since a commutes with every element of G. Continuing, we have

$$(ax^{-1})^{-1} = xa^{-1},$$

so $a^{-1}x = xa^{-1}$, and $a^{-1} \in Z(G)$. Therefore, $Z(G)$ is a subgroup of G. □

8. Show that if H and K are subgroups of an *abelian* group G, then

$$\{hk : h \in H \text{ and } k \in K\}$$

is a subgroup of G.

Proof. Define

$$HK = \{hk : h \in H \text{ and } k \in K\}.$$

Let $a, b \in HK$. Then $a = h_1k_1$ and $b = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Now we have

$$ab = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k_1)k_2 = (h_1h_2)(k_1k_2),$$

where we have used the fact that G is abelian to interchange h_2 and k_1. Since $H \leq G$, $h_1h_2 \in H$, and similarly, $k_1k_2 \in K$, so $ab \in HK$. Therefore, HK is closed. Since H and K are both subgroups of G, $e \in H$ and $e \in K$, so $e = ee \in HK$. Finally, suppose that $a = hk \in HK$. Then

$$a^{-1} = (hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1},$$

again since G is abelian. Since $h^{-1} \in H$ and $k^{-1} \in K$, $a^{-1} \in HK$. Therefore, $HK \leq G$.

Note that the fact that G is abelian is crucial here. The result is not true in general for nonabelian groups. □

Page67:2

Let Q be the group of rational numbers under addition and let $Q*$ be the group of nonzero rational numbers under multiplication. In Q, list the elements in $< \frac{1}{2} >$. In $Q*$, list the elements in $< \frac{1}{2} >$.

$< \frac{1}{2} >= \{\ldots, -3\frac{1}{2}, -2\frac{1}{2}, -1\frac{1}{2}, 0, 1\frac{1}{2}, 2\frac{1}{2}, 3\frac{1}{2} \ldots\}$ in Q
$< \frac{1}{2} >= \{\ldots, (\frac{1}{2})^{-3}, (\frac{1}{2})^{-2}, (\frac{1}{2})^{-1}, (\frac{1}{2})^{0}, (\frac{1}{2})^{1}, (\frac{1}{2})^{2}, (\frac{1}{2})^{3}, \ldots\}$ in $Q*$

Page67:10

Prove that an Abelian group with two elements of order 2 must have a subgroup of order 4.

Let G be an Abelian group with distinct elements a, b such that $a^2 = b^2 = e$. Then the set of $H = \{e, a, b, ab\}$ has order 4 and it is the subgroup of G by Finite subgroup test.

Page132:5
Show that $U(8)$ is isomorphic to $U(12)$.
We define isomorphism $\phi : U(8) \to U(12)$ as follows:

$$\phi(1) = 1, \phi(3) = 5, \phi(5) = 7, \phi(7) = 11.$$

The mapping ϕ is apparently one-to-one and onto, and the multiplication tables of $U(8)$ and $U(12)$ are described as belows That shows the ϕ preserves

U(8)	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

U(12)	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

the group operation

Page148:2
Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of H in S_4.

$|S_4| = 24$ and $|H| = 4$ then $|S_4|/|H| = 24/4 = 6$ by Lagrange's Theorem.

Page148:8
Suppose that a has order 15. Find all of the left cosets of $< a^5 >$ in $< a >$.

The cosets should be $< a^5 >$, $a < a^5 >$, $a^2 < a^5 >$, $a^3 < a^5 >$, $a^4 < a^5 >$.

Page148:14
Supposer that K is a proper subgroup of H and H is a proper subgroup of G.
If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?

By Lagrange's theorem, we know that only 2, 5 can be numbers satisfying that $|H| = 2 \cdot 42,\ 5 \cdot 42$.

Page191:18
What is the order of the factor group $\mathbb{Z}_{60}/ < 15 >$?

The order of $\mathbb{Z}_{60}$ is 60 and $< 15 >$ is 4 then the factor group of order is $60/4 = 15$

Page191:21
Prove that an Abelian group of order 33 is cyclic.

Let's say p divides the order of an Abelian group G then G has an element of order p. There will be 2 element say (a, b) such that $a^3 = e$ and $b^11 = e$ because $33 = 3 \times 11$. Now we know that $(ab)^3 = a^3b^3 \neq e$ and $(ab)^{11} = a^11b^11 = a^2 \neq e$ in Abelian group so that 2 orders exist. Thus, $< ab >$ generates the cyclic group G.

Page191:69
Let G be a group. If $H = \{g^2 | g \in G\}$ is a subgroup of G, prove that it is a normal subgroup of G.

Say $g_1 \in G$ and $h \in H$ such that $h = g^2$. Need to show $g_1 H g_1^{-1} \in G$. Rewrite $g_1 h g_{1^{-1}} = g_1 g^2 g_1^{-1} = (g_1 g g_1^{-1})(g_1 g g_1^{-1}) = (g_1 g g_1^{-1})^2 \in H$ since $g_1 g g_1^{-1} \in G$.

Example8
$Z \oplus Z$ is not an integral domain.

There are zero divisors. see $(1, 0) \cdot (0, 1) = (0, 0)$.

Page254:05
Show that every nonzero element of Z_n is a unit or a zero-divisor.

Suppose that $x \in Z_n$ is not a zero-divisor. Then power(x^k just say k) of x is not a zero-divisor, too. if not there is a $y \in Z_n$ such that $x^k \cdot y = x \cdot x^{k-1} y = 0$. x is turned out to be a zero-divisor.

Invertibility of elements is only that is left to prove. Let's consider the set of $\{x^k | k \in Z\}$. Since Z_n is finite, we think of x^k and x^j as $x^k = x^j$

$$x^k = x^j = 0$$
$$x^j - x^k = x^k(x^{j-k} - 1) = 0$$

And we know x^k is not a zero-divisor, $x^{j-k} = 1$ and the equation implies that $x \cdot x^{j-k-1} = 1$. Thus, x has the inverse (x^{j-k-1}) of x.

Page254:11
Give an example of a commutative ring without zero-divisors that is not an integral domain.

Even integers do.

Page254:14
Show that the nilpotent elements of a commutative ring form a subring

goal: let S be the nilpotent elements of a commutative ring R then, show the S is under subtraction and multiplication.

Let $a, b \in S$ and $a^m = 0, b^n = 0$ for certain integers (say m, n)
First, we will deal with subtraction

$$(a-b)^{m+n} = \sum_{i=0}^{m+n} M = \begin{pmatrix} m+n \\ i \end{pmatrix} (-1)^i a^{m+n-i} b^i, \; a^{m+n-i} b^i = 0$$

for $0 \leq i \leq m+n$

Thus, $(a-b)^{m+n} = 0$ that means $a - b \in S$.

Second, multiplication.
$(ab^m) = a^m b^m = 0 \cdot b^m = 0$ that means $ab \in S$.

Page254:18
Find a zero-divisor in $Z_5[i] = \{a + bi | a, b \in Z_5\}$.

$(2+i)(2-i) = 4 + 1 = 0$, where $2+i$ and $2-i$ are zero divisors.

2.34 (i) How many elements of order 2 are there in S_5 and in S_6?

(ii) How many elements of order 2 are there in S_n?

Answer:

Case A: Let $n = 2k$. Then there are

$$\binom{n}{2} + \frac{\binom{n}{2}\binom{n-2}{2}}{2!} + \frac{\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}}{3!} + \ldots + \frac{\binom{n}{2}\binom{n-2}{2}\cdots\binom{2}{2}}{k!}$$

elements of order 2 in S_n.

Case B: Let $n = 2k + 1$. Then there are

$$\binom{n}{2} + \frac{\binom{n}{2}\binom{n-2}{2}}{2!} + \frac{\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}}{3!} + \ldots + \frac{\binom{n}{2}\binom{n-2}{2}\cdots\binom{3}{2}}{k!}$$

elements of order 2 in S_n.

In particularly, it follows that S_4 has

$$\binom{4}{2} + \frac{\binom{4}{2}\binom{2}{2}}{2!} = 9$$

elements of order 2 and S_5 has

$$\binom{5}{2} + \frac{\binom{5}{2}\binom{3}{2}}{2!} = 25$$

elements of order 2.

2.39 Let $G = GL(2, \mathbb{Q})$, and let

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}.$$

Show that $A^4 = E = B^6$, but that $(AB)^n \neq E$ for all $n > 0$.

Solution:
We have

$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad A^4 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

and

$$B^2 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, \quad B^4 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix},$$

$$B^6 = B^4 B^2 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Finally, we show by induction that

$$(AB)^n = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}.$$

In fact, for $n = 1$ this is true, since

$$AB = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}.$$

Suppose this is true for some $n = k \geq 1$, that is

$$(AB)^k = \begin{bmatrix} 1 & -k \\ 0 & 1 \end{bmatrix}.$$

We prove that

$$(AB)^{k+1} = \begin{bmatrix} 1 & -k-1 \\ 0 & 1 \end{bmatrix}.$$

We have

$$(AB)^{k+1} = (AB)^k (AB) = \begin{bmatrix} 1 & -k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -k-1 \\ 0 & 1 \end{bmatrix}.$$

2.45 (i) Define a **special linear group** by

$$\mathrm{SL}(2,\mathbb{R}) = \{A \in GL(2,\mathbb{R}) : \det(A) = 1\}.$$

Prove that SL $(2,\mathbb{R})$ is a subgroup of GL $(2,\mathbb{R})$.

(ii) Prove that GL $(2,\mathbb{Q})$ is a subgroup of GL $(2,\mathbb{R})$.

Solution:

(i) We will use Theorem 4. In order to apply this Theorem we should check that SL $(2,\mathbb{R})$ is nonempty and that $M_1M_2^{-1} \in$ SL $(2,\mathbb{R})$ whenever $M_1 \in$ SL $(2,\mathbb{R})$ and $M_2 \in$ SL $(2,\mathbb{R})$.

First of all note that SL $(2,\mathbb{R})$ is nonempty, since $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in$ SL $(2,\mathbb{R})$. Let

$$M_1 = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \quad \text{and} \quad M_2 = \begin{bmatrix} a_2 & c_2 \\ b_2 & d_2 \end{bmatrix}$$

be from SL $(2,\mathbb{R})$. Then $\det(M_1M_2^{-1}) = 1$, since

$$\det(M_1M_2^{-1}) = \det(M_1)\det(M_2^{-1}) = \det(M_1)[\det(M_2)]^{-1} = 1 \cdot 1^{-1} = 1.$$

Finally,

$$M_1M_2^{-1} = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & c_2 \\ b_2 & d_2 \end{bmatrix}^{-1} = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} \dfrac{d_2}{a_2d_2 - b_2c_2} & -\dfrac{c_2}{a_2d_2 - b_2c_2} \\ -\dfrac{b_2}{a_2d_2 - b_2c_2} & \dfrac{a_2}{a_2d_2 - b_2c_2} \end{bmatrix},$$

which is equal to

$$\begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} d_2 & -c_2 \\ -b_2 & a_2 \end{bmatrix},$$

since $a_2d_2 - b_2c_2 = \det M_1 = 1$. So,

$$M_1M_2^{-1} = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} d_2 & -c_2 \\ -b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1d_2 - c_1b_2 & -a_1c_2 + c_1a_2 \\ b_1d_2 - d_1b_2 & b_1c_2 - d_1a_2 \end{bmatrix}.$$

From this, obviously, follows that if M_1 and M_2 have real entries, then $M_1M_2^{-1}$ has also real entries. So, $M_1M_2^{-1} \in$ SL $(2,\mathbb{R})$ whenever $M_1 \in$ SL $(2,\mathbb{R})$ and $M_2 \in$ SL $(2,\mathbb{R})$.

(ii) To prove that GL $(2,\mathbb{Q})$ is a subgroup of GL $(2,\mathbb{R})$, we use Theorem 4 again. First of all note that GL $(2,\mathbb{Q})$ is nonempty, since $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in$ GL $(2,\mathbb{Q})$. Let

$$M_1 = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \quad \text{and} \quad M_2 = \begin{bmatrix} a_2 & c_2 \\ b_2 & d_2 \end{bmatrix}$$

be from GL $(2,\mathbb{Q})$. Then $\det(M_1M_2^{-1}) \neq 0$, since

$$\det(M_1M_2^{-1}) = \det(M_1)\det(M_2^{-1}) = \det(M_1)[\det(M_2)]^{-1},$$

which is nonzero, since $\det M_1 \neq 0$ and $\det M_2 \neq 0$. Finally,

$$M_1 M_2^{-1} = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & c_2 \\ b_2 & d_2 \end{bmatrix}^{-1} = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} \dfrac{d_2}{a_2d_2 - b_2c_2} & -\dfrac{c_2}{a_2d_2 - b_2c_2} \\ -\dfrac{b_2}{a_2d_2 - b_2c_2} & \dfrac{a_2}{a_2d_2 - b_2c_2} \end{bmatrix}$$

$$= \begin{bmatrix} \dfrac{a_1d_2 - c_1b_2}{a_2d_2 - b_2c_2} & \dfrac{a_1c_2 - c_1a_2}{a_2d_2 - b_2c_2} \\ -\dfrac{b_1d_2 - d_1b_2}{a_2d_2 - b_2c_2} & \dfrac{b_1c_2 - d_1a_2}{a_2d_2 - b_2c_2} \end{bmatrix}.$$

From this, obviously, follows that if M_1 and M_2 have rational entries, then $M_1 M_2^{-1}$ has also rational entries. So, $M_1 M_2^{-1} \in \mathrm{GL}(2, \mathbb{Q})$ whenever $M_1 \in \mathrm{GL}(2, \mathbb{Q})$ and $M_2 \in \mathrm{GL}(2, \mathbb{Q})$.

2.46 Give an example of two subgroups H and K of a group G whose union $H \cup K$ is not a subgroup of G.

Solution:
Let $G = \mathbf{V}$, $H = \{(1), (12)(34)\}$, and $K = \{(1), (13)(24)\}$. Then $H \cup K = \{(1), (12)(34), (13)(24)\}$, which is not a subgroup, since it is not closed. In fact, $(12)(34)(13)(24) = (14)(23) \notin H \cup K$.

1. (Herstein) Let R be the ring of 2×2 matrices with rational numbers as coefficients. Prove that the only ideals of R are the zero ideal and the ring R itself.

   SOLUTION IDEA

   Observe that were R commutative with 1, this condition would imply that R is a field.

   Let $E = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Left multiplication of a 2×2 matrix A by E exchanges the rows of A, right multiplication exchanges its columns.

   Let J be a nontrivial ideal of R and let $A \in J$, $A \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. A has at least one nonzero entry. Multiply A (as necessary) by E on the left and on the right to obtain a matrix in J whose 1-1 entry, say a, is nonzero. Multiply that matrix on the left by $\begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$ to obtain $B \in J$ whose 1-1 entry is 1. Now $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} B \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in J$. Then $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in J$ from which $J = R$.

p

6. Find permutations α and β such that:

(a) $|\alpha| = 2$, $|\beta| = 2$, and $|\alpha\beta| = 2$.

Sample solution. Let $\alpha = (1\ 2)$, $\beta = (3\ 4)$. Then $\alpha\beta = (1\ 2)(3\ 4)$. About the order of $\alpha\beta$, since it's the product of cycles on two disjoint sets, $|\alpha\beta| = \text{lcm}(|\alpha|, |\beta|) = 2$.

(b) $|\alpha| = 2$, $|\beta| = 2$, and $|\alpha\beta| = 3$.

Sample solution. Let $\alpha = (1\ 2)$, $\beta = (2\ 3)$. Then $\alpha\beta = (1\ 2\ 3)$.

(c) $|\alpha| = 2$, $|\beta| = 4$, and $|\alpha\beta| = 4$.

Sample solution. Let $\alpha = (1\ 2)$, $\beta = (3\ 4\ 5\ 6)$. Then $\alpha\beta = (1\ 2)(3\ 4\ 5\ 6)$.

5. (a) How many permutations of order 5 are there in S_5?

Solution.

$$\frac{5!}{5} = 4 \times 3 \times 2 \times 1 = 24.$$

(b) How many permutations of order 5 are there in S_6?

Solution. If a permutation of six elements has order five, it should fix one element and permute the other five. So there are

$$\binom{6}{5} \cdot \frac{5!}{5} = 6 \times (4 \times 3 \times 2 \times 1) = 6 \times 24 = 144$$

permutations in S_6 which have order five. The expression in the parentheses is from Part (a) of the problem.

4. Let $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 9 & 4 & 7 & 1 & 2 & 8 & 5 & 10 & 6 \end{bmatrix}$, viewed as an element in S_{10}.

(a) Write α as products of disjoint cycles.

$\alpha = (1\ 3\ 4\ 7\ 8\ 5)(2\ 9\ 10\ 6)$.

(b) Find the order of α.

The order is the least common multiple of the orders of the two cycles. So it's $\text{lcm}(6, 4) = 12$.

(c) Write α as a product of transpositions.

$\alpha = (1\ 5)(1\ 8)(1\ 7)(1\ 4)(1\ 3)(2\ 6)(2\ 10)(2\ 9)$.

Example 3.7. Consider

$$\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8\ 9\ 10).$$

The cycles appearing here are disjoint. The order of σ is $[4, 6] = 12$.

If σ is not written as a product of disjoint cycles, determine its disjoint cycle decomposition first in order to compute the order of σ.

Example 3.8. Consider

$$\sigma = (123)(241).$$

The 3-cycles here each have order 3, but σ does *not* have order $[3, 3] = 3$. The cycles are not disjoint. The disjoint cycle decomposition of σ is

$$\sigma = (13)(24)$$

so the order of σ is 2.

Corollary 3.9. *A permutation $\sigma \in S_n$ has prime order p if and only if it is a product of disjoint p-cycles.*

Proof. Let the decomposition of σ into disjoint cycles be $\sigma_1\sigma_2 \cdots \sigma_t$, and we can assume the σ_i's are all nontrivial. Letting r_i be the order of σ_i, $r_i > 1$ and computing the order of this product tells us $p = [r_1, \ldots, r_t]$. Therefore each r_i is a factor of p and is greater than 1, so every r_i is p. Conversely, if each r_i is p then of course their least common multiple is p. So σ has order p if and only if it is a disjoint product of p-cycles. □

This theorem is not saying an element of order p is a p-cycle. It's a disjoint product of p-cycles. For example, $(12)(34)(56)$ has order 2 and $(123)(456)$ has order 3.

Example 4.3. Two elements can have finite order while their product has infinite order. Consider, in $\mathrm{GL}_2(\mathbf{R})$, the matrices

$$A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Check yourself that A^2 and B^2 equal the identity matrix, so A and B both have order 2. Meanwhile,

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

which has infinite order: $(AB)^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, which is the identity matrix only for $n = 0$. The product $BA = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) = (AB)^{-1}$ also has infinite order.

Example 7 We shall find the factorization that is described in the Unique Factorization Theorem for the polynomial

$$f(x) = 2x^4 + x^3 + 3x^2 + 2x + 4$$

over the field $\mathbf{Z}_5$.

We first determine the zeros of $f(x)$ in $\mathbf{Z}_5$:

$$f(0) = 4, \quad f(1) = 2, \quad f(2) = 0, \quad f(3) = 1, \quad f(4) = 1.$$

Thus 2 is the only zero of $f(x)$ in $\mathbf{Z}_5$, and the Factor Theorem assures us that $x - 2$ is a factor of $f(x)$. Dividing by $x - 2$, we get

$$f(x) = (x - 2)(2x^3 + 3x + 3).$$

By Exercise 16 at the end of this section, the zeros of $f(x)$ are 2 and the zeros of $g(x) = 2x^3 + 3x + 3$. We therefore need to determine the zeros of $g(x)$, and the only possibility is 2, since this is the only zero of $f(x)$ in $\mathbf{Z}_5$. We find that $g(2) = 0$, and this indicates that $x - 2$ is a factor of $g(x)$. Performing the required division, we obtain

$$2x^3 + 3x + 3 = (x - 2)(2x^2 + 4x + 1)$$

and

$$\begin{aligned} f(x) &= (x - 2)(x - 2)(2x^2 + 4x + 1) \\ &= (x - 2)^2(2x^2 + 4x + 1). \end{aligned}$$

We now find that $2x^2 + 4x + 1$ is irreducible over $\mathbf{Z}_5$, since it has no zeros in $\mathbf{Z}_5$. To arrive at the desired factorization, we need to only factor the leading coefficient of $f(x)$ from the factor $2x^2 + 4x + 1$:

$$\begin{aligned} f(x) &= (x - 2)^2(2x^2 + 4x + 1) \\ &= (x - 2)^2[2x^2 + 4x + (2)(3)] \\ &= 2(x - 2)^2(x^2 + 2x + 3). \end{aligned}$$

■

6. In the group $\mathbb{Z}_{12}$ find $|a|$, $|b|$, and $|a + b|$ for each case.

(a) $a = 6, b = 2$

$$a = 6, a + a = 12 = 0 \Rightarrow |a| = 2$$

$$b = 2, b + b = 4, 3 \cdot b = 6, 4 \cdot b = 8, 5 \cdot b = 10, 6 \cdot b = 12 = 0 \Rightarrow |b| = 6$$

$$a + b = 8, 2 \cdot (a + b) = 16 = 4, 3 \cdot (a + b) = 24 = 0 \Rightarrow |a + b| = 3$$

(b) $a = 3, b = 8$

$$a = 3, 2 \cdot a = 6, 3 \cdot a = 9, 4 \cdot a = 12 = 0 \Rightarrow |a| = 4$$

$$b = 8 \Rightarrow |b| = 3 \text{ (see (a).)}$$

$$a + b = 11 = -1 \Rightarrow |a + b| = |-1| = |1| = 12$$

15. If a is an element of a group G and $|a| = 7$, show that a is the cube of some element of G.

If $|a| = 7$, $a^7 = e$. Then

$$(a^5)^3 = a^{15} = a^{2\cdot 7+1} = (a^7)^2 a = e^2 a = a.$$

So a is the cube of a^5.

18. Suppose that a is a group element and $a^6 = e$. What are the possibilities for $|a|$? Provide reasons for your answer.

If $a^6 = e$, then $|a|$ must be at most 6. So only $1, 2, 3, 4, 5, 6$ are all possibilities. Furthermore, if $a^4 = e$, then $a^2 = a^2e = a^2a^6 = a^8 = (a^4)^2 = e^2 = e$. So $|a| = 4$ is impossible. Similarly, if $a^5 = e$, then $a^3 = a^3e^2 = a^3(a^6)^2 = a^{15} = (a^5)^3 = e^3 = e$. So $|a| = 5$ is impossible as well. In summary, only $1, 2, 3, 6$ are possible. (They are all divisors of 6. Of course, it is not an accident.)

24. Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all g in G.

Solution.
If G is cyclic, then we're done. So assume that G is not cyclic. Let $g \in G$. If $g = e$, then clearly $g^5 = e$. So suppose $g \neq e$. Then $|g|$ divides 25, *i.e.*, $|g| = 1$, 5, or 25. But $|g| \neq 1$ since we assumed $g \neq e$, and $|g| \neq 25$ since otherwise, G would be cyclic. So $|g| = 5$, *i.e.*, $g^5 = e$.

(3): The integers modulo 6, $\mathbb{Z}_6$, with addition and multiplication modulo 6, form a field.

TRUE **FALSE**

Solution: Since $2 \cdot 3 = 0$ in $\mathbb{Z}_6$, but also $2 \cdot 0 = 0$, then if $\mathbb{Z}_6$ were a field, we have $2 \cdot 3 = 2 \cdot 0$. Cancellation would give us $3 = 0$, a contradiction. The same argument can be adapted to show that whenever n is composite, $\mathbb{Z}_n$ is not a field.

79. Let $G = GL(2, \mathbb{R})$.

(a) Find $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$.

If $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$, then

$$\begin{bmatrix} a+b & a \\ c+d & c \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ a & b \end{bmatrix}.$$

So $a+b = a+c$, $a = b+d$, $c+d = a$, and $b = c$. These conditions are equivalent to $b = c$ and $a = b+d$. Conversely, for $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ with $b = c$ and $a = b+d$, then by the same equation, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$. Therefore

$$C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G \,\middle|\, a = b+d, b = c\right\}$$

(b) Find $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$.

