SOLUTIONS TO ARTIN'S *ALGEBRA*, 2ND ED. CH. 2 – GROUPS

COLIN COMMANS

Contents

§1 - Laws of Composition

1.1

Let S be a set. Prove that the law of composition defined by $ab = a$ for all a and b in S is associative. For which sets does this have an identity?

Solution.

Proof.
Let a, b, c be elements of S. Then

$$(ab)c = ac = a \quad \text{and} \quad a(bc) = ab = a$$

Thus $(ab)c = a(bc)$ and the law of composition is associative. □

We claim this has an identity if and only if S has one element.

Proof.
$\Longleftarrow$: Suppose S has one element, say $S = \{e\}$. Then $ee = e$, which by definition makes e an identity on all elements of S.

$\Longrightarrow$: Suppose S has at least two elements, and assume it has an identity element e. Then for any $a \neq e$ in S, we have $ea = e$ and so e is not an identity, which is a contradiction. □

1.2

Prove the properties of inverses that are listed below:

- If an element a has both a left inverse ℓ and a right inverse r, i.e. if $\ell a = 1$ and $ar = 1$, then $\ell = r$, a is invertible, and r is its inverse.
- If a is invertible, its inverse is unique.
- Inverses multiply in the opposite order: If a and b are invertible, so is the product ab and $(ab)^{-1} = b^{-1}a^{-1}$.

Solution.

Proof.
(i) Suppose $\ell a = ar = 1$. Then by definition of an identity element and associativity we have

$$\ell = \ell 1 = \ell(ar) = (\ell a)r = 1r = r$$

which also means $r = \ell$ is the inverse of a.

(ii) Suppose that a has two inverses b and c. Then

$$b = b1 = b(ac) = (ba)c = 1c = c$$

Thus the inverse of a is unique.

(iii) Let a and b be invertible. Then we have

$$\left.\begin{aligned} ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(1)a^{-1} = aa^{-1} = 1 \\ (b^{-1}a^{-1})ab = b^{-1}(aa^{-1})b = b^{-1}(1)b = b^{-1}b = 1 \end{aligned}\right\} \implies (ab)^{-1} = b^{-1}a^{-1}$$

□

1.3

Let $\mathbb{N}$ denote the set $\{1, 2, 3, \dots\}$ of natural numbers, and let $s : \mathbb{N} \to \mathbb{N}$ be the *shift* map, defined by $s(n) = n + 1$. Prove that s has no right inverse, but that it has infinitely many left inverses.

Solution.

Proof.
(i) Suppose there exists a function $r : \mathbb{N} \to \mathbb{N}$ such that $s \circ r$ is the identity function [$s(r(n)) = n$ for all $n \in \mathbb{N}$]. Note that this implies

$$1 = s(r(1)) = r(1) + 1$$

However there is no natural number that equals 1 after being increased by one. Hence $r(1) \notin \mathbb{N}$, which is a contradiction.

(ii) Choose $k \in \mathbb{N}$ and define a map $\ell_k : \mathbb{N} \to \mathbb{N}$ by the rule

$$\ell_k(n) = \begin{cases} n - 1 & \text{if } n > 1 \\ k & \text{if } n = 1 \end{cases}$$

Now note that for any $n \in \mathbb{N}$, we have

$$\ell_k(s(n)) = \ell_k(n + 1) = n$$

so ℓ_k is a left inverse of s, and there exists an ℓ_k for every natural number k, therefore s has infinitely many left inverses. □

§2 – Groups and Subgroups

2.1

Make a multiplication table for the symmetric group S_3.

Solution.
Writing $x = (123)$ and $y = (12)$, we have

	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	xy	1	x^2y	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

2.2

Let S be a set with an associative law of composition and with an identity element. Prove that the subset consisting of the invertible elements in S is a group.

Solution.

Proof.
Let S' be all invertible elements in S. We prove by definition.

- The law of composition is given to be associative.
- The identity element 1 is invertible since $1 \cdot 1 = 1$, so $1 \in S'$.
- Every $a \in S'$ is invertible, so we have $aa^{-1} = a^{-1}a = 1$. This also means a^{-1} is invertible, so $a^{-1} \in S'$.

Therefore by definition S' is a group. □

2.3

Let x, y, z, and w be elements of a group G.

(a) Solve for y, given that $xyz^{-1}w = 1$.

(b) Suppose that $xyz = 1$. Does it follow that $yzx = 1$? Does it follow that $yxz = 1$?

Solution.

(a) $y = x^{-1}w^{-1}z$

(b) Yes, $yzx = 1$ as

$$yzx = (x^{-1}x)yzx = x^{-1}(xyz)x = x^{-1}1x = x^{-1}x = 1$$

However, $yxz = 1$ is not necessarily true. If we take our group to be $GL_2(\mathbb{R})$ and let

$$x = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \quad y = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}, \quad z = (xy)^{-1} = \begin{bmatrix} 5 & 2 \\ 7 & 3 \end{bmatrix}^{-1} = \begin{bmatrix} 3 & -2 \\ -7 & 5 \end{bmatrix}$$

Then $xyz = 1$ but

$$yxz = (yx)z = \begin{bmatrix} 4 & 5 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 3 & -2 \\ -7 & 5 \end{bmatrix} = \begin{bmatrix} -23 & 17 \\ -19 & 14 \end{bmatrix} \neq 1$$

2.4

In which of the following cases is H a subgroup of G?

(a) $G = GL_n(\mathbb{C})$ and $H = GL_n(\mathbb{R})$

(b) $G = \mathbb{R}^\times$ and $H = \{-1, 1\}$

(c) $G = \mathbb{Z}^+$ and H is the set of positive integers

(d) $G = \mathbb{R}^\times$ and H is the set of positive reals

(e) $G = GL_2(\mathbb{R})$ and H is the set of matrices $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, with $a \neq 0$

Solution.

(a) Yes.

(b) Yes.

(c) No, the identity $0 \notin H$.

(d) Yes.

(e) No, the identity $I \notin H$.

2.5

In the definition of a subgroup, the identity element of H is required to be the identity of G. One might require only that H have an identity element, not that it need be the same as the identity in G. Show that if H has an identity at all, then it is the identity in G. Show that the analogous statement is true for inverses.

Solution.

Proof.
(i) Let 1 be the identity in G and $1'$ be an identity in H. In particular, $1'1' = 1'$. However, since $H \subset G$ we also have

$$1'1 = 1' = 1'1'$$

and by the cancellation law we have $1 = 1'$.
[To be more precise since the cancellation law depends on the chosen group and identity element, $1' \in H \subset G$ has an inverse in G, i.e. some $a \in G$ such that $a1' = 1'a = 1$. Then we have $1' = 11' = (a1')1' = a(1'1') = a1' = 1$]

(ii) Choose $a \in H$. Let a^{-1} be the inverse in G and suppose b is an inverse in H. Then

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

and by the cancellation law we have $b = a^{-1}$. □

2.6

Let G be a group. Define an *opposite group* G° with law of composition $a * b$ as follows: The underlying set is the same as G, but the law of composition is $a * b = ba$. Prove that G° is a group.

Solution.

Proof.
We prove by definition.

- Choose $a, b, c \in G^\circ$. Then since G's operation is associative we have

  $$(a * b) * c = (ba) * c = c(ba) = (cb)a = a * (cb) = a * (b * c)$$

  Thus $*$ is associative.

- Let $1 \in G^\circ$ be the identity element of G. Then for any $a \in G^\circ$ we have

  $$a * 1 = 1a = a = a1 = 1 * a$$

  Thus 1 is also the identity element of G°.

- Choose $a \in G^\circ$ and let a^{-1} be its inverse in G. Then

  $$a * a^{-1} = a^{-1}a = 1 = aa^{-1} = a^{-1} * a$$

  Thus a^{-1} is also the inverse of a in G°.

Therefore by definition G° is a group. □

§3 - Subgroups of the Additive Group of Integers

3.1

Let $a = 123$ and $b = 321$. Compute $d = \gcd(a, b)$, and express d as an integer combination $ra + sb$.

Solution.
We do the Euclidean algorithm to get

$$\begin{aligned} 321 &= 2 \cdot 123 + 75 \\ 123 &= 1 \cdot 75 + 48 \\ 75 &= 1 \cdot 48 + 27 \\ 48 &= 1 \cdot 27 + 21 \\ 27 &= 1 \cdot 21 + 6 \\ 21 &= 3 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

Therefore

$$\gcd(321, 123) = \gcd(123, 75) = \gcd(75, 48) = \gcd(48, 27) = \gcd(27, 21) = \gcd(21, 6) = \gcd(6, 3) = \gcd(3, 0) = 3$$

Now we work backward

$$\begin{aligned} 75 &= 1 \cdot 321 - 2 \cdot 123 \\ 48 &= 123 - 75 = 123 - (1 \cdot 321 - 2 \cdot 123) = -1 \cdot 321 + 3 \cdot 123 \\ 27 &= 75 - 48 = (1 \cdot 321 - 2 \cdot 123) - (-1 \cdot 321 + 3 \cdot 123) = 2 \cdot 321 - 5 \cdot 123 \\ 21 &= 48 - 27 = (-1 \cdot 321 + 3 \cdot 123) - (2 \cdot 321 - 5 \cdot 123) = -3 \cdot 321 + 8 \cdot 123 \\ 6 &= 27 - 21 = (2 \cdot 321 - 5 \cdot 123) - (-3 \cdot 321 + 8 \cdot 123) = 5 \cdot 321 - 13 \cdot 123 \end{aligned}$$

Thus $r = -13$ and $s = 5$.

3.2

Prove that if a and b are positive integers whose sum is a prime p, their greatest common divisor is 1.

Solution.

Proof.
Suppose otherwise, i.e. $\gcd(a, b) = d > 1$. Then d divides both a and b, hence d divides $a + b = p$. Since p is prime, this forces $d = p$. But $d \leq a$ and $d \leq b$ since it is a divisor of positive numbers, so

$$p = a + b \geq d + d = 2d = 2p \implies 1 \geq 2$$

which is a contradiction. □

3.3

(a) Define the greatest common divisor of a set $\{a_1, \ldots, a_n\}$ of n integers. Prove that it exists, and that it is an integer combination of $a_1, \ldots, a_n$.

(b) Prove that if the greatest common divisor of $\{a_1, \ldots, a_n\}$ is d, then the greatest common divisor of $\{a_1/d, \ldots, a_n/d\}$ is 1.

Solution.

(a) The greatest common divisor of $\{a_1, \ldots, a_n\}$ is the positive integer d where

$$\mathbb{Z}d = \mathbb{Z}a_1 + \ldots \mathbb{Z}a_n = \left\{ n \in \mathbb{Z} \;\middle|\; n = \sum_{i=1}^{n} r_i a_i \right\}$$

which we denote $d = \gcd(a_1, \ldots, a_n)$.
Since $\{n \in \mathbb{Z} \mid n = \sum_{i=1}^{n} r_i a_i\}$ is a subgroup of $\mathbb{Z}$, by Theorem 2.3.3 it can be written in the form $\mathbb{Z}d$, so $\gcd(a_1, \ldots, a_n)$ exists. Furthermore, since $d \in \mathbb{Z}d$, we can write it in the form $d = r_1 a_1 + \cdots + r_n a_n$.

(b) *Proof.*
Let $d = \gcd(a_1, \ldots, a_n)$. Then since $d \in \mathbb{Z}d = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$, there exists $r_1, \ldots, r_n$ such that $d = r_1 a_1 + \cdots + r_n a_n$. This means that

$$1 = r_1 \frac{a_1}{d} + \cdots + r_n \frac{a_n}{d} \in \mathbb{Z}\frac{a_1}{d} + \cdots + \mathbb{Z}\frac{a_n}{d}$$

In particular, every integer n can be written

$$n = n(1) = n(r_1 \tfrac{a_1}{d} + \cdots + r_n \tfrac{a_n}{d}) \in \mathbb{Z}\frac{a_1}{d} + \cdots + \mathbb{Z}\frac{a_n}{d}$$

Hence $\mathbb{Z} \subset \mathbb{Z}\frac{a_1}{d} + \cdots + \mathbb{Z}\frac{a_n}{d}$. We always have $\mathbb{Z}\frac{a_1}{d} + \cdots + \mathbb{Z}\frac{a_n}{d} \subset \mathbb{Z}$, so the two groups are equal and

$$\mathbb{Z}\frac{a_1}{d} + \cdots + \mathbb{Z}\frac{a_n}{d} = \mathbb{Z} \implies \gcd(a_1/d, \ldots, a_n/d) = 1$$

□

§4 - Cyclic Groups

4.1

Let a and b be elements of a group G. Assume that a has order 7 and that $a^3b = ba^3$. Prove that $ab = ba$.

Solution.

Proof.
We have

$$\begin{aligned} ab = (1)ab = (a^{14})ab = a^3a^3a^3a^3(a^3b) = a^3a^3a^3a^3(ba^3) &= a^3a^3a^3(a^3b)a^3 \\ &= a^3a^3a^3ba^3a^3 \\ &= a^3a^3ba^3a^3a^3 \\ &= a^3ba^3a^3a^3a^3 \\ &= ba^3a^3a^3a^3a^3 = ba(a^{14}) = ba \end{aligned}$$

□

4.2

An nth root of unity is a complex number z such that $z^n = 1$.

(a) Prove that the nth roots of unity form a cyclic subgroup of $\mathbb{C}^\times$ of order n.

(b) Determine the product of all the nth roots of unity

Solution.

(a) *Proof.*
Let $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$ be the nth roots of unity. Then we check the subgroup conditions individually:

- Choosing $a, b \in \mu_n$, note that since complex multiplication is commutative we have
$$(ab)^n = a^n \cdot b^n = 1 \cdot 1 = 1 \implies ab \in \mu_n$$
and so μ_n is closed under multiplication.
- Since $1^n = 1$, we have the identity $1 \in \mu_n$.
- Choosing $a \in \mu_n$, we have an inverse $a^{-1} \in \mathbb{C}^\times$. However, in $\mathbb{C}$ we can write
$$(a^{-1})^n = \left(\frac{1}{a}\right)^n = \frac{1^n}{a^n} = \frac{1}{1} = 1 \implies a^{-1} \in \mu_n$$
Thus μ_n is closed under inverses.

Therefore μ_n is a subgroup by definition. By the fundamental theorem of algebra, $z^n = 1$ has at most n distinct solutions, hence the order of μ_n is at most n. Now define
$$\zeta = e^{i\frac{2\pi}{n}}$$
Note that $\zeta^n = e^{i2\pi} = 1$ (e.g. by Euler's formula) so we have $\zeta \in \mu_n$. Furthermore, for any $k = 0, \ldots, n-1$ we have
$$(\zeta^k)^n = (e^{i\frac{2k\pi}{n}})^n = e^{i2\pi k} = 1$$
and $1 = \zeta^0, \zeta^1, \ldots, \zeta^{n-1}$ are all distinct complex numbers, so the order of μ_n is at least n. Thus μ_n has order n and furthermore is generated by ζ, therefore it is cyclic. □

(b) From (a) we know that
$$\mu_n = \langle\zeta\rangle = \{\zeta^0, \zeta^1, \ldots, \zeta^{n-1}\} = \left\{e^{i\frac{2k\pi}{n}} \;\middle|\; k = 0, \ldots, n-1\right\}$$
So the product of all the nth roots of unity is
$$\begin{aligned}\prod_{k=0}^{n-1} e^{i\frac{2k\pi}{n}} = e^{i\frac{2\pi 0}{n}} e^{i\frac{2\pi 1}{n}} \ldots e^{i\frac{2\pi(n-1)}{n}} &= e^{\frac{2\pi i}{n}(0+1+\cdots+(n-1)} \\ &= e^{\frac{2\pi i}{n}\cdot\frac{(n-1)n}{2}} \\ &= e^{\pi i(n-1)} \\ &= e^{n\pi i}e^{-\pi i} = (-1)^n(-1) = (-1)^{n+1}\end{aligned}$$

4.3

Let a and b be elements of a group G. Prove that ab and ba have the same order.

Solution.

Proof.
We first do the case of finite orders. Suppose that ab has finite order, say n. Then

$$1 = (ab)^n = \underbrace{abab\dots ab}_{n} = b^{-1}\underbrace{baba\dots ba}_{n}b = b^{-1}(ba)^n b \implies (ba)^n = \underbrace{baba\dots ba}_{n} = b1b^{-1} = 1$$

Hence ba has order at most n. If ba had an order k less than n, then the symmetric argument to the one above would show ab has order at most $k < n$, a contradiction. Thus ba has order n.

Now for infinite orders, suppose that ab has infinite order. If ba had a finite order, then the argument above would show ab has finite order which is a contradiction. Thus ba also has infinite order. □

4.4

Describe all groups G that contain no proper subgroup.

Solution.
Let G be a group with no proper subgroup. Clearly the trivial group is such a group, so assume that G is nontrivial and has some element $x \neq 1$. Note that G must be cyclic, since otherwise the cyclic subgroup $\langle x\rangle$ is a proper subgroup of G. Hence without loss of generality we have $G = \langle x\rangle$. G cannot be infinite cyclic since $\langle x^2\rangle$ would be a proper subgroup, therefore x has finite order, say n. Furthermore, n must be prime since if $n = pq$ for $p, q < n$ then $\langle x^p\rangle$ is a proper subgroup of order q. Therefore G is a cyclic group of prime order.

4.5

Prove that every subgroup of a cyclic group is cyclic. Do this by working with exponents, and use the description of the subgroups of $\mathbb{Z}^+$.

Solution.

Proof.
Let $G = \langle x\rangle$ be a cyclic group and let H be a subgroup. In particular every element of H is of the form x^m, so let k be the smallest positive integer such that $x^k \in H$. We claim that $H = \langle x^k\rangle$. Choose $y \in H$. As $H \subset \langle x\rangle$, we can write $y = x^m$ for some positive integer m. Now (e.g. by classification of $\mathbb{Z}^+$'s subgroups) there exists $q, r \in \mathbb{Z}$ such that $m = qk + r$ and $0 \leq r < k$. Note

$$y = x^m = x^{qk+r} = (x^k)^q x^r \implies x^r = ((x^k)^q)^{-1}y$$

But since $x^k \in H$, we have under closure that $((x^k)^q)^{-1} \in H$. Thus $x^r = (x^k)^{-q}y \in H$. But since $r < k$ and by choice of k as the smallest positive integer where $x^k \in H$, this forces $r = 0$. Thus $y = (x^q)^k \in \langle x^q\rangle$ and therefore $H \subset \langle x^k\rangle$. Clearly the reverse inclusion $H \supset \langle x^k\rangle$ also holds, so the groups are equal. □

4.6

(a) Let G be a cyclic group of order 6. How many of its elements generate G? Answer the same question for cyclic groups of orders 5 and 8.

(b) Describe the number of elements that generate a cyclic group of arbitrary order n.

Solution.

(a) (i) Let $G = \{1, x, x^2, x^3, x^4, x^5\}$ (without loss of generality). Then we have

$$\begin{aligned}
\langle 1 \rangle &= \{1\} \neq G \\
\langle x \rangle &= \{x, x^2, x^3, x^4, x^5, x^6 = 1\} = G \\
\langle x^2 \rangle &= \{x^2, x^4, x^6 = 1\} \neq G \\
\langle x^3 \rangle &= \{x^3, x^6 = 1\} \neq G \\
\langle x^4 \rangle &= \{x^4, x^8 = x^2, x^{12} = 1\} \neq G \\
\langle x^5 \rangle &= \{x^5, x^{10} = x^4, x^{15} = x^3, x^{20} = x^2, x^{25} = x, x^{30} = 1\} = G
\end{aligned}$$

Hence the elements that generate G are x and x^5.
(ii) Let $G = \{1, y, y^2, y^3, y^4\}$. Then we have

$$\begin{aligned}
\langle 1 \rangle &= \{1\} \neq G \\
\langle y \rangle &= \{y, y^2, y^3, y^4, y^5\} = G \\
\langle y^2 \rangle &= \{y^2, y^4, y^6 = y, y^8 = y^3, y^{10} = 1\} = G \\
\langle y^3 \rangle &= \{y^3, y^6 = y, y^9 = y^4, y^{12} = y^2, y^{15} = 1\} = G \\
\langle y^4 \rangle &= \{y^4, y^8 = y^3, y^{12} = y^2, y^{16} = y, y^{20} = 1\} = G
\end{aligned}$$

Hence the elements that generate G are y, y^2, y^3, and y^4.
(iii) Let $G = \{1, z, z^2, z^3, z^4, z^5, z^6, z^7\}$. By the same process shown above, the elements that generate G are z, z^3, z^5, and z^7.

