Appendix week 12

Proofs of results on permutations mentioned in the notes.

Recall example from notes:

Example Let $A = \{1, 2, 3, 4, 5, 6\}$ and

$$\pi = \left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{array} \right).$$

It is easy to check that $\pi^6 = 1_A$. Choose $1 \in A$ and repeatedly apply π to 1 six times to get

$$1 \rightarrow 5 \rightarrow 4 \rightarrow 1 \rightarrow 5 \rightarrow 4 \rightarrow 1.$$

If written as $(1, 5, 4, 1, 5, 4)$, this is **not** a cycle since the elements are not distinct. As a permutation it can be written as

$$(1, 5, 4, 1, 5, 4) = (1, 5, 4),$$

a cycle of length 3. ■

It cannot be assumed that starting with an element and repeatedly applying a permutation will give a cycle (and, in particular, return to the initial element). It has to be **proved** that

Theorem 1 *Given a permutation ρ on a finite set A and $a \in A$ then ρ applied repeatedly to a will give a cycle.*

Proof Consider the set

$$\left\{\rho^i (a) : j \geq 0\right\} \subseteq A.$$

Since A is finite the set $\{\rho^i (a) : j \geq 0\}$ is finite so we have reputation. Thus $\exists k > \ell \geq 0$ for which $\rho^k (a) = \rho^\ell (a)$. Out of all such pairs of (k, ℓ) choose ℓ_0 to be the minimum and then k_0 to be the minimum of all such k for this ℓ_0. This means in particular that $\rho^{k_0} (a) = \rho^{\ell_0} (a)$ yet $\rho^j (a) \neq \rho^{\ell_0} (a)$ for all $k_0 > j > \ell_0$.

We claim that $\ell_0 = 0$. For a contradiction assume that $\ell_0 \geq 1$. Apply ρ^{-1} to both sides of $\rho^{k_0} (a) = \rho^{\ell_0} (a)$ to get $\rho^{k_0 - 1} (a) = \rho^{\ell_0 - 1} (a)$, contradicting the choice of ℓ_0 as the *smallest* of all ℓ for which we can have such an equality. Hence $\ell_0 = 0$.

Let $a_j = \rho^j (a)$, so $a_0 = a$. Then $\rho^{k_0} (a) = \rho^{\ell_0} (a)$ with $\rho^j (a) \neq \rho^{\ell_0} (a)$ for all $k_0 > j > \ell_0$, along with $\ell_0 = 0$, becomes $a_{k_0} = a$ and $a_j \neq a$ for all $k_0 > j > 0$. Thus we have a cycle $(a, a_1, a_2, ..., a_{k_0 - 1})$. ■

Theorem 2 *A permutation on a finite set A is either a cycle or can be expressed as a product (composition) of disjoint cycles.*

Proof is by (strong) induction on the number, r, of points moved by a permutation.

Base case. If $r = 0$ then ρ is the identity which is a 1-cycle.

Inductive step. Assume result true for **all** $r \leq k$.

Let ρ be a permutation that moves $k+1$ points. Let $\mathcal{M}_\rho$ be the set of elements moved by ρ, so $|\mathcal{M}_\rho| = k+1$ Let $a \in \mathcal{M}_\rho$, so a point *moved* by ρ.

By the previous result we have a cycle $(a_0, a_1, a_2, ..., a_{n-1})$ where $a_0 = a$, $a_j = \rho^j(a)$ and $\rho(a_{n-1}) = a_0$. We label this cycle as σ.

Let $\mathcal{M}_\sigma$ be the set of elements moved by σ, so $|\mathcal{M}_\sigma| = n$.

Note that if σ moves an element a then, by definition, it sends it to the same place as ρ sends it, which can be written as

$$a \in \mathcal{M}_\sigma \Rightarrow (\sigma(a) = \rho(a)). \tag{1}$$

This is also means that σ moves only *some* of the elements moved by ρ, i.e.

$$\mathcal{M}_\sigma \subseteq \mathcal{M}_\rho.$$

In turn this means

$$n = |\mathcal{M}_\sigma| \leq |\mathcal{M}_\rho| = k+1$$

Thus $2 \leq n \leq k+1$.

Consider the permutation $\sigma^{-1} \circ \rho$ and two cases.

- Assume $a \notin \mathcal{M}_\rho$ in which case $a \notin \mathcal{M}_\sigma$ since $\mathcal{M}_\sigma \subseteq \mathcal{M}_\rho$. Thus a is fixed by both ρ and σ and hence σ^{-1}. Therefore

$$\begin{aligned}\left(\sigma^{-1} \circ \rho\right)(a) &= \sigma^{-1}(\rho(a)) \\ &= \sigma^{-1}(a) \quad \text{since } a \text{ is fixed by } \rho \\ &= a \quad \text{since } a \text{ is fixed by } \sigma^{-1}.\end{aligned}$$

  Hence if $a \notin \mathcal{M}_\rho$ then a is fixed by $\sigma^{-1} \circ \rho$.

- Assume $a \in \mathcal{M}_\sigma$. Then by (1) above, $\sigma(a) = \rho(a)$ .Therefore

$$\begin{aligned}\left(\sigma^{-1} \circ \rho\right)(a) &= \sigma^{-1}(\rho(a)) \\ &= \sigma^{-1}(\sigma(a)) \quad \text{since } \sigma(a) = \rho(a) \\ &= a.\end{aligned}$$

Hence if $a \in \mathcal{M}_\sigma$ then a is fixed by $\sigma^{-1} \circ \rho$.