If $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$, then

$$\begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}.$$

So $b = c$ and $a = d$. Conversely, for $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ with $b = c$ and $a = d$, then by the same equation, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$. Therefore

$$C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G \,\middle|\, a = d, b = c\right\}$$

(c) Find $Z(G)$.

Note that for any scalar matrix $\begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix}$ with $k \neq 0$ is in $Z(G)$, because

$$\begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ka & kb \\ kc & kd \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix}.$$

So $\left\{ \begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix} \mid k \neq 0 \right\} \subset Z(G)$.

Conversely, if $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(G)$, then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

so $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$. Similarly,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

so $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$.

Therefore $a = b + d$, $b = c$ and $a = d$. From $a = b + d$ and $a = d$, $b = c = 0$.

Hence $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$. Because this matrix is in $G = GL(2, \mathbb{R})$, $a \neq 0$.

So we have

$$Z(G) \subset \left\{ \begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix} \mid k \neq 0 \right\}$$

and hence,

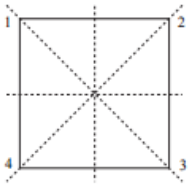
$$Z(G) = \left\{ \begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix} \mid k \neq 0 \right\}.$$

Exercise 2. The equivalence classes under the equivalence relation of exercise 1 are called *conjugacy classes*. Find the conjugacy classes in S_3, D_4 and A_4.

Solution.

The conjugacy classes in S_3 are
$\{e\}$
$\{(12), (13), (23)\}$, (2-cycles)
$\{(123), (321)\}$ (3-cycles).

For D_4, we number the square as in hw 2:



The congugacy classes in D_4 are
$\{e\}$
$\{(13)(24)\}$ (180 degree rotation),
$\{(14)(23), (12)(34)\}$ (edge reflections),
$\{(13), (24))\}$ (vertex reflections),
$\{(1234), (4321)\}$ (90 degree rotations).

Alternative solution with matrices:
$\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\}$
$\{\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\}$ (180 degree rotation),
$\{\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\}$ (edge reflections),
$\{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}\}$ (vertex reflections),
$\{\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\}$ (90 degree rotations).

The conjugacy classes in A_4 are
$\{e\}$,
$\{(12)(34), (13)(24), (23)(14)\}$, (edge reflections of tetrahedron),
$\{(123), (134), (142), (243))\}$ (face rotations in same direction),
$\{(123), (134), (142), (243))\}$ (face rotations in the other direction).

□

(1) (*Gallian Chapter 12 # 3*) Give an example of a subset of a ring that is a subgroup under addition but not a subring. Prove that your example works.

Solution (using hint in back of Gallian): In $\mathbb{R}$, consider

$$A = \{n\sqrt{2} : n \in \mathbb{Z}\}$$

We will prove that this example is a subgroup under addition but not a subring. We use the one-step subgroup test to prove that this (nonempty, because includes 0 for example) subset of $\mathbb{R}$ is a subgroup under addition. Let $x, y \in A$. Then there are $m, n \in \mathbb{Z}$ such that $x = m\sqrt{2}$ and $y = n\sqrt{2}$. Computing

$$x - y = m\sqrt{2} - n\sqrt{2} = (m-n)\sqrt{2} \in A$$

because $m - n \in \mathbb{Z}$. We will prove that A is not a subring of R by showing that it is not closed under multiplication. Consider $x = \sqrt{2} \in A$ (using $n = 1$). Then

$$x^2 = \sqrt{2}\sqrt{2} = 2.$$

But $\mathbb{Z} \cap A = \varnothing$ since $\sqrt{2}$ is not rational. Therefore, since $x^2 \in \mathbb{Z}$, $x^2 \notin A$ and we have shown that A is not closed under multiplication.

Alternate solution: Consider the ring $M_2(\mathbb{Z})$ of 2×2 matrices with integer entries. Consider the subset

$$B = \left\{ \begin{pmatrix} a & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z} \right\}.$$

Then $B \subseteq M_2(\mathbb{Z})$ and is nonempty. (For example, it contains the 0 matrix when we choose $a = b = 0$.) To confirm that B is a subgroup under addition, we use the one-step subgroup test: let $X, Y \in B$ so there are $a, b, a', b' \in \mathbb{Z}$ such that

$$X = \begin{pmatrix} a & a \\ 0 & b \end{pmatrix} \qquad Y = \begin{pmatrix} a' & a' \\ 0 & b' \end{pmatrix}.$$

Then

$$X - Y = \begin{pmatrix} a - a' & a - a' \\ 0 & b - b' \end{pmatrix} \in B$$

because $a - a', b - b' \in \mathbb{Z}$. But, B is not a subring because we will show that it is not closed under multiplication: for example,

$$\begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 0 & 1 \end{pmatrix},$$

which is not in B since $2 \neq 4$. Thus, B is a subgroup of $M_2(\mathbb{Z})$ under addition but is not a subring.

(3) (*Gallian Chapter 12 # 6*) Find an integer n that shows that the rings Z_n need not have the following properties (that the ring of integers $\mathbb{Z}$ does have)
(a) $a^2 = a$ implies $a = 0$ or $a = 1$.
(b) $ab = 0$ implies $a = 0$ or $b = 0$.
(c) $ab = ac$ and $a \neq 0$ implies $b = c$.
Is the n you found prime?

Solution: We will use $n = 6$ for all of these. Namely, consider $Z_6 = \{0, 1, 2, 3, 4, 5\}$.
Recall that to prove that an implication "P implies Q" fails, we need to find an example where P is true and Q is false.
(a) Consider $a = 3$. Then $a^2 = 9 \mod 6 = 3 = a$ but $3 \neq 0$ and $3 \neq 1$.
(b) Consider $a = 2$ and $b = 3$. Then $ab = 2 \cdot 3 \mod 6 = 6 \mod 6 = 0$ but $2 \neq 0$ and $3 \neq 0$.
(c) Consider $a = 2$, $b = 4$, $c = 1$. Then $ab = 2 \cdot 4 \mod 6 = 8 \mod 6 = 2 = 2 \cdot 1 \mod 6 = ac$ and $2 \neq 0$, but $4 \neq 1$.

4. (a) Give an example of a subset of a ring that is a subgroup under addition but not a subring.

(b) Give an example of a finite non-commutative ring.

Solution. (a) Example 1. Let $R = \mathbb{C}$ and $S = \{ix : x \in \mathbb{R}\}$. Then $0 \in S$ and $a - b \in S$ whenever $a, b \in S$. But $i \cdot i = -1 \notin S$.

Example 2. Let $H = \langle (2, 3) \rangle \in \mathbb{Z} \oplus \mathbb{Z}$. Then $H = \{(2k, 3k) : k \in \mathbb{Z}\}$ is a subgroup under addition. But $(2, 3)(2, 3) = (4, 9) \notin H$.

(b) Let $R = M_2(\mathbb{Z}_2)$. Then there are 2^4 elements because each entries has two choices. Clearly, $AB \neq BA$ if $A = B^t = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

8. Let R be a ring.

(a) Prove that R is commutative if and only if $a^2 - b^2 = (a + b)(a - b)$ for all $a, b \in R$.

(b) Prove that R is commutative if $a^2 = a$ for all $a \in R$.

(Such a ring is called a Boolean ring.)

Solution. (a) If R is commutative, then $(a + b)(a - b) = a^2 + ab - ba - b^2 = a^2 - b^2$ for any $a, b \in R$. Suppose $(a + b)(a - b) = a^2 + ab - ba - b^2 = a^2 - b^2$ for any $a, b \in R$. Then $ab - ba = 0$, i.e., $ab = ba$.

(b) Suppose $a^2 = a$ for all $a \in R$. Then for any $a, b \in R$, $a^2 + b^2 = a + b = (a + b)^2 = a^2 + ab + ba + b^2$ so that $ab + ba = 0$. Hence, $ab = -ba = (-ba)^2 = (ba)^2 = ba$.

9. Give an example of a Boolean ring with 4 elements. Give an example of a Boolean ring with infinitely many elements.

Solution. Let $B = \mathbb{Z}_2 = \{0, 1\}$ such that $0 + 0 = 0$ and $0 + 1 = 1 + 0 = 1 + 1 = 1$, and $00 = 01 = 10 = 0$ and $11 = 1$. Then B is a Boolean ring with 2 elements, and $B \oplus B$ is a Boolean ring with 4 elements.

Let $R = B^\infty = \{(a_1, a_2, \dots) : a_i \in B \text{ for each } i\}$. One can show that R is a ring under the entrywise addition and multiplication operation. Also, $(a_1, a_2, \cdots)^2 = (a_1, a_2, \dots)$. So, R is a Boolean ring with infinitely many elements.

65. If $|G| = 30$ and $|Z(G)| = 5$, what is the structure of $G/Z(G)$?

SOLUTION:

We know that $|G/Z(G)| = \frac{30}{5} = 6 = 2 \cdot p$, where $p = 3$ is a prime greater than 2 We also know that any group of order$2p$, where p ia prime greater than 2 is isomorphic to $\mathbb{Z}_{2p}$ or the dihedral group D_p of order $2p$. In the former case, since $\mathbb{Z}_{2p}$ is cyclic, then $G/Z(G)$ is cyclic, and so G must be abelian by a theorem we proved in class, but this cannot be the case, because in this case by the hypothesis, we have $G = Z(G)$. In the latter case, we have $G/Z(G) \cong D_p$.

10. Let a and b be nonidentity elements of different orders in a group G of order 155. Prove that the only subgroup of G that contains a and b is G itself.

SOLUTION:

By Lagrange's Theorem, the orders of a and b are divisors of $|G| = 155 = 5 \bullet 31$, and neither is 1, since $a, b \neq e$. Let $H \leq G$ contain both a and b. If either of a, b has order 155, then obviously $|H| \geq 155$, so $|H| = 155$, so $H = G$. Otherwise the orders of a and b are 5 and 31 in some order; but then 5 and 31 both divide $|H|$, so again $|H| \geq 155$, so again $H = G$.

---

13. Let $|G| = 60$. What are the possible orders for the subgroups of G?

14. Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?

SOLUTION:

We need 42 dividing $|H|$ and $|H|$ dividing 420, with $|H| \neq 42, 420$. The multiples of 42 that are divisors of 420 are $42 \bullet 2 = 84$ and $42 \bullet 5 = 210$.

F: Let $R = \mathbb{Q}[x]/(x^2 + 1)$. Show that R is a field.

Solution As explained in class, it suffices to show that $(x^2 + 1)$ is a maximal ideal in the ring $\mathbb{Q}[x]$. For that purpose, it suffices to prove that $x^2 + 1$ is an irreducible element in the ring $\mathbb{Q}[x]$. Suppose to the contrary that we have a factorization

$$x^2 + 1 \;=\; g(x)h(x)$$

where $g(x)$ and $h(x)$ are in $\mathbb{Q}[x]$ and that the degree of $g(x)$ and $h(x)$ are both < 2. This means that $g(x)$ and $h(x)$ have degree 1. Thus $g(x) = a + bx$ and $h(x) = c + dx$, where $a, b, c, d \in \mathbb{Q}$, $b \neq 0$ and $d \neq 0$. Let $J = (a + bx)$, the principal ideal in $\mathbb{Q}[x]$ generated by $a + bx$. Then $x^2 + 1$ is in J.

Consider the ring homomorphism $\varphi_\theta : \mathbb{Q}[x] \to \mathbb{Q}$ which was defined in class. We will take $\theta = -\frac{a}{b}$, which is an element of $\mathbb{Q}$. Thus, $\varphi\big(f(x)\big) = f(\theta)$ for all $f(x) \in \mathbb{Q}[x]$. Notice that

$$\varphi_\theta(a + bx) \;=\; a + b\theta \;=\; 0$$

and hence $a + bx \in Ker(\varphi_\theta)$. Therefore, $J \subseteq Ker(\varphi_\theta)$. (In fact, we have $Ker(\varphi_\theta) = J$, but this fact won't be needed.)

However, notice that $\varphi_\theta(x^2 + 1) = \theta^2 + 1 \geq 1$ since θ is a real number and therefore $\theta^2 \geq 0$. Hence, $\varphi_\theta(x^2 + 1) \neq 0$. Therefore, $x^2 + 1 \notin Ker(\varphi_\theta)$. Since $J \subseteq Ker(\varphi_\theta)$, it follows that $x^2 + 1$ cannot be in J. This is a contradiction. It follows that $x^2 + 1$ is indeed an irreducible element in the ring $\mathbb{Q}[x]$. Therefore, $\mathbb{Q}[x]/(x^2 + 1)$ is indeed a field.

G: Let $R = \mathbb{R}[x]/(x^2 - 2)$. Show that R is not a field.

Solution We have the following factorization in the ring $\mathbb{R}[x]$:

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

which shows that $x^2 - 2$ is a reducible element in the ring $\mathbb{R}[x]$. Therefore, the principal ideal $(x^2 - 2)$ is not a maximal ideal in that ring. Therefore, the quotient ring $\mathbb{R}[x]/(x^2 - 2)$ is not a field.

Theorem 9.3:

Let G be a group with center $Z(G)$. If $G/Z(G)$ is cyclic, then G is Abelian.

Proof:

Let $g \in G$ be such that $gZ(G)$ generates $G/Z(G)$.

For any $a, b \in G$, let

$$aZ(G) = (gZ(G))^i = g^i Z(G),$$

and let

$$bZ(G) = (gZ(G))^j = g^j Z(G).$$

Then $a = g^i x$ and $b = g^j y$, $\exists x, y \in Z(G)$.

Since x, y commute with everything, and g^i commutes with g^j, we see that
$ab = (g^i x)(g^j y) = g^{i+j} xy = (g^j y)(g^i x) = ba.$

Since the a, b were arbitrary, we have that G is abelian.

8. Describe all possible subgroups of $\mathbb{Z}/10$.

Solution: Since $\mathbb{Z}/10$ is cyclic, all subgroups are cyclic, by a result from class. Thus the subgroups are:

$$\begin{aligned}\langle 0\rangle &= \{0\}\\ \langle 1\rangle &= \mathbb{Z}/10 = \langle 3\rangle = \langle 7\rangle = \langle 9\rangle\\ \langle 2\rangle &= \{0,2,4,6,8\} = \langle 4\rangle = \langle 6\rangle = \langle 8\rangle\\ \langle 5\rangle &= \{0,5\}.\end{aligned}$$

4. What is the largest possible order of a permutation in S_{10}? Write down an explicit element of this order.

Solution. If $\sigma \in S_{10}$, we can express σ as a product of disjoint cycles $\sigma_1 \cdots \sigma_t$ of lengths $k_1, k_2, \ldots, k_t$ $(k_i \geq 2)$ where $k_1 + \cdots k_t \leq 10$. The order of σ is then $\text{lcm}(k_1, \ldots, k_t)$. Thus we have to find the maximum value of $\text{lcm}(k_1, \ldots, k_t)$ over all sets of integers $\{k_1, \ldots, k_t\}$ satisfying $k_i \geq 2$ and $k_1 + \ldots + k_t \leq 10$.

We may as well assume the k_i's are distinct from each other (since repeating one of them doesn't alter the lcm). This narrows the search considerably. We list the possibilities for $k_1 + \cdots k_t$ and the corresponding lcm:

$$\begin{aligned}2+3+4, &\qquad \text{lcm}(2,3,4) = 12\\ 2+3+5, &\qquad \text{lcm}(2,3,5) = 30\\ 2+4, &\qquad \text{lcm}(2,4) = 4\\ 2+5, &\qquad \text{lcm}(2,5) = 10\\ 2+6, &\qquad \text{lcm}(2,6) = 12\\ 2+7, &\qquad \text{lcm}(2,7) = 14\\ 2+8, &\qquad \text{lcm}(2,8) = 8\\ 3+4, &\qquad \text{lcm}(3,4) = 12\\ 3+5, &\qquad \text{lcm}(3,5) = 15\\ 3+6, &\qquad \text{lcm}(3,6) = 6\\ 3+7, &\qquad \text{lcm}(3,7) = 21\\ 4+5, &\qquad \text{lcm}(4,5) = 20\\ 4+6, &\qquad \text{lcm}(4,6) = 12\end{aligned}$$

We see that the highest possible order is 30 and this is achieved by the product of a 2-cycle, a 3-cycle and a 5-cycle; eg. (12)(345)(678910).

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

   (a) The permutation $\sigma \in S_8$ given by

   $$\sigma(1) = 5, \sigma(2) = 3, \sigma(3) = 7, \sigma(4) = 1$$
   $$\sigma(5) = 8, \sigma(6) = 2, \sigma(7) = 4, \sigma(8) = 6$$

   (b) $(135)(357)(579) \in S_9$

   (c) $(13)(234)(4578) \in S_8$

   (d) $(12)(23)(43)(57)(24)(61) \in S_7$

   Solution:

   (a) $\sigma = (15862374)$.

   (b) $(13)(79)$

   (c) (1345782)

   (d) $(162)(34)(57)$

Theorem 2.9 *Let F be a field, and let $p(x)$ be a nonconstant polynomial over F. Then $F[x]/\langle p(x)\rangle$ is a field if and only if $p(x)$ is irreducible over F.*

Example. Let $F = \mathbf{Z}_2$ and let $p(x) = x^2 + x + 1$. Then $p(x)$ is irreducible over $\mathbf{Z}_2$ since it has no roots in $\mathbf{Z}_2$, and so $\mathbf{Z}_2[x]/\langle x^2 + x + 1\rangle$ is a field. The congruence classes modulo x^2+x+1 can be represented by $[0]$, $[1]$, $[x]$ and $[1+x]$, since these are the only polynomials of degree less than 2 over $\mathbf{Z}_2$. Addition and multiplication are given in the following tables, which have been simplified by omitting all brackets for the congruence classes.

Addition in $\mathbf{Z}_2[x]/\langle x^2 + x + 1\rangle$.

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

Multiplication in $\mathbf{Z}_2[x]/\langle x^2 + x + 1\rangle$.

$\times$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

Returning to the earlier example of a field with 4 elements, let

$$F = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right\}.$$

Let I denote the identity matrix, and let $X = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. Then $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = I + X$, and $X^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = I + X$. This shows that addition and multiplication behave just like the similar operations in $\mathbf{Z}_2[x]/\langle x^2 + x + 1 \rangle$. To give the corresponding tables for F, we can simply substitute I in place of 1 and X in place of x in the addition and multiplication tables for $\mathbf{Z}_2[x]/\langle x^2 + x + 1 \rangle$.

If $q(x)$ is irreducible over $\mathbf{Z}_p$, then $\mathbf{Z}_p[x]/\langle q(x) \rangle$ has p^n elements if $\deg(q(x)) = n$, since there are exactly $p^n - 1$ polynomials over $\mathbf{Z}_p$ of degree less than n (including 0 gives p^n elements). It is possible to show that there exist polynomials of degree n irreducible over $\mathbf{Z}_p$ for each integer $n > 0$. This guarantees the existence of a finite field having p^n elements, for each prime number p and each positive integer n.

(b) Prove that if G is a cyclic group of order n and k divides n, then G has exactly one subgroup of order k.

(b) First, we claim that a subgroup of a cyclic group is still cyclic. Let $H \subset G = \langle a \rangle$ be a subgroup. Let m be the smallest positive integer such that $a^m \in H$. We claim that $\langle a^m \rangle = H$. Let $h \in H$, and let $h = a^s$. By the division algorithm, we may write

$$s = mq + r$$

where $0 \leq r < m$. Therefore $h = (a^m)^q a^r$. Since $a^m \in H$, $(a^m)^{-q} \in H$, and since H is closed we have $(a^m)^{-q} \cdot h = a^r \in H$. Since $r < m$ by assumption, this would contradict minimality if $r > 0$, so we have $r = 0$. We conclude $h = (a^m)^q$ for all $h \in H$, hence a^m generates H.

Now let $\langle a^m \rangle$ and $\langle a^{m'} \rangle$ be two subgroups of order k. Without loss of generality, we may let $m = n/k$, since this subgroup does have k elements. Since $|\langle a^{m'} \rangle| = d$, we know $(a^{m'})^d = e$, so $n \mid m'd$. Therefore write

$$qn = m'k \implies m' = q \cdot \frac{n}{k} = qm.$$

Therefore $\langle a^{m'} \rangle \subset \langle a^m \rangle$ and since these subgroups have equal order, $\langle a^{m'} \rangle = \langle a^m \rangle$. Hence there is only one subgroup for each $k \mid n$. □

Proposition. *The integer ring $\mathbb{Z}_n$ mod n is a field if and only if n is prime.*

Proof. First suppose that p is prime. To show that $\mathbb{Z}_p$ is a field we let $m \in \{0, 1, \ldots, p-1\}$ and suppose that m has no inverse in $\mathbb{Z}_p$. Then none of the p numbers

$$0m, 1m, 2m, \ldots, (p-1)m$$

can be equal to 1 so this list must contain two numbers which are equal in $\mathbb{Z}_p$.
Hence we have

$$im \equiv jm \pmod{p} \qquad \text{or} \qquad (i-j)m \equiv 0 \pmod{p}$$

for some i, j with $0 < i - j < p$. Since p is prime one of the numbers $i - j$ or m must be a multiple of p and considering their ranges the only possibility is $m = 0$
Hence 0 is the only element with no inverse and so $\mathbb{Z}_p$ is a field.
To complete the proof we show that if n is not prime, then $\mathbb{Z}_n$ is not a field. If $n \geq 2$ is not prime then we can write $n = qr$ for some $q, r \geq 2$. But now we have two nonzero elements q and r whose product is the zero element of $\mathbb{Z}_n$. Since this is not possible in a field it follows that $\mathbb{Z}_n$ is not a field. □

Proposition 1.9. *A finite integral domain R is a field.*

Proof. Suppose $r \in R$ with $r \neq 0$. The elements $1 = r^0, r, r^2, \ldots$ cannot all be different, since otherwise R would be infinite. Hence there exist $0 \leq n < m$ with $r^n = r^m$. Writing $m = n + k$ with $k \geq 1$, we see that $r^n = r^m = r^{n+k} = r^n r^k$. By induction, since R is an integral domain and $r \neq 0$, $r^n \neq 0$ for all $n \geq 0$. Applying cancellation to $r^n = r^n \cdot 1 = r^n r^k$ gives $r^k = 1$. Finally since $r^k = r \cdot r^{k-1}$, we see that r is invertible, with $r^{-1} = r^{k-1}$. □

DEFINITION 2.1.10. Let R be a nonzero ring. We say that R is ***simple*** if its only ideals are the zero ideal $\{0\}$ and the total ideal R.

PROPOSITION 2.1.11. *A (commutative) ring R is simple if and only if it is a field.*

PROOF. Assume that R is simple, and let $a \in R^*$. Since R is simple, one gets $(a) = R$, thus $1 \in (a)$, and hence there must exist some $b \in R$ such that $1 = ab$, and hence $a \in U(R)$; thus, every nonzero element of R is a unit.

Conversely, if R is a field, and $0 \neq I \trianglelefteq R$, let $a \in I$ a nonzero element of I. Since R is a field, a must be a unit, so there is $b \in R$ such that $ab = 1$, but since $a \in I$, the absorbency property ensures that $1 = ab \in I$, and thus $I = R$, so R is simple. □

2. *Let G be the group of all nonzero complex numbers under multiplication and let N be the set of complex numbers of absolute value 1. Show that $G = N$ is isomorphic to the group of all positive real numbers under multiplication.*

Let $f : G \mapsto \mathbb{R}^+$ by $f(x) = |x|$. It's routine to check f is well-defined, onto, homomorphism and $ker(f) = N$. Then by first homomorphism theorem we have $G/N \cong \mathbb{R}^+$. ■

Polynomial Rings

Let R be a ring. A *polynomial* (in an *indeterminate* x) with coefficients in the ring R is an expression $f(x)$ of the form

$$a_0 + a_1x + a_2x^2 + \cdots + a_mx^m,$$

where a_k is an element of R for $i = 0, 1, 2, \ldots, m$. If $a_k = 0$ then the term a_kx^k may be omitted when writing down the expression defining the polynomial. (Thus for example the polynomial $1 + 0x + 2x^2$ may be written as $1 + 2x^2$.) The elements a_k of R that determine the polynomial are referred to as *coefficients* of the polynomial. If $a_m \neq 0$, and if the polynomial contains no terms of the form a_kx^k with $k > m$ and $a_k \neq 0$, then the non-negative integer m is referred to as the *degree* of the polynomial, and the coefficient a_m is referred to as the *leading coefficient* of the polynomial.