(b) We claim that the number of elements that generate a cyclic group of order n is $\varphi(n)$, where $\varphi(n)$ is Euler's totient function that counts which of $1, 2, \ldots, n\text{-}1$ is relatively prime to n,

$$\varphi(n) = \left|\{k \in \{1, 2, \ldots, n\text{-}1\} \mid \gcd(k, n) = 1\}\right|$$

Proof.
Let $G = \langle x \rangle$ be a cyclic group of order n. Now suppose that $\gcd(k, n) = 1$. Then we can find integers r, s such that $rk + sn = 1 \implies rk = (-s)n + 1$. Now

$$(x^k)^r = x^{rk} = x^{(-s)n+1} = ((x^n)^s)^{-1}x = (1^s)^{-1}x = x \implies x \in \langle x^k \rangle$$

Conversely, if $x \in \langle x^k \rangle$ for some k, then there exists an integer r such that

$$x = (x^k)^r = x^{rk} \implies x^{rk-1} = 1 \implies rk - 1 = sn \implies rk + (-s)n = 1 \implies \gcd(k, n) = 1$$

Combining everything above gives $G = \langle x^k \rangle$ iff $\langle x \rangle \subset \langle x^k \rangle$ iff $x \in \langle x^k \rangle$ iff $\gcd(k, n) = 1$. $\square$

4.7

Let x and y be elements of a group G. Assume that each of the elements x, y, and xy has order 2. Prove that the set $H = \{1, x, y, xy\}$ is a subgroup of G, and that it has order 4.

Solution.

Proof.
Note that

$$yx = (xx)yx(yy) = x(xy)(xy)y = xy$$

which means that

$$yxy = (yx)y = (xy)y = x(yy) = x \quad \text{and} \quad xyx = x(yx) = x(xy) = (xx)y = y$$

Hence looking at the (induced) multiplication table

	1	x	y	xy
1	1	x	y	xy
x	x	1	xy	y
y	y	xy	1	x
xy	xy	y	x	1

We see that H is closed under multiplication and inverses, as well as has the identity 1, so it is a subgroup by definition. Finally, each element is distinct since if $xy = x$, then by the cancellation law we would have $y = 1$ which has order 1, a contradiction. Similarly $xy = y$ results in a contraction. Therefore H has order 4. □

4.8

(a) Prove that the elementary matrices of the first and third types (row-additions and row-scalings) generate $GL_n(\mathbb{R})$.

(b) Prove that the elementary matrices of the first type generate $SL_n(\mathbb{R})$. Do the 2×2 case first.

Solution.

(a) *Proof.*
Note that since every invertible matrix can be written as the product of elementary matrices (Theorem 1.2.16), we have that the elementary matrices of the first, second, and third types generate $GL_n(\mathbb{R})$. Hence it suffices to show that every elementary matrix of the second type, i.e. row-swaps, can be built from row-additions and row-scalings. Indeed, if we want to swap row i and row j, we can perform the following algorithm:

- $R_i \mapsto R_i + R_j$
- $R_j \mapsto R_j - R_i$
- $R_j \mapsto -1 \cdot R_j$
- $R_i \mapsto R_i - R_j$

Since now the new R_i' and R_j' become (in terms of the original R_i and R_j)

$$R_i' = (R_i + R_j) - (-(R_j - (R_i + R_j))) = (R_i + R_j) - (-(-R_i)) = R_j$$

$$R_j' = -(R_j - (R_i + R_j)) = -(-R_i) = R_i$$

Hence for any $A \in GL_n(\mathbb{R})$, we can write it as the product of elementary matrices, and any row-swap matrices in the decomposition can be replaced with row-additions and row-scalings. Thus A can be written as the product of elementary matrices of the first and third types. $\square$

(b) *Proof.*
Choose $A \in SL_n(\mathbb{R})$. Since $SL_n \subset GL_n$, by (a) we can write A as a product of row-additions and row-scalings. However, note the equivalence of row operations

$$\begin{array}{l} \bullet\ R_i \mapsto R_i + cR_j \\ \bullet\ R_i \mapsto dR_i \end{array} \iff \begin{array}{l} \bullet\ R_i \mapsto dR_i \\ \bullet\ R_i \mapsto R_i + (dc)R_j \end{array}$$

and

$$\begin{array}{l} \bullet\ R_i \mapsto R_i + cR_j \\ \bullet\ R_j \mapsto dR_j \end{array} \iff \begin{array}{l} \bullet\ R_j \mapsto dR_j \\ \bullet\ R_i \mapsto R_i + (\frac{c}{d})R_j \end{array}$$

and

$$\begin{array}{l} \bullet\ R_i \mapsto R_i + cR_j \\ \bullet\ R_k \mapsto dR_k \end{array} \iff \begin{array}{l} \bullet\ R_k \mapsto dR_k \\ \bullet\ R_i \mapsto R_i + R_j \end{array}$$

In particular, this means can do all of our row-scalings first, and then all of our row-additions to construct A. Hence without loss of generality we can write $A = XY$, where X is the product of row-scalings and Y is the product of row-additions. Furthermore,

$$A \in SL_n \implies 1 = \det(A) = \det(X)\det(Y)$$

Since each row-addition has determinant 1, we have $\det(Y) = 1$, which forces $\det(X) = 1$. Also, each row-scaling is a diagonal matrix, so X is also a diagonal matrix with entries $d_1, \ldots, d_n$. Finally, we have the property of diagonal matrices that $\det(X) = d_1 \times \cdots \times d_n$. Hence it suffices to prove the case where $A = \text{diag}(d_1, \ldots, d_n)$ where $\prod d_i = 1$.

We first start with $n = 2$. Then we have

$$A = \begin{bmatrix} d & 0 \\ 0 & \frac{1}{d} \end{bmatrix}$$

We can construct A from I with only row-additions via

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \xrightarrow{\mathbf{R_2} + \mathbf{d(d-1)R_1}} \begin{bmatrix} 1 & 0 \\ d(d-1) & 1 \end{bmatrix} \xrightarrow{\mathbf{R_1} + \frac{\mathbf{1}}{\mathbf{d}}\mathbf{R_2}} \begin{bmatrix} d & \frac{1}{d} \\ d(d-1) & 1 \end{bmatrix} \xrightarrow{\mathbf{R_2} - \mathbf{(d-1)R_1}} \begin{bmatrix} d & \frac{1}{d} \\ 0 & \frac{1}{d} \end{bmatrix} \xrightarrow{\mathbf{R_1} - \mathbf{R_2}} \begin{bmatrix} d & 0 \\ 0 & \frac{1}{d} \end{bmatrix}$$

Thus the 2×2 case is shown. Now more generally for $A = \text{diag}(d_1, \ldots, d_n)$, let E_i be the diagonal $n \times n$ matrix where the (i, i) entry is d_i and the (n, n) entry is $\frac{1}{d_i}$. Note that since $\det(A) = d_1 d_2 \ldots d_n = 1$, we have

$$E_1 E_2 \ldots E_{n-1} = \text{diag}(d_1, d_2, \ldots, \tfrac{1}{d_1 d_2 \ldots d_{n-1}}) = \text{diag}(d_1, d_2, \ldots, d_n) = A$$

and for each $i = 1, \ldots, n-1$, the generalized $n = 2$ case algorithm will construct E_i from I:

- $R_n \mapsto R_n + d_i(d_i - 1)R_i$
- $R_i \mapsto R_i + \frac{1}{d_i} R_n$
- $R_n \mapsto R_n - (d_i - 1)R_i$
- $R_i \mapsto R_i - R_n$

Therefore each E_i is the product of elementary matrices of the first type, hence A can be written as a product of them as well. $\square$

4.9

How many elements of order 2 does the symmetric group S_4 contain?

Solution.
Note that immediately any 3-cycles or 4-cycles (or any permutation $\sigma \in S_4$ with at least one of them) cannot have order 2. Hence we only want permutations that are transpositions of two indices, or multiple transpositions that swap pairs of indices independently. In other words, we want only the product of disjoint 2-cycles in S_4, which we can list exhaustively:

$$(12); \quad (23); \quad (34); \quad (13); \quad (14); \quad (24); \quad (12)(34); \quad (13)(24); \quad (14)(23)$$

which is nine order-2 elements of S_4 in total.

4.10

Show by example that the product of elements of finite order in a group need not have finite order. What if the group is abelian?

Solution.
In the group $GL_2(\mathbb{R})$, consider the following elements

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 0.5 \\ 2 & 0 \end{bmatrix}$$

Note that

$$A^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad B^2 = \begin{bmatrix} 0 & 0.5 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0.5 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Hence A and B have finite order. However,

$$AB = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0.5 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 0.5 \end{bmatrix} \implies (AB)^n = \begin{bmatrix} 2^n & 0 \\ 0 & 2^{-n} \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \ \forall n \geq 1$$

So AB does not have finite order.

Now let G be an abelian group with elements $a, b \in G$ with finite orders n and m respectively. Then since the group is abelian,

$$(ab)^{nm} = a^{nm} b^{nm} = (a^n)^m (b^m)^n = (1)^m (1)^n = 1$$

Thus ab also has finite order.

4.11

(a) Adapt the method of row reduction to prove that the transpositions generate the symmetric group S_n.

(b) Prove that, for $n \geq 3$, the three-cycles generate the alternating group A_n.

Solution.

(a) *Proof.*
Choose a permutation $\sigma \in S_n$, which has an associated permutation matrix P. By Prop 1.5.10(a), P has a single 1 in each row and column with zeros elsewhere. Thus we can perform only row-swaps to row reduce P into I (take the row with a 1 in the first column and swap it with the first row, etc.). Then we can write

$$I = S_1 \dots S_m P$$

Note that for each i we have $S_i^{-1} = S_i$ and therefore $P = S_k \dots S_1$. Furthermore, each S_i is the permutation matrix of a transposition τ_i: If S_i swaps rows j and k, then it is the permutation matrix associated to $\tau_i = (jk)$. Therefore $\sigma = \tau_m \dots \tau_1$ and S_n is generated by transpositions. □

(b) *Proof.*
Choose an even permutation $\sigma \in A_n$. By (a) we can write σ as a product of transpositions. Furthermore, σ is even, so the number of transpositions is necessarily even. Then write

$$\sigma = \tau_1\tau_2 \dots \tau_{2k-1}\tau_{2k} = (\tau_1\tau_2) \dots (\tau_{2k-1}\tau_{2k})$$

Therefore by the above grouping, it suffices to show that any product of two transpositions can be built with 3-cycles. Consider the product $(ab)(cd)$. We consider cases:

- a, b, c, d are all distinct: Then note $(acd)(abd) = (ab)(cd)$, as computing the LHS gives

$$\begin{aligned} a &\mapsto b \mapsto b \\ b &\mapsto d \mapsto a \\ c &\mapsto c \mapsto d \\ d &\mapsto a \mapsto c \end{aligned}$$

- $a = c, b = d$: Then

$$(ab)(bd) = (ab)(ab) = \mathrm{id} = (abx)(abx)(abx)$$

  for some index $x \neq a, b$ (which exists since $n \geq 3$).
- Only $b = c$: Then $(abd) = (ab)(bd)$ since the RHS gives

$$\begin{aligned} a &\mapsto a \mapsto b \\ b &\mapsto d \mapsto d \\ d &\mapsto b \mapsto a \end{aligned}$$

Any other case can be reduced to one of three above, as $(ab) = (ba)$ and $(cd) = (dc)$ [e.g. since $(ab)(cd) = (ba)(dc)$, then we apply the third case if only $a = d$].
Therefore the three cycles generate A_n. □

§5 - Homomorphisms

5.1

Let $\varphi : G \to G'$ be a surjective homomorphism. Prove that if G is cyclic, then G' is cyclic, and if G is abelian, then G' is abelian.

Solution.

Proof.
(i) Suppose $G = \langle x \rangle$ is cyclic. We claim $G' = \langle \varphi(x) \rangle$.
Choose $a \in G'$. Since φ is surjective, there exists $y \in G$ such that $\varphi(y) = a$. However, $G = \langle x \rangle$ implies there exists n such that $y = x^n$. Therefore

$$a = \varphi(y) = \varphi(x^n) \overset{(\star)}{=} (\varphi(x))^n \in \langle \varphi(x) \rangle$$

where $(\star)$ follows from φ being a homomorphism (specifically Prop 2.5.3(a)). Therefore $G' = \langle \varphi(x) \rangle$ is cyclic.

(ii) Suppose that G is abelian. Now for any $a, b \in G'$, by surjectivity there exists $x, y \in G$ such that $\varphi(x) = a$ and $\varphi(y) = b$. Since φ is a homomorphism and G is abelian we have

$$ab = \varphi(x)\varphi(y) = \varphi(xy) = \varphi(yx) = \varphi(y)\varphi(x) = ba$$

Therefore G' is abelian. □

5.2

Prove that the intersection $K \cap H$ of subgroups of a group G is a subgroup of H, and that if K is a normal subgroup of G, then $K \cap H$ is a normal subgroup of H.

Solution.

Proof.
(i) We show $K \cap H \leq H$ (i.e. is a subgroup of H) by definition:

- For any $x, y \in K \cap H$, since $K \leq G$ and $H \leq G$ we have

$$xy \in K \text{ and } xy \in H \implies xy \in K \cap H$$

  Thus we have closure in $K \cap H$.

- Since the identity $1 \in K$ and $1 \in H$, we have $1 \in K \cap H$.

- Choose $x \in K \cap H$. Then its inverse $x^{-1} \in G$ is necessarily in K and H since $K, H \leq G$. Thus $x^{-1} \in K \cap H$.

Therefore $K \cap H \leq H$.

(ii) Suppose $K \lhd G$ (i.e. is a normal subgroup of G).
Choose $x \in K \cap H$. For any $h \in H$, note that:

- Since $x \in K \lhd G$ and $H \leq G$, we have $h \in G$ and by definition of normal subgroup $hxh^{-1} \in K$

- Since $x \in H$ and $H \leq G$, we have by closure of H that $hxh^{-1} \in H$

Therefore $hxh^{-1} \in K \cap H$ and thus $K \cap H \lhd H$. □

5.3

Let U denote the group of invertible upper triangular 2×2 matrices $A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, and let $\varphi : U \to \mathbb{R}^\times$ be the map that sends $A \rightsquigarrow a^2$. Prove that φ is a homomorphism, and determine its kernel and image.

Solution.

Proof.
Choose $A, B \in U$, where

$$A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \quad \text{and} \quad X = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \implies AX = \begin{bmatrix} ax & ay + bz \\ 0 & dz \end{bmatrix}$$

Then we have

$$\varphi(AX) = (ax)^2 = a^2x^2 = \varphi(A)\varphi(X)$$

and therefore φ is a homomorphism. □

We also have that

$$\ker \varphi = \{A \in U \mid \varphi(A) = 1\} = \left\{ \begin{bmatrix} \pm 1 & b \\ 0 & d \end{bmatrix} \;\middle|\; d \neq 0 \right\}$$

$$\operatorname{im} \varphi = \left\{ a \in \mathbb{R}^\times \;\middle|\; \begin{bmatrix} \sqrt{a} & b \\ 0 & d \end{bmatrix} \in U \right\} = (0, \infty) \subset \mathbb{R}$$

5.4

Let $f : \mathbb{R}^+ \to \mathbb{C}^\times$ be the map $f(x) = e^{ix}$. Prove that f is a homomorphism, and determine its kernel and image.

Solution.

Proof.
Choose $x, y \in \mathbb{R}^+$. Then

$$f(x)f(y) = e^{ix}e^{iy} = e^{i(x+y)} = f(x + y)$$

Thus f is a homomorphism. □

We also have that

$$\ker f = \{x \in \mathbb{R}^+ \mid 1 = e^{ix}\} = \{x \in \mathbb{R}^+ \mid x = 0, \pm 2\pi, \pm 4\pi, \dots\} = \mathbb{Z}2\pi$$

$$\operatorname{im} \varphi = \{z \in \mathbb{C}^\times \mid |z| = 1\} = \text{complex plane unit circle}$$

5.5

Prove that the $n \times n$ matrices that have the block form $M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$, with A in $GL_r(\mathbb{R})$ and D in $GL_{n-r}(\mathbb{R})$, form a subgroup H of $GL_n(\mathbb{R})$, and that the map $H \to GL_r(\mathbb{R})$ that sends $M \rightsquigarrow A$ is a homomorphism. What is its kernel?

Solution.

Proof.
First note that by block matrix multiplication we have

$$\begin{bmatrix} A & B \\ 0 & D \end{bmatrix} \begin{bmatrix} X & Y \\ 0 & Z \end{bmatrix} = \begin{bmatrix} AX + B0 & AY + BZ \\ 0X + D0 & 0Y + DZ \end{bmatrix} = \begin{bmatrix} AX & AY + BZ \\ 0 & DZ \end{bmatrix}$$

Now we show $H \leq GL_n(\mathbb{R})$ by definition:

- Choose $\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}, \begin{bmatrix} X & Y \\ 0 & Z \end{bmatrix} \in H$. For the product to also be in H, we need $AX \in GL_r(\mathbb{R})$ and $DZ \in GL_{n-r}(\mathbb{R})$. But this is ensured by the closure of $GL_r(\mathbb{R})$ and $GL_{n-r}(\mathbb{R})$.
- We have $n \times n$ identity in block form

$$I_n = \begin{bmatrix} I_r & 0 \\ 0 & I_{n-r} \end{bmatrix} \in H$$

- Choose $\begin{bmatrix} A & B \\ 0 & D \end{bmatrix} \in H$. Then it has inverse

$$\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}^{-1} = \begin{bmatrix} A^{-1} & A^{-1}(-BD^{-1}) \\ 0 & D^{-1} \end{bmatrix} \in H$$

Next, let $\varphi : M \mapsto A$ be the map defined above. Then

$$\varphi\left(\begin{bmatrix} A & B \\ 0 & D \end{bmatrix} \begin{bmatrix} X & Y \\ 0 & Z \end{bmatrix}\right) = \varphi\left(\begin{bmatrix} AX & AY + BZ \\ 0 & DZ \end{bmatrix}\right) = AX = \varphi\left(\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}\right) \varphi\left(\begin{bmatrix} X & Y \\ 0 & Z \end{bmatrix}\right)$$

So φ is a homomorphism. Finally, it has kernel

$$\ker \varphi = \left\{ \begin{bmatrix} I_r & B \\ 0 & D \end{bmatrix} \;\middle|\; D \in GL_{n-r}(\mathbb{R}) \right\}$$

□

5.6

Determine the center of $GL_n(\mathbb{R})$.
Hint: You are asked to determine the invertible matrices A that commute with every invertible matrix B. Do not test with a general matrix B. Test with elementary matrices.

Solution.
We claim the center of $GL_n(\mathbb{R})$, which we denote $Z(GL_n(\mathbb{R}))$, is all scalar multiples of I, which we denote $\mathbb{Z}I$.

Proof.
First, choose a matrix $A \in \mathbb{Z}I$. Note that we can write $A = dI$ for some nonzero d. Now for any invertible matrix $B \in GL_n(\mathbb{R})$ we have $BA = AB = dB$ since both matrices multiply every entry in B by d. Thus $\mathbb{Z}I \subset Z(GL_n(\mathbb{Z}))$.