A polynomial determines and is determined by an infinite sequence $a_0, a_1, a_2, \ldots$ of elements of the ring R, where a_k is the coefficient of x^k in the polynomial. An infinite sequence $a_0, a_1, a_2, \ldots$ of elements of R determines a polynomial $a_0 + a_1x + a_2x^2 + \cdots$ if and only if the number of values of k for which $a_k \neq 0$ is finite. If the polynomial is non-zero then its degree is the largest value of m for which $a_m \neq 0$.

One can add and multiply polynomials in the usual fashion. Thus if

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$$

and

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$$

then

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_p + b_p)x^p,$$

where p is the maximum of m and n, and where $a_i = 0$ if $i > m$ and $b_i = 0$ if $i > n$. Also

$$f(x)g(x) = u_0 + u_1x + u_2x^2 + \cdots + u_{m+n}x^{m+n},$$

where, for each integer i between 0 and $m + n$, the coefficient u_i of x^i in $f(x)g(x)$ is the sum of those products a_jb_k for which $0 \leq j \leq m$, $0 \leq k \leq n$ and $j + k = i$. Straightforward calculations show that the set $R[x]$ of polynomials with coefficients in a ring R is itself a ring with these operations of addition and multiplication. The zero element of this ring is of course the polynomial whose coefficients are all equal to zero.

We obtain in this way rings $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$ of polynomials with coefficients in the rings of integers, rational numbers, real numbers and complex numbers respectively.

We now consider various properties of polynomials whose coefficients belong to a *field* K (such as the field of rational numbers, real numbers or complex numbers).

1. *Suppose G is a group, a and b are elements of G of finite order, and $ab = ba$.*

   (a) *Prove that $|ab|$ is a divisor of lcm$(|a|, |b|)$. Note, lcm denotes least common multiple.*

   Let $n = |a|$, $m = |b|$, and let r be a common multiple of n and m. Then there exist integers s and t such that $r = ns$ and $r = mt$ (because r is a common multiple of n and m). Then

$$\begin{aligned}(ab)^r &= a^r b^r && \text{because } ab = ba\\ &= (a^n)^s (b^m)^t\\ &= e^s e^t\\ &= e\end{aligned}$$

   So, r is a multiple of the order of ab. In particular, this applies to $\text{lcm}(n, m)$.

   (b) *Disprove: $|ab| = lcm(|a|, |b|)$.*

   Take $a = b = 1$ in $\mathbf{Z}_2$. Then $|a| = |b| = 2$, so $\text{lcm}(|a|, |b|) = 2$, but $ab = 1 + 1 = 0$ in $\mathbf{Z}_2$ (operation in $\mathbf{Z}_2$ is addition), and $|ab| = |0| = 1$.

   (c) *Prove that if $|a|$ and $|b|$ are relatively prime, then $|ab| = |a| \cdot |b|$.*

   Again let $n = |a|$ and $m = |b|$. Since $\gcd(n, m) = 1$, there exist integers r and s such that $rn + sm = 1$. By our proof in part (a), $(ab)^{nm} = e$, so we just have to show that this is the least power. Now if $k > 0$ such that $(ab)^k = e$, then $a^k b^k = e$ (since $ab = ba$), and so $b^k = a^{-k}$.

   Consider $\langle b^k \rangle = \langle a^{-k} \rangle$. This is a subgroup of $\langle b \rangle$, and a subgroup of $\langle a \rangle$. By Lagrange's theorem, the order of $\langle b^k \rangle$ then divides n and m, which have gcd of 1, so $\langle b^k \rangle = \{e\}$. But then $a^{-k} = b^k = e$, which implies $a^k = e$. Thus k is a multiple of $|a|$ and of $|b|$. Since $|a|$ and $|b|$ are relatively prime, k is a multiple of $|a| \cdot |b|$, and we are done.

13.20 Find all units, zero-divisors, idempotents, and nilpotent elements in $\mathbb{Z}_3 \oplus \mathbb{Z}_6$.

An element (a, b) is a unit if there is (c, d) such that $(a, b)(c, d) = (ab, cd) = (1, 1)$. This can occur only if both a and b are units. The units of $\mathbb{Z}_3$ are $\{1, 2\}$, and the units of $\mathbb{Z}_6$ are $\{1, 5\}$ (here I am using that the units in $\mathbb{Z}_n$ are $1 \leq k < n$ such that $(k, n) = 1$), so the units of $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ are $(1, 1)$, $(1, 5)$, $(2, 1)$, and $(2, 5)$.

An element (a, b) is a zero divisor if $(a, b) \neq (0, 0)$ and there is $(c, d) \neq (0, 0)$ such that $(a, b)(c, d) = (ac, bd) = (0, 0)$. Of course, $\mathbb{Z}_3$ contains no zero divisors (it is a field), so we know that $ac = 0$ implies $a = 0$ or $c = 0$. On the other hand, $\mathbb{Z}_6$ contains several zero divisors, in particular, $\{2, 3, 4\}$, so $bd = 0$ implies that $b \in \{0, 2, 3, 4\}$ or $d = 0$. We can then write down the zero divisors by choosing all the possible non-zero zero divisor combinations. We get $(0, 1)$, $(0, 2)$, $(0, 3)$, $(0, 4)$, $(0, 5)$, $(1, 0)$, $(2, 0)$, $(1, 2)$, $(2, 2)$, $(1, 3)$, $(2, 3)$, $(1, 4)$, and $(2, 4)$.

An element (a, b) is an idempotent if $(a, b)(a, b) = (a^2, b^2) = (a, b)$. This can only happen if $a^2 = a$ and $b^2 = b$. But $a^2 \neq a$ only if $a = 0, 1$ in $\mathbb{Z}_3$. We can check that $b^2 = b$ for $b = 0, 1, 3, 4$ in $\mathbb{Z}_6$, and thus the idempotents of $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ are $(0, 0)$, $(0, 1)$, $(0, 3)$, $(0, 4)$, $(1, 0)$, $(1, 1)$, $(1, 3)$, and $(1, 4)$.

Finally, an element is nilpotent if there exists an $n > 0$ such that $(a, b)^n = (0, 0)$. This occurs only if there is an n such that $a^n = 0$ for $a \in \mathbb{Z}_3$ (and because $\mathbb{Z}_3$ is a field we conclude immediately that $a = 0$), and $b^n = 0$. The only such element in $\mathbb{Z}_6$ is 0. We can easily check this: clearly there is no $n > 0$ such that $1^n = 0$. The element 5 is a unit, so if there were an $n > 0$ with $5^n = 0$, then $5 = (5^{-1})^{n-1} 5^n = 0$ a contradiction. Both 3 and 4 are idempotents, so that $3^n = 3$ and $4^n = 4$ for all $n > 0$. Finally, $2^1 = 2$, $2^2 = 4$, $2^3 = 2$, $2^4 = 4$, and so on, so that $2^n \neq 0$ for $n > 0$. Thus the nilpotent of $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ is $(0, 0)$.

13.38 Suppose that a and b belong to a commutative ring and ab is a zero-divisor. Show that either a or b is a zero-divisor.

If ab is a zero divisor then $ab \neq 0$ and there exists a $t \in R$ such that $t \neq 0 = abt$. If it is the case that $bt = 0$, then b is a zero divisor (neither b or t is zero, but their product is zero). But if $bt \neq 0$, then $a \neq 0 \neq bt$, but the product $a(bt) = 0$, so a is a zero divisor. Thus either a or b is a zero divisor.

13.40 Suppose that R is a commutative ring without zero-divisors. Show that the characteristic of R is zero or prime.

It is enough to show that if the characteristic is not zero, then it is prime. So suppose that $\mathrm{char}R = n \neq 0$ and let $r \in R$ be an element such that $n \cdot r = 0$ and $l \cdot r \neq 0$ for all $0 < l < n$ (such an element exists because otherwise the characteristic of R would be strictly less than n). If n is not prime then $n = ab$ for integers $1 < a, b < n$. Of course, $0 = n \cdot r = \underbrace{r + \cdots + r}_{n-\text{times}}$, and thus, multiplying both sides of the equation by r, we get $0 = \underbrace{r^2 + \cdots + r^2}_{n-\text{times}}$. Then it follows that $0 = \underbrace{r^2 + \cdots + r^2}_{ab-\text{times}} = \big(\underbrace{r + \cdots + r}_{a-\text{times}}\big)\big(\underbrace{r + \cdots + r}_{b-\text{times}}\big)$, and because R has no zero divisors, it must be that $a \cdot r = 0$ or $b \cdot r = 0$. Both of these options force contradictions because $1 < a, b < n$ and we chose r such that there does not exist an $l < n$ such that $l \cdot r = 0$. We conclude that n is prime as required. Note: $ab \cdot r^2 = (a \cdot r)(b \cdot r)$ is clear if one thinks about the number of r^2's which occur if one multiplies out $\big(\underbrace{r + \cdots + r}_{a-\text{times}}\big)\big(\underbrace{r + \cdots + r}_{b-\text{times}}\big)$.

13.60 Let F be a field of order 32. Show that the only subfields of F are F itself and $\{0, 1\}$.

Note that the set $F^* = \{f \in F \mid f \neq 0\}$ is a multiplicative group: in particular, multiplication is associativity by hypothesis, there is a multiplicative identity (because every field contains such an element), and there always exist multiplicative inverses (again because F is a field and we have excluded 0). Now given a subfield G, it must be that G is a non-zero subgroup of F (it contains unity, which is non-zero by definition) and G^* must be a subgroup of F^* (the latter assertion could use some justification: we already know that G^* is a group, so the only remaining question is if it is a subgroup of F^*; but this follows because G^* contains the unity and consists of non-zero elements and is thus clearly a non-empty subset of F^*). Note that F has order 32, while F^* has order 31. By Lagrange's theorem $|G|$ divides 32 while $|G| - 1$ divides 31. The only divisors of 31 are 1 and 31, so this implies that G has order 32 (whence it is F) or order 2. In the latter case, because G must contain 0 and 1, $G = \{0, 1\}$ as required.

15.50 Let $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ and $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. Show that these rings are not isomorphic.

First we note that any isomorphism $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{5}]$ must be the identity on $\mathbb{Z}$, that is $\phi(a) = a$ for all $a \in \mathbb{Z}$. This follows because both rings in question have unity. In particular, by theorem 15.2.6 $\phi(1) = 1$, and therefore if $a \in \mathbb{Z}_+$, then $\phi(a) = \phi(a \cdot 1) = a \cdot \phi(1) = a \cdot 1 = a$ (theorem 15.2.1), and if $a < 0$, then $\phi(a) = \phi(-|a|) = -\phi(|a|) = -|a| = a$ (we have used that ring homomorphisms preserve additive inverses). Finally, $\phi(0) = 0$ because any homomorphism preserves additive identities.

Now suppose that $\phi(\sqrt{2}) = (a + b\sqrt{5})$, where $a, b \in \mathbb{Q}$. Thus

$$2 = \phi(2) = \phi\Big((\sqrt{2})^2\Big) = \phi(\sqrt{2})^2 = (a + b\sqrt{5})^2 = a^2 + 5b^2 + 2ab\sqrt{5}.$$

We know that $\sqrt{5}$ is irrational, so if $2 = (a^2 + 5b^2) + 2ab\sqrt{5}$ it must be that $2ab = 0$. But if $a = 0$, then $5b^2 = 2$ which implies that $b^2 = \frac{2}{5}$. This is a contradiction, because $b \in \mathbb{Q}$, but the square root of $\frac{2}{5}$ is not rational. If $b = 0$, then $a^2 = 2$, which yields a similar contradiction ($a \in \mathbb{Q}$ is rational, but $\sqrt{2}$ is not rational). Thus we conclude that $\mathbb{Z}[\sqrt{2}]$ is not isomorphic to $\mathbb{Z}[\sqrt{5}]$.

12.50 Give an example of a subset of a ring that is a subgroup under addition but not a subring.

We showed in class that the set $T = \left\{ \begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$ is not a subring of $M_2(\mathbb{R})$ because it is not closed under multiplication (for instance $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 2 & 0 \end{bmatrix} \notin T$). But T is a subgroup because it is not empty and whenever $\begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix}, \begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} \in T$ we have that $\begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} - \begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} = \begin{bmatrix} a-c & a-c+b-d \\ a-c+b-d & b-d \end{bmatrix}$ is an element in T (so it passes the one-step subgroup test).

20.34 Find the splitting field for $f(x) = (x^2+x+2)(x^2+2x+2)$ over $\mathbb{Z}_3[x]$. Write $f(x)$ as a product of linear factors.

Using the quadratic formula, we see that the roots of $x^2 + x + 2$ and $x^2 + 2x + 2$ are $\frac{-1 \pm \sqrt{-7}}{2}$ and $\frac{-2 \pm \sqrt{-4}}{2}$ over $\mathbb{Q}$. To translate these into roots over $\mathbb{Z}_3$, we note that $\frac{1}{2} = 2$, $-2 = 1$, and $-1 = -7 = -4 = 2$. So over $\mathbb{Z}_3$ we have roots $2(2 + \sqrt{2}) = 1 + 2\sqrt{2}$, $2(2 + 2\sqrt{2}) = 1 + \sqrt{2}$, $2(1 + \sqrt{2}) = 2 + 2\sqrt{2}$, and $2(1 + 2\sqrt{2}) = 2 + \sqrt{2}$. We can show that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1 + 2\sqrt{2}, 1 + \sqrt{2}, 2 + 2\sqrt{2}, 2 + \sqrt{2})$ (as in the first two assigned problems: one inclusion is obvious and the other follows because $\sqrt{2} = (1 + 2\sqrt{2}) + (2 + 2\sqrt{2})$ is an element of $\mathbb{Q}(1 + 2\sqrt{2}, 1 + \sqrt{2}, 2 + 2\sqrt{2}, 2 + \sqrt{2})$ by closure) and hence $\mathbb{Q}(\sqrt{2})$ is the splitting field for $f(x)$ over $\mathbb{Q}$ (I am using that if $a_1, \ldots, a_n \in E$ are the roots of a polynomial $f(x) \in F[x]$ for E some extension field of F, then $F(a_1, \ldots, a_n)$ is the splitting field of $f(x)$ over F). We can factor $f(x)$ as $f(x) = (x - (1 + 2\sqrt{2}))(x - (1 + \sqrt{2}))(x - (2 + 2\sqrt{2}))(x - (2 + \sqrt{2}))$ in $\mathbb{Q}(\sqrt{2})$. (To be technically correct, we should point out that by $\sqrt{2}$ we mean the element in an extension field of $\mathbb{Z}_3$ whose square is 2).

17.12 Suppose that $f(x) \in \mathbb{Z}_p[x]$ and is irreducible over $\mathbb{Z}_p$, where p is a prime. If $\deg f(x) = n$, prove that $\mathbb{Z}_p[x]/\langle f \rangle$ is a field with p^n elements.

We know by theorem 17.5 that $\mathbb{Z}_p[x]/f(x)$ is a field because $f(x)$ is irreducible over $\mathbb{Z}_p$. Of course, we may express any element of $\mathbb{Z}_p[x]/f(x)$ uniquely in the form $a_{n-1}x^{n-1} + \cdots + a_0$ where the $a_i \in \mathbb{Z}_p$ (more precisely, $a_{n-1}x^{n-1} + \cdots + a_0 + \langle f(x) \rangle$). This follows from the division algorithm: to wit, if $g(x)$ is a polynomial in $\mathbb{Z}_p[x]$ then there are unique $q(x)$ and $r(x)$ such that $g(x) = f(x)q(x) + r(x)$ and $\deg r(x) < \deg f(x)$. But $r(x) = g(x) - f(x)q(x)$ implies that $r(x) + \langle f(x) \rangle = g(x) + \langle f(x) \rangle$ so that we may certainly represent any element in $\mathbb{Z}_p[x]/f(x)$ with a polynomial of degree $< n$. This polynomial is unique because if $r(x), r'(x) \in \mathbb{Z}_p[x]$ with $\deg r(x), r'(x) < \deg f(x)$ and $r(x) + \langle f(x) \rangle = r'(x) + w\langle f(x) \rangle$, then $r(x) - r'(x) \in \langle f(x) \rangle$. Because non-zero polynomials in $\langle f(x) \rangle$ have degree at least n, it must be that $r(x) - r'(x) = 0$, or that $r(x) = r'(x)$.

Hence we conclude that $\mathbb{Z}_p[x]/f(x) = \{a_{n-1}x^{n-1} + \cdots + a_0 + \langle f(x) \rangle \mid a_i \in \mathbb{Z}_p\}$. This set is easy to count as each a_i can take $p = |\mathbb{Z}_p|$ possible values (and each of the resulting elements is unique). We conclude that this field has p^n elements as required.

17.32 Prove that the ideal $\langle x^2 + 1 \rangle$ is prime in $\mathbb{Z}[x]$, but not maximal in $\mathbb{Z}[x]$.

To show that $\langle x^2 + 1 \rangle$ is not maximal, we demonstrate that $\mathbb{Z}[x]/\langle x^+1 \rangle$ is not a field. Let $R = \mathbb{Z}[x]/\langle x^2 + 1 \rangle$ and consider the element $\overline{2} \in R$. Because we may uniquely represent the cosets of R with polynomials of degree < 2, if $\overline{2}$ is invertible then $\overline{2}(\overline{ax + b}) = \overline{1}$. But $2(ax + b) = 2ax + 2b$ and hence $2a = 0$ while $2b = 1$. The latter equation is impossible to solve over the integers, so we conclude that $\overline{2}$ is not a unit in R, and thus that R is not a field as required.

To show that $\langle x^2 + 1 \rangle$ is prime we show that the quotient R is an integral domain. So suppose that $(ax+b+\langle x^2+1 \rangle)(cx+d+\langle x^2+1 \rangle) = \langle x^2+1 \rangle$. It is enough to show that $ax+b$ or $cx+d$ is zero. But $(ax+b+\langle x^2+1 \rangle)(cx+d+\langle x^2+1 \rangle) \in \langle x^2+1 \rangle$ implies that $(ax+b)(xc+d) \in \langle x^2+1 \rangle$ and hence either $(ax+b)(cx+d) = 0$ or $(ax+b)(cx+d) = x^2+1$. Of course, the latter cannot occur as x^2+1 is irreducible, so it must be that $acx^2 + (ad+bc)x + bd = 0$, or $ac = ad+bc = bd = 0$. But because these are elements of $\mathbb{Z}$, it must then follow that a or c equals zero. Without loss of generality we assume that $a = 0$, and our equations become $bc = bd = 0$. Thus either $b = 0$ (whence $ax + b = 0$), or both c and d are zero (so that $cx + d = 0$), and we are done.

Proposition 1.3 *Every integral domain R can be embedded isomorphically in a field.*

PROOF: Let R be an integral domain and R^* the set of non-zero elements of R. On $R \times R^*$, we define the relation: $(a, b) \sim (c, d)$ if $ad = bc$. Since R contains no zero-divisors, it can be verified that this is an equivalence relation. We make the quotient $K = R \times R^*/\sim$ a ring by defining the ring operations as follows. If x/y denotes the equivalence class containing $(x, y) \in R \times R^*$ then define $a/b + c/d = (ad+bc)/bd$ and $(a/b)(c/d) = ac/bd$. These operations are well defined and K is a ring. In fact, K is a field, since b/a is an inverse for a/b, $a \neq 0$. The map $i: R \to K$ given only by $i(a) = a/1$ for $a \in R$ is a one-one homomorphism of R into K.

We shall identify R with the subring $i(R)$ of K.

40. Let $M_2(\mathbb{Z})$ be the ring of all 2×2 matrices over the integers and let

$$R = \left\{ \begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} \middle| a, b \in \mathbb{Z} \right\}.$$

Prove or disprove that R is a subring of $M_2(\mathbb{Z})$.

SOLUTION:

The set R is not a subring of $M_2(\mathbb{Z})$ because the set R is not closed under multiplication.

$$M = \begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} \text{ and } N = \begin{bmatrix} c & c+d \\ c+d & d \end{bmatrix},$$

$$MN = \begin{bmatrix} ac+(a+b)(c+d) & a(c+d)+(a+b)d \\ (a+b)c+b(c+d) & (a+b)(c+d)+bd \end{bmatrix},$$

but $a(c+d)+(a+b)d \neq (a+b)c+b(c+d)$.

41. Let $M_2(\mathbb{Z})$ be the ring of all 2×2 matrices over the integers and let

$$R = \left\{ \begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix} \middle| a, b \in \mathbb{Z} \right\}.$$

Prove or disprove that R is a subring of $M_2(\mathbb{Z})$.

SOLUTION:

The subring test is satisfied and so R is a subring of $M_2(\mathbb{Z})$.

44. Suppose that there is a positive even integer n such that $an = a$ for all elements of some ring. Show that $-a = a$ for all a in the ring.

SOLUTION:

First note that in a ring $(-a)(-b) = ab$ (property 3, Theorem 12.1), and therefore $(-a)^2 = a^2$.

n is even, say $n = 2k$.

Then $-a = (-a)^n = (-a)^{2k} = \left((-a)^2\right)^k = \left(a^2\right)^k = a^{2k} = a^n = a$.

Therefore $-a = a$ for all a in the ring.

Let $R = \{a + bi : a, b \in \mathbb{Z}\}$ be a subring of $\mathbb{C}$. Consider two principal ideals $I = (7)$ and $J = (13)$ in R. Is the ideal I maximal? How about J?

Hint

$\mathbb{Z}[i]$ is a PID. If (7) or (13) is not maximal, it can be included in some larger ideal (m).

This means that $m|7$ or $m|11$ in $\mathbb{Z}[i]$. Now all you need is to figure out if you can find $a + bi$ and $c + di$ which are not units and

$$(a + bi)(c + di) = 7$$

respectively

$$(a + bi)(c + di) = 13$$

Example of infinite groups such that all its elements are of finite order.

Here is one. Let $(\mathbb{Q}, +)$ denote the groups of rational numbers under addition, and consider it's subgroup $(\mathbb{Z}, +)$ of integers. Then any element from the group $\mathbb{Q}/\mathbb{Z}$ has elements of the form $\frac{p}{q} + \mathbb{Z}$ which is of order at-most q. Hence it's of finite order.

- Group of all roots of unity in $\mathbb{C}^\times$.

5. Let r and s be positive integers, and define

$$H = \{nr + ms : n, m \in \mathbb{Z}\}.$$

(a) Show that H is a subgroup of $\mathbb{Z}$.

(b) We saw in class that every subgroup of $\mathbb{Z}$ is cyclic. Therefore, $H = \langle d \rangle$ for some $d \in \mathbb{Z}$. What is this integer d? Prove that the d you've found is in fact a generator for H.

Proof. (a) We can verify directly that $H \leq \mathbb{Z}$. If $nr + ms, nt + mu \in H$, then

$$(nr + ms) + (nt + mu) = n(r + t) + m(s + u),$$

which is again in H. Thus H is closed. Also, $0 = n \cdot 0 + m \cdot 0 \in H$, and if $nr + ms \in H$, then

$$-(nr + ms) = n(-r) + m(-s) \in H,$$

so H is indeed a subgroup of $\mathbb{Z}$.

4. [Saracino, #5.14] Let G be a group. If H and K are subgroups of G, show that $H \cap K$ is also a subgroup of G.

Proof. Suppose that $a, b \in H \cap K$. Then $a, b \in H$, so $ab \in H$ since H is a subgroup. Similarly, $a, b \in K$, so $ab \in K$. Then $ab \in H \cap K$, so $H \cap K$ is closed. Since H and K are both subgroups, $e \in H$ and $e \in K$, hence $e \in H \cap K$. Finally, if $a \in H \cap K$, then $a^{-1} \in H$ and $a^{-1} \in K$, so $a^{-1} \in H \cap K$. Therefore, $H \cap K \leq G$.

Alternatively, we could use the subgroup criterion that we proved in class. Suppose that $a, b \in H \cap K$. Then $ab^{-1} \in H$ and $ab^{-1} \in K$, since H and K are both subgroups, so $ab^{-1} \in H \cap K$. Since a and b are arbitrary elements of $H \cap K$, it follows that $H \cap K \leq G$ by the subgroup criterion. □

2.22. Find $\operatorname{sgn}(\alpha)$ and α^{-1}, where

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

We begin by rewriting α as the cycle $(19)(28)(37)(46)$. Because α is written as four 2-cycles, we know that α is an even permutation and that $\operatorname{sgn}(\alpha) = 1$. We also notice that all the 2-cycles of α are disjoint, so that

$$\alpha^2 = (19)(28)(37)(46)(19)(28)(37)(46) = (19)(19)(28)(28)(37)(37)(46)(46) = (1),$$

and $\alpha = \alpha^{-1}$.

2.25.

(a) If α is an r-cycle, show that $\alpha^r = (1)$.

Proof. Suppose α is the r-cycle represented as $(a_0 a_1 a_2 \dots a_{r-1})$. We will show by induction n that the image of a_k under α^n is a_d where $d = k + n \pmod r$.

For the base case when $n = 1$, the result is clear: a_k is mapped to a_{k+1} except in the case when $k = r - 1$. In this case, $k + 1 = r$ which is $0 \pmod r$.

The induction step is just as easy. Assume that the result is true for n. The image $\alpha^{n+1}(a_k)$ can be rewritten as $\alpha(\alpha^n(a_k))$. Applying our inductive hypothesis, we see that $\alpha^{n+1}(a_k)$ is going to be $\alpha(a_d)$ where $d \equiv k + n \pmod r$ and $0 \leq d < r$. In particular, we have that $d + 1 \equiv k + (n + 1) \pmod r$. Applying α to a_d we find that the image of a_d is a_{d+1} if $d < r - 1$ and a_0 otherwise. Specifically, the image of a_k under α^r is a_l where $l \equiv d + 1 \equiv k + (n + 1) \pmod r$, as required.

Now we shall investigate $\alpha^r(a_k)$. By our lemma, we see that $\alpha^r(a_k) = a_d$ where $d = k + r \pmod r$. In particular, $d = k$, and $\alpha^r(a_k) = a_k$ for all $0 \leq k < r$. In other words, $\alpha^r = (1)$. □

(b) If α is an r-cycle, show that r is the smallest positive integer k such that $\alpha^k = (1)$.

Proof. Using the setup and the lemma we proved above, let $d < r$. We will show that $\alpha^d \neq (1)$. Specifically, notice that $\alpha^d(a_0) = a_d$, since $d < r$. Since the a_i are all distinct, we have that $\alpha^d \neq r$. Hence, r is the least positive integer with $\alpha^r = (1)$. □

2.39.

(a) How many elements of order 2 are there in S_5 and S_6?

We will solve the more general problem below, but you should work these things out in cases of small order first to gain an intuition.

(b) How many elements of order 2 are there in S_n?

Proof. We have that an element of order two in S_n must be the product of disjoint transpositions, and therefore must be of the cycle type

$$(a_1 a_2)(a_3 a_4) \cdots (a_{j-1} a_j)(a_{j+1}) \cdots (a_n).$$

The maximum number of disjoint two cycles that such an element of S_n can contain is $\lfloor \frac{n}{2} \rfloor$ where $\lfloor * \rfloor$ is the floor function. Assume that m is the number of disjoin two cycles in a given cycle type. The number of elements remaining is $n - 2m$ which can be arranged in any order to achieve the same element in S_n. Similarly, each two cycle may be written in two distinct ways, and all the two cycles may be arranged in $m!$ ways to achiave the same element of S_n. Therefore, there are

$$\frac{n!}{2m \cdot m! \cdot (n - 2m)!}$$

such cycles of this type. Taking the sum from $m = 1$ to $m = \lfloor \frac{n}{2} \rfloor$ gives

$$\sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \frac{n!}{2m \cdot m! \cdot (n - 2m)!}$$

elements of order two. □

2.42. Let $G = GL(2, \mathbb{Q})$, and let

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

Show that $A^4 = I = B^6$, but that $(AB)^n \neq I$ for all $n > 0$. Conclude that AB can have infinite order even though both factors A and B have finite order (this cannot happen in a finite group).

Proof. For the first part, just compute it:

$$A^4 = (A^2)^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = I,$$

and

$$B^6 = (B^2)^3 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}^3 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = I.$$

To see that $AB^n \neq I$ for any $n > 0$, we prove the stronger result that

$$AB^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

by induction on n. The base case is trivial since

$$AB = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

For the induction step, assume that the result holds for n, then

$$AB^{n+1} = AB^n \cdot AB = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -(n+1) \\ 0 & 1 \end{pmatrix}$$

by the inductive hypothesis.

We conclude the last part due to the counter example we just computed. □

2.43.

(a) Prove, by induction on $k \geq 1$, that

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^k = \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix}.$$

Proof. The base case when $k = 1$ is obvious. Now suppose that the hypothesis holds for arbitrary k, and notice that

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{k+1} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^k \cdot \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix} \cdot \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

by the inductive hypothesis. Now perform the multiplication to achieve the matrix

$$\begin{pmatrix} \cos k\theta\cos\theta - \sin k\theta\sin\theta & -\sin\theta\cos k\theta - \sin k\theta\cos\theta \\ \cos k\theta\sin\theta + \sin k\theta\cos\theta & -\sin k\theta\sin\theta + \cos k\theta\cos\theta \end{pmatrix},$$

and apply the angle sum and difference identities to obtain the result. □

(b) Find all the element of finite order in $SO(2, \mathbb{R})$, the special orthogonal group.

Proof. We know that $SO(2, \mathbb{R})$ is all matrices representing rotation about the origin by some angle θ. By what we did above, we see that only rotations such that $k\theta = 2\pi l$ for some $l \in \mathbb{Z}$ will have finite order, and therefore rotations by angles $2\pi q$ for $q \in \mathbb{Q}$ will have finite order. □

2.44. If G is a group in which $x^2 = 1$ for every $x \in G$, prove that G must be abelian.

Proof. Let $a, b \in G$. We must show that a and b commute. Notice that the requirement that $x^2 = 1$ for all $x \in G$ is equivalent to saying that x is its own inverse for all $x \in G$. Hence,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1} = ba,$$

so the two commute. Since our choice of $a, b \in G$ was arbitrary, we are done. □

2.48. The *stochastic group* $\Sigma(2,\mathbb{R})$ consists of all those matrices in $GL(2,\mathbb{R})$ whose column sums are 1; that is, $\Sigma(2,\mathbb{R})$ consists of all the nonsingular matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ with $a+b=1=c+d$.

Prove that the product of two stochastic matrices is again stochastic, and that the inverse of a stochastic matrix is stochastic.

Proof. We first show that the subset of stochastic matrices is closed. Let

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \text{ and } \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

be stochastic matrices so that $a+b=c+d=x+z=y+w=1$. Their product is

$$\begin{pmatrix} ax+cz & ay+cw \\ bx+dz & by+dw \end{pmatrix}$$

with

$$(ax+cz)+(bx+dz)=x(a+b)+z(c+d)=x+z=1$$

and

$$(ay+cw)+(by+dw)=y(a+b)+w(c+d)=y+w=1.$$

Hence, the product of any two stochastic matrices is stochastic.

Using the a,c,b,d matrix above, its inverse is

$$\frac{1}{ad-bc}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

whose left column sums to

$$\frac{d-b}{ad-bc}.$$

However, since $c+d=1$, we have that $d=1-c$ and $ad-bc=a(1-c)-bc=a-c(a+b)=a-c$ while $a+b-(c+d)=0$ so $a-c=d-b$ and the fraction above is equal to one. The right column is analogous, so that we have that the stochastic matrices are closed under inverses and are therefore a subgroup of $GL(2,\mathbb{R})$. □

2.51. Let $e_1=(1,0)$ and $e_2=(0,1)$, If φ is an isometry of the plane fixing O, let $\varphi(e_1)=(a,b)$, $\varphi(e_2)=(c,d)$, and let $A=\begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Prove that $\det(A)=\pm 1$.

Proof. We need to show that $ad-bc=\pm 1$. This is equivalent to showing that $(ad-bc)^2=1$, so we will show this instead. Since φ is an isometry, it preserves distance and therefore length of vectors. It follows that

$$a^2+b^2=c^2+d^2=1$$

and that

$$(a-c)^2+(b-d)^2=(1-0)^2+(0-1)^2=2.$$

Using the latter, we find that

$$a^2+b^2+c^2+d^2=2(ac+bd)+2,$$

but $a^2+b^2=c^2+d^2=1$. Hence,

$$ac+bd=0,$$

and more importantly, its square is zero. Multiplying the two equations from the first equality and rearranging the terms gives

$$1=(a^2+b^2)(c^2+d^2)=(ad-bc)^2+(ac+bd)^2,$$

so $(ad-bc)^2=1$ as required. □

(vii) The intersection of two cyclic subgroups of G is a cyclic subgroup.

The intersection of two subgroups is a subgroup of each. Subgroups of cyclic groups are cyclic, so this is true.

(viii) If X is a finite subset of G, then $\langle X \rangle$ is a finite subgroup.

False. The set $\{1\}$ containing only the element $1 \in \mathbb{Z}$ is a finite subgroup, but generates all of $\mathbb{Z}$.

(ix) If X is an infinite set, then

$$F = \{\sigma \in S_X : \sigma \text{ moves only finitely many elements of } X\}$$

is a subgroup of S_X.

Proof. This is true. The composition of two such elements moves only a finite number of elements of X, and the inverse of such an element σ moves on the elements moved by σ. Thus F is closed under products and inverses, and the identity is clearly in F. This proves F is a subgroup. □

(x) Every proper subgroup of S_3 is cyclic.

Proof. True, every proper subgroup of S_3 has order $1, 2$, or 3 by Lagranges theorem, which all must be cyclic. □

(xi) Every proper subgroup of S_4 is cyclic.

False. S_3 is a subgroup of S_4 in a natural way, and is not cyclic.

2.55. Give an example of two subgroups H and K of a group G whose union $H \cup K$ is not a subgroup of G.

Proof. We appeal to our favorite counter example, S_3. In particular, take the subgroup generated by the cycle (12) and the subgroup generated by the cycle (123). The former has order two, while the latter has order three, and their intersection is just the identity (see the following problem for a proof, or just compute it!). Their union is a set of order four, which cannot be a subgroup of S_3 by Lagrange's theorem. □

2.57. If H and K are subgroups of a group G and if $\#H$ and $\#K$ are relatively prime, prove that $H \cap K = \{1\}$.

Proof. The intersection $H \cap K$ of two subgroups H, K of G is a subgroup of H, K, and G (if this is not clear you should prove it yourself). By Lagrange's theorem, we have that the order of $H \cap K$ must divide the order of H and divide the order of K. But $\#H, \#K$ are coprime, so the only positive integer dividing both is one. Hence, $\#(H \cap K) = 1$, and therefore $\#(H \cap K) = \{1\}$. □

3.6. Find multiplicative inverses of nonzero elements in $\mathbb{I}_{11}$.

Proof. Every element but 0 has a multiplicative inverse since 11 is prime. Also, every element but 1 generates the group of units of $\mathbb{Z}/11\mathbb{Z}$ which has order 10, so that its inverse is itself to the ninth power modulo 11. □

3.13. Prove that the only subring of $\mathbb{Z}$ is $\mathbb{Z}$ itself.

Proof. $\mathbb{Z}$ is a cyclic group under addition with generator 1. In particular, if $1 \in S \subseteq \mathbb{Z}$ and S is closed under sums and inverses, then $S = \mathbb{Z}$, but every subring of $\mathbb{Z}$ is closed under sums and inverses and contains 1. □

3.19. Define $\mathbb{F}_4$ to be the set of all 2×2 matrices

$$\mathbb{F}_4 = \left\{ \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} : a, b \in \mathbb{F}_2 \right\}.$$

(a) Prove that $\mathbb{F}_4$ is a commutative ring whose operations are matrix addition and matrix multiplication.

Proof. It suffices to show that $\mathbb{F}_4$ is closed under sums and additive inverses, and that it is closed under products since it is a subset of $M_2(\mathbb{F}_2)$, the set of 2×2 matrices with coefficients in $\mathbb{F}_2$. This is clear by direct computation. □

(b) Prove that $\mathbb{F}_4$ is a field having exactly four elements.

Proof. The entries of any matrix in $\mathbb{F}_4$ have two degrees of freedom, and there are 2 choices for each, hence there are four such matrices. To see that any nonzero ones are invertible, we simply compute the determinant

$$\det \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} = a(a+b) - b^2 = a^2 - b^2 + ab$$

with the requirement that either a or b is nonzero. In any of the three cases, the determinant is nonzero and the matrix is invertible. □

(c) Show that $\mathbb{I}_4$ is not a field.

Proof. 2 is a zero divisor in $\mathbb{I}_4$. □

3.21. Find all the units in the ring $\mathbb{Z}[i]$ of Gaussian integers.

Proof. We define the *norm function* $N : \mathbb{Z}[i] \to \mathbb{N}$ to be the multiplicative function

$$N(a+bi) = (a+bi)(a-bi) = a^2 + b^2.$$

You should verify this function is multiplicative, that is, that $N(z)N(w) = N(zw)$ for $z, w \in \mathbb{Z}[i]$. If $u \in \mathbb{Z}[i]$ is a unit, then its norm $N(u)$ divides $N(1) = 1$ since $N(u)N(u^{-1}) = N(1) = 1$. If $N(u) = a^2 + b^2$ and divides 1, then it follows that $N(u) = \pm 1$ so that either $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$. Indeed, any such choice of a, b produces a number $a + bi$ which is a unit, and we have therefore exhibited them all. To be succinct,

$$U(\mathbb{Z}[i]) = \{1, -1, i, -i\},$$

the fourth roots of unity. □

1. Let G be a group and let a be an element of G with order n.

   (a) Prove $(bab^{-1})^n = e$.

   •

$$\begin{aligned}
(bab^{-1})^n &= \underbrace{bab^{-1} \cdot bab^{-1} \cdot bab^{-1} \cdot \ldots \cdot bab^{-1}}_{\text{n times}} \\
&= ba \cdot (b^{-1}b) \cdot a \cdot (b^{-1}b) \cdot a \cdot (b^{-1}b) \cdot \ldots \cdot (b^{-1}b) \cdot ab^{-1} \\
&= ba \cdot e \cdot a \cdot e \cdot a \cdot e \cdot \ldots \cdot e \cdot ab^{-1} \\
&= ba^n b^{-1} \\
&= beb^{-1} \\
&= bb^{-1} \\
&= e
\end{aligned}$$

   (b) Prove that the order of bab^{-1} is exactly n.

   - By (a), we know that the order of bab^{-1} is no greater than n. So, suppose that the order of bab^{-1} is m with $m < n$. Therefore, it must be true that $e = (bab^{-1})^m = ba^m b^{-1}$. Consequently, $b^{-1}eb = b^{-1}ba^m b^{-1}b$. Reducing both sides, we get that $e = a^m$. But this implies that the order of a is less than n, in violation of our hypothesis. We conclude that the order of bab^{-1} must be n.

5. For $a, b \in G$ we say a is *conjugate* to b if there exists some $x \in G$ such that $a = xbx^{-1}$.

   (a) Prove that if a is conjugate to b, then b is conjugate to a.

   - Since $a = xbx^{-1}$, we multiply on the left and right by x^{-1} and x, respectively, to get $x^{-1}ax = b$. But, since, $x = (x^{-1})^{-1}$, we're done.

   (b) Prove that if a is conjugate to b, then there exists some $y \in G$ such that $a = y^{-1}by$.

   - Let $y = x^{-1}$. Since $y^{-1} = (x^{-1})^{-1} = x$, we see that $a = y^{-1}by$. Notice that we use no additional elements besides those implied by the definition of conjugate.

   (c) Prove that a is conjugate to a.

   - Since a is in G, a has an inverse a^{-1}. Notice that $a = ae = aaa^{-1}$.

   (d) Prove that if a is conjugate to b and b is conjugate to c, then a is conjugate to c.

   - So, we have that $a = xbx^{-1}$ and $b = ycy^{-1}$ for some pair of elements $x, y \in G$. But, this means that $a = x(ycy^{-1})x^{-1} = (xy)c(y^{-1}x^{-1})$. By the Socks-Shoes Lemma, $(xy)^{-1} = y^{-1}x^{-1}$, so we're done.

   (e) Determine all g in S_3 which are conjugate to (12).

   - The element (12) is conjugate to (12), (23), and (13). The justification follows: $(12) = (23)(13)(23) = (13)(23)(13) = (12)(12)(12)$.

   (f) Determine all g in S_3 which are conjugate to (123).

   - The element (123) is conjugate to (123), and (132).

   (g) Determine all g in D_4 which are conjugate to R_{90}.

   - The elements R_{90} and R_{270} are conjugate to R_{90}.

- *7.1* Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the lelft cosets of H in A_4.
  - Since H is a subgroup of A_4, its cosets are all disjoint. First note that one coset is given by the elements in H, namely $H = (1)H = (12)(34)H = (13)(24)H = (14)(23)H$. To find the others, begin by multiplying H on the left by some element not in H, say (123). The result is $(123)H = \{(123), (134), (243), (142)\} = (134)H = (243)H = (142)H$. This leaves four elements of A_4 that are not in a left coset, one of which is (132). Multiplying H on the left by (132), we see that the last coset is $(132)H = \{(132), (143), (234), (124)\} = (143)H = (234)H = (124)H$.
- *7.2* Let H be as in Exercise 1. How many left cosets of H in S_4 are there?
  - Since H is a subgoup of A_4, and A_4 is a subgroup of S_4, we know that H is a subgroup of S_4. Since H is a subgroup, its distinct left cosets partition S_4 into equal-sized sets. Since H has order 4, we see that there are exactly $| S_4 | /4 = 24/4 = 6$ distinct cosets of H.
- *7.24* Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all g in G.
  - If G is not cyclic, there is no element in g with order 25. Since the order of every element must divide the order of G, and 25 is divisible only by 1, 5, and 25, we see that all elements of G must have order 1 or order 5. In either case, $g^5 = e$ for all $g \in G$.

- *7.26* Let $|G| = 8$. Show that G must have an element of order 2.
  - The possible orders of an element of G are 1, 2, 4, and 8. Since G has only one element of order 1, it must have at least one element that has order 2, 4, or 8. In the case of 2, there's nothing to prove. In the case of 4, we call the element g. Then $g^4 = (g^2)^2 = e$, which implies that g^2 has order 2. In the case of 8, we again call the element g, and note that $g^8 = (g^4)^2 = e$, so that g^4 has order 2. Thus, in all cases, we see that G must have at least one element of order 2.
- *7.34* Prove that a group of order 12 must have an element of order 2.
  - Each non-identity element of the group must have an order of 2, 3, 4, 6, or 12. In the case that there is some element that has order 2, 4, 6, or 12, it's easy to see that there must be an element of order 2 by applying the same argument used in the solution to 7.26. Thus, the only possible case in which there is no element of order 2 is when all non-identity elements have order 3. So, let's assume that this is true. Choose one such element of order 3, call it g. Notice that g generates a subgroup of order 3: $\{e, g, g^2\}$. Also notice that both g and g^2 generate this group. Since every non-identity element lies in exactly one such order-3 subgroup (suppose otherwise and you'll derive a contradiction), we can use this knowledge to generate a formula for the order of the group. Since every order-3 subgroup contains the identity, we set it aside. Thus, each such subgroup contains two elements distinct from all the others, so we can say that if there are n such subgroups, then the order of G will be $2n + 1$ (with the 1 coming from the identity). But, notice that $2n + 1$ is odd for all integers, but the order of our group is 12, which is even. Thus, we have derived a contradiction, and can conclude that the group cannot have all non-identity element of order 3.

The following are from Gallian, Chapters 7 and 9. The numbering is first given for the 7th edition, and is then followed by the 6th edition's numbering (if the numbering is different).

- *# 7.15*: Suppose $|G| = pq$ with p and q prime numbers. By Lagrange's Theorem, the possible subgroups of G have orders 1, p, q, or pq. For a subgroup H of G to be proper, it must have order less than G, so we can immediately eliminate pq. In the case that $|H| = 1$, H contains only e so it is clearly cyclic. In the case that $|H| = p$ or $|H| = q$, then H has prime order, so it must be cyclic. This completes the argument.
- *# 7.20*: Since H and K are both subgroups of G, we know that $H \cap K$ must contain e, so it is nonempty. Suppose there is some other element, g, that is in $H \cap K$. Then $g \in H$ and $g \in K$, so $|g| > 1$ must divide the order of H and of K, since both H and K are themselves groups. But, since $|H| = 12$ and $|K| = 35$ have no common divisors greater than 1, we have derived a contradiction. Thus, the only element in $H \cap K$ is e, so $|H \cap K| = 1$.
- *# 7.39* (resp. *# 7.35*): Since G has elements of orders 1 through 10, it's clear that if $|G| = k$, then $10 \mid k$, $9 \mid k$, ..., $2 \mid k$. Thus, the least possible order of G is $lcm(1, 2, 3, 4, 5, 6, 7, 8, 9, 10)$ which is $2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$.
- *# 9.1*: No, H is not normal in S_3. Consider that $(13)H = \{(13), (123)\} \neq H(13) = \{(13), (132)\}$.
- *# 9.7*: Suppose that H has index 2 in G. Then, for any a not in H, we have that $aH \cap H = \emptyset$ and $aH \cup H = G$. Therefore, the complement of H in G is simply aH. The exact same argument where Ha is considered instead of aH shows that the complement of H also equals Ha. Thus $aH = Ha$ for all a not in H. For any $b \in H$, $bH = H = Hb$. Thus, for all $g \in G$, we have $gH = Hg$, so that H is normal.
- *# 9.8a*: Referencing Table 5.1, consider that $(123)H = \{(123), (134)\} \neq H(123) = \{(123), (243)\}$.

Assignment: Prove that if G is a simple group of size less than 60, then G is cyclic of prime size.
Recall from class the following lemmas:

- Lemma P: If $|G| = p$ with p a prime, then G is a simple group.
- Lemma Z: If $|G| = p^a$ with p a prime and a an integer greater than 1, then G is not a simple group.
- Lemma S: If $|G|$ is not a prime, and G has a singleton conjugacy class not equal to $\{e\}$, then G is not simple.
- Lemma r!: If G has a conjugacy class of size $r > 1$ and $|G| > r!$, then G is not simple.
- Super Lemma r!: If G has a conjugacy class of size $r > 1$ with $|G| < r!$, and $|G|$ does not divide $r!$, then G is not simple.

As a consequence of the above lemmas, we can add the following:

- Lemma PQ: If $|G| = pq$ with p and q both primes, then G is not a simple group.
  - *Proof*: Seeking a contradiction, let G be a group of order pq that is simple. By Lemma S, G has no singleton conjugacy class besides the identity. Since the size of any conjugacy class of G must divide $|G| = pq$, the possible sizes of the non-identity conjugacy classes can only be p or q. Since neither p nor q divides $pq - 1$, any sum of multiples of p and q equaling $pq - 1$ must contain multiples of both p and q. Thus, G has conjugacy classes of size p and q. If $p = q$ then we're done (Lemma Z), so suppose without loss of generality that $p < q$. In the case that $|G| > p!$, Lemma r! immediately provides the contradiction we seek. In the case that $|G| < p!$, then $|G|$ does not divide $p!$ since the prime factorization of $p!$ contains no prime equal to q. Once again, we derive a contradiction. Lastly, consider the case where $|G| = p!$. Then $p! = pq$ which only happens if $p = 3$ and $q = 2$ which violates the condition that $p < q$. This completes the proof.