Now choose a matrix $A \in Z(GL_n(\mathbb{R}))$. Then A commutes with all invertible matrices, so in particular it commutes with all elementary matrices. We specifically will look at the row-additions, letting E_{rc} correspond to the row operation of adding row c to row r ($r \neq c$). We use r and c since we can write this using a unit matrix: $E_{rc} = I + e_{rc}$, where e_{rc} has a 1 at row r and column c. Since A is in the center, we have

$$E_{rc}A = AE_{rc} \implies (I + e_{rc})A = A(I + e_{rc}) \implies A + e_{rc}A = A + Ae_{rc} \implies e_{rc}A = Ae_{rc}$$

From Exercise 1.1.15 (or thinking about the row operation E_{rc}), we have that $e_{rc}A$ takes the cth row of A and puts it at the rth row with zeros elsewhere; Ae_{rc} takes the rth column of A and puts it at the cth column with zeros elsewhere. The above states that every entry of these two matrices will match for any value of r and c, i.e.

$$(Ae_{rc})_{ij} = (e_{rc}A)_{ij} \quad \text{for all } r, c, i, j = 1, \ldots, n, \quad r \neq c \tag{$\star$}$$

We consider cases:

- $i \neq r, j \neq c$: Then we have $(Ae_{rc})_{ij} = 0$ since we are not looking at the cth column. Similarly, $(e_{rc}A)_{ij} = 0$ since we are not looking at the rth row. Thus all ($\star$) says is that $0 = 0$.
- $i = r, j \neq c$: Then again we have $(Ae_{rc})_{ij} = 0$. However, we are now looking at the rth row of $(e_{rc}A)$ which is the cth row of A. Therefore as we change value of j to move along that row, ($\star$) says that every off-diagonal entry in the cth row of A is zero. However, an invertible matrix cannot have a row of all zeros, so this also means that the entry A_{cc} is nonzero.
- $i = r, j = c$: Then $(Ae_{rc})_{ij}$ is the entry A_{rr} and $(e_{rc}A)_{ij}$ is entry A_{cc}. Thus ($\star$) tells us that $A_{cc} = A_{rr}$.

Therefore as we change the values of r and c, the last two points tell us the following: the offdiagonal entries of A are zero and the diagonal entries of A are the same nonzero number d. Hence $A = dI \in \mathbb{Z}I$ and $Z(GL_n(\mathbb{R})) \subset \mathbb{Z}I$. □

[As a side note, see Schur's lemma (Section 10.7)]

§6 - Isomorphisms

6.1

Let G' be the group of real matrices of the form $\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}$. Is the map $\mathbb{R}^+ \to G'$ that sends x to this matrix an isomorphism?

Solution.
We claim yes.

Proof.
Let $\varphi : \mathbb{R}^+ \to G'$ be the map $x \mapsto \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$. Clearly the map $\psi : \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} \mapsto y$ is the inverse of φ, so it suffices to show φ is a homomorphism. Indeed, we have

$$\varphi(x)\varphi(y) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix} = \varphi(x+y)$$

Therefore φ is an isomorphism. □

6.2

Describe all homomorphisms $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$. Determine which are injective, which are surjective, and which are isomorphisms.

Solution.
Since $\mathbb{Z}^+ = \langle 1 \rangle$, any homomorphism φ is determined by where it sends 1. To elaborate, for any $n \in \mathbb{Z}$ we have

$$\varphi(n) = \varphi(\underbrace{1 + \cdots + 1}_{n}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{n} = n(\varphi(1))$$

We thus consider cases:

- $\varphi(1) = 1$: Then $\varphi(n) = n$ is the identity function and is an isomorphism.
- $\varphi(1) = 0$: Then $\varphi(n) = 0$ is the trivial homomorphism, neither surjective nor injective.
- $\varphi(1) = -1$: Then $\varphi(n) = -n$ is injective ($\varphi(n) = -n = 0 \iff n = 0$) and surjective (for any $n \in \mathbb{Z}$, $\varphi(-n) = n$), thus it is an isomorphism.
- $\varphi(1) = k \neq -1, 0, 1$: Then $\varphi(n) = kn$, which is injective ($\varphi(n) = kn = 0 \iff n = 0$) but not surjective ($\varphi(n) = kn \neq 1$ for all $n \in \mathbb{Z}$).

This exhausts all possible cases.

6.3

Show that the functions $f = 1/x$, $g = (x-1)/x$ generate a group of functions, the law of composition being composition of functions, that is isomorphic to the symmetric group S_3.

Solution.

Proof.
Function composition is a law of composition, and we have the identity function via f:

$$f^2(x) = (f \circ f)(x) = \frac{1}{\frac{1}{x}} = x = \mathrm{id}(x)$$

For inverses, it suffices to show each generator has an inverse. We just demonstrated that $f^{-1} = f$, and we also have

$$g^3(x) = (g \circ g \circ g)(x) = 1 - \frac{1}{1 - \frac{1}{1-\frac{1}{x}}} = 1 - \frac{1}{\frac{x-1}{x-1} - \frac{x}{x-1}} = 1 - \frac{1}{\frac{-1}{x-1}} = 1 + (x-1) = x$$

Thus $g^{-1} = g^2$ and we have a group $G = \langle f, g \rangle$. To create an isomorphism to S_3, we map generators to generators of the same order. (12) and (123) generate S_3, so define our map

$$\varphi : G \to S_3, \quad \varphi(f) = (12),\ \varphi(g) = (123)$$

Note that in G we have the formula $fg = g^2 f$ as

$$(f \circ g)(x) = f(\tfrac{x-1}{x}) = \frac{x}{x-1} = \frac{-x}{1-x}$$

$$(g \circ g \circ f)(x) = g(g(\tfrac{1}{x})) = g(1 - \tfrac{1}{1/x}) = g(1-x) = \frac{(1-x)-1}{1-x} = \frac{-x}{1-x}$$

Therefore G has generators f and g with relations $f^2 = g^3 = 1$ and $fg = g^2 f$, which are the defining properties of the symmetric group S_3 so we have $G \cong S_3$. □

6.4

Prove that in a group, the products ab and ba are conjugate elements.

Solution.

Proof.
We have

$$aba = aba \implies ab = a(ba)a^{-1}$$

Thus ab and ba are conjugate. □

6.5

Decide whether or not the two matrices $A = \begin{bmatrix} 3 & \\ & 2 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix}$ are conjugate elements of the general linear group $GL_2(\mathbb{R})$.

Solution.
We claim yes.
We want to find a matrix X such that $AX \overset{\star}{=} XB$. Hence we would like

$$\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 3a & 3b \\ 2c & 2d \end{bmatrix} \overset{\star}{=} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix} = \begin{bmatrix} a-2b & a+4b \\ c-2d & c+4d \end{bmatrix}$$

Then we have the system

$$\begin{cases} 3a = a - 2b \\ 3b = a + 4b \\ 2c = c - 2d \\ 2d = c + 4d \end{cases} \implies \begin{cases} a = -b \\ c = -2d \end{cases}$$

So we can choose any such values that also satisfy $ad - bc \neq 0$ to ensure $X \in GL_2(\mathbb{R})$. We take $a = 1, b = -1, c = 2, d = -1$. Then we have

$$X = \begin{bmatrix} 1 & -1 \\ 2 & -1 \end{bmatrix} \quad \text{and} \quad X^{-1} = \begin{bmatrix} -1 & 1 \\ -2 & 1 \end{bmatrix}$$

and indeed

$$XBX^{-1} = \begin{bmatrix} 1 & -1 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ -2 & 1 \end{bmatrix} = \begin{bmatrix} 3 & -3 \\ 4 & -2 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ -2 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} = A$$

6.6

Are the matrices $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix}$ conjugate elements of the group $GL_2(\mathbb{R})$? Are they conjugate elements of $SL_2(\mathbb{R})$?

Solution.

Yes, they are conjugate in $GL_2(\mathbb{R})$. Let $A = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix}$.

We then want to find a matrix X such that $AX \overset{\star}{=} XB$. Hence we would like

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

Then we have the system

$$\begin{cases} a+c = a+b \\ b+d = b \\ c = c+d \\ d = d \end{cases} \implies \begin{cases} c = b \\ d = 0 \end{cases}$$

So we can choose any such values that also satisfy $ad - bc \neq 0$ to ensure $X \in GL_2(\mathbb{R})$. We take $a = 0, b = 1, c = 1, d = 0$. Then we have

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad X^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X$$

and indeed

$$XBX^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = A$$

However, they are not conjugate in $SL_2(\mathbb{R})$. To see this, suppose that there exists a matrix $Y = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{R})$ such that $A = YBY^{-1}$. But the above system must hold, so we have $b = c$ and $d = 0$. Then since $Y \in SL_2(\mathbb{R})$ we have

$$1 = \det(Y) = ad - bc = -b^2$$

which implies $b = \pm\sqrt{-1} \notin \mathbb{R}$, a contradiction. Thus such a Y does not exist and A, B are not conjugate in $SL_2(\mathbb{R})$.

6.7

Let H be a subgroup of G, and let g be a fixed element of G. The *conjugate subgroup* gHg^{-1} is defined to be the set of all conjugates ghg^{-1}, with $h \in H$. Prove that gHg^{-1} is a subgroup of G.

Solution.

Proof.
We prove $gHg^{-1} \leq G$ by definition:

- Choose $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$. Then we have

$$(gh_1g^{-1})(gh_2g^{-1}) = gh_1(gg^{-1})h_2g^{-1} = g(h_1h_2)g^{-1} \in gHg^{-1}$$

  since the closure of $H \leq G$ implies $h_1h_2 \in H$.

- Since $H \leq G$ we have the identity $1 \in H$. Thus

$$1 = gg^{-1} = g1g^{-1} \in gHg^{-1}$$

- Choose $ghg^{-1} \in gHg^{-1}$. It has inverse

$$(ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$$

  since the closure of $H \leq G$ implies $h^{-1} \in H$.

Therefore $gHg^{-1} \leq G$. □

Another (slicker) proof:

Proof.
Note that the "conjugate by g" map

$$c_g : H \to G, \quad h \mapsto ghg^{-1}$$

is a homomorphism:

$$c_g(h_1)c_g(h_2) = (gh_1g^{-1})(gh_2g^{-1}) = gh_1(g^{-1}g)h_2g^{-1} = g(h_1h_2)g^{-1} = c_g(h_1h_2)$$

Then $gHg^{-1} = c_g(H)$ is the image of a homomorphism and so is a subgroup of the codomain G. □

6.8

Prove that the map $A \rightsquigarrow (A^t)^{-1}$ is an automorphism of $GL_n(\mathbb{R})$.

Solution.

Proof.
Let $\varphi : GL_n(\mathbb{R}) \to GL_n(\mathbb{R})$ be the described map. First note (e.g. from Exercise 1.3.1) that $(A^t)^{-1} = (A^{-1})^t$. Hence

$$\varphi(\varphi(A)) = ([\varphi(A)]^t)^{-1} = ([(A^{-1})^t]^t)^{-1} = (A^{-1})^{-1} = A$$

and φ is its own inverse. In particular, it is invertible. Furthermore,

$$\varphi(A)\varphi(B) = (A^t)^{-1}(B^t)^{-1} = (B^tA^t)^{-1} = ((AB)^t)^{-1} = \varphi(AB)$$

Hence φ is also a homomorphism, therefore it is an isomorphism. □

6.9

Prove that a group G and its opposite group G° (Exercise 2.6) are isomorphic.

Solution.

Proof.
For reference, G° has the same underlying set as G with group operation $a * b = ba$. Define

$$\varphi : G \to G^\circ, \qquad a \mapsto a^{-1}$$

Then we have for any $a, b \in G$

$$\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = \varphi(b)\varphi(a) = \varphi(a) * \varphi(b)$$

Thus φ is a homomorphism. Furthermore it is clearly also invertible [$\psi : G^\circ \to G, \psi(b) = b^{-1}$ is the inverse, which is not *exactly* φ]. Therefore φ is an isomorphism and $G \cong G^\circ$. □

6.10

Find all automorphisms of

(a) a cyclic group of order 10.

(b) the symmetric group S_3.

Solution.

(a) Let $G = \langle x \rangle = \{1, x, \ldots, x^9\}$ be a cyclic group of order 10 and let $\varphi : G \to G$ be an automorphism. Note that φ is completely determined by where it sends x, and since it is an isomorphism it must send x to a generator of G. From Exercise 4.6 we have that G is generated by the following elements: x, x^3, x^7, x^9. Hence we have four automorphisms

$$\varphi_1 : x \mapsto x \qquad \varphi_2 : x \mapsto x^3 \qquad \varphi_3 : x \mapsto x^7 \qquad \varphi_4 : x \mapsto x^9$$

(b) Since $S_3 = \langle (12), (123) \rangle$, any automorphism $\psi : S_3 \to S_3$ is completely determined by where it sends the generators. Furthermore, as an isomorphism $\psi(\sigma)$ must preserve the order of σ. In particular, $\psi((12))$ must have order 2 and $\psi((123))$ must have order 3. Hence there are three possible values of $\psi((12))$ and two possible values of $\psi((123))$, leaving at most six possible automorphisms.

However, S_3 has six elements and for each permutation $\sigma \in S_3$ we have the "conjugate by σ" automorphism $c_\sigma : S_3 \to S_3, \quad c_\sigma(\tau) = \sigma\tau\sigma^{-1}$. Furthermore, each of these automorphisms are distinct since if $c_{\sigma_1} = c_{\sigma_2}$, then in particular we have for any $\tau \in S_3$ that

$$c_{\sigma_1}(\tau) = c_{\sigma_2}(\tau) \implies \sigma_1\tau\sigma_1^{-1} = \sigma_2\tau\sigma_2^{-1} \implies \sigma_2^{-1}\sigma_1\tau = \tau\sigma_2^{-1}\sigma_1 \implies \sigma_2^{-1}\sigma_1 \in Z(S_3)$$

However, $Z(S_3) = \{\mathrm{id}\}$ (e.g. by examining the multiplication table in Exercise 2.1) and thus $\sigma_2^{-1}\sigma_1 = \mathrm{id} \implies \sigma_1 = \sigma_2$. Therefore $c_{\sigma_1} = c_{\sigma_2}$ if and only if $\sigma_1 = \sigma_2$, so we have six distinct automorphisms which must be all of them by the upper bound shown above. Explicitly,

$$\psi_1 : \sigma \mapsto \sigma \qquad \psi_2 : \sigma \mapsto (12)\sigma(12) \qquad \psi_3 : \sigma \mapsto (13)\sigma(13)$$

$$\psi_4 : \sigma \mapsto (23)\sigma(23) \qquad \psi_5 : \sigma \mapsto (123)\sigma(132) \qquad \psi_6 : \sigma \mapsto (132)\sigma(123)$$

6.11

Let a be an element of a group G. Prove that if the set $\{1, a\}$ is a normal subgroup of G, then a is in the center of G.

Solution.

Proof.
Suppose $\{1, a\} \lhd G$. By definition for any $g \in G$ we have $gag^{-1} \in \{1, a\}$. However, if there exists g' such that $g'ag'^{-1} = 1$, then

$$g'ag'^{-1} = 1 \implies g'a = g' \implies a = 1$$

and clearly $1 \in Z(G)$. Otherwise, we have for all $g \in G$ that

$$gag^{-1} = a \implies ga = ag \implies a \in Z(G)$$

□

§7 - Equivalence Relations and Partitions

7.1

Let G be a group. Prove that the relation $a \sim b$ if $b = gag^{-1}$ for some g in G is an equivalence relation on G.

Solution.

Proof.
We check each axiom:

- Suppose $a \sim b$ and $b \sim c$. Then there exists $g_1, g_2 \in G$ such that $b = g_1 a g_1^{-1}$ and $c = g_2 b g_2^{-1}$. Then
$$c = g_2 b g_2^{-1} = g_2(g_1 a g_1^{-1})g_2^{-1} = (g_2 g_1)a(g_2 g_1)^{-1} \implies a \sim c$$
- Suppose that $a \sim b$. Then there exists $g \in G$ such that $b = gag^{-1}$. This implies
$$a = g^{-1}ag = g^{-1}a(g^{-1})^{-1} \implies b \sim a$$
- Choose $a \in G$. Then
$$a = 1a1 = 1a1^{-1} \implies a \sim a$$

Therefore $\sim$ is an equivalence relation. □

7.2

An equivalence relation on S is determined by the subset R of the set $S \times S$ consisting of those pairs (a, b) such that $a \sim b$. Write the axioms for an equivalence relation in terms of the subset R.

Solution.
We can write our axioms as follows:

- Transitivity: If $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.
- Symmetry: If $(a, b) \in R$, then $(b, a) \in R$.
- Reflexivity: For every $a \in S$, $(a, a) \in R$.

7.3

With the notation of Exercise 7.2, is the intersection $R \cap R'$ of two equivalence relations R and R' an equivalence relation? Is the union?

Solution.
We claim $R \cap R'$ is an equivalence relation. We check each axiom:

- Suppose $(a, b), (b, c) \in R \cap R'$. Then

$$(a, b), (b, c) \in R \implies (a, c) \in R$$

  and similarly for R'. Thus $(a, c) \in R \cap R'$.

- Suppose $(a, b) \in R \cap R'$. Then

$$(a, b) \in R \implies (b, a) \in R$$

  and similarly for R'. Thus $(b, a) \in R \cap R'$.

- We have for every $a \in S$ that $(a, a) \in R$ and $(a, a) \in R'$. Thus $(a, a) \in R \cap R'$ for all $a \in S$.

Therefore $R \cap R'$ is an equivalence relation.

However, $R \cup R'$ is not necessarily an equivalence relation. Consider the following:
Let $S = \{a, b, c\}$ and set

$$R = \{(a, a), (b, b), (c, c), (a, b), (b, a)\} \qquad R' = \{(a, a), (b, b), (c, c), (b, c), (c, b)\}$$

Then both are equivalence relations and we have

$$R \cup R' = \{(a, a), (b, b), (c, c), (a, b), (b, a), (b, c), (c, b)\}$$

Now $(a, b) \in R \cup R'$ and $(b, c) \in R \cup R'$ but $(a, c) \notin R \cup R'$, so transitivity fails and $R \cup R'$ is not an equivalence relation.

7.4

A relation R on the set of real numbers can be thought of as a subset of the (x, y)-plane. With the notation of Exercise 7.2, explain the geometric meaning of the reflexive and symmetric properties.

Solution.
Thinking of R as a subset of $\mathbb{R}^2$, the reflexive property tells us that the entire line $y = x$ will be in our subset. The symmetric property tells us that our subset is symmetric across this line $y = x$: If a point (a, b) is in our subset, then so is the point (b, a).

7.5

With the notation of Exercise 7.2, each of the following subsets R of the (x, y)-plane defines a relation on the set $\mathbb{R}$ of real numbers. Determine which of the axioms are satisfied:

(a) The set $\{(s, s) \mid s \in \mathbb{R}\}$

(b) The empty set

(c) The locus $\{xy + 1 = 0\}$

(d) The locus $\{x^2y - xy^2 - x + y = 0\}$

Solution.

(a)
- Transitivity: Holds, since $(a, b), (b, c) \in R$ forces $a = b = c$ and so $(a, c) = (a, a) \in R$.
- Symmetry: Holds, since $(a, b) \in R$ forces $b = a$ and so $(b, a) = (a, a) \in R$.
- Reflexivity: Holds, since for every $s \in \mathbb{R}$ we have by construction $(s, s) \in R$.

(b)
- Transitivity: Holds, vacuously.
- Symmetry: Holds, vacuously.
- Reflexivity: Fails, since $(1, 1) \notin R$.

(c)
- Transitivity: Fails, since $(1, -1) \in R$ and $(-1, 1) \in R$ but $(1, 1) \notin R$.
- Symmetry: Holds, since if $ab + 1 = 0$, then $ba + 1 = 0$.
- Reflexivity: Fails, since $(1, 1) \notin R$.

(d)
- Transitivity: Holds. Note that we can write

$$x^2y - xy^2 - x + y = xy(x - y) - 1(x - y) = (xy - 1)(x - y)$$

  Then if $(ab-1)(a-b) = (bc-1)(b-c) = 0$, then either $a = b \implies (ac-1)(a-c) = 0$, or $a = \frac{1}{b}$, which combined with $b = c$ or $b = \frac{1}{c}$ gives $(ac - 1)(a - c) = 0$.
- Symmetry: Holds, since if $x^2y - xy^2 - x + y = 0$, then

$$y^2x - yx^2 - y + x = -(-y^2x + yx^2 + y - x) = -(x^2y - xy^2 - x + y) = -0 = 0$$

- Reflexivity: Holds, since $x = y$ implies

$$x^2y - xy^2 - x + y = y^3 - y^3 - y + y = 0$$

7.6

How many different equivalence relations can be defined on a set of five elements?