2. Let A and B be normal subgroups of a group G such that $A \cap B = \{e\}$. Prove that $ab = ba$ for all $a \in A$ and $b \in B$.

   [Hint: Prove that $aba^{-1}b^{-1} \in A \cap B$.]

   - Note first that for all $a \in A$ and $b \in B$, we have $aba^{-1} \in B$ and $ba^{-1}b^{-1} \in A$. Correspondingly, $(aba^{-1})b^{-1} \in Bb^{-1} = B$ and $a(ba^{-1}b^{-1}) \in aA = A$. Thus, $aba^{-1}b^{-1} \in A \cap B$. Since $A \cap B = \{e\}$, we know that $aba^{-1}b^{-1} = e$, and therefore that $ab = ba$. This completes the proof.

3. Let G be a group of size 15. Let a be an element of order 3 and b be an element of order 5. Set $A = \langle a \rangle$ and $B = \langle b \rangle$.

   (a) Prove that $AB = G$.

   - Since A and B have prime orders 3 and 5, each non-identity element of A and B also has an order of 3 and 5, respectively. Therefore $A \cap B = \{e\}$, for otherwise we could conclude $|A| = 5$ or $|B| = 3$, both of which would be contradictions.
     One way to accomplish our task is to determine if the set $AB = \{ab \mid a \in A \text{ and } b \in B\}$ has size 15. We can do this using properties of cosets. Let $A = \{e, a_1, a_2\}$. Then $B = eB \neq a_1B$ and $B = eB \neq a_2B$, since $a_1, a_2 \notin B$. Since different cosets are disjoint, the only case in

   which $|AB| < 15$ is if $a_1B = a_2B$. Seeking a contradiction, suppose $a_1B = a_2B$. Then for every $b_1 \in B$, there exists a $b_2 \in B$ such that $a_1b_1 = a_2b_2$ with $b_1 \neq b_2$ (since otherwise we get $a_1 = a_2$), and consequently $a_1b_1b_2^{-1} = a_2 \in A$. Let $b_1b_2^{-1} = b_3 \in B$ and note that $b_3 \neq e$. Thus, $a_1b_3 \in Ab_3$ and $a_1b_3 \in A$, which is a contradiction since $b_3 \notin A$. We conclude that $a_1B \neq a_2B$, so they are disjoint. Finally, since B, a_1B, and a_2B are all disjoint and all have size 5, $|B \cup a_1B \cup a_2B| = 15$. But notice that $B \cup a_1B \cup a_2B$ is precisely AB. Thus $|AB| = 15$ and the proof is complete.

(b) Prove that both A and B are normal subgroups.
[Hint: Use the Sylow theorems.]

- We apply Sylow's Third Theorem as follows:
  - Since $n_3 \mid 15$, we have that $n_3 = 1$, 3, 5, or 15. Only $1 \equiv 1 \pmod 3$, so $n_3 = 1$ and A is the only 3-Sylow subgroup. By the corollary to Sylow's Third Theorem, we conclude that A is normal.
  - Since $n_5 \mid 15$, we have that $n_5 = 1$, 3, 5, or 15. Only $1 \equiv 1 \pmod 5$, so $n_5 = 1$ and B is the only 5-Sylow subgroup. By the corollary to Sylow's Third Theorem, we conclude that B is normal.

(c) Prove that G is an abelian group and thus $G = \mathbb{Z}_{15}$.
[Hint: Use a previous question on the set.]

- Since A and B are both normal and $A \cap B = \{e\}$, we know from question 2 that $ab = ba$ for all $a \in A$ and $b \in B$. Furthermore, since $AB = G$ from part (a), two arbitrary elements $x, y \in G$ may be expressed as $x = a_1b_1$ and $y = a_2b_2$. So,

$$\begin{aligned} xy &= (a_1b_1)(a_2b_2) \\ &= a_1(b_1a_2)b_2 \\ &= a_1(a_2b_1)b_2 \end{aligned}$$

since $ab = ba$ for all $a \in A$ and $b \in B$.
Furthermore,

$$\begin{aligned} a_1(a_2b_1)b_2 &= (a_1a_2)(b_1b_2) \\ &= (a_2a_1)(b_2b_1) \end{aligned}$$

since A and B are both cyclic, hence Abelian.
Lastly,

$$\begin{aligned} (a_2a_1)(b_2b_1) &= a_2(a_1b_2)b_1 \\ &= a_2(b_2a_1)b_1 \\ &= yx \end{aligned}$$

- *# 4.8*: Let a be an element of a group and let $|\ a\ | = 15$. Compute the orders of the following elements of G:
  - a^3, a^6, a^9, a^{12}
    - For each a^k above, $\gcd(15, k) = 3$. Thus, the order of each is $15/3 = 5$.
  - a^5, a^{10}
    - For each a^k above, $\gcd(15, k) = 5$. Thus, the order of each is $15/5 = 3$.
  - a^2, a^4, a^8, a^{14}
    - For each a^k above, $\gcd(15, k) = 1$. Thus, the order of each is $15/1 = 15$.

- *# 4.14*: Suppose that a cyclic group G has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 7. What is $|\ G\ |$? What can you say if 7 is replaced with p where p is a prime?
  - Since G is cyclic, there is some element a in G such that $\langle a \rangle = G$. Since G has a subgroup of order 7, and G is cyclic, we know that 7 divides the order of G. That is, $|\ \langle a \rangle\ | = |\ G\ | = 7n$ for some positive integer n. We now test a few possible values of n:
    - Suppose $n = 1$. Then G and one of its subgroups both have order 7. By the Fundamental Theorem of Cyclic Groups (FTCG), G and its subgroup of order 7 are the same, contradicting the condition that G has 3 distinct subgroups.
    - Suppose n is 2, 3, 4, 5, or 6. Then, by FTCG, $G = \langle a \rangle$ has a subgroup of order n. Thus, G has at least 4 subgroups: $\{e\}$, the subgroup of order 7, the subgroup of order n, and G itself. This contradicts the fact that G has exactly three subgroups.
    - Suppose $n = 7$. Then $|\ G\ | = 7 \cdot 7 = 49$. Since 7 is the only positive divisor of 49 between 1 and 49, it is the only possible order of a subgroup other than $\{e\}$ or G. FTCG also tells us that there is *exactly* one subgroup of order 7. This fits the supposed criteria.
    - In general, if we suppose that n is any positive integer besides 7, we see that G is guaranteed a subgroup of order n by the FTCG, which means that G will have *at least* 4 distinct subgroups.

    We therefore conclude that the order of G must be $7^2 = 49$.
  - More generally, if 7 is replaced by any prime p under the supposed conditions, the the order of G must be p^2.

- *# 4.22*: Prove that a group of order 3 must be cyclic.
  - Seeking a contradiction, let G be a group of order 3 that is not cyclic. Thus G has an identity element e, and two additional elements, call them a and b. Since $\langle a \rangle$ and $\langle b \rangle$ are both subgroups of G, they both contain e. Since G is not cyclic, b is not in $\langle a \rangle$ and a is not in $\langle b \rangle$. Thus, it must be true that $a^2 = e$ and $b^2 = e$, or else we would have that $ea = aa = a$ and $eb = bb = b$, which would mean that not G is not a group (see HW#2, Question 5). Putting all of this into a multiplication table, we see:

$G =$

	e	a	b
e	e	a	b
a	a	e	
b	b		e

    Thus we now only need to determine the products ab and ba. But notice that ab and ba cannot be e, a, or b (by HW#2, Question 5). Thus, G is not closed, which contradicts the fact that G is a group. Since the assumption that G is not cyclic leads to this absurdity, we conclude that G must be cyclic.

- *# 5.3*: What is the order of each of the following permutations?
  - (124)(357): disjoint, both of length 3, so the order of the permutation is $lcm(3,3) = 3$
  - (124)(3567): disjoint and of lengths 3 and 4, so the order of the permutation is $lcm(3,4) = 12$
  - (124)(35): disjoint and of lengths 3 and 2, so the order of the permutation is $lcm(3,2) = 6$
  - (124)(357869): disjoint and of lengths 3 and 6, so the order of the permutation is $lcm(3,6) = 6$
  - (1235)(24567): not disjoint, so we rewrite this permutation as a product of disjoint cycles. The result is (124)(3567), with cycles of orders 3 and 4, so the order of the permutation is $lcm(3,4) = 12$
  - (345)(245): not disjoint, so we rewrite this permutation as a product of disjoint cycles. The result is (25)(34), so the order of the permutation is $lcm(2,2) = 2$
- *# 5.4*: What is the order of each of the following permutations?
  - $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 6 & 3 \end{bmatrix}$
    Writing this as a product of cycles, we get (12)(356). Since this is a disjoint product of cycles of lengths 2 and 3, the order of the permutation is $lcm(2,3) = 6$.
  - $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{bmatrix}$
    Writing this as a product of cycles, we get (1753)(264). Since this is a disjoint product of cycles of lengths 4 and 3, the order of the permutation is $lcm(4,3) = 12$.
- *# 5.9*: Determine whether the following permutations are even or odd.
  - (135): Written as a product of 2-cycles, we get (15)(13), so this is even.
  - (1356): Written as a product of 2-cycles, we get (16)(15)(13), so this is odd.
  - (13567): Written as a product of 2-cycles, we get (17)(16)(15)(13), so this is even.
  - (12)(134)(152): Written as a product of disjoint cycles, we get (15)(234). Rewritten as a product of 2-cycles, we get (15)(24)(23), so this is odd.
  - (1243)(3521): Written as a product of disjoint cycles, we get (354). Rewritten as a product of 2-cycles, we get (34)(35), so this is even.
- *# 5.18*: Let $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}$. Write α, β, and $\alpha\beta$ as
  - products of disjoint cycles,
    - $\alpha = (12345)(678)$
    - $\beta = (23847)(56)$
    - $\alpha\beta = (12345)(678)(23847)(56) = (12485736)$
  - products of 2-cycles.
    - $\alpha = (15)(14)(13)(12)(68)(67)$
    - $\beta = (27)(24)(28)(23)(56)$
    - $\alpha\beta = (16)(13)(17)(15)(18)(14)(12)$

- *# 5.20*: Compute the order of each member of A_4. What arithmetic relationship do these orders have with the order of A_4?
  - Referencing the table for A_4 given in Chapter 5, we see that
    - α_1 has order 1 (the identity)
    - α_2, α_3, and α_4 have order 2
    - α_5 through α_{12} have order 3
  - The order of each permutation divides the order of A_4, which is $4!/2 = 4 \cdot 3 = 12$.
- *# 5.28*: Let $\beta = (123)(145)$. Write β^{99} in disjoint cycle form.
  - In disjoint cycle form, $\beta = (14523)$. Thus, the permutation has order 5, and $\beta^5 = e$. Therefore,
$$\begin{aligned}\beta^{99} &= \beta^{5\cdot 19+4} \\ &= (\beta^{5\cdot 19})\beta^4 \\ &= (\beta^5)^{19}\beta^4 \\ &= e^{19}\beta^4 \\ &= \beta^4\end{aligned}$$
  - Now we compute $\beta^4 = (14523)(14523)(14523)(14523) = (13254)$. Thus, $\beta^{99} = (13254)$.
- *# 5.30*: What cycle is $(a_1a_2...a_n)^{-1}$?
  - We can restate this question as: what cycle β gives $\beta(a_1a_2...a_n) = (a_1a_2...a_n)\beta = e$? Our knowledge of the Socks-Shoes Lemma might lead us to try $(a_n...a_2a_1)$, and in fact letting $\beta = (a_n...a_2a_1)$ gives the desired result.
- *# 5.34*: Let $H = \{\beta \in S_5 \mid \beta(1) = 1 \text{ and } \beta(3) = 3\}$. Prove that H is a subgroup of S_5. Is your argument valid when 5 is replaced by any $n \geq 3$?
  - We use the Two-Step Subgroup Test. Let α, γ be elements of H. Then:
$$\begin{aligned}\alpha\gamma(1) &= \alpha(\gamma(1)) \\ &= \alpha(1) = 1,\end{aligned}$$
    and
$$\begin{aligned}\alpha\gamma(3) &= \alpha(\gamma(3)) \\ &= \alpha(3) = 3,\end{aligned}$$
    so $\alpha\gamma$ is in H. Also, since $1 = \alpha^{-1}(\alpha(1)) = \alpha^{-1}(1)$ and $3 = \alpha^{-1}(\alpha(3)) = \alpha^{-1}(3)$, we see that α^{-1} is in H. This gives the desired result.
  - Replacing S_5 with S_n for any $n \geq 3$ does not affect the argument.
- *# 5.36*: In S_4, find a cyclic subgroup of order 4 and a noncyclic subgroup of order 4.
  - The subgroup of S_4 generated by (1234) is cyclic, since $(1234)^4 = e$, and the set $\{e, (1234), (1234)^2, (1234)^3\}$ is closed under composition.
  - Referencing the table given for A_4 in chapter 5 (note that A_4 is a subgroup of S_4), we can see readily that $\{(1), (12)(34), (13)(24), (14)(23)\}$ gives a non-cyclic subgroup of S_4 that has order 4.

- *# 1*:
  - $\mathbb{Z}_{12}$:
    - $|\ \mathbb{Z}_{12}\ | = 12$;
    - $|\ 0\ | = 1$; $|\ 1\ | = 12$; $|\ 2\ | = 6$; $|\ 3\ | = 4$; $|\ 4\ | = 3$; $|\ 5\ | = 12$; $|\ 6\ | = 2$; $|\ 7\ | = 12$; $|\ 8\ | = 3$; $|\ 9\ | = 4$; $|\ 10\ | = 6$; $|\ 11\ | = 12$.
  - $U(10)$:
    - $|\ U(10)\ | = \phi(10) = \phi(2 \cdot 5) = (1)(4) = 4$;
    - $|\ 1\ | = 1$; $|\ 3\ | = 4$; $|\ 7\ | = 4$; $|\ 9\ | = 2$.
  - $U(12)$:
    - $|\ U(12)\ | = \phi(12) = \phi(2^2 \cdot 3) = (2)(2) = 4$;
    - $|\ 1\ | = 1$; $|\ 5\ | = 2$; $|\ 7\ | = 2$; $|\ 11\ | = 2$.
  - $U(20)$:
    - $|\ U(20)\ | = \phi(20) = \phi(2^2 \cdot 5) = (2)(4) = 8$;
    - $|\ 1\ | = 1$; $|\ 3\ | = 4$; $|\ 7\ | = 4$; $|\ 9\ | = 2$; $|\ 11\ | = 2$; $|\ 13\ | = 4$; $|\ 17\ | = 4$; $|\ 19\ | = 2$.
  - D_4:
    - $|\ D_4\ | = 8$;
    - $|\ R_0\ | = 1$; $|\ R_{90}\ | = 4$; $|\ R_{180}\ | = 2$; $|\ R_{270}\ | = 4$; $|\ H\ | = 2$; $|\ V\ | = 2$; $|\ D\ | = 2$; $|\ D'\ | = 2$.
  - *Observations*: The order of every element divides the order of the group.
- *# 2*:
  - In $\mathbb{Q}$, we have $\langle \frac{1}{2} \rangle = \{0, \pm\frac{1}{2}, \pm 1, \pm\frac{3}{2}, \pm 2, \pm\frac{5}{2}, ...\}$
  - In $\mathbb{Q}^*$, we have $\langle \frac{1}{2} \rangle = \{..., \frac{1}{2^n}, ..., \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, ..., 2^n, ...\}$
- *# 3*:
  - In $\mathbb{Q}$, $|\ 0\ | = 1$. All other elements have infinite order.
  - In $\mathbb{Q}^*$, $|\ 1\ | = 1$, and $|\ -1\ | = 2$. All other elements have infinite order.

6. Find the order of the following elements in $GL_4(\mathbb{R})$.

   (a)

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$A^2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

   Thus $|A| = 2$.

(b)

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$A^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$A^4 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Thus $|A| = 4$.

9. For each of the following values of n, find all generators of the cyclic group $\mathbb{Z}_n$ under addition.

(a) $n = 8$

$\mathbb{Z}_8 = \langle [1] \rangle$, so $[1]$ generates $\mathbb{Z}_8$. All other generators are $m[1]$ where m and 8 are relatively prime. Thus $m = 1, 3, 5, 7$.

Therefore $\mathbb{Z}_8$ has four generators, namely $\boxed{[1], [3], [5] \text{ and } [7].}$

(d) $n = 15$

$\mathbb{Z}_{15} = \langle [1] \rangle$, so $[1]$ generates $\mathbb{Z}_{15}$. All other generators are $m[1]$ where m and 15 are relatively prime. Thus $m = 1, 2, 4, 7, 8, 11, 13, 14$.

Therefore $\mathbb{Z}_{15}$ has eight generators, namely $\boxed{[1], [2], [4], [7], [8], [11], [13] \text{ and } [14].}$

10. For each of the following values of n, find all subgroups of the cyclic group $\mathbb{Z}_n$ under addition and state their order.

(a) $n = 12$

Since $[1]$ generates $\mathbb{Z}_{12}$, the distinct subgroups of $\mathbb{Z}_{12}$ will be generated by $m[1]$ where m is a divisor of 12. Thus $m = 1, 2, 3, 4, 6, 12$. Therefore the distinct subgroups of $\mathbb{Z}_{12}$ are:

$$\begin{aligned} \langle [1] \rangle &= \mathbb{Z}_{12} & |\langle [1] \rangle| &= 12 \\ \langle [2] \rangle &= \{[0], [2], [4], [6], [8], [10]\} & |\langle [2] \rangle| &= 6 \\ \langle [3] \rangle &= \{[0], [3], [6], [9]\} & |\langle [3] \rangle| &= 4 \\ \langle [4] \rangle &= \{[0], [4], [8]\} & |\langle [4] \rangle| &= 3 \\ \langle [6] \rangle &= \{[0], [6]\} & |\langle [6] \rangle| &= 2 \\ \langle [12] \rangle &= \{[0]\}\} & |\langle [12] \rangle| &= 1 \end{aligned}$$

(b) $n = 8$

Since $[1]$ generatds $\mathbb{Z}_8$, the distinct subgroups of $\mathbb{Z}_8$ will be generated by $m[1]$ where m is a divisor of 8. Thus $m = 1, 2, 4, 8$. Therefore the distinct subgroups of $\mathbb{Z}_8$ are:

$$\begin{aligned} \langle [1] \rangle &= \mathbb{Z}_8 & |\langle [1] \rangle| &= 8 \\ \langle [2] \rangle &= \{[0], [2], [4], [6]\} & |\langle [2] \rangle| &= 4 \\ \langle [4] \rangle &= \{[0], [4]\} & |\langle [4] \rangle| &= 2 \\ \langle [8] \rangle &= \{[0]\}\} & |\langle [8] \rangle| &= 1 \end{aligned}$$

11(a) Show that $(\mathbb{Z}_7^*, \times)$ is cyclic.

Proof.

$$\mathbb{Z}_7^* = \{[1], [2], [3], [4], [5], [6]\}$$

$$\begin{aligned} [3]^0 &= [1] & [3]^4 &= [4] \\ [3]^1 &= [3] & [3]^5 &= [5] \\ [3]^2 &= [2] & [3]^6 &= [1] \\ [3]^3 &= [6] \end{aligned}$$

All elements in $\mathbb{Z}_7^*$ can be written as a power of $[3]$, thus $\mathbb{Z}_7^* = \langle [3] \rangle$.

□

12(a) Find all generators of $\mathbb{Z}_7^*$.

Since $\mathbb{Z}_7^* = \langle [3] \rangle$, all other generators will be $[3]^m$ where m and 6 are relatively prime. Thus $m = 1, 5$. $[3]^5 = [5]$, so $[5]$ is also a generator. Thus $\mathbb{Z}_7^*$ has two generators, namely $[3]$ and $[5]$.

13(a) Find all subgroups of $\mathbb{Z}_7^*$.

Since $\mathbb{Z}_7^* = \langle[3]\rangle$, each subgroup will be generated by $[3]^m$ where m is a divisor of 6. Thus $m = 1, 2, 3, 6$. Since $[3]^1 = [3]$, $[3]^2 = [2]$, $[3]^3 = [6]$ and $[3]^6 = [1]$. Therefore the subgroups are as follows:

$$\langle[1]\rangle = \{[1]\}$$
$$\langle[2]\rangle = \{[1], [2], [4]\}$$
$$\langle[3]\rangle = \mathbb{Z}_7^*$$
$$\langle[6]\rangle = \{[1], [6]\}$$

14. Prove that the set $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{Z} \right\}$ is a cyclic subgroup of $GL_2(\mathbb{R})$.

Proof. First let's prove that H is a subgroup of the invertible 2 by 2 real matrices.

Claim: $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ for all positive integers n.

Clearly the statement holds when $n = 1$. Assume $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$. Then we have the following.

$$\begin{aligned} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{k+1} &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

Thus by induction $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ for all positive integers n.

By definition $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Suppose $n > 0$, then we have the following.

$$\begin{aligned} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-n} &= \left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \right)^{-1} \\ &= \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}^{-1} \\ &= \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} \end{aligned}$$

Thus for all integers n, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

Now we will prove H is cyclic. Let $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k \in \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$, then $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \in H$.

Thus $\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle \subseteq H$.

Now we will show $H \subseteq \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$. Let $A \in H$. Then $A = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ for some $n \in \mathbb{Z}$. By above claim, $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \in \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$.

Thus $H = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$.

□

28. Let a and b be elments of a finite group G.

(b) Prove that a and bab^{-1} have the same order.

Proof. Let $a, b \in G$. To prove a and bab^{-1} have the same order, we need the following fact.

Claim: Let n be a natural numbers, then $(bab^{-1})^n = ba^nb^{-1}$.
We will prove this by induction on n. Clearly $(bab^{-1})^1 = ba^1b^{-1}$.
Assume $(bab^{-1})^k = ba^kb^{-1}$. Then we have the following.

$$(bab^{-1})^{k+1} = (bab^{-1})^k(bab^{-1}) = ba^kb^{-1}bab^{-1} = ba^kab^{-1} = ba^{k+1}b^{-1}$$

Thus by induction, $(bab^{-1})^n = ba^nb^{-1}$.

Assume $|a| = r$ and $|bab^{-1}| = s$. So $a^r = e$ and $(bab^{-1})^s = e$. Thus we have the following.

$$\begin{aligned} a^r &= e \\ ba^rb^{-1} &= beb^{-1} \\ ba^rb^{-1} &= e \\ (bab^{-1})^r &= e \end{aligned}$$

So since $|bab^{-1}| = s$ the above implies $s|r$. Moreover we have the following.

$$\begin{aligned} (bab^{-1})^s &= e \\ ba^sb^{-1} &= e \\ b^{-1}ba^sb^{-1}b &= b^{-1}eb \\ a^s &= e \end{aligned}$$

So since $|a| = r$ the above implies $r|s$.
Therefore we have that $r = s$. In other words, $|a| = |bab^{-1}|$. □

(c) Prove that ab and ba have the same order.

Proof. Assume $|ab| = m$ and $|ba| = n$, then $(ab)^m = e$ and $(ba)^n = e$. Therefore we have the following.

$$\begin{aligned} (ab)^m &= e \\ a(ba)^{m-1}b &= e \\ a^{-1}a(ba)^{m-1}b &= a^{-1}e \\ (ba)^{m-1}b &= a^{-1} \\ (ba)^{m-1}ba &= a^{-1}a \\ (ba)^m &= e \end{aligned}$$

Since $|ba| = n$, the above gives us that $n|m$. Similarly to above, you can show that $(ba)^n = e$ implies $(ab)^n = e$, and since $|a| = m$, we can conclude $m|n$. Therefore $n = m$. In other words, $|ab| = |ba|$. □

33. If G is a cyclic group, prove that the equation $x^2 = e$ has at most two distinct solutions in G.

Proof. Clearly e is a solution to $x^2 = e$. If there are no other solutions then we are done.

Suppose $b, c \in G$ are solutions and are not equal to the identity. Since G is cyclic there exists $a \in G$ such that $G = \langle a \rangle$. Thus $b = a^k$ and $c = a^l$ for some $k, l \in \mathbb{Z}$. Now since they are both solutions we have that $(a^k)^2 = e$ and $(b^l)^2 = e$. Thus $|a^k| = 2 = |a^l|$ since $a^k \neq e$ and $a^l \neq e$. Note this also implies $|a| \leq 2k$, so G must be a finite cyclic group. Since the order of a^k is 2 it generates a subgroup of order 2. Similarly a^l generates a subgroup or order 2. Namely, $\langle a^k \rangle = \{e, a^k\}$ and $\langle a^l \rangle = \{e, a^l\}$. However, since G is cyclic there is only one subgroup of each order. Thus $\{e, a^k\}$ must equal $\{e, a^l\}$ and hence $a^k = a^l$. Thus there is at most one non-identity solution to $x^2 = e$. □

35. If G is a cyclic group of order p and p is prime, how many elements in G are generators of G?

Proof. Let a be a generator of G, so $|a| = p$. All other generators are of the form a^m where m and p are relatively prime. However, p is prime, thus all natural numbers less than p are relatively prime to p. So $m = 1, 2, 3, \ldots, p-1$. Thus all of the following are generators of G: $\boxed{a, a^2, a^3, \ldots, a^{p-1}}$.

□

38. Assume that $G = \langle a \rangle$ is a cyclic group of order n. Prove that if r divides n, then G has a subgroup of order r.

Proof. Let $|a| = n$ and assume $r|n$. Thus $a^n = e$ and $n = rq$ for some $q \in \mathbb{Z}$. We claim that $\langle a^q \rangle$ is a subgroup or order r. By the formula we proved in class, $|a^q| = \dfrac{n}{(n, q)}$. However, since $q|n$ then $(n, q) = q$. Thus $|a^q| = \dfrac{n}{q} = r$. Thus since $|a^q| = r$, then $\langle a^q \rangle$ has order r. □

#1 Let G be a group of prime order. Show that G is cyclic.

Let g be any element other than the identity in G. We will show that $\langle g \rangle = G$. By Lagrange's theorem, any subgroup of G has order dividing p, so has order either 1, or p. The subgroup $\langle g \rangle$ contains at least two elements, namely e and g (which are distinct because $g \neq e$). Thus, $|\langle g \rangle| = p$. Thus, this subgroup is the whole group.

#2 Show that in an abelian group every subgroup is normal.

Let G be an abelian group, and N a subgroup. Let $g \in G$. Then

$$gNg^{-1} = \{gng^{-1} : n \in N\} = \{gg^{-1}n : n \in N\} = \{n : n \in N\} = N$$

Thus, N is normal.

#3 Show that any abelian group of order 21 is cyclic.

By Cauchy's theorem, there are elements x, y of orders 3 and 7, respectively. We claim that xy is of order 21. First, of course, we can note that $\langle x\rangle \cap \langle y\rangle = \{e\}$, since (by Lagrange) the order of the intersection must divide both $|\langle x\rangle = 3$ and $|\langle y\rangle = 7$, so must be 1. By Lagrange's theorem, the order of xy is in the list $1, 3, 7, 21$. If $xy = e$, then $x = y^{-1}$, and the latter element lies in $\langle x\rangle \cap \langle y\rangle = \{e\}$. This would imply that $x = y^{-1} = e$, which is not the case, so the order of xy is not 1. Suppose that $(xy)^3 = e$. Since the group is abelian, this would imply that $x^3y^3 = e$, so $e = x^3 = y^{-3}$ since $x^3 = e$. But $y^7 = e$ by hypothesis, so that if also $y^{-3} = e$ then $y = y^7 \cdot (y^{-3})^2 = e$, contradiction. So the order of xy is not 3. Symmetrically, its order is not 7, so by default it is 21. That is xy generates the group, so the group is cyclic.

#1 Suppose that $G = \langle g\rangle$ is a cyclic group of order 144. What is the order of g^{60}?

The question is to find the smallest positive integer n so that $(g^{60})^n = e$. We have shown that $g^{60n} = e$ if and only if $60n = 0 \bmod |g|$. That is, we want the smallest positive solution of $60x = 0 \bmod 144$. That is, we want $144|60n$. The gcd of 144 and 60 is easily found (for example, by the Euclidean Algorithm) to be 12. Taking this common factor out, we are trying to solve $12|5n$. This requires that $12|n$. Thus, $n = 12$ is the smallest solution. That is, $g^{60} = 12$.

#2 Find all elements of order 10 in $\mathbf{Z}/100$ with addition.

The element $g = 1$ is a generator of $\mathbf{Z}/100$. The order of $n \cdot 1$ is (by definition) the smallest ℓ so that $\ell \cdot n = 0 \bmod 100$. That is, $\ell = 100/\gcd(n, 100)$. We want to find all n in the range $0, \ldots, 99$ so that $10 = \gcd(n, 100)$. In particular, 10 must divide n, but $n/10$ must have no factor of 2 or 5. Write $n = 10m$. Then $0 \le m < 9$. For $n/10$ to be coprime to 10 means that m is coprime to 10. Thus, m can be in the list $1, 3, 7, 9$ only. That is, $n = 10, 30, 70, 90$ are the integers mod 100 which have (additive) order exactly 10.

#1 Find the greatest common divisor of $x^2 + x + 1$ and $x^4 + x^3 + x + 1$ in $k[x]$ where $k = \mathbf{Z}/2$.

Use the Euclidean Algorithm for polynomials over a field: first, reduce $x^4 + x^3 + x + 1 \bmod x^2 + 1$ by dividing-with-remainder:

The Euclidean algorithm (with divisions done just below):

$$(x^4 + x^3 + x + 1) \quad - \quad (x^2 + 1)(x^2 + x + 1) \quad = \quad 0$$

Since we got a 0, the divisor itself is the gcd: it is $x^2 + x + 1$.

$$\begin{array}{r} x^2 + 0 + 1 \text{ R } 0 \\ x^2 + x + 1 \overline{)\, x^4 + x^2 + 0 + x + 1} \\ \underline{x^4 + x^3 + x^2} \\ x^2 + x + 1 \\ \underline{x^2 + x + 1} \\ 0 \end{array}$$

#2 Find the greatest common divisor of x^2+x+1 and x^4+x^3+x+1 in $k[x]$ where $k=\mathbf{Z}/3$.

Use the Euclidean Algorithm. Divisions are shown after.

$$\begin{array}{rcrcl} (x^4+x^3+x+1) & - & (x^2-1)(x^2+x+1) & = & 2x+2 \\ (x^2+x+1) & - & (2x)(2x+2) & = & 1 \end{array}$$

Since $1 \in k^\times$, the gcd is 1.

$$\begin{array}{rl} & x^2+0-1 \text{ R } 2x+2 \\ x^2+x+1 & \overline{\left| x^4+x^2+0+x+1 \right.} \\ & \underline{x^4+x^3+x^2} \\ & \quad -x^2+x+1 \\ & \quad \underline{-x^2-x-1} \\ & \qquad 2x+2 \end{array}$$

$$\begin{array}{rl} & 2x+0 \text{ R } 1 \\ 2x+2 & \overline{\left| x^2+x+1 \right.} \\ & \underline{x^2+x} \\ & \qquad 1 \end{array}$$

#1 The polynomial x^5+x^3+2x+2 in $\mathbf{Z}/3[x]$ has a repeated factor. Find it.

The derivative is $5x^4+3x^2+2 = 2x^4+2$. We could replace this by the *monic* version of the polynomial, which would make life a little simpler, but we won't here, just to show that it's not necessary. Note that $2^{-1}=2 \bmod 3$. The polynomial does not fall into the special case, so we should use the Euclidean Algorithm to compute the gcd of it and its derivative: (without showing all the long divisions...)

$$\begin{array}{rcrcl} (x^5+x^3+2x+2) & - & (2x)(2x^4+2) & = & x^3+x+2 \\ (2x^4+2) & - & (2x)(x^3+x+2) & = & x^2+2x+2 \\ (x^3+x+2) & - & (x+1)(x^2+x+2)=0 & & \end{array}$$

Thus, the gcd is x^2+2x+2. We test the latter for irreducibility by testing for roots to the equation $x^2+2x+2=0$ in $\mathbf{Z}/3$, since if it factored it would have to have a linear factor (being just quadratic). But $0^2+2\cdot 0+2=2\neq 0$, $1^2+2\cdot 1+2=2\neq 0$, $2^2+2\cdot 2+2=8=2\neq 0$, so there are no roots, and no linear factors. Thus, by the theorem, $(x^2+2x+2)^2$ divides the original polynomial.

#2 Show that $f(x)=x^3$ is a homomorphism $\mathbf{Z}/7^\times \to \mathbf{Z}/7^\times$.

What must be checked is that $f(xy)=f(x)f(y)$. In the present example,

$$f(xy)=(xy)^3=x^3y^3 \qquad \text{(because } \mathbf{Z}/7^\times \text{ is abelian)}$$

$$=f(x)\cdot f(y)$$

Thus, this f is a homomorphism.

#2 Show that any group of order 35 is cyclic.

Assume that the group G of order 35 is not cyclic. Then there is no element of order 35. By Lagrange, the only possible orders of elements are 1,5,7. As discussed in class, each subgroup of order 5 contains $5-1$ elements of order 5, and two distinct subgroups of order 5 have no elements of order 5 in common (by Lagrange's theorem again), since 5 is prime. The same applies to subgroups and elements of order 7, since 7 is prime. Invoking Sylow's theorem, for some non-negative integers a, b the number of subgroups of order 5 is $5a+1$ and the number of subgroups of order 7 is $7b+1$. Then, counting the elements of G two ways,

$$35 = 1 + (5a+1)(5-1) + (7b+1)(7-1)$$

Simplifying, this is

$$24 = 20a + 42b$$

Since $42 > 24$, it must be that $b = 0$. But then $24 = 20a$ is impossible, since 20 doesn't divide 24. Thus, there must have been an element of order 35 in G, so G is cyclic.

#3 List the 8 abelian groups of order 900.

Invoke the Structure Theorem for finite abelian groups: find all tuples of integers $d_1, d_2, \ldots, d_n$ all bigger than 1, whose product is 900, and so that $d_i | d_{i+1}$ for all indices i. Invoking Sun Ze's theorem, it suffices to solve this problem for the maximal prime powers 2^2, 3^2, 5^2 occurring in 900, and then combine the results. Quite generally, for prime p there are exactly two abelian groups of order p^2: $\mathbf{Z}/p^2$ and $\mathbf{Z}/p \oplus \mathbf{Z}/p$, corresponding to the two sequences of elementary divisors (p^2) and (p, p). Thus, in the case at hand, there are two choices for the 2-part of the group, 2 choices for the 3-part, and 2 choices for the 5-part. Combining and listing these, we have $8 = 2^3$ abelian groups: $\mathbf{Z}/900$, $\mathbf{Z}/2 \oplus \mathbf{Z}/450$, $\mathbf{Z}/3 \oplus \mathbf{Z}/300$, $\mathbf{Z}/5 \oplus \mathbf{Z}/180$, $\mathbf{Z}/6 \oplus \mathbf{Z}/150$, $\mathbf{Z}/10 \oplus \mathbf{Z}/90$, $\mathbf{Z}/15 \oplus \mathbf{Z}/60$, $\mathbf{Z}/30 \oplus \mathbf{Z}/30$.

#1 Verify that $x^3 + x + 1$ is irreducible in $(\mathbf{Z}/2)[x]$.

Since $1^3 + 1 + 0 = 1 \neq 0$ and $0^3 + 0 + 1 = 1 \neq 0$, the equation $x^3 + x + 1 = 0$ has no roots in $\mathbf{Z}/2$. By the Division Algorithm, this means that $x^3 + x + 1$ is irreducible in $(\mathbf{Z}/2)[x]$.

#2 In the field $K = (\mathbf{Z}/2)[x]/(x^2 + x + 1)$ let α be the image of x, and compute in reduced form α^5.

Compute the reduction of x^5 modulo $x^2 + x + 1$ (by dividing)

$$(x^5) - (x^3 + x^2 + 1)(x^2 + x + 1) = x + 1$$

Therefore, $\alpha^5 = \alpha + 1$.

#3 In the field $K = (\mathbf{Z}/2)[x]/(x^3+x+1)$ let α be the image of x, and compute in reduced form $(1+\alpha+\alpha^2)^{-1}$.

Run the Euclidean Algorithm on x^3+x+1 and x^2+x+1:

$$\begin{array}{lll} (x^3+x+1) & -(x+1)(x^2+x+1) & = x \\ (x^2+x+1) & -(x+1)(x) & = 1 \end{array}$$

Then, going backwards:

$$\begin{aligned} 1 &= (x^2+x+1)-(x+1)(x) = (x^2+x+1)-(x+1)((x^3+x+1)-(x+1)(x^2+x+1)) \\ &= (x+1)(x^3+x+1)+((x+1)^2+1)(x^2+x+1) \\ &= (x+1)(x^3+x+1)+(x^2)(x^2+x+1) \end{aligned}$$

Thus, looking at this equation modulo x^3+x+1, we see that x^2 is the multiplicative inverse of x^2+x+1 modulo x^3+x+1. That is,

$$(\alpha^2+\alpha+1)^{-1} = \alpha^2$$

#3 Prove that there is no field with 35 elements.

Suppose k were a field with $p \cdot q$ elements with p, q distinct primes. By Cauchy's theorem applied to the group k-with-addition, there is an element x of (additive) order p, and an element y of (additive) order q. Certainly neither x nor y is 0, since the order of 0 is 1. Let $z = xy$. Then since neither x nor y is 0, and since k is a field, $z \neq 0$. As usual, for an ordinary integer n and $w \in k$, $n \cdot w$ is merely an abbreviation for adding together n copies of w. Then

$$p \cdot (xy) = (px) \cdot y = 0 \cdot y = 0$$

and also

$$q \cdot (xy) = x \cdot (qy) = x \cdot 0 = 0$$

Let s, t be integers so that $sp + tq = 1$. Then

$$xy = 1 \cdot (xy) = (sp+tq) \cdot (xy) = s(px)y + tx(qy) = 0 + 0 = 0$$

contradiction.

Note that what we've actually proven is that the number of elements in a finite field cannot be divisible by two distinct primes.

3.1 For each group in the following list, find the order of the group and the order of each element in the group. What relation do you see between the orders of the elements of a group and the order of the group? $\mathbb{Z}_{12}$, $U(10)$, $U(12)$, $U(2)$, D_4.

The relationship you are supposed to notice in this exercise is that the order of an element always seems to divide the order of the group. We will show later that this is always true (at this point we have just shown that it holds for cyclic groups). I'll leave listing all the element orders as an exercise!

4.7 Find an example of a noncyclic group, all of whose proper subgroups are cyclic.

The easiest example of this behavior is our group of order 4 which is not cyclic. That is, $G = \{e, a, b, c\}$ with multiplication table

$*_G$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(It is clear from the multiplication table that G itself is not cyclic).

The possible proper nonempty subsets which contain e (as any subgroup must) are:

(a) $\{e\}$,
(b) $\{e, a\}$,
(c) $\{e, b\}$,
(d) $\{e, c\}$,
(e) $\{e, a, b\}$,
(f) $\{e, a, c\}$, and
(g) $\{e, b, c\}$.

The first 4 are cyclic (because each of a, b, and c constitutes its own inverse). The remaining 3 are not subgroups because they are not closed under multiplication ($ab = c$, $ac = b$, and $bc = a$). Thus all nonempty proper subgroups are cyclic as required.

4.13 Suppose that $|a| = 24$. Find a generator for $\langle a^{21}\rangle \cap \langle a^{10}\rangle$. In general, what is a generator for the subgroup $\langle a^m\rangle \cap \langle a^n\rangle$?

We know that $\langle a^{21}\rangle \cap \langle a^{10}\rangle$ is a subgroup of $\langle a\rangle$ (the intersection of subgroups is a subgroup), so by theorem 4.3, $\langle a^{21}\rangle \cap \langle a^{10}\rangle$ is cyclic. By theorem 4.2, $\langle a^{21}\rangle = \langle a^3\rangle$ and $\langle a^{10}\rangle = \langle a^2\rangle$

and thus a^6 is clearly an element in the intersection. We claim that a^6 is a generator. The order of $\langle a^6\rangle$ is $|a^6| = 24/6 = 4$ (using theorem 4.2) and we note that $\langle a^{21}\rangle \cap \langle a^{10}\rangle$ must have order dividing $8 = 24/3 = |\langle a^{21}\rangle|$ and $12 = 24/2 = |\langle a^{10}\rangle|$ (by theorem 4.3 and because the intersection is also a subgroup of both $\langle a^{21}\rangle$ and $\langle a^{10}\rangle$). No integer larger than 4 can do this, and as $|a^6| = 4$, we conclude that a^6 is a generator.

In general, we might guess that a generator of

$$\langle a^m\rangle \cap \langle a^n\rangle$$

for $|a| = p$ is $a^{\text{lcm}((p,n),(p,m))}$. As above, we have that $\langle a^n\rangle = \langle a^{(p,n)}\rangle$, and $\langle a^m\rangle = \langle a^{(p,m)}\rangle$. Furthermore,

$$\gcd(\text{lcm}((p,n),(p,m))), p) = \text{lcm}((p,n),(p,m))$$

and hence

$$|\langle a^{\text{lcm}((p,n),(p,m))}\rangle| = p/(\gcd(\text{lcm}((p,n),(p,m))), p) = p/\text{lcm}((p,n),(p,m)),$$

again using theorem 4.2 (for the first equality). Finally, $p/\text{lcm}((p,n),(p,m))$ is the largest integer which divides both $p/(p,n)$ and $p/(p,m)$. We can thus conclude that $a^{\text{lcm}((p,n),(p,m))}$ is the generator of the intersection as surmised.

1. Let G and G' be two groups whose orders have no common factor. Prove that the only homomorphism $\phi : G \to G'$ is the trivial one $\phi(x) = 1$ for all x.

   Solution: Let $\phi : G \to G'$. We know that $|G| = |\ker(\phi)| \cdot |\mathrm{im}(\phi)|$, so in particular $|\mathrm{im}(\phi)|$ divides $|G|$. As $\mathrm{im}(\phi) \leq G'$, it is also the case that $|\mathrm{im}(\phi)|$ divides $|G'|$, so it must be that $|\mathrm{im}(\phi)| = 1$, i.e. $\phi(x) = 1$ for all x.

2. Give an example of a permutation of even order which is odd and an example of one which is even.

   Solution: (12) has order 2 and is odd; (12)(34) likewise has order 2, and is even.

4. Prove that a group of order 30 can have at most 7 subgroups of order 5.

   Solution: A group of order 5 is cyclic, generated by each of its non-identity elements. Therefore any two subgroups of order 5 must intersect trivially, since any non-identity element in the intersection would generate both of them. So if a group has n subgroups of order 5, it must have at least $4n + 1$ elements (as we must also consider the identity). Therefore a group of order 30 can have at most 7 subgroups of order 5.

5. Is the symmetric group S_3 a direct product of nontrivial groups?

   Solution: No. $|S_3| = 6$, so if S_3 were a direct product of nontrivial groups it would have to be a direct product of a group of order 2 and a group of order 3. The only groups of these orders are cyclic. But a direct product of cyclic groups is abelian (in fact, in this case, cyclic) and S_3 is not.

9. Prove that if $G/Z(G)$ is cyclic, then G is abelian.

   Solution: Suppose $G/Z(G)$ is cyclic, generated by the coset $xZ(G)$. Then every element of G can be written as $x^n z$ for some $n \in \mathbb{Z}$ and some $z \in Z(G)$. But two elements of this form commute, as powers of x commute with other powers of x, and elements of $Z(G)$ commute with everything. Therefore G is abelian.

27. Prove that $\mathrm{SL}_n(\mathbf{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbf{R})$.

    Solution: Let $G = \mathrm{GL}_n(\mathbf{R})$ and $N = \mathrm{SL}_n(\mathbf{R})$. The condition we need to check, that $gxg^{-1} \subseteq N$ for all $n \in N$ and all $g \in G$, translates into the condition that if P is any invertible matrix and $\det(A) = 1$, then PAP^{-1} has determinant 1. This follows immediately from the fact that

$$\det(PAP^{-1}) = \det(P)\det(A)\det(P^{-1} = \det(P)\det(A)\frac{1}{\det(P)} = \det(A)\ ,$$

    which you may remember from your linear algebra course as the proposition that similar matrices have the same determinant.

37. Let G be a group, with a subgroup $H \subseteq G$. Define $N(H) = \{g \in G \mid gHg^{-1} = H\}$.
    (b) Let $G = S_4$. Find $N(H)$ for the subgroup H generated by $(1, 2, 3)$ and $(1, 2)$.
    Answer: In this example, $N(H) = H$.

38. Find all normal subgroups of A_4.
    Answer: $\{(1)\}$, $N = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$, and A_4 are the normal subgroups of A_4.

21. Find all group homomorphisms from $\mathbf{Z}_4$ into $\mathbf{Z}_{10}$.

Solution: As noted in Example 3.7.7, any group homomorphism from $\mathbf{Z}_n$ into $\mathbf{Z}_k$ must have the form $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. Under any group homomorphism $\phi : \mathbf{Z}_4 \to \mathbf{Z}_{10}$, the order of $\phi([1]_4)$ must be a divisor of 4 and of 10, so the only possibilities are $o(\phi([1]_4) = 1$ or $o(\phi([1]_4) = 2$. Thus $\phi([1]_4) = [0]_{10}$, which defines the zero function, or else $\phi([1]_4) = [5]_{10}$, which leads to the formula $\phi([x]_4) = [5x]_{10}$, for all $[x]_4 \in \mathbf{Z}_4$.

22. (a) Find the formulas for all group homomorphisms from $\mathbf{Z}_{18}$ into $\mathbf{Z}_{30}$.

Solution: As noted in Example 3.7.7, any group homomorphism from $\mathbf{Z}_{18}$ into $\mathbf{Z}_{30}$ must have the form $\phi([x]_{18}) = [mx]_{30}$, for all $[x]_{18} \in \mathbf{Z}_{18}$. Since $\gcd(18, 30) = 6$, the possible orders of $[m]_{30} = \phi([1]_{18})$ are $1, 2, 3, 6$. The corresponding choices for $[m]_{30}$ are $[0]_{30}$ (order 1), $[15]_{30}$ (order 2), $[10]_{30}$ and $[20]_{30}$ (order 3), and $[5]_{30}$ and $[25]_{30}$ (order 6).

(b) Choose one of the nonzero formulas in part (a), and name it ϕ. Find $\phi(\mathbf{Z}_{18})$ and $\ker(\phi)$, and show how elements of $\phi(\mathbf{Z}_{18})$ correspond to equivalence classes of $\sim_\phi$.