Solution.
Let $S = \{a, b, c, d, e\}$. By Prop 2.7.4, equivalence relations and partitions of S are the same, so we look at the number of ways to partition S, where we go by "bin sizes":

- $1+1+1+1+1$: There is only one such partition.
- $2+1+1+1$: There are $\binom{5}{2} = 10$ ways to break down S like so.
- $2+2+1$: There are $\frac{1}{2}(\binom{5}{2} \cdot \binom{3}{2}) = 15$ such partitions.
- $3+1+1$: There are $\binom{5}{3} = 10$ such partitions.
- $3+2$: There are $\binom{5}{3} = 10$ such partitions.
- $4+1$: There are $\binom{5}{4} = 5$ such partitions.
- 5: There is only one such partition.

In total, this gives $1+10+15+10+10+5+1 = 52$ different partitions of S.

§8 - Cosets

8.1

Let H be the cyclic subgroup of A_4 generated by the permutation (123). Exhibit the left and right cosets of H explicitly.

Solution.
We can write out all of A_4 in cycle notation:

$$A_4 = \{\mathrm{id}, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

and we have the subgroup $H = \langle(123)\rangle = \{\mathrm{id}, (123), (132)\}$.
Note that $|A_4| = \frac{1}{2}(4!) = 12$ and $|H| = 3$. Therefore we have $[A_4 : H] = 12/3 = 4$ cosets.
The four left cosets are:

1. $\{\mathrm{id}, (123), (132)\} = \mathrm{id}\, H = (123)H = (132)H$
2. $\{(124), (14)(23), (134)\} = (124)H = (14)(23)H = (134)H$
3. $\{(142), (234), (13)(24)\} = (142)H = (234)H = (13)(24)H$
4. $\{(143), (12)(34), (243)\} = (143)H = (12)(34)H = (243)H$

The four right cosets are:

1. $\{\mathrm{id}, (123), (132)\} = H\,\mathrm{id} = H(123) = H(132)$
2. $\{(124), (13)(24), (243)\} = H(124) = H(13)(24) = H(243)$
3. $\{(142), (143), (14)(23)\} = H(142) = H(143) = H(14)(23)$
4. $\{(134), (234), (12)(34)\} = H(134) = H(234) = H(12)(34)$

8.2

In the additive group $\mathbb{R}^m$ of vectors, let W be the set of solutions of a system of homogeneous linear equations $AX = 0$. Show that the set of solutions of an inhomogeneous system $AX = B$ is either empty, or else it is an (additive) coset of W.

Solution.

Proof.
Let $S \subset \mathbb{R}^m$ be the solution set to $AX = B$, and suppose that $S \neq \varnothing$. Then there exists $\bar{x} \in \mathbb{R}^m$ such that $A\bar{x} = B$. We claim that $S = W + \bar{x}$.
Choose $w + \bar{x} \in W + \bar{x}$. Then we have $Aw = 0$ which implies

$$A(w + \bar{x}) = Aw + A\bar{x} = 0 + B = B \implies w + \bar{x} \in S \implies W + \bar{x} \subset S$$

Now choose $s \in S$. Note that

$$A(s - \bar{x}) = As - A\bar{x} = B - B = 0 \implies (s - \bar{x}) \in W \implies s = (s - \bar{x}) + \bar{x} \in W + \bar{x} \implies S \subset W + \bar{x}$$

Therefore $S = W + \bar{x}$ is a coset of W. □

8.3

Does every group whose order is a power of a prime p contain an element of order p?

Solution.
We claim yes.

Proof.
Let G be a group of order p^n. We use strong induction on n.
Base: $n = 1$. Then by Corollary 2.8.11, G is cyclic and any generator a has order $|G| = p$.
IH: Assume any group of order p^k $(k < n)$ has an element of order p. Choose an element $a \in G$ that is not the identity. Then consider the subgroup $\langle a \rangle \leq G$. We consider cases:

- a does not generate G: Then the order of a divides p^n but is not equal to it, thus it has order p^k for $k < n$. Then by IH $\langle a \rangle$ has an element b of order p, which is also an element of G.
- $G = \langle a \rangle$: Then set $k = p^{n-1}$ and $b = a^k$. We claim b has order p. Note that since $k = p^{n-1}$, it is not the order of a so $b = a^k \neq 1$. Furthermore, the order of b must divide p^n, and

  $$b^p = (a^k)^p = a^k p = a^{p^n} = 1$$

  which is the smallest $(\neq 1)$ divisor of p^n, so it must be the order of b.

Therefore in both cases we can find an element $b \in G$ with order p. □

8.4

Does a group of order 35 contain an element of order 5? of order 7?

Solution.
We claim yes, both elements always exist.

Proof.
Take a group G of order 35. If $G = \langle x \rangle$ is cyclic, then x^7 has order 5 and x^5 has order 7. Otherwise, assume that G is not cyclic, i.e. has no element of order 35. Choose a nonidentity element $x \in G$. By assumption $\langle x \rangle \neq G$, but the order of x must divide $35 = 5 \cdot 7$, so it is either order 5 or 7. Consider cases:

- $|\langle x \rangle| = 5$: Suppose that G has no elements of order 7. In particular this means that every nonidentity element has order 5. Furthermore, for any nonidentity $y \in G$, note that $\langle x \rangle \cap \langle y \rangle$ is a subgroup of $\langle x \rangle$ (see Exercise 5.2). Since 5 is prime, by Lagrange either $\langle x \rangle \cap \langle y \rangle = \{1\}$ or $\langle x \rangle = \langle y \rangle$. In the first case, the elements y, y^2, y^3, y^4 are all distinct from those in $\langle x \rangle$. However, since every nonidentity element of G has order 5, we can write G as the union of these cyclic subgroups of order 5, say n of them, by taking y from $G \setminus \langle x \rangle$, then z from $G \setminus (\langle x \rangle \cup \langle y \rangle)$, and so on. Then we have

  $$G = \{1\} \cup \langle y_1 \rangle \cup \langle y_2 \rangle \cup \cdots \cup \langle y_n \rangle, \quad \text{where } \langle y_i \rangle \cap \langle y_j \rangle = \{1\} \quad (i \neq j)$$

  But since each of these cyclic subgroups have 4 distinct elements, this implies that $35 = |G| = 1 + 4n$, which implies $n = 34/4 \notin \mathbb{Z}$ and is a contradiction. Thus G has an element of order 7.

- $|\langle x \rangle| = 7$: Again, suppose that G has no elements of order 5. The same argument above applies, where we have

  $$G = \{1\} \cup \langle y_1 \rangle \cup \langle y_2 \rangle \cup \cdots \cup \langle y_n \rangle, \quad \text{where } \langle y_i \rangle \cap \langle y_j \rangle = \{1\} \quad (i \neq j)$$

  but with the change that each $\langle y_i \rangle$ will now contribute 6 distinct elements. Therefore we have $35 = 1 + 6n$, which forces n to be a non-integer and is a contradiction. Thus G has an element of order 5.

Therefore G has elements of order 5 and 7. □

8.5

A finite group contains an element x of order 10 and also an element y of order 6. What can be said about the order of G?

Solution.
Let $|G| = n$. By Lagrange we immediately have 6 and 10 both divide n. Therefore their least common multiple $\operatorname{lcm}(6, 10) = 30$ also divides n. Hence $n = 30k$ for some positive integer k. This necessary condition is also a sufficient condition, since for every cyclic group $G = \langle g \rangle$ of order $30k$, the elements $x = g^{3k}$ and $y = g^{5k}$ have orders 10 and 6 respectively.

8.6

Let $\varphi : G \to G'$ be a group homomorphism. Suppose that $|G| = 18, |G'| = 15$, and that φ is not the trivial homomorphism. What is the order of the kernel?

Solution.
We immediately have $|\operatorname{im}\varphi| \neq 1$ since φ is not trivial. From Corollary 2.8.13, we know that $18 = |G| = |\ker\varphi| \cdot |\operatorname{im}\varphi|$ and that $|\operatorname{im}\varphi|$ divides $|G'| = 15$. In particular,

$$|\operatorname{im}\varphi| \mid 18 = 2 \cdot 3^2 \text{ and } |\operatorname{im}\varphi| \mid 15 = 3 \cdot 5 \implies |\operatorname{im}\varphi| = 3$$

Therefore

$$|\ker\varphi| = \frac{|G|}{|\operatorname{im}\varphi|} = \frac{18}{3} = 6$$

8.7

A group G of order 22 contains elements x and y, where $x \neq 1$ and y is not a power of x. Prove that the subgroup generated by these elements is the whole group G.

Solution.

Proof.
Let $H = \langle x, y \rangle \leq G$ and $I = \langle x \rangle \leq H$. By assumption we have $I, H \neq \{1\}$ (since $x \neq 1$) and $H \neq I$ (since $y \neq x^k$). In particular, we have

$$\{1\} \subsetneq I \subsetneq H \subseteq G \tag{$\star$}$$

By Lagrange, we have that $|I|$ divides $|G| = 22 = 2 \cdot 11$ and $(\star)$ says that $|I| \neq 1$ and $|I| \neq 22$. We consider cases

- $|I| = 2$: Now since H is a subgroup of G, it has order that divides 22. However, since $H \neq I$ we have $|H| \neq 2$ and since $2 = |I|$ must divide $|H|$ we also have $|H| \neq 11$. Therefore $|H| = 22$.
- $|I| = 11$: Since $I \subsetneq H$, we have $11 = |I| < |H|$. The only possible value of $|H|$ $(= 2, 11, 22$ from Lagrange) that satisfies this is $|H| = 22$.

In both cases, H has order 22 which forces $\langle x, y \rangle = H = G$. □

8.8

Let G be a group of order 25. Prove that G has at least one subgroup of order 5, and that if it contains only one subgroup of order 5, then it is a cyclic group.

Solution.

Proof.
By Exercise 8.3 we have G has an element x of order 5, so G has a subgroup $\langle x \rangle$ of order 5.

Now suppose that $\langle x \rangle \leq G$ is the only subgroup of order 5. Then choose a nonidentity element $y \in G \setminus \langle x \rangle$. The order of y must divide $|G| = 25$, but it cannot have order 5 since $\langle y \rangle$ would be another subgroup of order 5. This forces y to have order 25, in which case it generates all of G and $G = \langle y \rangle$ is cyclic. □

8.9

Let G be a finite group. Under what circumstances is the map $\varphi : G \to G$ defined by $\varphi(x) = x^2$ an automorphism of G?

Solution.
We first check when φ is a homomorphism:

$$\varphi(x)\varphi(y) = \varphi(xy) \iff xxyy = xyxy \iff xy = yx$$

so we need G to be abelian. Next,

$$\varphi(x) = 1 \iff x^2 = 1$$

So for φ to be injective we need G to not have an element of order 2, which is equivalent to saying that G does not have an even order (see Exercise M.2). Finally, since G is a finite group we have φ injective $\implies$ φ surjective.

Therefore φ is an automorphism if and only if G is an abelian group with odd order.

8.10

Prove that every subgroup of index 2 is a normal subgroup, and show by example that a subgroup of index 3 need not be normal.

Solution.

Proof.
Let G be a group and $H \leq G$ be a subgroup of index 2, which by definition means that H has two cosets. For any $g \in G$, we have the cosets gH and Hg. We consider cases:

- $g \in H$: Then $gH = H = Hg$.
- $g \notin H$: Then $gH \neq H$ and $Hg \neq H$. But since H only has two cosets and one is H itself, this forces $gH = Hg$.

Therefore in both cases we have $gH = Hg \implies gHg^{-1} = H \implies H \lhd G$. □

For a counterexample for index 3, let $G = S_3$ and $H = \{\mathrm{id}, (12)\}$. Note that

$$[G : H] = \frac{|G|}{|H|} = \frac{6}{2} = 3$$

so H has index 3, but it is not a normal subgroup since

$$(123)(12)(123)^{-1} = (123)(12)(132) = (123)(13) = (23) \notin H$$

8.11

Let G and H be the following subgroups of $GL_2(\mathbb{R})$:

$$G = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \right\}, \quad H = \left\{ \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} \right\},$$

with x and y real and $x > 0$. An element of G can be represented by a point in the right half plane. Make sketches showing the partitions of the half plane into left cosets and into right cosets of H.

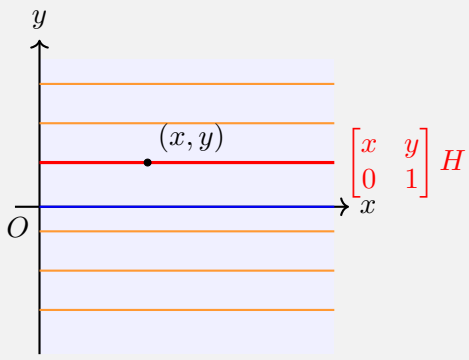
Solution.
We have left cosets:

$$\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ax & y \\ 0 & 1 \end{bmatrix} \in \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} H$$

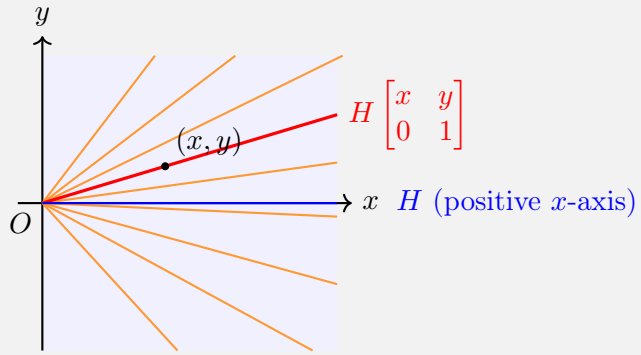
which as we vary elements of H, i.e. the value of $a > 0$, we are keeping y constant and so the coset becomes a horizontal line.
We also have right cosets:

$$\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ax & ay \\ 0 & 1 \end{bmatrix} \in H \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}$$

which as we vary the value of a, the coset becomes a line from the origin through (x, y).
We sketch a few of these cosets in orange and red below:



Left cosets: horizontal lines



Right cosets: rays from the origin

8.12

Let S be a subset of a group G that contains the identity element 1, and such that the left cosets aS, with a in G, partition G. Prove that S is a subgroup of G.

Solution.

Proof.
We show by definition:

- Choose $s_1, s_2 \in S$. Then we have $s_1 \in G, s_2 \in S$ and so $s_1 s_2$ is in the left coset $s_1 S$. However, since $s_1 \in S$, we have that $s_1 S = S$. Thus $s_1 s_2 \in S$ and we have closure.
- It is given that the identity 1 is in S.
- Choose $s \in S$. Then the inverse s^{-1} exists in G, and so $1 = s^{-1}s \in s^{-1}S$. However, since $1 \in S$ and the cosets partition G, this means that $s^{-1}S = S$. Thus $s^{-1} \in S$ are we are closed under inverses.

Therefore by definition $S \leq G$. □

8.13

Let S be a set with a law of composition. A partition $\Pi_1 \cup \Pi_2 \cup \dots$ of S is *compatible* with the law of composition if for all i and j, the product set

$$\Pi_i \Pi_j = \{xy \mid x \in \Pi_i, y \in \Pi_j\}$$

is contained in a single subset Π_k of the partition.

(a) The set $\mathbb{Z}$ of integers can be partitioned into three sets [Pos], [Neg], [$\{0\}$]. Discuss the extent to which the laws of composition $+$ and $\times$ are compatible with this partition.

(b) Describe all partitions of the integers that are compatible with the operation $+$.

Solution.

(a) First, we look at addition $+$. Our "products" are really additions, so we use the notation $\Pi_i + \Pi_j$. Note that [Pos] + [Neg] is not contained in only one subset, since $1 + (-2) \in$ [Neg] and $2 + (-1) \in$ [Pos], so the partition is not compatible with $+$.
Next, we look at multiplication $\times$. We look at (pairwise, as $\times$ is commutative) products:

- [Pos][Neg] is all products of a positive number with a negative number, which is always negative so [Pos][Neg] $\subset$ [Neg]
- [Neg][Neg] is all products of a negative number with a negative number, which is always positive so [Neg][Neg] $\subset$ [Pos]
- [Pos][Pos] $\subset$ [Pos]
- Clearly [Pos][$\{0\}$], [Neg][$\{0\}$], and [$\{0\}$][$\{0\}$] are all contained in [$\{0\}$]

Therefore $\times$ is compatible with this partition.

(b) Suppose $\Pi_1, \Pi_2, \dots$ is a partition compatible with addition, i.e. for each i and integer a, there exists some j such that

$$x \in \Pi_i \implies (x + a) \in \Pi_j$$

In other words, adding any integer a translates the entire subset Π_i into another subset. We can apply this translation invariance when we repeatedly add 1 to a some integer x, as this new integer moves to another subset. If the partition has only finitely many subsets, eventually $x, x+1, x+2, \dots$ must end back in a previously-visited subset, say after n steps. Then $x + n$ is in the same Π_i as x. However by translation invariance, the same must be true for every integer, so the partition groups together all integers that differ by multiples of n, which is simply congruence modulo n.

Another possibility is that if the partition has infinitely many Π_i's, then this wrap-around never occurs, and adding 1 keeps sending integers to different subsets, which is only possible if each subset contains a single integer. Finally, it is possible that adding 1 always remains in the same subset, in which case the partition is simply all of $\mathbb{Z}$. Therefore all partitions of $\mathbb{Z}$ compatible with $+$ are:

- $\Pi = \mathbb{Z}$
- $\Pi_i = \{i\}$ for all $i \in \mathbb{Z}$
- $\Pi_i = \{x \in \mathbb{Z} \mid x \equiv i \mod n\}$ for $i = 0, \dots, n-1$.

§9 - Modular Arithmetic

9.1

For which integers n does 2 have a multiplicative inverse in $\mathbb{Z}/\mathbb{Z}n$?

Solution.
We want to solve $2x \equiv 1 \mod n$. Equivalently, we want to find $k \in \mathbb{Z}$ such that $2x + nk = 1$. This is true if and only if $\gcd(2, n) = 1$ (Corollary 2.3.6), which is true if and only if n is odd.

9.2

What are the possible values of a^2 modulo 4? modulo 8?

Solution.
It suffices to only look at values of a modulo 4 and 8:
(i): Modulo 4, we have

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 0,\ 3^2 \equiv 1$$

Hence the possible values are 0 and 1.
(ii): Modulo 8, we have

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 1,\ 4^2 \equiv 0,\ 5^2 \equiv 1,\ 6^2 \equiv 4,\ 7^2 \equiv 1$$

Hence the possible values are 0, 1, and 4.

9.3

Prove that every integer a is congruent to the sum of its decimal digits modulo 9.

Solution.

Proof.
Writing our integer a digit-by-digit, we have

$$a = d_n \cdot 10^n + \cdots + d_1 \cdot 10 + d_0$$

since $10 \equiv 1 \mod 9$, we have

$$a \equiv d_n \cdot 1^n + \cdots + d_1 \cdot 1 + d_0 \equiv d_n + \cdots + d_1 + d_0 \mod 9$$

which is exactly the sum of its digits. □

9.4

Solve the congruence $2x \equiv 5$ modulo 9 and modulo 6.

Solution.
(i) We have the table

x		0	1	2	3	4	5	6	7	8
$2x$	mod 9	0	2	4	6	8	1	3	5	7

Hence the only solution is $x = 7$.

(ii) We have the table

x		0	1	2	3	4	5
$2x$	mod 6	0	2	4	0	2	4

Hence we have no solutions.

9.5

Determine the integers n for which the pair of congruences $2x - y \equiv 1$ and $4x + 3y \equiv 2$ modulo n has a solution.

Solution.
Note that

$$2x - y \equiv 1 \iff 6x - 3y \equiv 3 \iff -4x + 2y \equiv -2 \mod n$$

Hence adding these last two congruences to $4x + 3y \equiv 2$ gives the system

$$\begin{cases} 10x \equiv 5 \mod n \\ 5y \equiv 0 \mod n \end{cases}$$

Note that if n is even, then the first congruence has no solution (if it did, then there exists k such that $10x + nk = 5$, but the LHS is even and RHS is odd). By Exercise 9.1, if n is odd there exists x such that

$$2x \equiv 1 \mod n \implies 10x \equiv 5 \mod n$$

Hence the first congruence has a solution if and only if n is odd. The second congruence will always have a solution, namely $y = n$. Therefore the pair of congruences has a solution if and only if n is odd.