Solution: For example, consider $\phi([x]_{18}) = [5x]_{30}$. The image of ϕ consists of the multiples of 5 in $\mathbf{Z}_{30}$, which are $0, 5, 10, 15, 20, 25$. We have $\ker(\phi) = \{0, 6, 12\}$, and using Proposition 3.7.9 to find the equivalence classes of $\sim_\phi$, we add 1, 2, 3, 4, and 5, respectively, to the kernel. We have the following correspondence:

$$\{[0]_{18}, [6]_{18}, [12]_{18}\} \longleftrightarrow \phi([0]_{18}) = [0]_{30}, \quad \{[3]_{18}, [9]_{18}, [15]_{18}\} \longleftrightarrow \phi([3]_{18}) = [15]_{30},$$
$$\{[1]_{18}, [7]_{18}, [13]_{18}\} \longleftrightarrow \phi([1]_{18}) = [5]_{30}, \quad \{[4]_{18}, [10]_{18}, [16]_{18}\} \longleftrightarrow \phi([4]_{18}) = [20]_{30},$$
$$\{[2]_{18}, [8]_{18}, [14]_{18}\} \longleftrightarrow \phi([2]_{18}) = [10]_{30}, \quad \{[5]_{18}, [11]_{18}, [17]_{18}\} \longleftrightarrow \phi([5]_{18}) = [25]_{30}.$$

1. Prove that there are no simple groups of order 56.

Solution First observe that $56 = 2^3 \cdot 7$. Suppose G is a group of order 56 and let n_2 and n_7 denote the number of Sylow 2 and 7 subgroups, respectively. By the Sylow Theorem we know

$$\begin{array}{llll} n_2 \equiv 1 \ mod \ 2 & \text{and} & n_2 | 7 & \Rightarrow \quad n_2 = 1 \text{ or } 7 \\ n_7 \equiv 1 \ mod \ 7 & \text{and} & n_7 | 8 & \Rightarrow n_7 = 1 \text{ or } 8 \end{array}$$

If $n_7 = 1$, then there is a unique Sylow 7 subgroup, which must therefore be normal proving G is not simple. So, suppose $n_7 = 8$. It follows that there are $n_7 \cdot 6 = 8 \cdot 6 = 48$ elements of order 7 (since the Sylow 7 subgroup has order 7, hence is cyclic generated by any nontrivial element). That leaves $56 - 48 = 8$ elements. Since all Sylow 2–subgroups must have order 8, and be contained in the complement of the set of elements of order 7, we see that there can be only one Sylow 2–subgroup, which is therefore normal. This shows that G is not simple, completing the proof.

17. For the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 6 & 9 & 2 & 4 & 8 & 1 & 3 \end{pmatrix}$, write σ as a product of disjoint cycles. What is the order of σ? Write σ as a product of transpositions. Is σ an even permutation? Compute σ^{-1}.

Solution: Starting with 1, we have $\sigma(1) = 7$, $\sigma^2(1) = \sigma(7) = 8$, and $\sigma^3(1) = \sigma(8) = 1$, so the first cycle is $(1,7,8)$. The smallest number not in this cycle is 2, and starting with 2 we get the cycle $(2,\sigma(2)) = (2,5)$. Continuing, we get $\sigma = (1,7,8)(2,5)(3,6,4,9)$. By Proposition 2.3.8, σ has order 12, since $\text{lcm}[3,2,4] = 12$.

To write σ as a product of transpositions, we can simply write $(1,7,8)(2,5)(3,6,4,9) = (1,7)(7,8)(2,5)(3,6)(6,4)(4,9)$. Since σ can be expressed as the product of 6 transpositions, it is an even permutation.

Finally, we have $\sigma^{-1} = (1,8,7)(2,5)(3,9,4,6)$. (Note that since the cycles are disjoint they commute with each other, and so here the order of the cycles is not important.)

18. For the permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 1 & 8 & 3 & 6 & 4 & 7 & 9 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 7 & 2 & 6 & 8 & 9 & 3 \end{pmatrix}$, write each of these permutations as a product of disjoint cycles: σ, τ, $\sigma\tau$, $\sigma\tau\sigma^{-1}$, σ^{-1}, τ^{-1}, $\tau\sigma$, $\tau\sigma\tau^{-1}$.

Solution: $\sigma = (1,2,5,3)(4,8,7)$; $\tau = (2,5)(3,4,7,8,9)$; $\sigma\tau = (1,2,3,8,9)$;
$\sigma\tau\sigma^{-1} = (1,8,4,7,9)(3,5)$; $\sigma^{-1} = (1,3,5,2)(4,7,8)$; $\tau^{-1} = (2,5)(3,9,8,7,4)$;
$\tau\sigma = (1,5,4,9,3)$; $\tau\sigma\tau^{-1} = (1,5,2,4)(7,9,8)$.

19. Let $\sigma = (2,4,9,7,)(6,4,2,5,9)(1,6)(3,8,6) \in S_9$. Write σ as a product of disjoint cycles. What is the order of σ? Compute σ^{-1}.

Solution: We have $\sigma = (1,9,6,3,8)(2,5,7)$, so it has order $15 = \text{lcm}[5,3]$, and $\sigma^{-1} = (1,8,3,6,9)(2,7,5)$.

20. Compute the order of $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 2 & 11 & 4 & 6 & 8 & 9 & 10 & 1 & 3 & 5 \end{pmatrix}$. For $\sigma = (3,8,7)$, compute the order of $\sigma\tau\sigma^{-1}$.

Solution: Since $\tau = (1,7,9)(3,11,5,6,8,10)$, it has order $6 = \text{lcm}[3,6]$. Then $\sigma\tau\sigma^{-1} = (3,8,7)(1,7,9)(3,11,5,6,8,10)(3,7,8) = (1,3,9)(8,11,5,6,7,10)$, so the cycle structure of $\sigma\tau\sigma^{-1}$ is the same as that of τ, and thus $\sigma\tau\sigma^{-1}$ has order 6.

22. Show that S_{10} has elements of order 10, 12, and 14, but not 11 or 13.

Solution: The element $(1,2)(3,4,5,6,7)$ has order 10, the element $(1,2,3)(4,5,6,7)$ has order 12, and $(1,2)(3,4,5,6,7,8,9)$ has order 14. On the other hand, since 11 and 13 are prime, any element of order 11 or 13 would have to be a cycle, and there are no cycles of that length in S_{10}.

25. Consider the following permutations in S_7.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 6 & 1 & 7 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 7 & 4 & 6 & 3 \end{pmatrix}$$

Compute the following products.

Answer: (a) $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 6 & 7 & 4 & 1 & 5 \end{pmatrix}$

Answer: (c) $\sigma\tau\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 7 & 6 & 4 & 5 \end{pmatrix}$

26. Using the permutations σ and τ from Problem 25, write each of the permutations $\sigma\tau$, $\tau\sigma$, $\tau^2\sigma$, σ^{-1}, $\sigma\tau\sigma^{-1}$, $\tau\sigma\tau^{-1}$ and $\tau^{-1}\sigma\tau$ as a product of disjoint cycles. Write σ and τ as products of transpositions.

Answers: $\sigma = (1,3,5,6) = (1,3)(3,5)(5,6)$ $\tau = (1,2)(3,5,4,7) = (1,2)(3,5)(5,4)(4,7)$

$\sigma\tau = (1,2,3,6)(4,7,5)$ $\sigma\tau\sigma^{-1} = (2,3)(4,7,5,6)$ $\tau^{-1}\sigma\tau = (2,7,3,6)$

28. Let $\sigma = (3,6,8)(1,9,4,3,2,7,6,8,5)(2,3,9,7) \in S_9$.

(b) Is σ an even permutation or an odd permutation? *Answer:* Odd

(c) What is the order of σ in S_9? *Answer:* 12

29. Let $\sigma = (2,3,9,6)(7,3,2,5,9)(1,7)(4,8,7) \in S_9$.

(b) Is σ an even permutation or an odd permutation? *Answer:* Even

(c) What is the order of σ in S_9? *Answer:* 15

2. (a) Let $\alpha = (1,3,5,7,9,8,6)(2,4,10)$. What is the smallest positive integer n such that $\alpha^n = \alpha^{-5}$?

   Solution. We need to find the smallest n such that $\alpha^{n+5} = \varepsilon$. Since $|\alpha| = \text{lcm}(7,3) = 21$, we see that $n = 16$.

   (b) Let $\beta = (1,3,5,7,9)(2,4,6)(8,10)$. If β^m is a 5-cycle, what can you say about m?

   Solution. Note that β^m is a 5-cycle if and only if $(2,4,6)^m = (8,10)^m = \varepsilon$ and $(1,3,5,7,9)^m$ is a five cycle. This happen if and only if m is a multiple of $6 = \text{lcm}(3,2)$ and m is not a multiple of 5. That is $m = 6k$ and k is not a multiple of 5.

3. In S_7 show that $x^2 = (1,2,3,4)$ has no solutions, but $x^3 = (1,2,3,4)$ has at least two.

   Solution. Note that $(x^2)^4 = \varepsilon$, the identity map. So, the order $|x| = 1, 2, 4$. Clearly, $|x| \neq 1, 2$, else $x^2 \neq (1,2,3,4)$. If $|x| = 4$, then x is a 4-cycle, or the product of a 4-cycle and a 2-cycle; in either case, $x^2 \neq (1,2,3,4)$.

   A shorter proof is to observe that $x^2 = (1,2,3,4) = (1,4)(1,3)(1,2)$ is an odd permutation. But x^2 must be an even permutation for any $x \in S_n$.

   Let $x \in \{(1,4,3,2), (1,4,3,2)(5,6,7), (1,4,3,2)(5,7,6)\}$. Then $x^3 = (1,2,3,4)$. In fact, these are all the solution because in the disjoint cycle decomposition of the solution x, $(1,4,3,2)$ is needed to produce the cycle $(1,2,3,4)$ in x^3. Clearly, either there is no other cycle in the decomposition of x, or there is a 3-cycle using the numbers $5,6,7$, which must be of the form $(5,6,7)$ or $(5,7,6)$.

4. Describe all elements of order 5 in A_6.

   Solution. Note that $\sigma \in A_6$ satisfies $|\sigma| = 5$ must be a 5-cycle $(i_1, \ldots, i_5)$, and that a 5-cycle is an even permutation lying in A_6.

   One may determine the numbers of such elements. There are 6 ways to choose 5 elements from $\{1, \ldots, 6\}$, and $5!/5 = 24$ ways to arrange the five elements in a cycle. Thus, there are $24 \cdot 6 = 144$ such permutations.

1.) Let $a = (12345)(13)$. Write a^{2013} as a product of disjoint cycles.

Solution: First, we write a itself as a product of disjoint cycles, and we see that $a = (145)(23)$. Thus $|a| = lcm(3,2) = 6$. We can compute that the largest multiple of 6 which is ≤ 2013 is 2010, that is, $2013 = 3 \mod 6$. This implies $a^{2013} = a^{2010}a^3 = a^3 = (145)^3(23)^3 = (23)$.

2.) How many elements of order 4 are there in A_6? Justify your answer.

Solution: The answer is 90. We know from homework 5 that any element of order 4 in S_6 is of the form σ, where σ is a 4-cycle, or $\sigma\tau$, where σ is a 4-cycle and τ is a transposition. Since we are only interested in elements of A_6, that is, even permutations, we exclude the 4 cycles since a cycle of even length is an odd permutation. Thus any element of order 4 in A_6 must be of the form $\sigma\tau$, where σ is a 4-cycle and τ is a transposition, and we have shown in homework 5 that there are 90 of them.

3.) In Z_{18}, find all: (1) generators, (2) elements of order 6. Justify your answer.

Solution: (1) Recall that $Z_{18} = \{0, 1, 2, \ldots, 17\}$ under addition modulo 18. The generators of Z_{18} will be those elements which are relatively prime to 18, so the set of generators is: $\{1, 5, 7, 11, 13, 17\}$.

(2) The order of an element $a \in Z_n$ is $|a| = n/gcd(a, n)$. If $a \in Z_{18}$ has order 6, then $|a| = 18/gcd(a, 18) = 6$, so $gcd(a, 18) = 3$. Thus the elements of order 6 are: $\{3, 15\}$.

4.) List all subgroups of $U(7)$. Justify your answer.

Solution: Recall that $U(7)$ is the set $\{1, 2, 3, 4, 5, 6\}$ under multiplication modulo 7. We compute the *cyclic* subgroups of $U(7)$ by computing the powers of each element:

$$\begin{aligned} <1> &= \{1\} \\ <2> &= \{2, 4, 1\} \\ <3> &= \{3, 2, 6, 4, 5, 1\} \\ <4> &= \{4, 2, 1\} \\ <5> &= \{5, 4, 6, 2, 3, 1\} \\ <6> &= \{6, 1\} \end{aligned}$$

Since $U(7)$ is *cyclic* (we see from above that both 3 and 5 are generators), we know that every subgroup is a cyclic subgroup. Thus we have found *all* subgroups of $U(7)$.

5.) Let G be a cyclic group of order 21 and a is a generator of G. What is the order of the subgroup $< a^{14} > \cap < a^{15} >$? Justify your answer.

Solution: The answer is 1. In the cyclic group generated by a, where $|a| = n$, we know that $< a^k > = < a^{gcd(k,n)} >$. Thus $< a^{14} > = < a^7 > = \{a^7, a^{14}, a^0 = e\}$. We also compute $< a^{15} > = < a^3 > = \{a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21} = e\}$. We see then that $< a^{14} > \cap < a^{15} > = \{e\}$, which has order 1.

Example 2.22 Prove that the set of all bijective functions from a non-empty set X onto itself is a group with respect to usual compositions of functions.

Solution Since for bijective, $f : X \to Y$, and bijective $g : X \to X$, $g \circ f$ is also bijective, the closure property follows. For bijective function $f : X \to Y$, $g : X \to X$, $h : X \to X$, it is easy to observe $h \circ (g \circ f) = (h \circ g) \circ f$ and hence associativity follows. The identity function $I_x : X \to X$ defined by $I_x(x) = x$ is a bijective function and $f \circ I_x = I_x \circ f = f$ and hence is the identity element. Further, since every bijective function f possesses an inverse function which is also bijective, the existence of inverse follows. Hence the result.

Remark: If X is a finite set having n elements, a bijective function from X onto X is called a permutation and the group of all bijections, i.e. permutations is called the *symmetric group of degree n*. Note the order of this group is $n!$.

Example 2.24 Show that the set $K_4 = \{e, a, b, c\}$ equipped with the binary operation $*$ given by

$$e * a = a * e = a,\ e * b = b * e = b,\ e * c = c * e = c,\ a * b = b * a = c,$$
$$b * c = c * b = a,\ c * a = a * c = b,\ a * a = b * b = c * c = e$$

is an Abelian group.

Solution First observe that the binary operation can be demonstrated by the following composition table:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Clearly, by definition of $*$, the set S possesses the closure property. Associativity follows trivially. The element e is clearly the identity element. The inverse of a is a, that of b is b, that of c is c and that of e is e. The commutivity of $*$ is obvious.

Subgroups of A_4

The alternating group A_4 is written in cycle notation as follows:

$$A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}.$$

We find its subgroups.

By Lagrange's Theorem, the proper subgroups of A_4 can only have orders 1, 2, 3, 4 or 6. Looking first for cyclic subgroups, we see that A_4 has one element of order 1 (e), three of order 2 (the pairs of disjoint transpositions), and eight of order 3. There are thus no cyclic subgroups of order 4 or 6. Indeed the only cyclic subgroups of A_4 are the following:

$$C_1 = \{e\},$$
$$C_2 \cong \{e, (12)(34)\} \cong \{e, (13)(24)\} \cong \{e, (14)(23)\},$$
$$C_3 \cong \{e, (123), (132)\} \cong \{e, (124), (142)\} \cong \{e, (134), (143)\} \cong \{e, (234), (243)\}.$$

We are left with the possibility of non-cyclic subgroups of orders 4 or 6, i.e. either the Klein 4-group V or the symmetric group S_3. V consists of the identity plus three elements of order 2. There are only three elements of order 2 in A_4 and indeed you can check by multiplying out that the identity together with the three pairs of disjoint 2-cycles forms a group:

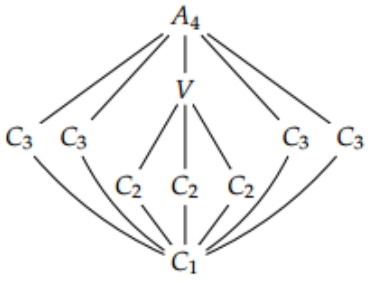
$$V \cong \{e, (12)(34), (13)(24), (14)(23)\}.$$

We are left with the possibility of non-cyclic subgroups of orders 4 or 6, i.e. either the Klein 4-group V or the symmetric group S_3. V consists of the identity plus three elements of order 2. There are only three elements of order 2 in A_4 and indeed you can check by multiplying out that the identity together with the three pairs of disjoint 2-cycles forms a group:

$$V \cong \{e, (12)(34), (13)(24), (14)(23)\}.$$

Now consider the possibility of S_3 being a subgroup of A_4. S_3 consists of the identity, three elements of order 2, and two elements of order 3. However, there are only three elements of order 2 in A_4, so if S_3 was a subgroup of A_4 then these elements must be in S_3. However this means that the subgroup V given above is in S_3; a contradiction of Lagrange, since $4 = |V|$ is not a divisor of $6 = |S_3|$.

The full subgroup diagram of A_4 is as follows:



In particular there is no subgroup of order 6, showing that the converse to Lagrange's Theorem is false:

$$6 \,\big|\, |A_4| \implies \exists H \leq A_4 \text{ with } |H| = 6$$

Examples

8. In $R = Z$, if $a = 9, b = -48$ then $d = 3$ is a gcd of a, b.

9. Let $R = \{a + b\sqrt{-5} \mid a, b \in Z\}$, $\alpha = 1 + 2\sqrt{-5}$, $\beta = 3$. Any common divisor of α and β must have a norm which divides $N(\alpha) = 21$ and $N(\beta) = 9$, i.e. it must have the norm 1 or 3. Since no element can have the norm 3, the gcd has the norm 1, i.e. it must be a unit. Since a unit always divides α and β, the gcd of α and β is a unit.

Definition 2.10.9. If $a, b \in R$, then a and b are said to be *relatively prime* if their gcd is a unit.

Example

10. Let $R = \{a + b\sqrt{-5} \mid a, b \in Z\}$. Then $\alpha = 2(1+\sqrt{-5})$ and $\beta = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ do not have a gcd for if d is a gcd of α and β, $N(d)$ divides $N(\alpha) = 24$ and $N(\beta) = 36$. Hence $N(d) = 1, 2, 3, 4, 6$ or 12. Now $d_1 = 1 + \sqrt{-5}$ is a common divisor of α and β, so that $N(d_1) = 6$ divides $N(d)$. Similarly $d_2 = 2$ is a common divisor of α and β so that $N(d_2) = 4$ divides $N(d)$. Hence $N(d) = 12$. But there is no element in R with norm 12, as the norm of every element is of the form $a^2 + 5b^2$. Hence α and β have no gcd in R.

Prove that in the ring $\mathbb{Z}[\sqrt{-5}]$ there's no gcd to 6 and $2 \cdot (1 + \sqrt{-5})$.

I'm assuming a greatest common divisor of a and b means something that divides both a and b, such that every divisor of a and b divides the gcd.

Use the norm function $N(r + s\sqrt{5}i) = r^2 + 5s^2$, and show that $N(ab) = N(a)N(b)$. This leads to the important fact that if c divides d in the ring, then $N(c)$ divides $N(d)$ as integers. This places restrictions on the possible norms of a gcd $r + s\sqrt{5}i$: you need $r^2 + 5s^2$ to divide $N(2(1 + \sqrt{5}i)) = 24$ and $N(6) = 36$. Thus $r^2 + 5s^2$ divides 12. Going through the possibilities, this can only happen if $(r, s) = (2, 0)$ or $(1, 1)$. So the only possibilities for the greatest common divisor are 2 and $1 + \sqrt{5}i$.

To see 2 can't be the gcd: Note that $6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$. So $1 + \sqrt{5}i$ divides both 6 and $2(1 + \sqrt{5}i)$. Thus it would have to divide the gcd. Since $1 + \sqrt{5}i$ has norm 6 and 2 has norm 4, 2 can't be the gcd: 6 does not divide 4.

To see $1 + \sqrt{5}i$ can't be the gcd: Since 2 divides 6 and $2(1 + \sqrt{5}i)$, 2 divides the gcd. If $1 + \sqrt{5}i$ were the gcd, then $N(2) = 4$ would have to divide $N(1 + \sqrt{5}i) = 6$, again a contradiction.

Thus we see both potential gcd's don't work: we conclude that 6 and $2(1 + \sqrt{5}i)$ have no gcd.

Let R be a finite integral domain, with $n = |R|$. Then R is a finite field, and therefore we must have $n = p^k$ for some prime number p and $k \geq 1$. Conversely, for any prime power p^k, there is an integral domain with that number of members, namely $\mathbb{F}_{p^k}$. Thus, there is an integral domain with n elements if and only if n is a power of a prime number.

Thus $\mathbb{F}_4$ is an integral domain with 4 elements, but there is no integral domain with 6 elements because 6 is not a prime power.

The proof that any finite integral domain R is in fact a finite field is quite simple. Given any $a \in R$, $a \neq 0$, let $f : R \to R$ be the map defined by $f(x) = ax$. Because R is an integral domain, this map must be injective. But because R is finite, an injective map from R to R must be a bijection. Thus, there is some $x \in R$ such that $f(x) = ax = 1$, and this x is a multiplicative inverse of a.

We can define $\mathbb{F}_{p^k}$ to be the ring $\mathbb{F}_p[x]/(f)$ for any irreducible $f \in \mathbb{F}_p[x]$ of degree k - no matter what such f we choose, the result is the same up to isomorphism. Note that $\mathbb{F}_p$ is just an alternate notation for $\mathbb{Z}/p\mathbb{Z}$, the integers modulo p. Thus, the multiplication in $\mathbb{F}_{p^k}$ is just multiplication of polynomials, taken modulo the polynomial f. For example, in $\mathbb{F}_4$, we take $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$, and letting $\overline{g}$ denote $g \in \mathbb{F}_2[x]$ taken modulo $x^2 + x + 1$, addition and multiplication look like

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

7. Find an example of a noncyclic group, all of whose proper subgroups are cyclic.

Solution: Let G be an abelian group of order 4, with elements $\{e, a, b, ab|\ \ |a| = |b| = 2\}$. Then the proper subgroups of G are: $H_1 = \{e, a\} =< a >$, $H_2 = \{e, b\} =< b >$, and $H_3 = \{e, ab\} =< ab >$. Note that, since the product of any two of a, b or ab is the third, that a subgroup with any two of a, b, and ab is equal to G. Thus, all the proper subgroups of G are cyclic. On the other hand, G is not cyclic, since we see that $< a >$, $< b >$, and $< ab >$ are all proper subgroups of G.□

18. If a cyclic group has an element of infinite order, how many elements of finite order does it have?

Solution Since $|e| = 1$, there is at least one element of G of finite order. Let $G =< a >$. Since G has an element of infinite order, a is of infinite order. Suppose a^j is an element of finite order, for some $j \neq 0$. Then $(a^j)^n = e$, and therefore, $a^{jn} = e$. By the Corollary to Theorem 4.1, the order of a divides jn. Thus $|a| = \ell$ for some $\ell < \infty$. But, if $|a| = \ell$, then $G =< a >= \{e, a, a^2, \ldots, a^{\ell-1}\}$ is a finite group. This contradicts our assumption that G has an element of infinite order. Therefore, a^j is of infinite order for every $j \neq 0$, and therefore e is the only element of G of finite order.□

10. Let $G = \langle a \rangle$ and let $|a| = 24$. List all generators for the subgroup of order 8.

Proof. The subgroup of order 8 is generated by a^3. The generators of $\langle a^3 \rangle$ are the powers of a^3 that are relatively prime to 8, namely $(a^3)^1 = a^3$, $(a^3)^3 = a^9$, $(a^3)^5 = a^{15}$ and $(a^3)^7 = a^{21}$. □

44. Suppose that G is a cyclic group and that 6 divides $|G|$. How many elements of order 6 does G have? If 8 divides $|G|$, how many elements of order 8 does G have? If b is one element of order 8, list the other elements of order 8.

Proof. Since G is cyclic and 6 divides $|G|$, G has $\phi(6) = 2$ elements of order 6. Similarly, G has $\phi(8) = 4$ elements of order 8. If b is an element of order 8, then the other elements of order 8 are b^3, b^5, b^7. (Notice how problem #10 is a special case of this one.) □

8. List the elements of the subgroup $< 8 >$ in the group $\mathbb{Z}_{20}$, of integers modulo 20 (under addition modulo 20).
$< 8 >= \{0, 1.8, 2.8, 3.8, 4.8\} = \{0, 8, 16, 4, 12\}$.