9.6

Prove the *Chinese Remainder Theorem*: Let a, b, u, v be integers, and assume that the greatest common divisor of a and b is 1. Then there is an integer x such that $x \equiv u$ modulo a and $x \equiv v$ modulo b.
Hint: Do the case $u = 0$ and $v = 1$ first.

Solution.

Proof.
Suppose that $u = 0$ and $v = 1$. Since $\gcd(a, b) = 1$, there exists integers r and s such that $ra + sb = 1$. Now set $x = ra$. Then

$$\begin{cases} x = ra & \implies x \equiv 0 \mod a \\ x = 1 - sb & \implies x \equiv 1 \mod b \end{cases}$$

Hence we have our desired x.

Now suppose u and v are arbitrary integers.
By the argument above, there exists integers x_1 and x_2 such that

$$\begin{cases} x_1 \equiv 0 \mod a \\ x_1 \equiv 1 \mod b \end{cases} \quad \text{and} \quad \begin{cases} x_2 \equiv 1 \mod a \\ x_2 \equiv 0 \mod b \end{cases}$$

Now set $x = ux_2 + vx_1$. Then working modulo a we have

$$x \equiv u \cdot 1 + v \cdot 0 \equiv u$$

and working modulo b we have

$$x \equiv u \cdot 0 + v \cdot 1 \equiv v$$

Hence we have our desired x. □

9.7

Determine the order of each of the matrices $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ when the matrix entries are interpreted modulo 3.

Solution.
We have, working modulo 3,

$$A \equiv \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad A^2 \equiv \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad A^3 \equiv \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Hence A has order 3.

Next, we have modulo 3

$$B \equiv \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad B^2 \equiv \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \quad B^3 \equiv \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix} \equiv \begin{bmatrix} 0 & 2 \\ 2 & 1 \end{bmatrix}, \quad B^4 \equiv \begin{bmatrix} 2 & 0 \\ 3 & 2 \end{bmatrix} \equiv \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \quad B^5 \equiv \begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix}$$

$$B^6 \equiv \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} \equiv \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}, \quad B^7 \equiv \begin{bmatrix} 3 & 1 \\ 4 & 2 \end{bmatrix} \equiv \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}, \quad B^8 \equiv \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Hence B has order 8.

§10 - The Correspondence Theorem

10.1

Describe how to tell from the cycle decomposition whether a permutation is odd or even.

Solution.
A permutation is odd if and only if its cycle decomposition has an odd number of even-length cycles. This is because a cycle of length n can be written as $n-1$ transpositions, so every even-length cycle can be written as an odd number of transpositions and each additional even-length cycle will flip the parity.

10.2

Let H and K be subgroups of a group G.

(a) Prove that the intersection $xH \cap yK$ of two cosets of H and K is either empty or else is a coset of the subgroup $H \cap K$.

(b) Prove that if H and K have finite index in G then $H \cap K$ also has finite index in G.

Solution.

(a) *Proof.*
Suppose that $xH \cap yK$ is not empty (otherwise we are done). Then we can choose an element g from it and can write $g = xh_0 = yk_0$. We claim that $xH \cap yK = g(H \cap K)$.

- Choose $z \in xH \cap yK$. Then we can write $z = xh = yk$. However, $x = gh_0^{-1}$ and $y = gk_0^{-1}$, so we have

$$z = xh = g(h_0^{-1}h) \quad \text{and} \quad z = yk = g(k_0^{-1}k)$$

  Thus setting $h_1 = h_0^{-1}h \in H, k_1 = k_0^{-1}k \in K$ we have

$$gh_1 = z = gk_1 \implies h_1 = k_1 \in H \cap K \implies z \in g(H \cap K)$$

  thus $xH \cap yK \subset g(H \cap K)$.
- Choose $gj \in g(H \cap K)$. Then

$$j \in H \implies h_0 j \in H \implies gj = (xh_0)j = x(h_0 j) \in xH$$

  and

$$j \in K \implies k_0 j \in K \implies gj = (yk_0)j = y(k_0 j) \in yK$$

  Thus $gj \in xH \cap yK$ and $g(H \cap K) \subset xH \cap yK$.

Therefore $xH \cap yK$ is a coset of $H \cap K$. □

(b) *Proof.*
Since cosets partition G, let $X, Y \subset G$ be sets such that $|X| = [G : H], |Y| = [G : K]$, and

$$G = \bigcup_{x \in X} xH = \bigcup_{y \in Y} yK$$

In particular, this means that for every $g \in G$ there exists $x_i \in X$ and $y_j \in Y$ such that $g \in x_iH$ and $g \in y_jK$, i.e. $g \in x_iH \cap y_jK$. Thus the union of the $x_iH \cap y_jK$'s covers G:

$$G = \bigcup_{x_i \in X, y_j \in Y} x_iH \cap y_jK$$

From (a), each $x_iH \cap y_jK$ is either empty or a coset of $H \cap K$, and since we cover all of G all cosets are present. Furthermore, there are at most $|X| \cdot |Y|$ cosets here, which is finite since $|X|$ and $|Y|$ are both finite by assumption. Therefore by definition

$$[G : H \cap K] \leq |X| \cdot |Y| < \infty$$

□

10.3

Let G and G' be cyclic groups of order 12 and 6, generated by elements x and y, respectively, and let $\varphi : G \to G'$ be the map defined by $\varphi(x^i) = y^i$. Exhibit the correspondence referred to in the Correspondence Theorem explicitly.

Solution.
Note that $K = \ker \varphi = \{1, x^6\}$. The subgroups of G that contain K are corresponded with:

$$\begin{aligned} G = \langle x \rangle &\leftrightsquigarrow \langle y \rangle = G' \\ \langle x^2 \rangle &\leftrightsquigarrow \langle y^2 \rangle \\ \langle x^3 \rangle &\leftrightsquigarrow \langle y^3 \rangle \\ K = \langle x^6 \rangle &\leftrightsquigarrow \langle 1 \rangle = \{1\} \end{aligned}$$

and as expected, the subgroups of G' are corresponded with:

$$\begin{aligned} \{1\} &\leftrightsquigarrow \varphi^{-1}(\{1\}) = K \\ \langle y^3 \rangle &\leftrightsquigarrow \varphi^{-1}(\{1, y^3\}) = \{1, x^3, x^6, x^9\} = \langle x^3 \rangle \\ \langle y^2 \rangle &\leftrightsquigarrow \varphi^{-1}(\{1, y^2, y^4\}) = \{1, x^2, x^4, x^6, x^8, x^{10}\} = \langle x^2 \rangle \\ G' = \langle y \rangle &\leftrightsquigarrow \varphi^{-1}(G') = \langle x \rangle = G \end{aligned}$$

10.4

With the notation of the Correspondence Theorem, let H and H' be corresponding subgroups. Prove that $[G : H] = [G' : H']$.

Solution.

Proof.
Let $\varphi : G \to G'$ be a surjective homomorphism and $H \leq G, H' \leq G'$ be subgroups that correspond, i.e. $H' = \varphi(H)$ and $H = \varphi^{-1}(H)$. We claim that the map ψ that sends a coset gH to $\varphi(g)H'$ is a bijection.

- First, we need to check that ψ is well-defined on cosets. If $g_1H = g_2H$, then we have $g_2^{-1}g_1H = H \implies g_2^{-1}g_1 \in H$. Then we have $\varphi(g_2^{-1}g_1) \in \varphi(H) = H'$, so

  $$\varphi(g_2^{-1}g_1)H' = H' \implies \varphi(g_2)^{-1}\varphi(g_1)H' = H' \implies \varphi(g_1)H' = \varphi(g_2)H' \implies \psi(g_1) = \psi(g_2)$$

  Thus ψ is well-defined.

- Note that for any coset $g'H'$, since φ is surjective there exists $g \in G$ such that $\varphi(g) = g'$, and so $\psi(gH) = g'H'$ and ψ is surjective.

- Suppose that $\psi(g_1) = \psi(g_2)$. Then we have

  $$\varphi(g_1)H' = \varphi(g_2)H' \implies H' = \varphi(g_2)^{-1}\varphi(g_1)H' = \varphi(g_2^{-1}g_1)H' \implies \varphi(g_2^{-1}g_1) \in H'$$

  which implies (see the bullet points (2.8.5)) that

  $$g_2^{-1}g_1 \in \varphi^{-1}(H') = H \implies g_1 \in g_2H \implies g_1H = g_2H$$

  Thus ψ is injective.

Therefore we have a bijection between the cosets of H and the cosets of H', so in particular we have $[G : H] = [G' : H']$. □

10.5

With reference to the homomorphism $S_4 \to S_3$ described in Example 2.5.13, determine the six subgroups of S_4 that contain K.

Solution.
By the Correspondence Theorem, we can start with the six subgroups of S_3 and take the inverse image of each. For reference, we have partitions of $\{1,2,3,4\}$

$$\Pi_1 = \{1,2\} \cup \{3,4\}, \quad \Pi_2 = \{1,3\} \cup \{2,4\}, \quad \Pi_3 = \{1,4\} \cup \{2,3\}$$

and our map φ sends a permutation σ of S_4 to the permutation of the set $\{\Pi_1, \Pi_2, \Pi_3\}$ (which we then think of as an element of S_3) that corresponds to how σ acts on the 2-element subsets of $\{1,2,3,4\}$. We also have

$$K = \ker \varphi = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$$

We now go through each subgroup of S_3:

1. S_3: Since φ is surjective, we have $\varphi^{-1}(S_3) = S_4$.
2. $\{\mathrm{id}\}$: By definition of kernel, we have $\varphi^{-1}(\{\mathrm{id}\}) = K$.
3. $\{\mathrm{id}, (12)\}$: We now want to find all $\sigma \in S_4$ that act as the transposition $(\Pi_1\Pi_2)$ and fixes Π_3. These are $\sigma = (23)$, $\sigma = (14)$, as well as $\sigma = (1243)$ and $\sigma = (1342)$. Thus we have
$$\varphi^{-1}(\{\mathrm{id}, (12)\}) = \varphi^{-1}(\{\mathrm{id}\}) \cup \varphi^{-1}(\{(12)\}) = K \cup \{(23), (14), (1243), (1342)\}$$
4. $\{\mathrm{id}, (13)\}$: Similarly, we want to swap Π_1 and Π_3 while fixing Π_2, which is achieved by $\sigma = (24), \sigma = (13)$ and $\sigma = (1234), \sigma = (1432)$. Thus we have
$$\varphi^{-1}(\{\mathrm{id}, (13)\}) = K \cup \{(24), (13), (1234), (1432)\}$$
5. $\{\mathrm{id}, (23)\}$: This is achieved with $\sigma = (34), \sigma = (12)$ and $\sigma = (1324), \sigma = (1423)$. Thus
$$\varphi^{-1}(\{\mathrm{id}, (23)\}) = K \cup \{(34), (12), (1324), (1423)\}$$
6. $\{\mathrm{id}, (123), (132)\}$: Now we want to find permutations that leave no Π_i fixed. Breaking it up, we have
$$\varphi^{-1}(\{(123)\}) = \{(234), (143), (124), (132)\}$$
and
$$\varphi^{-1}(\{(132)\}) = \{(243), (134), (142), (123)\}$$
Thus
$$\varphi^{-1}(\{\mathrm{id}, (123), (132)\}) = K \cup \{(234), (143), (124), (132)\} \cup \{(243), (134), (142), (123)\}$$
which is exactly the alternating group A_4.

This gives all subgroups of S_4 containing K.

§11 - Product Groups

11.1

Let x be an element of order r of a group G, and let y be an element of G' of order s. What is the order of (x, y) in the product group $G \times G'$?

Solution.
We claim the order of (x, y) is $\ell := \text{lcm}(r, s)$.

Proof.
Since ℓ is a multiple of r, we have $x^\ell = 1$ and since ℓ is a multiple of s, we have that $y^\ell = 1$. Thus

$$(x, y)^\ell = (x^\ell, y^\ell) = (1, 1) = 1 \in G \times G'$$

and so the order of (x, y) is at most ℓ. Next note that

$$(x, y)^k = 1 \implies (x^k, y^k) = (1, 1) \implies \begin{cases} x^k = 1 \\ y^k = 1 \end{cases} \implies \begin{cases} k = n_1 r \\ k = n_2 s \end{cases}$$

Thus k is a multiple of r and s, so by definition we have $k \geq \ell$ and that the order of (x, y) is at least ℓ.
Therefore the order of (x, y) is ℓ. □

11.2

What does Proposition 2.11.4 tell us when, with the usual notation for the symmetric group S_3, K and H are the subgroups $\langle y \rangle$ and $\langle x \rangle$?

Solution.
For reference, we have $x = (123)$ and $y = (12)$ and $f : H \times K \to S_3$ is the multiplication map $f(x^i, y^j) = x^i y^j$. Note that

- $H \cap K = \langle x \rangle \cap \langle y \rangle = \{1\}$.
- The elements of K do not commute with elements of H, since $yx = x^2 y \neq xy$.
- H has index 2, so it is a normal subgroup of S_3 (see Exercise 8.10).
- However, K is not a normal subgroup, as $xyx^{-1} = x^2 y \notin K$.

Therefore the first point lets us apply Prop 2.11.4(a) to say that f is injective; the second point lets us apply Prop 2.11.4(b) to say that f is not a homomorphism; the third point lets us apply Prop 2.11.4(c) to say that $HK \leq G$; the fourth point lets us apply Prop 2.11.4(d) to say that f is not an isomorphism.

11.3

Prove that the product of two infinite cyclic groups is not infinite cyclic.

Solution.

Proof.
Let $G = \langle x \rangle$ and $H = \langle y \rangle$ be two infinite cyclic groups, and suppose otherwise, i.e. the product is infinite cyclic, i.e. $G \times H = \langle z \rangle$. Then we can write $z = (g, h)$ for some $g \in G$ and $h \in H$. This implies that there exists m, n such that

$$\begin{cases} (x, 1) = z^m = (g^m, h^m) \\ (1, y) = z^n = (g^n, h^n) \end{cases} \implies \begin{cases} g^m = x \\ g^n = 1 \end{cases}$$

In particular, x having infinite order means that $1 \neq x^k = (g^m)^k$ for all k. However, for $k = n$ we have that $(g^m)^n = (g^n)^m = 1^m = 1$, which is a contradiction and $G \times H$ is not infinite cyclic. $\square$

11.4

In each of the following cases, determine whether or not G is isomorphic to the the product group $H \times K$.

(a) $G = \mathbb{R}^\times$, $H = \{\pm 1\}$, $K = \{\text{positive real numbers}\}$

(b) $G = \{\text{invertible upper triangular } 2 \times 2 \text{ matrices}\}$, $H = \{\text{invertible diagonal matrices}\}$, $K = \{\text{upper triangular matrices with diagonal entries } 1\}$

(c) $G = \mathbb{C}^\times$, $H = \{\text{unit circle}\}$, $K = \{\text{positive real numbers}\}$

Solution.

(a) Yes, $G \cong H \times K$. We can decompose any nonzero real number into sign and magnitude via

$$\varphi : G \to H \times K, \quad x \mapsto (\tfrac{x}{|x|}, |x|)$$

Since $|x||y| = |xy|$, we have that

$$\varphi(x)\varphi(y) = (\tfrac{x}{|x|}, |x|)(\tfrac{y}{|y|}, |y|) = (\tfrac{x}{|x|}\tfrac{y}{|y|}, |x||y|) = (\tfrac{xy}{|xy|}, |xy|) = \varphi(xy)$$

and φ is a homomorphism. It is also clearly invertible, with inverse $\psi(\pm 1, y) = \pm y$. Hence φ is an isomorphism.

Another way to show this is that ψ defined above is exactly the multiplication map, with $H \cap K = \{1\}$, ψ surjective, and $H, K \lhd G$ (since G is abelian). So by Prop 2.11.4(d) we have $G \cong H \times K$.

(b) No, $G \ncong H \times K$. Consider the map

$$\psi : H \times K \to G, \quad \left(\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}, \begin{bmatrix} 1 & b' \\ 0 & 1 \end{bmatrix} \right) \mapsto \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix} \begin{bmatrix} 1 & b' \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} d_1 & d_1 b' \\ 0 & d_2 \end{bmatrix}$$

Next note that H is not normal in G, as

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 4 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix} \notin H$$

Hence by Prop 2.11.4(d) we have that ψ is not an isomorphism.

(c) Yes, $G \cong H \times K$. Consider the map

$$\psi : H \times K \to G, \quad (e^{i\theta}, r) \mapsto re^{i\theta}$$

Note that

$$H \cap K = \{z \in \mathbb{C} \mid |z| = 1\} \cap \{x \in \mathbb{R} \mid r > 0\} = \{1\}$$

and that ψ is surjective (as it is simply polar coordinates), and that since G is abelian we have $H, K \lhd G$. Therefore by Prop 2.11.4(d) we have ψ is an isomorphism.

11.5

Let G_1 and G_2 be groups, and let Z_i be the center of G_i. Prove that the center of the product group $G_1 \times G_2$ is $Z_1 \times Z_2$.

Solution.

Proof.
Choose an element $(z_1, z_2) \in Z_1 \times Z_2$. Then for any $(g_1, g_2) \in G_1 \times G_2$, since $z_1 \in Z_1$ and $z_2 \in Z_2$ we have

$$(g_1, g_2)(z_1, z_2) = (g_1 z_1, g_2 z_2) = (z_1 g_1, z_2 g_2) = (z_1, z_2)(g_1, g_2) \implies (z_1, z_2) \in Z(G_1 \times G_2)$$

Hence $Z_1 \times Z_2 \subset Z(G_1 \times G_2)$.
Now choose $(h, h') \in Z(G_1, G_2)$. Then for any $g_1 \in G_1$, we have

$$(h, h')(g_1, 1) = (g_1, 1)(h, h') \implies (hg_1, h') = (g_1 h, h') \implies hg_1 = g_1 h$$

Hence $h \in Z_1$. A symmetric argument shows that $h' \in Z_2$. Thus we have $(h, h') \in Z_1 \times Z_2$ and so $Z(G_1 \times G_2) \subset Z_1 \times Z_2$. Therefore $Z(G_1 \times G_2) = Z_1 \times Z_2$. □

11.6

Let G be a group that contains normal subgroups of orders 3 and 5, respectively. Prove that G contains an element of order 15.

Solution.

Proof.
Let $H \lhd G$ be a normal subgroup of order 3 and $K \lhd G$ be a normal subgroup of order 5. Since 3 and 5 are prime we have that H and K are both cyclic (Corollary 2.8.11), so write $H = \langle h \rangle$ and $K = \langle k \rangle$. Now define the map

$$\varphi : H \times K \to G, \quad (h^i, k^j) \mapsto h^i k^j$$

By Prop 2.11.4(c) we have that $H \lhd G \implies HK \leq G$. Now take the map

$$\psi : H \times K \to HK, \quad \psi(h^i, k^j) = \varphi(h^i, k^j)$$

Note that $H \cap K = \{1\}$ since every nonidentity element of H has order 3 and every nonidentity element of K has order 5. Also by construction we have ψ surjective. Finally, since H and K are normal in G and HK is a subgroup of G, we have that H and K are normal in HK. Therefore by Prop 2.11.4(d) we have $H \times K \cong HK$.

Next note that since H and K are cyclic with relatively prime orders, by Prop 2.11.3 we have that the product $H \times K$ is isomorphic to a cyclic group $\langle x \rangle$ of order 15. But note that

$$\langle x \rangle \cong H \times K \cong HK \leq G$$

So HK must also have an element of order 15, and this element is necessarily in G. □

11.7

Let H be a subgroup of a group G, let $\varphi : G \to H$ be a homomorphism whose restriction to H is the identity map, and let N be its kernel. What can one say about the product map $H \times N \to G$?

Solution.
Let $\psi : H \times N \to G$ be the product map $(h, n) \mapsto hn$. Note that

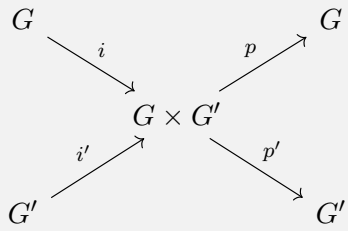
$$H \cap N = H \cap \{g \in G \mid \varphi(g) = 1\} = \{h \in H \mid 1 = \varphi|_H(h) = \mathrm{id}_H(h) = h\} = \{1\}$$

Hence by Prop 2.11.4(a) we have ψ is injective. Futhermore since the kernel is always a normal subgroup we have that $N \lhd G$ and by Prop 2.11.4(c) we have that its image is a subgroup of G. However, ψ is not necessarily a homomorphism since elements of H and K do not necessarily commute.

11.8

Let G, G', and H be groups. Establish a bijective correspondence between homomorphisms $\Phi : H \to G \times G'$ from H to the product group and pairs (φ, φ') consisting of a homomorphism $\varphi : H \to G$ and a homomorphism $\varphi' : H \to G'$.

Solution.
First recall the inclusion and projection maps



Now given a homomorphism $\Phi : H \to G \times G'$, we can define the corresponding homomorphisms

$$\varphi : H \to G, \quad h \mapsto p(\Phi(h)) = (p \circ \Phi)(h) \qquad \varphi' : H \to G', \quad h \mapsto p'(\Phi(h)) = (p' \circ \Phi)(h)$$

Conversely, given two homomorphisms $\varphi : H \to G$ and $\varphi' : H \to G'$, we define the corresponding homomorphism

$$\Phi : H \to G \times G', \quad h \mapsto i(\varphi(h))i'(\varphi'(h)) = (\varphi(h), \varphi'(h))$$

11.9

Let H and K be subgroups of a group G. Prove that the product set HK is a subgroup of G if and only if $HK = KH$.

Solution.

Proof.
$\implies$: Suppose that $HK \leq G$. Choose elements $h \in H$ and $k \in K$.
Then $hk \in HK$ and by closure of inverses, we have $(hk)^{-1} \in HK$, so there exists $h' \in H$ and $k' \in K$ such that $(hk)^{-1} = h'k'$. Now note

$$hk = ((hk)^{-1})^{-1} = (h'k')^{-1} = k'^{-1}h^{-1} \in KH$$

Thus $HK \subset KH$.
Furthermore, we have $(kh)^{-1} = h^{-1}k^{-1} \in HK$, so by closure of inverses we have $kh = ((kh)^{-1})^{-1} \in HK$, which implies $HK \subset HK$. Therefore $HK = KH$.

$\impliedby$: Suppose that $HK = KH$. We show $HK \leq G$ by definition, borrowing arguments from the proof of Prop 2.11.4(c):

- Closure follows from $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$.
- Since 1 in H and $1 \in K$, then $1 = (1)(1) \in HK$ and we have the identity.
- Given $hk \in HK$, we have $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$, so inverses are closed.

Therefore by definition $HK \leq G$. □

§12 - Quotient Groups

12.1

Show that if a subgroup H of a group G is not normal, there are left cosets aH and bH whose product is not a coset.

Solution.
Take $G = S_3 = \langle x, y\rangle$ and $H = \langle y\rangle$ for $x = (123)$ and $y = (12)$. Note that H is not normal ($xyx^{-1} = x^2y \notin H$) and consider the cosets

$$(xy)H = \{xy, x\} \text{ and } (x^2y)H = \{x^2y, x^2\}$$

Now

$$(xy)H(x^2y)H = \{xyx^2y, xyx^2, xx^2y, xx^2\} = \{x^2, x^2y, y, 1\}$$

which is not a coset, since it has 4 elements.
In fact, we claim we can always find such cosets aH and bH as long as $H \leq G$ is not normal.

Proof.
We prove the contrapositive: If for a subgroup $H \leq G$, every product of cosets is a coset, then H is normal.
Let H be such a group. Then for any $g \in G$, we have that $(gH)(g^{-1}H) = aH$ for some $a \in G$. However, the identity

$$1 = (g^{-1}1)(g1) \in (gH)(g^{-1}H) = aH$$

so we have $(gH)(g^{-1}H) = H$. This means that for any $h \in H$, there exists h' such that

$$ghg^{-1}h^{-1} = h' \implies ghg^{-1} = h'h \in H \implies gHg^{-1} = H$$

Therefore $H \lhd G$. □

12.2

In the general linear group $GL_3(\mathbb{R})$, consider the subsets

$$H = \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}, \quad \text{and} \quad K = \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where $*$ represents an arbitrary real number. Show that H is a subgroup of $GL_3(\mathbb{R})$, that K is a normal subgroup of H, and identify the quotient group H/K. Determine the center of H.

Solution.
Let $U \leq GL_3(\mathbb{R})$ be the subgroup of upper-triangular matrices and define a map

$$\psi : U \to \mathbb{R}^\times \times \mathbb{R}^\times \times R^\times, \quad \begin{bmatrix} a & * & * \\ 0 & b & * \\ 0 & 0 & c \end{bmatrix} \mapsto (a, b, c)$$

This is a homomorphism since for $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{bmatrix}$, $B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ 0 & b_{22} & b_{23} \\ 0 & 0 & b_{33} \end{bmatrix} \in U$,

$$\begin{aligned} \psi(AB) &= \psi\left(\begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} + a_{12}b_{22} & a_{11}b_{13} + a_{12}b_{23} + a_{13}b_{33} \\ 0 & a_{22}b_{22} & a_{22}b_{23} + a_{23}b_{33} \\ 0 & 0 & a_{33}b_{33} \end{bmatrix}\right) \\ &= (a_{11}b_{11}, a_{22}b_{22}, a_{33}b_{33}) \\ &= (a_{11}, a_{22}, a_{33})(b_{11}, b_{22}, b_{33}) \\ &= \psi(A)\,\psi(B) \end{aligned}$$

and thus $H = \ker\psi \leq U \leq GL_3(\mathbb{R})$ is a subgroup.

Next, define a map

$$\varphi : H \to \mathbb{R}^+ \times \mathbb{R}^+, \quad \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mapsto (a, c)$$

This is also a homomorphism since for $A = \begin{bmatrix} 1 & a_{12} & a_{13} \\ 0 & 1 & a_{23} \\ 0 & 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & b_{12} & b_{13} \\ 0 & 1 & b_{23} \\ 0 & 0 & 1 \end{bmatrix} \in H$,

$$\begin{aligned} \varphi(AB) &= \varphi\left(\begin{bmatrix} 1 & b_{12} + a_{12} & b_{13} + a_{12}b_{23} + a_{13} \\ 0 & 1 & b_{23} + a_{23} \\ 0 & 0 & 1 \end{bmatrix}\right) \\ &= (b_{12} + a_{12}, b_{23} + a_{23}) \\ &= (a_{12}, a_{23}) + (b_{12}, b_{23}) \\ &= \varphi(A)\,\varphi(B) \end{aligned}$$

and thus $K = \ker\varphi \lhd H$ is a normal subgroup.
By the first isomorphism theorem, $H/K \cong \operatorname{im}\varphi = \mathbb{R}^+ \times \mathbb{R}^+$, since φ is clearly surjective.

Finally, for the center of H note that for $A, B \in H$ we have

$$AB = \begin{bmatrix} 1 & b_{12}+a_{12} & b_{13}+a_{12}b_{23}+a_{13} \\ 0 & 1 & b_{23}+a_{23} \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad BA = \begin{bmatrix} 1 & a_{12}+b_{12} & a_{13}+b_{12}a_{23}+b_{13} \\ 0 & 1 & a_{23}+b_{23} \\ 0 & 0 & 1 \end{bmatrix}$$

thus

$$AB = BA \iff a_{12}b_{23} = b_{12}a_{23} \qquad (\star)$$

If we suppose $B \in Z(H)$ and vary $A \in H$, then $(\star)$ holding for every possible A can occur if and only if $b_{12} = b_{23} = 0$, which holds if and only if $B \in K$. Therefore $Z(H) = K$.

12.3

Let P be a partition of a group G with the property that for any pair of elements A, B of the partition, the product set AB is contained entirely within another element C of the partition. Let N be the element of P that contains 1. Prove that N is a normal subgroup of G and that P is the set of its cosets.

Solution.

Proof.
First, we check that N is a subgroup of G. For any $n_1, n_2 \in N$, we have $n_1 n_2 \in NN$ which by assumption is contained in some element C of the partition. However, taking $n_1 = n_2 = 1$ means that $1 \in C$, which by definition of partition forces $C = N$. Thus $NN \subset N$ and we are closed under multiplication. Furthermore, for any $n \in N$, say its inverse n^{-1} exists in $A \in P$. Then $1 = nn^{-1} \in NA \subset C'$ forces $C' = N$. But now $n^{-1} = 1n^{-1} \in NA \subset N$, so N is closed under inverses as well. Finally, N contains the identity, so by definition $N \leq G$.

Now choose $g \in G$. Then there exists an element C of the partition such that $(gN)(g^{-1}N) \subset C$. Now for any $n \in N$,

$$gng^{-1} = (gn)(g^{-1}1) \in (gN)(g^{-1}N) \subset C$$

However taking $n = 1$ means that $g(1)g^{-1} = 1 \in C$, so we have $C = N$. Therefore $gng^{-1} \in N$ and N is normal.

Finally, choose $g \in G$ and let A be the element of the partition that contains g. We have for any $n \in N$ that $gn \in AN \subset C$ for some C, but taking $n = 1$ gives $g \in C \implies C = A$. Thus $gN \subset A$. Furthermore, let B be the element of the partition that contains g^{-1}. Then $AB \subset C'$ for some C', but $1 = gg^{-1} \in AB$ forces $C' = N$. Thus $AB \subset N$, and in particular for every $a \in A$ we have $ag^{-1} \in N$ which implies $a \in gN$, so we have $A \subset gN$. Therefore $gN = A$, so the elements of P and cosets of N coincide. $\square$

12.4

Let $H = \{\pm 1, \pm i\}$ be the subgroup of $G = \mathbb{C}^\times$ of fourth roots of unity. Describe the cosets of H in G explicitly. Is G/H isomorphic to G?

Solution.
Given $z = x + iy \in \mathbb{C}$, we have the coset

$$zH = \{\pm(x+iy), \pm(ix + i^2 y)\} = \{\pm(x+iy), \pm(-y+ix)\}$$

which are the rotations of z by $0, \pi/2, \pi$, and $3\pi/2$ about the origin.

Next take the map

$$\varphi : G \to G, \qquad z \mapsto z^4$$

Note that this map is a homomorphism since multiplication is commutative, so

$$\varphi(z_1)\varphi(z_2) = z_1^4 z_2^4 = (z_1 z_2)^4 = \varphi(z_1 z_2)^4$$

Furthermore, it is surjective since for any $re^{i\theta} \in G$, we have

$$\varphi(\sqrt[4]{r}e^{i\theta/4}) = (\sqrt[4]{r}e^{i\theta/4})^4 = ((\sqrt[4]{r})^4 e^{4\cdot i\theta/4}) = re^{i\theta}$$

Finally, we have

$$\ker\varphi = \{z \in G \mid z^4 = 1\} = H$$

Therefore by the first isomorphism theorem we have $G/H \cong \operatorname{im}\varphi = G$.

12.5

Let G be the group of upper triangular real matrices $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, with a and d different from zero. For each of the following subsets, determine whether or not S is a subgroup, and whether or not S is a normal subgroup. If S is a normal subgroup, identify the quotient subgroup G/S.

(i) S is the subset defined by $b = 0$.

(ii) S is the subset defined by $d = 1$.

(iii) S is the subset defined by $a = d$.

Solution.

(i) We claim S is a subgroup, but not normal.
First note that $I \in S$, and that

$$\begin{bmatrix} a_1 & 0 \\ 0 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ 0 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & 0 \\ 0 & d_1 d_2 \end{bmatrix} \in S$$

So it is closed under multiplication. Finally,

$$\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{d} \end{bmatrix} \in S$$

so S is closed under inverses, therefore $S \leq G$. However,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 0 & 1 \end{bmatrix} \notin S$$

so S is not normal.

(ii) We claim that S is normal. Take the map

$$\varphi : G \to \mathbb{R}^\times, \quad \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mapsto d$$

This is a homomorphism since for $A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, $B = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \in G$ we have

$$\varphi(AB) = \varphi\left(\begin{bmatrix} ax & ay + bz \\ 0 & dz \end{bmatrix}\right) = dz = \varphi(A)\varphi(B)$$

Furthermore,

$$\ker \varphi = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in G \;\middle|\; d = 1 \right\} = S$$

Therefore S is a normal subgroup of G.
Finally, as φ is clearly surjective we have by the first isomorphism theorem that $G/S \cong \mathbb{R}^\times$.

(iii) We claim S is normal. Take the map

$$\varphi : G \to \mathbb{R}^\times, \quad \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mapsto \frac{a}{d}$$

This is a homomorphism since for $A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, $B = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \in G$ we have

$$\varphi(AB) = \varphi\left(\begin{bmatrix} ax & ay+bz \\ 0 & dz \end{bmatrix}\right) = \frac{ax}{dz} = \frac{a}{d} \cdot \frac{x}{z} = \varphi(A)\varphi(B)$$

Furthermore,

$$\ker \varphi = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in G \;\middle|\; \frac{a}{d} = 1 \iff a = d \right\} = S$$

Therefore S is a normal subgroup of G.
Finally, as φ is clearly surjective we have by the first isomorphism theorem that $G/S \cong \mathbb{R}^\times$.

M.1

Describe the column vectors $(a, c)^t$ that occur as the first column of an integer matrix A whose inverse is also an integer matrix.

Solution.
Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Since A^{-1} by assumption has integer entries, by Exercise 1.6.2 we have $ad - bc = \det A = \pm 1$. However note that if we fix a and c, then

$$ad - bc = \pm 1 \iff ad - bc = 1 \text{ or } bc - ad = 1 \iff ap + cq = 1 \text{ for some integers } p, q$$

This last condition is equivalent to saying $\gcd(a, c) = 1$. Therefore $(a, c)^t$ is a column of such a matrix A if and only if a and c are relatively prime.

M.2

(a) Prove that every group of even order contains an element of order 2.

(b) Prove that every group of order 21 contains an element of order 3.

Solution.

(a) *Proof.*
Let G be a group of order $2n$. Now partition G into three sets:

$$G = \{1\} \cup \{g \in G \mid g^2 = 1,\ g \neq 1\} \cup \{g \in G \mid g^k = 1\ (k > 2),\ g, g^2 \neq 1\} =: \{1\} \cup A \cup B$$

Then if $g \in B$ has order k and g^{-1} has order m, note

$$g^m = g^m(1) = g^m(g^{-1})^m = g^m(g^m)^{-1} = 1 \implies m = |g^{-1}| \geq |g| = k > 2$$

So in particular we have $g^{-1} \in B$ (in reality $m = k$, but only this inequality is needed). Furthermore, inverses are unique and $(g^{-1})^{-1} = 1$, so we can partition B further into pairs (g, g^{-1}) which are distinct elements, since $g = g^{-1} \implies g^2 = 1 \implies g \notin B$. Therefore $|B|$ is even, say $2m$. However now we have

$$2n = |G| = |\{1\}| + |A| + |B| = 1 + |A| + 2m$$

Since the LHS is even, this forces $|A|$ to be odd, and in particular $|A| \neq 0$. Therefore there exists $g \in A$, which is necessarily an element of order 2. □

(b) *Proof.*
Let G be a group of order 21. Assume otherwise, i.e. every element does not have order 3. If $G = \langle x \rangle$ is cyclic, then x^7 has order 3, which is a contradiction. Now suppose G is not cyclic, so no element has order 21. By Lagrange, every nonidentity element in G divides $21 = 3 \cdot 7$, so by assumption every nonidentity element must have order 7. This means that if we take $x \in G \setminus \{1\}$, we have distinct elements $x, x^2, \ldots, x^6$ (6 in total). Now if we take $y \in G \setminus \langle x \rangle$, this gives another set of 6 distinct elements. We can keep doing this process until we exhaust all of G, say after taking $x_1, \ldots x_n$. We then have

$$G = \{1\} \cup \langle x_1 \rangle \cup \cdots \cup \langle x_n \rangle, \quad \text{where } \langle x_i \rangle \cap \langle x_j \rangle = \{1\} \ \ (i \neq j)$$

and since each cyclic subgroup has 6 distinct elements, this implies that $21 = 1 + 6n$, which implies $n = 20/6 \notin \mathbb{Z}$ and is a contradiction. Therefore G has an element of order 3. □

M.3

Classify groups of order 6 by analyzing the following three cases:

(i) G contains an element of order 6.

(ii) G contains an element of order 3 but none of order 6.

(iii) All elements of G have order 1 or 2.

Solution.
First, if G has an element x of order 6, then we have $G = \langle x \rangle$ is cyclic.

Now suppose that G has an element x of order 3 and none of order 6. Note that G necessarily has an element of order 2, since otherwise every nonidentity element would have order 3 and we could find distinct elements $1, z_1, z_1^2, z_2, z_2^2, z_3, z_3^2$ which contradicts G having order 6. Thus let y be an element of order 2. Note that if $xy = yx$, then it would have order $\text{lcm}(2,3) = 6$ which contradicts our assumption. Thus $xy \neq yx$ and we now have six distinct elements, which must be the whole group and so we can start filling in G's multiplication table:

	1	x	x^2	y	xy	yx
1	1	x	x^2	y	xy	yx
x	x	x^2	1	xy	?	?
x^2	x^2	1	x	**?**	y	?
y	y	yx	?	1	?	x
xy	xy	?	?	x	?	x^2
yx	yx	?	y	?	?	?

Note that the property every element appears in each row and column exactly once forces the red **?** to be the element yx (since only x^2 and yx are missing in the fourth column and x^2 is already present in the third row). Thus $x^2y = yx$, which along with $x^3 = 1$ and $y^2 = 1$ are the defining rules of S_3 so G is isomorphic to it.

Finally, suppose every nonidentity element of G has order 2. Then for distinct elements x and y, we have $x^2 = y^2 = (xy)^2 = 1$. However, note that

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

Hence $H = \{1, x, y, xy\}$ is actually a subgroup of G, so by Lagrange $|H| = 4 \mid 6 = |G|$, which is a contradiction and therefore such a G is impossible.

This exhausts all cases, so every group of order 6 is isomorphic to $\mathbb{Z}/6\mathbb{Z}$ or S_3.

M.4

A *semigroup* S is a set with an associative law of composition and with an identity. Elements are not required to have inverses, and the Cancellation Law need not hold. A semigroup S is said to be generated by an element s if the set $\{1, s, s^2, \dots\}$ of nonnegative powers of s is equal to S. Classify semigroups that are generated by one element.

Solution.
Let S be a semigroup generated by s. If s^m is distinct for all $m = 0, 1, \dots$, then we have

$$S_\infty = \{1, s, s^2, \dots\}$$

which is isomorphic to $\mathbb{N}$.
[NB: $\mathbb{Z}$ is generated by a single element **as a group**, but to be generated as a monoid it needs both 1 and -1, because we are taking only nonnegative powers.]
Otherwise, there exists $0 \leq m < n$ such that $s^m = s^n$ (and n is the smallest such value). In this case S is finite with n elements:

$$S_{m,n} = \{1, s, \dots, s^m, \dots, s^{n-1}\}$$

note that m has n possible values, so there are n non-isomorphic semigroups of order n. Therefore every semigroup generated by one element is of the form S_∞ or $S_{m,n}$.

[NB: What Artin calls a semigroup here is typically called a *monoid* in modern abstract algebra, which reserves the term semigroup for simply a set with associative law of composition; hence with these definitions a monoid is a semigroup with an identity]

M.5

Let S be a finite semigroup (see Exercise M.4) in which the Cancellation Law 2.2.3 holds. Prove that S is a group.

Solution.

Proof.
It suffices to show that every element in S has an inverse. Choose a nonidentity element $s \in S$. Since S is a finite set, eventually the sequence of elements $s, s^2, s^3, \dots$ must repeat, i.e. there exists $1 < m < n$ such that $s^m = s^n$. However, we can apply the cancellation law and get

$$s^m = s^n = s^{n-m}s^m \implies 1 = s^{n-m} \implies ss^{n-m-1} = 1 \implies s^{-1} = s^{n-m-1}$$

Thus s has an inverse and S is a group. □

M.6

Let $a = (a_1, \ldots, a_k)$ and $b = (b_1, \ldots, b_k)$ be points in k-dimensional space $\mathbb{R}^k$. A *path* from a to b is a continuous function on the unit interval $[0,1]$ with values in $\mathbb{R}^k$, a function $X : [0,1] \to \mathbb{R}^k$, sending $t \rightsquigarrow X(t) = (x_1(t), \ldots, x_k(t))$, such that $X(0) = a$ and $X(1) = b$. If S is a subset of $\mathbb{R}^k$ and if a and B are in S, define $a \sim b$ if a and b can be joined by a path lying entirely in S.