9. Let $G =< a >$ and let $|a| = 16$.

   (a) List all generators of G.
   Since the integers 1, 3, 5, 7, 9, 11, 13 and 15 are relatively prime to 16, the set of generators of G is $\{a, a^3, a^5, a^7, a^9, a^{11}, a^{13}, a^{15}\}$.

   (b) List all elements of the subgroup, of G, of order 4.
   The subgroup, of G, of order 4 is : $< a^{\frac{16}{4}} >=< a^4 > = \{(a^4)^1, (a^4)^2, (a^4)^3, (a^4)^4 = e\} = \{a^4, a^8, a^{12}, e\} =$.

   (c) List all generators of the subgroup, of G, of order 8.
   The subgroup, of G, of order 8 is : $< a^{\frac{16}{8}} >=< a^2 > = \{(a^2)^1, (a^2)^2, (a^2)^3, (a^2)^4, (a^2)^5, (a^2)^6, (a^2)^7, (a^2)^8 = e\}$. Since 1, 3, 5, and 7 are relatively prime to 8, the set of generators for this group is $\{(a^2)^1, (a^2)^3, (a^2)^5, (a^2)^7\} = \{a^2, a^6, a^{10}, a^{14}\}$.

10. List the elements of the subgroup $< 4 >$ in the group $\mathbb{Z}_{16}$, of integers modulo 16 (under addition modulo 16).
Note $4.4 = 16 \equiv_{16} 0$ and $|4| = 4$. Thus $< 4 >= \{0, 4, 8, 12\}$.

1. List the elements of the subgroups $< 6 >$ and $< 18 >$ in $\mathbb{Z}_{24}$.
$< 6 >= \{0, 6, 12, 18\}$ and note that 18 is also a generator of $< 6 >$, from this or otherwise, $< 18 >= \{0, 18, 12, 6\}$.

2. Let $G =< a >$ and let $|a| = 45$.

   (a) List all generators of G.
   By Theorem 4.2, the powers of a that are relatively prime to 45, a, a^2, a^4, $a^7, a^8, a^{11}, a^{13}, a^{14}, a^{16}, a^{17}, a^{19}, a^{22}, a^{23}, a^{26}, a^{28}, a^{29}, a^{31}$, $a^{32}, a^{34}, a^{37}, a^{38}, a^{41}, a^{43}$, and a^{44}, are the generators.

   (b) List all generators for the subgroup, of G, of order 9.
   The subgroup, of G, of order 9 is: $< a^{\frac{45}{9}} >=< a^3 >= \{e, (a^5)^1, (a^5)^2, (a^5)^3, (a^5)^4, (a^5)^5, (a^5)^6, (a^5)^7, (a^5)^8\}$. By Theorem 4.2, the elements of order 9 are the powers of a^5 that are relatively prime to 9: $(a^5)^1, (a^5)^2, (a^5)^4, (a^5)^5, (a^5)^7, (a^5)^8$. Thus the generators for the subgroup are $a^5, a^{10}, a^{20}, a^{25}, a^{35}$, and a^{40}.

   (c) Compute the orders of the elements a^8, a^{10}, and a^{15}.
   Since $\gcd(8, 45) = 1$, the element a^8 is a generators of G (Theorem 4.2). Thus $|a^8| = |a| = |G| = 45$. Also, since $15|45$, $|a^{15}| = \frac{45}{15} = 3$. Apply the formula $|a^k| = \frac{|a|}{\gcd(k,|a|)}$ to compute the orders of a^{10}. Thus $|a^{10}| = \frac{45}{\gcd(10,45)} = \frac{45}{5} = 9$.

4. Suppose that a cyclic group has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 5. What is $|G|$?
Since $|\{e\}| = 1$, and the order of a sugroup of G divides the order of G, we need to find a positive integer $|G|$ such that $1||G|, 5||G|$, and $|G||G|$, and no other positive integer divides $|G|$. $5||G| \implies |G| = 5k$, for some $k \in \mathbb{Z}^+$. We must have k=5 because otherwise $|G|$ will have positive divisor d other than 1, 5 and $|G|$ and G does not have a subgroup of order d. Hence $|G| = 25$.

6. Suppose that G is a cyclic group and that 10 divides $|G|$. How many elements of order 10 does G have? If 7 divides $|G|$, how many elements of order 7 does G have? If a is one element of order 10, list the other elements of order 10.
7 divide $|G| \implies$ G has $\phi(7) = 6$ elements of order 7 and 10 divide $|G| \implies$ G has $\phi(10) = 4$ elements of order 10 (since If d is a positive divisor of $|G|$, then G has $\phi(d)$ elements of order d). Since $10||G|$, the elements of order 10 are the generators of the subgroup, of G order 10. This subgroup of order 10 can be written as $< a >$ (given). The elements of order 10 of $< a >$ are a^k, $1 \leq k < 10$ and $\gcd(10, k) = 1$. Thus a, a^3, a^7 and a^9 are all elements of order 10 in G.

Question:

b.) Show by example that the product of elements of finite order in a nonabelian group need not have finite order.

Answer:

b.) Let $G = GL_2(\mathbb{R})$ and let $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$. Both $A^2 = B^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$; so both elements have order 2. $AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $(AB)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$, which means that for all $n \geq 1$ $(AB)^n \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, so that the order of AB is infinite.

Question:

14. Let G be a cyclic group order of n, and let r be an integer dividing n. Prove that G contains exactly one subgroup of order r.

Answer:

If G is a cyclic group of order n, then $G = \{1, g, g^2, \ldots g^{n-1}\}$. If r divides n, there exists an integer p such that $n = rp$. The subgroup $H = \{g^p, g^{2p}, \ldots, g^{(r-1)p}, g^{rp} = g^n = 1\}$ generated by g is a subgroup of order r. Moreover, since G is cyclic all its subgroups are cyclic. Thus, if there is another subgroup H' of G which is cyclic then H' is generated by an element of G of order r. Let $H' = \langle g^k \rangle$, then $(g^k)^r = 1$ and $kr = np$ for some integer p. But then $k = \left(\frac{n}{r}\right)s = ps$, and $g^k = (g^p)^s \in \langle g^p \rangle$ which means $H' \subseteq H$. But this implies that $|H'| = r = |H|$, hence $H' = H$.

Question:

20. a.) Let a, b be elements of an abelian group of orders m, n respectively. What can you say about the order of their product ab?

Answer:

a.) If G is abelian then $(ab)^m = a^m b^m$. If $|a| = s$ and $|b| = t$ and ℓ = least common multiple of s and t then $\ell = sp = tq$. But $(ab)^\ell = a^\ell b^\ell = a^{sp} b^{tq} = (a^s)^p (b^t)^q = 1.1 = 1$. So we can only conclude that the order of ab divides ℓ. For example, if $|a| = m$ then $|a^{-1}| = m$ (prove it!) and $\ell = m$. But $|a\,a^{-1}| \neq m$, since $|a\,a^{-1}| = 1$.

Question:

12. Let G be a group, and let $\varphi: G \to G$ be the map $\varphi(x) = x^{-1}$.

a.) Prove that φ is bijective.

Answer:

a.) $\varphi: G \to G$, $\varphi(x) = x^{-1}$

φ is a surjective map for if $x \in G$, then $\varphi(x^{-1}) = (x^{-1})^{-1} = x$.

Let $x, y \in G$ and $\varphi(x) = \varphi(y)$. This means that

$x^{-1} = y^{-1} \Rightarrow yx^{-1} = yy^{-1} = 1 \Rightarrow yx^{-1}x = x \Rightarrow y = x$.

Thus φ is objective.

Question:

b) Prove that φ is an automorphism if and only if G is abelian.

Answer:

b) $G \to G$ is an automorphism if and only if φ is an homomorphism and φ is a bijection. By (a) we showed that φ is a bijection. Assume that G is abelian. Then $\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y)$ and φ is an homomorphism.

Let G be a non abelian group then $y^{-1}x^{-1}$ is not necessarily equal to $x^{-1}y^{-1}$ and φ is not necessarily an homomorphism. For example if $G = S_3$

$\varphi((12)(23)) = \varphi((123)) = (123)^{-1} = (132)$ but

$\varphi((12)) \cdot \varphi((23)) = (12)^{-1}(23)^{-1} = (12)(123) = (123)$.

1. Let G be a group of order pq where p and q are prime numbers.

(i) Let H be a proper subgroup of G. What are the possible values of $|H|$?

Solution. By a theorem of Lagrange, $|H|$ must divide $|G|$. Since the only divisors of $|G|$ are 1, p, q and $pq = |G|$, and the order of a proper subgroup of a finite group is strictly smaller than the order of the group, we conclude that $|H| \in \{1, p, q\}$.

(ii) Show that every proper subgroup of G is cyclic.

Solution. If $|H| = 1$ then H consists of the identity element only and is cyclic. Otherwise, by (i), $|H|$ is a prime number say p. Let h be an element of H different from the identity element which exists since we assume that $|H| > 1$. Since H is a group, $\langle h \rangle$ is a subgroup of H. Again, by a theorem of Lagrange, $|\langle h \rangle| > 1$ is a divisor of $|H| = p$ and therefore equals p, p being prime. Thus, $|H| = |\langle h \rangle|$ and so $H = \langle h \rangle$ and therefore H is cyclic.

If G is non-abelian group of order 6, it is isomorphic to S_3

Note that G has an element a of order 3 hence at least two as a^2 has order 3, but can't have an element of order 6 or it would be cyclic and hence abelian.

Suppose the elements of order 2 are b, c, d, then the elements of the group are $1, a, a^2, b, c, d$. No element of order 3 can commute with any element of order 2 else the product would have order 6

Now $ab \neq ba$ implies both $aba^{-1} \neq a$ and $bab^{-1} \neq b$ - so neither the elements of order 3 nor those of order 2 can have a trivial action.

4. Let $A = \{e, a, b, c\}$ be a set of cardinality 4.

(i) Complete the following table

$*$	e	a	b	c
e	e	a	b	c
a	a			
b	b		e	
c	c			

to a multiplication table of a group of order 4 in at least two different ways. Is any of these groups abelian?

Solution. The crucial point in this argument is that left and right multiplication maps $\lambda_x : g \mapsto xg$ and $\rho_x : g \mapsto gx$ are permutations. In particular, if our table defines a group structure on the set, every element has to appear in every row and every column exactly once.

Since a appears already in the 1st row of the 2rd column of our table, it cannot appear anywehere else in that column, in particlar in the row containing b. Since e already appears in that row, the only possibility left for $b*a$ is c. Then we will have only one possible choice for $b * c$, namely a. A similar argument shows that $a * b = c$ and $c * b = a$. Thus, we obtain the following table

$*$	e	a	b	c
e	e	a	b	c
a	a		c	
b	b	c	e	a
c	c		a	

Now we have two possible choices for $a * a$: $a * a = b$ or $a * a = e$.

Suppose first that $a * a = b$. Then using the same argument as before (every line and every column must contain each element of the group exactly once) we obtain

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Then $\langle A, * \rangle$ is isomorphic to $\langle \mathbb{Z}_4, +_4 \rangle$. Indeed, define $\psi : A \to \mathbb{Z}_4$ as $\psi(e) = 0$, $\psi(a) = 1$, $\psi(b) = 2$ and $\psi(c) = 3$. Then it is easy to see that $\psi(x * y) = \psi(x) +_4 \psi(y)$ for all $x, y \in A$. Since ψ is obviously bijective, it is an isomorphism of binary structures, which in particular implies that $\langle A, * \rangle$ is a group.

Suppose that $a*a=e$. Then the permutation argument yields the following table

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This table has the property that for all $x \in A$, $x*x=e$. One of the ways of showing that this table is a multiplication table of a group is to observe that the map $\phi : A \to \mathbb{Z}_2 \times \mathbb{Z}_2$ defined by $\phi(e)=(0,0)$, $\phi(a)=(1,0)$, $\phi(b)=(1,1)$ and $\phi(c)=(0,1)$ is bijective and satisfies $\phi(x*y)=\phi(x)+\phi(y)$. Thus, ϕ is an isomorphism of binary structures and therefore $\langle A, * \rangle$ is a group.

Both tables are symmetric with respect to the main diagonal and so both operations are commutative, that is the corresponding groups are abelian.

(ii) Is there another way of making the above table into a multiplication table of a group? Why?

Solution. There is no other way since any other completion would require putting an element twice in the same row or in the same column and thus the result cannot be a multiplication table of a group.

This agrees with the already established fact that there are only 2 non-isomorphic groups of order 4.

11. Prove that a group of order 4 is cyclic or isomorphic to the Klein four group.

Proof. Let G be a group of order 4, say $G=\{e,x,y,z\}$. The order of each element must divide 4, so the order of each element is 1,2 or 4.

Since $x,y,z \neq e$, then $|x|,|y|,|z| \neq 1$. If there exists an element of order 4, then G is cyclic.

Suppose there does not exist an element of order 4. Then $|x|=|y|=|z|=2$. With this information we can see that the Cayley table for G must be the one given below. And this table is equivalent to the Cayley Table for the Klein four group under the mapping $e \mapsto e$, $x \mapsto a$, $y \mapsto b$, $z \mapsto c$.

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

22. Let G be a group of order pq where p and q are distinct primes. Prove that any non-trivial subgroup of G is cyclic.

Proof. Let H be a non-trivial subgroup of G. Thus $H \neq \{e\}$ and $H \neq G$.

The order of H must divide the order of G. Since the order of G is pq where p and q are prime, the only divisors are $1, p, q$ or pq. Thus $|H| = 1, p, q$ or pq. Since $H \neq \{e\}$, $|H| \neq 1$ and since $H \neq G$, $|H| \neq pq$. Thus $|H|$ is p or q, hence the order of H is prime. We proved in class a group of prime order is cyclic. Thus H is cyclic. □

1. (10 POINTS) Let $f(x) = x^4 + rx^3 + 5x^2 + 1 \in \mathbf{Z}[x]$. For which integers r is $f(x)$ irreducible? Prove your answer.

SOLUTION: If a is a zero of $f(x)$, then $x - a$ is a factor of $f(x)$, $f(a) = 0$ and a must be ± 1 since the constant term in $f(x)$ is one. Since $f(1) = 7 + r$, and $f(-1) = 7 - r$, $f(x)$ has zero if $r = \pm 7$.

Now suppose that $f(x)$ has two quadratic factors

$$\begin{aligned} f(x) &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd. \end{aligned}$$

Since $bd = 1$, $b = d = \pm 1$, and the coefficient of x is $\pm(a + c) = 0$. This means that $r = 0$ and the coefficient of x^2 is $-a^2 \pm 2 = 5$, or $a^2 = -5 \pm 2 < 0$, but there is no integer a that satisfies this condition.

Therefore, $f(x)$ is irreducible unless $r = \pm 7$.

A common mistake was to say that $f(x)$ is reducible if $r = 0$, but this is not the case, as explained above.

THEOREM. *Suppose p and q are primes with $q < p$ and q does not divide $p - 1$. Then any group G of order pq is cyclic.*

Proof. Assume the statement is false. By Lagrange's Theorem we may assume that every nonidentity element of G has order p or q. Let $a \neq e$ belong to G. If $|C(a)| = pq$, then for any $b \notin \langle a \rangle$ we have $|b| \neq |a|$, for otherwise $|\langle a, b \rangle| = p^2$ or q^2. But $|b| \neq |a|$ and $b \in C(a)$ implies $|ab| = pq$. So, we may assume that for all nonidentity elements a in G, $|C(a)| = p$ or q.

We now count the elements of order p and q. Since $|a| = p$ implies $|\mathrm{cl}(a)| = |G|/|C(a)| = q$, the number of elements of order p is a multiple of q. Moreover, because $|a| = p$ implies $|a^i| = p$ for $i = 2, \ldots, p - 1$, the number of elements of order p is also a multiple of $p - 1$. Since $\gcd(q, p - 1) = 1$, the number of elements of order p is a multiple of $q(p - 1)$. Analogously, the number of elements of order q is a multiple of $p(q - 1)$. Since neither $q(p - 1)$ nor $p(q - 1)$ divides $pq - 1$, not all the nonidentity elements of G can have the same order. Thus, there must be at least $q(p - 1) + p(q - 1) > pq$ elements in G. This contradiction finishes the proof.

Example of infinite groups such that all its elements are of finite order

Here is one. Let $(\mathbb{Q}, +)$ denote the groups of rational numbers under addition, and consider it's subgroup $(\mathbb{Z}, +)$ of integers. Then any element from the group $\mathbb{Q}/\mathbb{Z}$ has elements of the form $\frac{p}{q} + \mathbb{Z}$ which is of order at-most q. Hence it's of finite order.

- Group of all roots of unity in $\mathbb{C}^{\times}$.

Problem 3: *Show by an example that we can have a homomorphism $f : R \to R'$, such that $f(1)$ is not unity of R', where 1 is unity of R.*

Solution: Consider the map $f : \mathbf{Z} \to \mathbf{Z}$, s.t.,

$$f(x) = 0 \quad \text{for all } x \in \mathbf{Z}$$

where $\mathbf{Z}$ = ring of integers

then f is a homomorphism (verify)

Again $f(1) = 0$, but 0 is not unity of $\mathbf{Z}$.

Thus although $\mathbf{Z}$ (on R.H.S.) has unity it does not equal $f(1)$.

Remarks: (*i*) If we take the map $f : \mathbf{Z} \to \mathbf{E}$, where $\mathbf{E}$ = ring of even integers, defined by $f(x) = 0$ for all x, we find, $\mathbf{E}$ does not have unity, whereas 1 is unity of $\mathbf{Z}$.

(*ii*) We recall (see page 116) that the map $f : \mathbf{Z} \to \mathbf{E}$, s.t., $f(x) = 2x$ is a group isomorphism. Thus $\mathbf{Z}$ and $\mathbf{E}$ are isomorphic as groups whereas $\mathbf{Z}$ and $\mathbf{E}$ are not isomorphic as rings. Indeed, $\mathbf{Z}$ has unity but $\mathbf{E}$ does not possess unity. In fact, f will not be a ring homomorphism.

Problem 4: *Find all the ring homomorphisms from $\mathbf{Z}_{20} \to \mathbf{Z}_{30}$.*

Solution: Let $f : \mathbf{Z}_{20} \to \mathbf{Z}_{30}$ be any ring homomorphism.

Let $f(1) = a$, then $f(x) = xa$ and as done in Problem 24 under groups on page 120 we find $o(a) | o(\mathbf{Z}_{30}) = 30$ and $o(a) \mid 20 = o(\mathbf{Z}_{20})$

Thus possible values of $o(a)$ are 1, 2, 5, 10 and so possible values of a will be

$$0, 3, 6, 9, 12, 15, 18, 21, 24, 27$$

which give us the ten group homomorphisms.

Since f is a ring homomorphism and in $\mathbf{Z}_{20}$, $1.1 = 1$, we find $f(1.1) = f(1)$

or $\quad f(1)(1) = f(1)$

or $\quad a^2 = a$ in $\mathbf{Z}_{30}$

This is satisfied by 0, 6, 15, 21 values of a .

Hence there exist four ring homomorphisms from $\mathbf{Z}_{20} \to \mathbf{Z}_{30}$.

Problem 6: *Let* $\mathbf{Z}$ *be the ring of integers. Show that the only homomorphisms from* $\mathbf{Z} \to \mathbf{Z}$ *are the identity and zero mappings.*

Solution: Let $f : \mathbf{Z} \to \mathbf{Z}$ be a homomorphism

Since $(f(1))^2 = f(1) f(1) = f(1.1) = f(1)$

$f(1)[f(1) - 1] = 0$

$\Rightarrow f(1) = 0$ or $f(1) = 1$

If $f(1) = 0$ then $f(x) = 0 \ \forall$ integers x

as $f(x) = f(1 \cdot x) = f(1) f(x) = 0 \cdot f(x) = 0 \ \forall \ x$

Thus in this case f is the zero homomorphism.

If $f(1) = 1$, then for any $x \in \mathbf{Z}$

$f(x) = f(1 + 1 + ...+ 1) = x f(1) = x \qquad (x > 0)$

$f(x) = f(-y) = -f(y) = -[f(1 + 1 + ...+ 1)] = -y f(1) = x f(1) = x$

$(x < 0, \ y = -x)$

$f(0) = 0$

So in this case f is identity map, which proves the result.

Problem 1: *If* R *is a ring with unity and* $f : R \to R'$ *is a homomorphism where* R' *is an integral domain such that Ker* $f \neq R$ *then show that* $f(1)$ *is unity of* R'.

Solution: Let $a' \in R'$ be any element. We show

$f(1) \ a' = a' f(1) = a'$

Now $f(1) \ a' - f(1) \ a' = 0'$

$\Rightarrow f(1.1) \ a' - f(1) \ a' = 0'$

$\Rightarrow f(1) \ f(1) \ a' - f(1) \ a' = 0'$

$\Rightarrow f(1) \ [f(1) \ a' - a'] = 0'$

$\Rightarrow$ either $f(1) = 0'$ or $f(1) \ a' - a' = 0'$ as R' is an integral domain.

$f(1) = 0' \Rightarrow 1 \in \text{Ker } f \Rightarrow \text{Ker } f = R$ which is not true.

Hence $f(1) a' - a' = 0'$

$\Rightarrow \quad f(1) \ a' = a'$

Similarly, we can show $a' = a' f(1)$.

Problem 2: *Let* $f : R \to R'$ *be an onto homomorphism, where* R *is a ring with unity. Show that* $f(1)$ *is unity of* R'.

Solution: Let $a' \in R'$ be any element.

Since f is onto, $\exists \ a \in R$, s.t., $f(a) = a'$

Now $a' . f(1) = f(a) \ . f(1) = f(a \ . \ 1) = f(a) = a'$

Similarly $f(1) \ . \ a' = a'$.

Showing, thereby that $f(1)$ is unity of R'.

Problem 5: *Show that $2\mathbf{Z}$ is not isomorphic to $3\mathbf{Z}$ as rings. What can be said about isomorphism between $m\mathbf{Z}$ and $n\mathbf{Z}$, where m, n are positive integers?*

Solution: Suppose $2\mathbf{Z} \cong 3\mathbf{Z}$ and let $f: 2\mathbf{Z} \to 3\mathbf{Z}$ be the isomorphism.

As $\quad 2 \in 2\mathbf{Z}, f(2) = 3n$ for some $n \in \mathbf{Z}$

Now $\quad f(4) = f(2 + 2) = f(2) + f(2) = 6n$

$\quad f(4) = f(2 \cdot 2) = f(2) \cdot f(2) = (3n)^2$

Thus $\quad 6n = 3n^2$ or that $2 = 3n$

But this is not possible for any $n \in \mathbf{Z}$

Hence f is not an isomorphism.

Suppose now $f: m\mathbf{Z} \to n\mathbf{Z}$ is any ring isomorphism

Then $\quad f(\underbrace{m + m + \cdots + m}_{m \text{ times}}) = f(m) + f(m) + \cdots + f(m)$

$\qquad = mf(m)$

$\Rightarrow f(mm) = mf(m)$

$\Rightarrow f(m) f(m) = mf(m) \Rightarrow f(m) = m \qquad (1)$

Again as f is onto and $n \in n\mathbf{Z}$, $\exists\, mr \in m\mathbf{Z}$

s.t., $\quad f(mr) = n \quad$ or $\quad rf(m) = n$

$\Rightarrow f(m) \mid n$

Again as $\quad m \in m\mathbf{Z}, f(m) \in n\mathbf{Z}$

$\Rightarrow f(m) = nk$ for same k

$\Rightarrow n \mid f(m)$

and hence $\quad f(m) = n$

or that $\quad m = n \quad$ from (1)

So if $m\mathbf{Z} \cong n\mathbf{Z}$, then $m = n$. The converse, of course, is obviously true.

Hence we conclude: $m\mathbf{Z} \cong n\mathbf{Z}$ as rings if and only if $m = n$.