(a) Show that $\sim$ is an equivalence relation on S. Be careful to check that any paths you construct stay within the set S.

(b) A subset S is *path connected* if $a \sim b$ for any two points a and b in S. Show that every subset S is partitioned into path-connected subsets with the property that two points in different subsets cannot be connected by a path in S.

(c) Which of the following loci in $\mathbb{R}^2$ are path-connected: $\{x^2 + y^2 = 1\}$, $\{xy = 0\}$, $\{xy = 1\}$?

Solution.

(a) *Proof.*

- Choose $a \in S$. Define the path $X : [0,1] \to S$ by $X(t) = a$ for all $0 \leq t \leq 1$. The constant function is continuous, so X is a path from $X(0) = a$ to $X(1) = a$ and so $a \sim a$.
- Suppose $a \sim b$. Then there exists a path $X : [0,1] \to S$ from a to b. Then define $X' : [0,1] \to S$ by $X'(t) = X(1-t)$. This is continuous since it is a composition of continuous functions X and $t \mapsto 1 - t$, so X' is a path from $X'(0) = X(1) = b$ to $X'(1) = X(0) = a$ and so $b \sim a$.
- Suppose $a \sim b$ and $b \sim c$. Then there exists paths X from a to b and Y from b to c. Then define a path

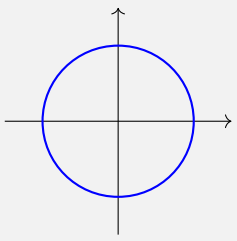
$$Z : [0,1] \to S \quad \text{by} \quad Z(t) = \begin{cases} X(2t) & \text{if } 0 \leq t \leq \frac{1}{2} \\ Y(2t-1) & \text{if } \frac{1}{2} < t \leq 1 \end{cases}$$

  Each piece is continuous by continuity of X and Y, and $X(1) = Y(0) = b$ so the pieces agree at $t = \frac{1}{2}$ so Z is continuous and is a path from a to c, thus $a \sim c$.

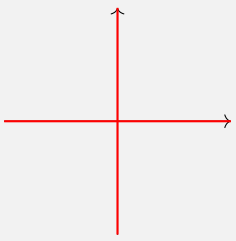
□

(b) *Proof.*
An equivalence relation on a set determines a partition of equivalence classes on that set by Lemma 2.7.6, so by (a) the path-connected components partition S. Also the components are necessarily disjoint, so points in different components cannot be path connected. □

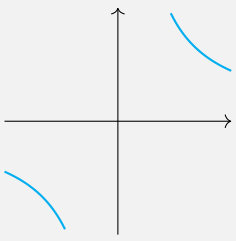
(c) We can visually see that the first two loci are path-connected and the third locus is not.



$x^2 + y^2 = 1$



$xy = 0$



$xy = 1$

M.7

The set of $n \times n$ matrices can be identified with the space $\mathbb{R}^{n \times n}$. Let G be a subgroup of $GL_n(\mathbb{R})$. With the notation of Exercise M.6, prove:

(a) If A, B, C, D are in G, and if there are paths in G from A to B and from C to D, then there is a path in G from AC to BD.

(b) The set of matrices that can be joined to the identity I forms a normal subgroup of G. (It is called the *connected component* of G).

Solution.

Proof.
(a)
Let X be a path from A to B and Y a path from C to D. We have the matrix-to-vector map $v : GL_n(\mathbb{R}) \to \mathbb{R}^{n \times n}$ and the matrix-multiplication map $m : \mathbb{R}^{n \times n} \times \mathbb{R}^{n \times n} \to \mathbb{R}^{n \times n}$, i.e. usual matrix multiplication has corresponding operation in $\mathbb{R}^{n \times n}$ via

$$AB \leftrightsquigarrow m(v(A), v(B))$$

Hence our paths X and Y are really paths from $v(A)$ to $v(B)$ and from $v(C)$ to $v(D)$. Also note that m is a continuous function. Hence consider the continuous map

$$Z : [0,1] \to \mathbb{R}^{n \times n} \quad t \mapsto m(X(t), Y(t)) \leftrightsquigarrow [X(t)][Y(t)]$$

Then this is a path from $Z(0) = m(X(0), Y(0)) \leftrightsquigarrow AC$ to $Z(1) = m(X(1), Y(1)) \leftrightsquigarrow BD$.

(b)
Let H be the set of matrices path-connected to I. We first show H is a subgroup.

- The identity is clearly path-connected to I, so $I \in H$.
- Choose $A, B \in H$. Then there exists paths from I to A and from I to B. Then from (a), there exists a path from $II = I$ to AB, so $AB \in H$ and we have closure.
- Choose A in H and let X be a path from I to A. Then using the maps from (a), we also have an the matrix-inverse map $i : \mathbb{R}^{n \times n} \to \mathbb{R}^{n \times n}$ by sending $v(A)$ to $v(A^{-1})$. This map is continuous, and so we can define the continuous map

  $$Y : [0,1] \to \mathbb{R}^{n \times n} \quad t \mapsto i(X(t)) \leftrightsquigarrow [X(t)]^{-1}$$

  This then is a path from $Y(0) = i(X(0)) \leftrightsquigarrow I^{-1} = I$ to $Y(1) = i(X(1)) \leftrightsquigarrow A^{-1}$. Thus $A^{-1} \in H$.

Next, choose $A \in H$ and $B \in G$. We want to show that there is a path from I to BAB^{-1}. By assumption there exists a path X from I to A, and so we define the continuous map

$$Y : [0,1] \to \mathbb{R}^{n \times n} \quad t \mapsto m(m(B, X(t)), B^{-1}) \leftrightsquigarrow B[X(t)]B^{-1}$$

This then is a path from $Y(0) \leftrightsquigarrow BIB^{-1} = I$ to $Y(1) \leftrightsquigarrow BAB^{-1}$. Therefore $BAB^{-1} \in H$ and H is normal in G. □

M.8

(a) The group $SL_n(\mathbb{R})$ is generated by elementary matrices of the first type (see Exercise 4.8). Use this fact to prove that $SL_n(\mathbb{R})$ is path-connected.

(b) Show that $GL_n(\mathbb{R})$ is a union of two path-connected subsets, and describe them.

Solution.

(a) *Proof.*
First note that elementary matrices of the first type have the form

$$\begin{bmatrix} 1 & & & & \\ & 1 & & a & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix} = I + a \cdot e_{ij}$$

So for a given row-addition elementary matrix $E = I + a \cdot e_{ij}$, we define a continuous map

$$X : [0,1] \to SL_n(\mathbb{R}) \quad t \mapsto X(t) \leftrightsquigarrow I + (ta) \cdot e_{ij}$$

This then is a path from $X(0) \leftrightsquigarrow I$ to $X(1) \leftrightsquigarrow E$. Hence every such elementary matrix is path-connected to I, and by Exercise M.7 the set H of all matrices path-connected to I is a subgroup of $SL_n(\mathbb{R})$. In particular, this means if we have two elementary matrices E_1, E_2 of the first type, then $E_1 E_2 \in H$ which implies that any product of elementary matrices of the first type is in H, which implies $H = SL_n(\mathbb{R})$. Now for any $A, B \in SL_n(\mathbb{R}) = H$, there is a path from I to A and from I to B, which implies there is a path from A to B and therefore $SL_n(\mathbb{R})$ is path-connected. □

(b) *Proof.*
We claim that $GL_n(\mathbb{R}) = \{\det(A) > 0\} \cup \{\det(A) < 0\} =: D^+ \cup D^-$ is a union of two path-connected subsets.

First choose $A, B \in D^+$ and define the continuous map

$$X_A : [0,1] \to D^+ \quad t \mapsto (\det A)^{-t/n} \cdot A$$

This is a path from $X_A(0) = A$ to $X_A(1) = (\det A)^{-1/n} \cdot A$, and note that the property for $M \in GL_n(\mathbb{R})$ that $\det(a \cdot M) = a^n \det(M)$ implies

$$\det(X_A(1)) = ((\det A)^{-1/n})^n (\det A) = (\det A)^{-1}(\det A) = 1 \implies X_A(1) \in SL_n(\mathbb{R})$$

We can similarly define the path X_B from B to $X_B(1) \in SL_n(\mathbb{R})$. However by (a) we know $SL_n(\mathbb{R})$ is path-connected, so there is a path from $X_A(1)$ to $X_B(1)$. Combining our paths gives a path from A to B and so D^+ is path-connected.

Next choose $A, B \in D^-$. If we take a matrix $C \in D^-$ with $\det(C) = -1$ (e.g. $C = I - 2e_{11}$), then we have $\det(AC) = \det(A)\det(C) = -\det(A) > 0$ implies that $AC \in D^+$ and similarly $BC \in D^+$. Thus from above we know there is a path from AC to BC, and clearly there is a path from C^{-1} to C^{-1}. Then by Exercise M.7(a) there is a path from $ACC^{-1} = A$ to $BCC^{-1} = B$. Therefore D^- is path-connected. □

M.9

Let H and K be subgroups of a group G, and let g be an element of G.
The set $HgK = \{x \in G \mid x = hgk \text{ for some } h \in H, k \in K\}$ is called a *double coset*. Do the double cosets partition G?

Solution.
We claim yes.

Proof.
First clearly $g = 1g1$ implies

$$G = \bigcup_{g \in G} HgK$$

So it suffices to show the double cosets are disjoint, which is equivalent to showing that $Hg_1K \cap Hg_2K \neq \varnothing \implies Hg_1K = Hg_2K$. Indeed, if $g \in Hg_1K \cap Hg_2K$ then there exists $h, h' \in H$ and $k, k' \in K$ such that $g = hg_1k = h'g_2k'$. Then

$$g_1 = h^{-1}gk^{-1} = h^{-1}(h'g_2k')k^{-1} = (h^{-1}h')g_2(k'k^{-1})$$

Using this, we have $g_1 \in Hg_2K \implies Hg_1K \subset Hg_2K$.
We also have $g_2 = (h^{-1}h')^{-1}g_1(k'k^{-1})^{-1} \in Hg_1K \implies Hg_2K \subset Hg_1K$.
Therefore $Hg_1K = Hg_2K$. □

M.10

Let H be a subgroup of a group G. Show that the double cosets (see Exercise M.9)

$$HgH = \{h_1gh_2 \mid h_1, h_2 \in H\}$$

are the left cosets gH if and only if H is normal.

Solution.

Proof.
$\implies$: Suppose the double cosets are the left cosets. Then

$$(gHg^{-1})H = g(Hg^{-1}H) = g(g^{-1}H) = (gg^{-1})H = H \implies gHg^{-1} \subset H$$

The symmetric argument (swapping g and g^{-1}) then shows that

$$(g^{-1}Hg)H = g^{-1}(HgH) = g^{-1}(gH) = (g^{-1}g)H = H \implies H \supset g^{-1}Hg$$

which implies $gHg^{-1} \supset H$. Thus combining with the above gives $gHg^{-1} = H$ and H is normal.
$\impliedby$: Suppose $H \lhd G$. Then

$$HgH = (Hg)H \overset{\star}{=} (gH)H = gHH = gH$$

where $\star$ is where we use normality. Therefore the double cosets are the left cosets. □

M.11

Most invertible matrices can be written as a product $A = LU$ of a lower triangular matrix L and an upper triangular matrix U, where in addition all diagonal entries of U are 1.

(a) Explain how to compute L and U when the matrix A is given.

(b) Prove uniqueness, that there is at most one way to write A as such a product.

(c) Show that every invertible matrix can be written as a product LPU, where L, U are as above and P is a permutation matrix.

(d) Describe the double cosets LgU (see Exercise M.9).

Solution.

(a) We start with a_{11}. If it is zero, then we cannot decompose A. Otherwise, we scale row 1 by $\frac{1}{a_{11}}$ and clear out the first column of rows 2 through n with the proper row additions. Note that all of these operations are done with lower triangular elementary matrices. Next, we look at a_{22} and if it is nonzero (otherwise we cannot continue), we scale row 2 by $\frac{1}{a_{22}}$ and clear out the second column of rows 3 through n. This again only uses lower triangular elementary matrices, and we repeat this process on the entire matrix using lower triangular elementary matrices until it is upper triangular with all diagonal entries of 1. We can write this as

$$\ell_k \dots \ell_1 A = U$$

and since the product and inverse of lower triangular matrices are lower triangular, we have $A = (\ell_k \dots \ell_1)^{-1} U =: LU$.

(b) *Proof.*
Suppose that $A = L_1 U_1 = L_2 U_2$. Since A is invertible and $\det(U_1) = \det(U_2) = 1$, we have L_1, L_2, U_1, U_2 invertible and

$$A^{-1} = U_1^{-1} L_1^{-1} = U_2^{-1} L_2^{-1} \implies U_2 U_1^{-1} = L_2^{-1} L_1$$

Note that $U_2 U_1^{-1}$ is upper triangular with ones on the diagonal and $L_2^{-1} L_1$ is lower triangular, and since they are the same matrix these properties all simultaneously hold only when it is the identity I. Hence

$$U_2 U_1^{-1} = I \implies U_1 = U_2 \quad \text{and} \quad L_2^{-1} L_1 = I \implies L_1 = L_2$$

Therefore the decomposition is unique. □

(c) *Proof.*
The general idea is to perform the algorithm from (a) while also taking into account the pivots possibly not occurring along the diagonal, and then row swapping to get into upper triangular form. We start with the first column and find the smallest k such that a_{k1} is nonzero. Then like in (a) we scale row k by $\frac{1}{a_{k1}}$ and clear out the $n-k$ entries below in the first column. Note that this only uses lower triangular elementary matrices. Next we look at the second column, starting at the first row, and find the smallest $j \neq k$ such that a_{j2} is nonzero. Then again we scale and clear out the entries below again using only lower triangular matrices. Again, we now find the smallest $i \neq j, k$ such that a_{i3} is nonzero, and repeat the process. Crucially, this process can always continue since all we are doing is row reduction and a failure to find these pivot indices means that the semi row-reduced matrix, and hence A itself, is not invertible which is a contradiction.

By the end of this process, we will have a matrix $(\ell_k \dots \ell_1)A$ that has a pivot 1 in each row and column, so let $\overline{P}$ be the permutation matrix such that $X := \overline{P}(\ell_k \dots \ell_1)A$ puts these pivots along the diagonal via row-swaps. We claim X is an upper triangular matrix U, i.e. every 1 on the diagonal has zeros below it. Indeed given a diagonal element $x_{cc} = 1$, then at the entry x_{rc} for $r > c$, either it was still below the pivot before swapping rows (in which case it was eliminated to zero via (a)'s algorithm) or it was above the pivot prior to swapping (in which case it was not chosen to be the pivot because it was already zero); in either case $x_{rc} = 0$ and so X is an upper triangular matrix U.

Therefore we can write

$$\overline{P}(\ell_k \dots \ell_1)A = U \implies A = (\ell_k \dots \ell_1)^{-1}\overline{P}^{-1}U =: LPU$$

□

(d) First we clarify notation. Let $G = GL_n(\mathbb{R})$ be the group of invertible matrices, let U be the subgroup of upper triangular matrices with diagonal entries all 1, and let L be the subgroup of lower triangular matrices. Finally, let $\mathcal{P}$ be the set of all permutation matrices. Then we claim the collection of double cosets can be written

$$\{LgU \mid g \in G\} = \{LPU \mid P \in \mathcal{P}\} \tag{$\star$}$$

Furthermore, for $P, Q \in \mathcal{P}$ we claim $LPU = LQU$ if and only if $P = Q$.

Proof.
First choose $g \in G$. Then from (c), we have that there exists $l \in L, u \in U, P \in \mathcal{P}$ such that $g = lPu$. Thus $LgU = L(lPu)U = (Ll)P(uU) = LPU$ and $(\star)$ holds.

Next, suppose that $LPU = LQU$. Then in particular there exists $l \in L$ and $u \in U$ such that $P = lQu$, which implies $Q^{-1}l^{-1}P = u$. This means by permuting the rows and columns of $\ell := l^{-1}$ (lower triangular), we can construct u (upper triangular with diagonal entries all 1). Let σ be the permutation corresponding to P and τ corresponding to Q. Then we claim

$$u_{ij} = [Q^{-1}\ell P]_{ij} = \ell_{\tau(i)\sigma(j)} \tag{$\dagger$}$$

To see this,

By definition, $Q_{ij} = 1$ iff $i = \tau(j)$ and $P_{ij} = 1$ iff $i = \sigma(j)$. Since $Q^{-1} = Q^T$, then

$$[Q^{-1}\ell]_{ij} = \sum_{k=1}^{n} Q^T_{ik}\ell_{kj} = \sum_{k=1}^{n} Q_{ki}\ell_{kj} = \ell_{\tau(i)j}$$

Thus

$$[Q^{-1}\ell P]_{ij} = \sum_{k=1}^{n} [Q^{-1}\ell]_{ik}P_{kj} = \sum_{k=1}^{n} \ell_{\tau(i)k}P_{kj} = \ell_{\tau(i)\sigma(j)}$$

Since $u_{ii} = 1$, by $(\dagger)$ we have $\ell_{\tau(i)\sigma(i)} = 1$ for $i = 1, \ldots, n$. Furthermore, ℓ is lower triangular so $\ell_{rc} = 0$ when $r < c$. In particular we have $\tau(i) \geq \sigma(i)$ for all i, since otherwise there would exist i such that $\tau(i) < \sigma(i) \implies \ell_{\tau(i)\sigma(i)} = 0 \neq 1$, which is a contradiction. However, since τ and σ are bijections from $\{1, \ldots, n\}$ to itself, we have

$$\sum_{i=1}^{n}(\tau(i) - \sigma(i)) = \sum_{i=1}^{n}\tau(i) - \sum_{i=1}^{n}\sigma(i) = (1 + \cdots + n) - (1 + \cdots + n) = 0$$

Also, $\tau(i) \geq \sigma(i)$ implies $\sum_{i=1}^{n}(\tau(i) - \sigma(i))$ is a series of nonnegative terms adding to zero, which forces each term to be zero and $\tau(i) = \sigma(i)$ for all i. Therefore $\tau = \sigma$ and $P = Q$. $\square$

M.12

Let a and b be positive, relatively prime integers.

(a) Prove that every sufficiently large positive integer n can be obtained as $ra + sb$, where r and s are positive integers.

(b) Determine the largest integer that is not of this form.

Solution. We first solve the exercise as-written:

(a) *Proof.*
Since $\gcd(a, b) = 1$, then there exists integers R and S such that $Ra + Sb = 1$.
Also let R' be the integer such that $1 \le R' < b$ and $R \equiv R' \mod b$. Similarly find S' such that $1 \le S' < a$ and $S \equiv S' \mod a$. Then we have

$$\begin{aligned} 1 = Ra + Sb &\equiv R'a \mod b \\ &\equiv S'b \mod a \end{aligned}$$

Now note by construction

$$\begin{cases} R'a + S'b \equiv 1 \mod a \\ R'a + S'b \equiv 1 \mod b \end{cases} \implies R'a + S'b \equiv 1 \mod ab$$

So there exists an integer k such that $R'a + S'b = 1 + k(ab)$. But $R' < b$ and $S' < a$ means

$$R'a < ab,\ S'b < ab \implies 2 \le R'a + S'b < 2ab$$

So $1 + k(ab)$ is bigger than 1 but less than $2ab$, which forces $k = 1$. Thus we have $m := R'a + S'b = 1 + ab$. We claim if $n \ge m$, then it has a solution of the above form.

To see this, note that since $Ra + Sb = 1$ if we write $n = m + \ell$ for $\ell \ge 0$, then

$$[\ell R + R']a + [\ell S + S']b = \ell(Ra + Sb) + [R'a + S'b] = \ell(1) + m = n$$

It remains to adjust the coefficients if either is not positive. Setting $r_0 := \ell R + R'$ and $s_0 := \ell S + S'$, note for any integer t that

$$(r_0 + tb)a + (s_0 - ta)b = r_0a + tab + s_0b - tab = r_0a + s_0b = n \qquad (\star)$$

So if either r_0 or s_0 is not positive, we want to find t such that both $r_0 + tb > 0$ and $s_0 - ta > 0$, i.e. both coefficients of $(\star)$ are now positive. Let r' be the integer such that $0 < r' \le b$ and $r_0 \equiv r' \mod b$. Then there exists an integer t such that $r_0 = r' - tb$, and we claim this t is what we want. Indeed, we have

$$s_0 - ta = \frac{s_0 b}{b} - \frac{(r' - r_0)a}{b} = \frac{r_0a + s_0b - r'a}{b} = \frac{n - r'a}{b} \ge \frac{n - ba}{b}$$

Then since $n \ge m$, we have

$$n - ba \ge (ab + 1) - ba = 1$$

Hence $s_0 - ta \ge \frac{1}{b} > 0$, and since $s_0 - ta$ is an integer we have $s_0 - ta \ge 1$. Furthermore, by construction $r_0 + tb = r' \ge 1$, and therefore $(r_0 + tb)a + (s_0 - ta)b$ is our solution.

□

(b) We claim that the largest such integer is ab.

Proof.
By the proof in (a), every integer $n \geq ab+1$ can be written in that form, so it suffices to show ab cannot. Suppose otherwise, i.e. there exists positive integers r, s such that $ra + sb = ab$. Then note that

$$ra + sb = ab \implies ra = ab - sb = (a - s)b$$

So by definition $b \mid ra$. However $\gcd(a, b) = 1$, which forces $b \mid r$. But note

$$ra = ab - sb < ab \implies r < b$$

Hence b (a positive integer) divides a positive integer r strictly less than it, which is impossible and so we have a contradiction.
Therefore no such r and s exist. □

There is a similar problem is known as the Frobenius Coin Problem, whose statement is the same as the exercise but allows r and s to be zero, i.e. they are now nonnegative integers. We solve this problem below:

(a) *Proof.*
Since $\gcd(a,b) = 1$, then there exists integers R and S such that $Ra + Sb = 1$.
Also let R' be the integer such that $1 \leq R' < b$ and $R \equiv R' \mod b$. Similarly find S' such that $1 \leq S' < a$ and $S \equiv S' \mod a$. Then we have

$$\begin{aligned} 1 = Ra + Sb &\equiv R'a \mod b \\ &\equiv S'b \mod a \end{aligned}$$

Now note

$$(R'-1)a + (S'-1)b = R'a + S'b - a - b =: m$$

Furthermore, by construction

$$\begin{cases} R'a + S'b \equiv 1 \mod a \\ R'a + S'b \equiv 1 \mod b \end{cases} \implies R'a + S'b \equiv 1 \mod ab$$

So there exists an integer k such that $R'a + S'b = 1 + k(ab)$. But $R' < b$ and $S' < a$ means

$$R'a < ab,\ S'b < ab \implies 2 \leq R'a + S'b < 2ab$$

So $1 + k(ab)$ is bigger than 1 but less than $2ab$, which forces $k = 1$. Thus we have $m = 1 + ab - a - b$. We claim if $n \geq m$, then it has a solution of the above form.

To see this, note that since $Ra + Sb = 1$ if we write $n = m + \ell$ for $\ell \geq 0$, then

$$[\ell R + (R'-1)]a + [\ell S + (S'-1)]b = \ell(Ra+Sb) + [(R'-1)a + (S'-1)b] = \ell(1) + m = n$$

It remains to adjust the coefficients if either is negative. Setting $r_0 := \ell R + (R'-1)$ and $s_0 := \ell S + (S'-1)$, note for any integer t that

$$(r_0 + tb)a + (s_0 - ta)b = r_0a + tab + s_0b - tab = r_0a + s_0b = n \qquad (\star)$$

So if either r_0 or s_0 is negative, we want to find t such that both $r_0 + tb \geq 0$ and $s_0 - ta \geq 0$, i.e. both coefficients of $(\star)$ are now nonnegative. Let r' be the integer such that $0 \leq r' < b$ and $r_0 \equiv r' \mod b$. Then there exists an integer t such that $r_0 = r' - tb$, and we claim this t is what we want. Indeed, we have

$$s_0 - ta = \frac{s_0 b}{b} - \frac{(r' - r_0)a}{b} = \frac{r_0 a + s_0 b - r'a}{b} = \frac{n - r'a}{b} \geq \frac{n - (b-1)a}{b}$$

where the last inequality comes from $r' < b$. Then since $n \geq m$, we have

$$n - (b-1)a \geq (ab - a - b + 1) - ba + a = -b + 1$$

Hence $s_0 - ta \geq \frac{-b+1}{b} = -1 + \frac{1}{b} > -1$, and since $s_0 - ta$ is an integer we have $s_0 - ta \geq 0$. Furthermore, by construction $r_0 + tb = r' \geq 0$, and therefore $(r_0 + tb)a + (s_0 - ta)b$ is our solution.

□

(b) We claim that the largest such integer is $ab - a - b$.

Proof.
By the proof in (a), every integer $n \geq ab - a - b + 1$ can be written in that form, so it suffices to show $ab - a - b$ cannot. Suppose otherwise, i.e. there exists nonnegative integers r, s such that $ra + sb = ab - a - b$. Then note

$$\begin{cases} ra + sb = ab - a - b \\ ra + sb = ab - a - b \end{cases} \implies \begin{cases} sb \equiv -b \mod a \\ ra \equiv -a \mod b \end{cases} \implies \begin{cases} s \equiv -1 \mod a \\ r \equiv -1 \mod b \end{cases}$$

But since $s \geq 0$, this means $s \geq a - 1$. Similarly, we have $r \geq b - 1$. Thus

$$ab - a - b = ra + sb \geq (b-1)a + (a-1)b = ab - a + ab - b \implies 0 \geq ab$$

However a and b both positive means $ab > 0$, which is a contradiction.
Therefore no such r and s exist. □

M.13

The starting position is the point $(1, 1)$, and a permissible "move" replaces a point (a, b) by one of the points $(a + b, b)$ or $(a, a + b)$. So the position after the first move will be either $(2, 1)$ or $(1, 2)$. Determine the points that can be reached.

Solution.
Let P be set of all points that can be reached. We claim $P = \{(a, b) \mid a, b > 0 \text{ and } \gcd(a, b) = 1\}$. First, a (possibly obvious) lemma:

> **Lemma.** *If $a > b$, then $\gcd(a - b, b) = \gcd(a, b)$.*
>
> *Proof.* (*of Lemma*)
> Let $k = \gcd(a, b)$ and $\ell = \gcd(a - b, b)$. Then by definition
>
> $$\ell \mid b \text{ and } \ell \mid (a - b) \implies \ell \mid a$$
>
> Hence ℓ is a divisor of a and b, which by definition means $\ell \leq k$. However
>
> $$k \mid b \text{ and } k \mid a \implies k \mid (a - b)$$
>
> Hence k is a divisor of $a - b$ and b, which by definition means $k \leq \ell$. Thus $k = \ell$. $\square$

Now we prove the claim.

Proof.
We first show that for any two positive, relatively prime integers a and b, we have that $a, b < n \implies (a, b) \in P$ for all $n \geq 2$. We induct on n.
The base case is when $a, b < 2$, which forces $(a, b) = (1, 1)$ and is our starting point, so $(a, b) \in P$. Now assume that the result holds for some n. It suffices to show that $(a, b) \in P$ when either $a = n$ or $b = n$. Both cannot be simultaneously true (otherwise $\gcd(a, b) = n \neq 1$), and by the symmetry of the game moves, it suffices to only show the case when $a = n$. Thus fix $a = n$ and suppose $1 \leq b < n$ such that $\gcd(a, b) = 1$. Then note by the lemma that $\gcd(a - b, b) = \gcd(a, b) = 1$. Furthermore we have $b < n$ and $a - b = n - b \leq n - 1 < n$, so we can apply the IH to get $(a - b, b) \in P$. Then we can apply the first move to get $([a - b] + b, b) = (a, b) \in P$, which completes the induction and gives the inclusion $P \supset \{(a, b) \mid a, b > 0 \text{ and } \gcd(a, b) = 1\}$.

Next, choose $(a, b) \in P$. Clearly from the starting point and rules we have that a, b are both positive, so we just have to show that $\gcd(a, b) = 1$. Note that we can write

$$A := \begin{bmatrix} a \\ b \end{bmatrix} = E_n \dots E_1 \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad \text{where } E_i \in \left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\} =: \{E, E'\}$$

Hence we have

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix} = E_1^{-1} \dots E_n^{-1} A \quad \text{where } E_i^{-1} \in \{E^{-1}, E'^{-1}\} = \left\{ \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \right\}$$

But note that

$$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} c-d \\ d \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} c \\ d-c \end{bmatrix}$$

And so if $E_n^{-1} = E^{-1}$, then $(a-b, b)$ was the previous position and in particular $a-b$ is positive and $a > b$. Similarly if $E_n^{-1} = E'^{-1}$, then we can guarantee that $b > a$. Hence if we define

$$GCD\left(\begin{bmatrix} c \\ d \end{bmatrix}\right) := \gcd(c, d)$$

then our lemma applies and says that $GCD(E_n^{-1}A) = GCD(A)$. The same reasoning and application of the lemma again says that $GCD(E_{n-1}^{-1}E_n^{-1}A) = GCD(A)$. Indeed, all we are doing here is the Euclidean algorithm. Hence after doing n steps we have

$$GCD(A) = GCD(E_1^{-1} \dots E_n^{-1}A) = GCD\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = \gcd(1, 1) = 1$$

Therefore $\gcd(a, b) = 1$. □

M.14

Prove that the two matrices

$$E = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad E' = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

generate the group $SL_2(\mathbb{Z})$ of all *integer* matrices with determinant 1. Remember that the subgroup they generate consists of all elements that can be expressed as products using the four elements E, E', E^{-1}, E'^{-1}.
Hint: Do not try to write a matrix directly as a product of the generators. Use row reduction.

Solution.

Proof.
Choose $M := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$. This means that $ad - bc = 1$, which by Corollary 2.3.6 means that $\gcd(a, c) = 1$. Note that

$$E^{-1}M = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a-c & b-d \\ c & d \end{bmatrix} \quad \text{and} \quad E'^{-1}M = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c-a & d-b \end{bmatrix}$$

Hence we can perform the Euclidean algorithm to reduce M: Set $M_0 = M$ and define

$$M_i = \begin{cases} E^{-1}M_{i-1} & \text{if } [M_{i-1}]_{11} \geq [M_{i-1}]_{21} \\ E'^{-1}M_{i-1} & \text{if } [M_{i-1}]_{11} < [M_{i-1}]_{21} \end{cases}$$

Each of these steps preserves the gcd of the first column (see Lemma in the proof of Exercise M.13), so we can keep going until $\gcd(a, c) = \gcd(1, 0)$ or $\gcd(a, c) = \gcd(0, 1)$ and, say after n steps, $M_n = E_n \dots E_1 M$ (for $E_i \in \{E^{-1}, E'^{-1}\}$) looks like

$$M_n = \begin{bmatrix} 1 & b' \\ 0 & d' \end{bmatrix} \quad \text{or} \quad M_n = \begin{bmatrix} 0 & b' \\ 1 & d' \end{bmatrix}$$

Note that $\det(E^{-1}) = \det(E'^{-1}) = 1$, so $\det(M_i) = \det(M) = 1$ for all i. In particular, $\det(M_n) = 1$ which forces $(b', d') = (k, 1)$ in the first case and $(b', d') = (-1, \ell)$ in the second. Furthermore,

$$E^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad (E'^{-1})^{\ell-1}(E^{-1}E') = \begin{bmatrix} 1 & 0 \\ -(\ell-1) & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & \ell \end{bmatrix}$$

Hence in the first case,

$$E_n \dots E_1 M = M_n = E^k \implies M = (E_n \dots E_1)^{-1} E^k \in \langle E, E' \rangle$$

and in the second case,

$$E_n \dots E_1 M = M_n = E'^{\ell-1} E^{-1} E' \implies M = (E_n \dots E_1)^{-1} E'^{\ell-1} E^{-1} E' \in \langle E, E' \rangle$$

Therefore M, and hence all of $SL_2(\mathbb{Z})$, is generated by E and E'. □

M.15

Determine the semigroup S (see Exercise M.4) of matrices A that can be written as a product, of arbitrary length, each of whose terms is one of the two matrices

$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix} \quad \text{or} \quad \begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}.$$

Show that every element of S can be expressed as such a product in exactly one way.

Solution.
We claim S is the semigroup of integer matrices with nonnegative entries and determinant 1.

Lemma. *Let* $A = \begin{bmatrix}a & b\\ c & d\end{bmatrix}$ *with nonnegative entries and determinant 1.*
If $a+b > c+d$, *then* $a \geq c$ *and* $b \geq d$. *Similarly, if* $a+b < c+d$, *then* $a \leq c$ *and* $b \leq d$.

Proof. (*of Lemma*)
Suppose $a+b > c+d$. Then if $a < c$, we have

$$d < a+b-c < a+b-a = b$$

But now

$$0 \leq a < c,\ 0 \leq d < b \implies ad < bc \implies 1 = \det A = ad - bc < 0$$

which is a contradiction. The symmetric argument shows $b < d$ leads to a contradiction also, so we have $a \geq c$ and $b \geq d$. Finally, flipping inequalities proves the second statement. □

Now we prove our original claim.

Proof.
Let $E = \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}, E' = \begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}$. Note that both E and E' have nonnegative entries and determinant 1, so any product of them will also have nonnegative entries and determinant 1. Hence it suffices to show any matrix $A = \begin{bmatrix}a & b\\ c & d\end{bmatrix}$ with nonnegative entries and determinant 1 can be written as a product of E and E', i.e. $A \in S$. If we let $k = \gcd(a+b, c+d)$, note that

$$k \mid (a+b),\ k \mid (c+d) \implies k \mid ([a+b]d - [c+d]b) \implies k \mid (ad-bc) \implies k \mid 1 \implies k = 1$$

Hence we can take

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

and, similar to the proofs of the previous two exercises, use E^{-1} and E'^{-1} to perform the Euclidean algorithm: let $A_0 = A$ and for

$$A_i\begin{bmatrix}1\\ 1\end{bmatrix} = \begin{bmatrix}a_i & b_i\\ c_i & d_i\end{bmatrix}\begin{bmatrix}1\\ 1\end{bmatrix} = \begin{bmatrix}a_i+b_i\\ c_i+d_i\end{bmatrix}, \quad \text{define } A_{i+1} = \begin{cases}E^{-1}A_i & \text{if } a_i+b_i > c_i+d_i\\ E'^{-1}A_i & \text{if } a_i+b_i < c_i+d_i\end{cases}$$

and stop if $a_i + b_i = c_i + d_i$. Note that each A_{i+1} has nonnegative entries by the lemma since

$$E^{-1}\begin{bmatrix}a & b\\ c & d\end{bmatrix} = \begin{bmatrix}a-c & b-d\\ c & d\end{bmatrix} \text{ and } E'^{-1}\begin{bmatrix}a & b\\ c & d\end{bmatrix} = \begin{bmatrix}a & b\\ c-a & d-b\end{bmatrix}$$

Furthermore, this process, the Euclidean algorithm, preserves the gcd, i.e. $\gcd(a_i + b_i, c_i + d_i) = \gcd(a + b, c + d) = 1$ for every i (see proof of Exercise M.13). Hence when this algorithm terminates after n steps (which it must since A_{i+1} has entries necessarily smaller than A_i but remain all nonnegative), we will have

$$\gcd(a_n + b_n, c_n + d_n) = 1 \text{ and } m := a_n + b_n = c_n + d_n \implies \gcd(m, m) = 1 \implies m = 1$$

Thus

$$\begin{bmatrix}1\\1\end{bmatrix} = \begin{bmatrix}a_n + b_n\\c_n + d_n\end{bmatrix} = A_n \begin{bmatrix}1\\1\end{bmatrix}$$

and the entries of A_n being nonnegative force $a_n = 1, b_n = 0$ or $a_n = 0, b_n = 1$, and similarly for c_n, d_n. However we also have $\det(A_n) = 1$, so $a_n d_n - b_n c_n = 1$ is only satisfied when $a_n = d_n = 1$ and $b_n = c_n = 0$, i.e. $A_n = I$. Thus

$$I = A_n = B_n \dots B_1 A \implies A = (B_n \dots B_1)^{-1} = B_1^{-1} \dots B_n^{-1}$$

where each B_i is either E^{-1} or E'^{-1}. But now A is a product of matrices that are either E and E', therefore $A \in S$.

Finally, for uniqueness suppose for any $A \in S$ that $A = E_1 \dots E_n$ for $E_i \in \{E, E'\}$. We claim this product is unique for every $n \geq 0$. We induct on n.
For the base case, $n = 0$ means $A = I$, whose product is the empty product and is unique.
Now assume every product of length $n - 1$ is unique. Then write $A = E_1 E_2 \dots E_n =: E_1 A'$. By IH the factorization of A' is unique, so it suffices to show that the choice of E_1 is forced. Denote $A = \begin{bmatrix}a & b\\c & d\end{bmatrix}$ and $A' = \begin{bmatrix}a' & b'\\c' & d'\end{bmatrix}$ and consider cases:

- $E_1 = E$. Then we have $A' = E^{-1}A$ and

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

  Since all of these entries are nonnegative, we thus have

$$A' = E^{-1}A \iff \begin{cases}a' = a - c \geq 0\\b' = b - d \geq 0\end{cases} \iff \begin{cases}a \geq c\\b \geq d\end{cases}$$

- $E_1 = E'$. Then we have and similarly can deduce

$$A' = E'^{-1}A \iff \begin{bmatrix}a' & b'\\c' & d'\end{bmatrix} = \begin{bmatrix}1 & 0\\-1 & 1\end{bmatrix}\begin{bmatrix}a & b\\c & d\end{bmatrix} = \begin{bmatrix}a & b\\c - a & d - b\end{bmatrix} \iff \begin{cases}a \leq c\\b \leq d\end{cases}$$

Also note that for $n \geq 1$ that $E_1 \dots E_n \neq I$ (e.g. since each E_i only increases an off-diagonal entry and both starting matrices E and E' have a 1 on the off-diagonal), so in particular $A \neq I$ and either $a + b > c + d$ or $a + b < c + d$. Then by the lemma either $a \geq c, b \geq d$ or $a \leq c, b \leq d$. It is impossible for both to be true simultaneously, since that would force $a = c$ and $b = d$ and then $1 = \det A = ad - bc = 0$ which is a contradiction. Thus exactly one is true, so exactly one of $A' = E^{-1}A$ or $A' = E'^{-1}A$ is true, so exactly one of $E_1 = E$ or $E_1 = E'$ is true. Therefore the choice of E_1 is forced, which completes the induction and the product is unique. $\square$

M.16

By definition, English words have the same pronunciation if their phonetic spellings in the dictionary are the same. The homophonic group $\mathcal{H}$ is generated by the letters of the alphabet, subject to the following relations: English words with the same pronunciation represent equal elements of the group. Thus $be = bee$, and since $\mathcal{H}$ is a group, we can cancel be to conclude that $e = 1$. Try to determine the group $\mathcal{H}$.

Solution.
The 1993 paper "Homophonic Quotients of Free Groups" by Jean-François Mestre, René Schoof, Lawrence Washington, and Don Zagier (which is what Artin references in a footnote) shows that $\mathcal{H}$ is trivial, whose proof we replicate here:

Proof.
From the fact that $e = 1$, we can also conclude that the other vowels a, i, o, u, y are all the identity from the homophones

$$lead = led \qquad maid = made \qquad sow = sew \qquad buy = by \qquad lye = lie$$

With this, we next show w, y, h, k, n, p, b are all trivial via

$$sow = so \quad hour = our \quad knight = night \quad damn = dam \quad psalter = salter \quad plumb = plum$$

Next, we have s, t, l, r, m are all trivial by

$$base = bass \quad butt = but \quad tolled = told \quad barred = bard \quad dammed = damned$$

Now d and g are the identity by

$$chased = chaste \qquad sign = sine$$

Moving along, we have z, c, j, q, x trivial via

$$daze = days \quad cite = sight \quad jeans = genes \quad queue = cue \quad tax = tacks$$

This finally leaves $f = v = 1$ by

$$phase = faze \quad leitmotiv = leitmotif$$

Therefore every letter is the identity and the group $\mathcal{H}$ is trivial. □