The two bullet points imply that the only elements moved by $\sigma^{-1} \circ \rho$ satisfy $a \in \mathcal{M}_\rho$ and $a \notin \mathcal{M}_\sigma$, i.e. $a \in \mathcal{M}_\rho \setminus \mathcal{M}_\sigma$. Thus the number of points moved by $\sigma^{-1} \circ \rho$ is

$$\begin{aligned} &\leq |\mathcal{M}_\rho \setminus \mathcal{M}_\sigma| \\ &= |\mathcal{M}_\rho| - |\mathcal{M}_\sigma| \quad \text{since } \mathcal{M}_\sigma \subseteq \mathcal{M}_\rho \\ &= (k+1) - n \\ &\leq (k+1) - 2 \quad \text{since } n \geq 2, \\ &= k - 1.\end{aligned}$$

Because this number is $\leq k$ we can apply the inductive hypothesis to express $\sigma^{-1} \circ \rho$ as a product of disjoint cycles, i.e.

$$\sigma^{-1} \circ \rho = \sigma_1 \circ \cdots \circ \sigma_t.$$

The elements moved by $\sigma_1 \circ \cdots \circ \sigma_t$ are fixed by σ and so $\sigma_1 \circ \cdots \circ \sigma_t$ and σ are disjoint, and thus $\sigma_1, \cdots, \sigma_t$ and σ are all disjoint. Finally

$$\rho = \sigma \circ \sigma_1 \circ \cdots \circ \sigma_t,$$

so the result holds for permutations that move $k+1$ elements. Hence by induction it holds for all permutations. ■

Example continued Let $A = \{1, 2, 3, 4, 5, 6\}$ and π as above. We have found the cycle $(1, 5, 4)$. Next $2 \notin (1, 5, 4)$ so we find the cycle starting with 2, namely $(2, 6)$. Finally, 3 is in neither of these cycles, and the permutation starting with 3 is simply (3). The method now ends, as it always must when A is a finite set. Therefore

$$\pi = (1, 5, 4) \circ (2, 6) \circ (3) = (1, 5, 4) \circ (2, 6).$$

Question What happens if we start with a different number, say 2 in place of 1 in the above example? We would get $\pi = (2,6) \circ (1,5,4)$. But we know that composition of permutations is not commutative in general so can we have

$$(2,6) \circ (1,5,4) = \pi = (1,5,4) \circ (2,6)?$$

Answer Yes!

Theorem 3 *Disjoint permutations on a set commute.*

Proof Let ρ and π be disjoint permutations on A. Let $a \in A$.

There are three cases,

i) a is moved only by ρ,

ii) a is moved only by π and

iii) a is not moved by either.

(Since ρ and π are disjoint there is no fourth case.)

Case (i) Assume a is fixed by π. Let $b = \rho(a)$, so $b \neq a$ since ρ moves a. Note that *if* ρ were to fix b *then* $\rho(b) = b = \rho(a)$ But ρ is injective, so $b = a$, contradicting $b \neq a$. Hence ρ moves b. But ρ and π are disjoint so π fixes b. We can now justify every step in

$$\begin{aligned}
\rho \circ \pi(a) &= \rho(\pi(a)) \quad \text{by definition of } \circ, \\
&= \rho(a), \quad \text{since } \pi \text{ fixes } a, \\
&= b, \quad \text{by definition of } b, \\
&= \pi(b), \quad \text{since } \pi \text{ fixes } b, \\
&= \pi(\rho(a)) \quad \text{by definition of } b, \\
&= \pi \circ \rho(a). \quad \text{by definition of } \circ.
\end{aligned}$$

Case (ii) Assume a is fixed by ρ. Just interchange $\rho \leftrightarrow \pi$ in the proof of case (i) to get a proof in this case.

Case (iii) a is not moved by neither σ or ρ.

$$\begin{aligned}
\rho \circ \pi(a) &= \rho(\pi(a)) = \rho(a), \quad \text{since } \pi \text{ fixes } a, \\
&= a \quad \text{since } \rho \text{ fixes } a, \\
&= \pi(a) \\
&= \pi(\rho(a)) = \pi \circ \rho(a).
\end{aligned}$$

In all cases we get $\rho \circ \pi (a) = \pi \circ \rho (a)$, an equality on *elements* in A. True for all $a \in A$ means $\rho \circ \pi = \pi \circ \rho$, an equality of *functions*, and hence π and ρ commute. ■

We can go further and prove that the decomposition into disjoint cycles is unique. A proof of this is by induction and within it you need to be able to "cancel" permutations.

Lemma 4 ***Cancellation Law*** *Assume that α, β and γ are permutations on a set A. If $\gamma \circ \alpha = \gamma \circ \beta$ then $\alpha = \beta$. If $\alpha \circ \gamma = \beta \circ \gamma$ then $\alpha = \beta$.*

Proof Assume $\gamma \circ \alpha = \gamma \circ \beta$. Then

$$\begin{aligned} \alpha &= 1_A \circ \alpha = \left(\gamma^{-1} \circ \gamma\right) \circ \alpha \\ &= \gamma^{-1} \circ (\gamma \circ \alpha) \quad \text{composition is associative} \\ &= \gamma^{-1} \circ (\gamma \circ \beta) \quad \text{by assumption} \\ &= \left(\gamma^{-1} \circ \gamma\right) \circ \beta \\ &= 1_A \circ \beta = \beta. \end{aligned}$$

Leave the other case to students. ■

A further result is needed in the proof of uniqueness.

Lemma 5 *If β and γ are cycles on A that both move an element $a \in A$, and $\beta^r (a) = \gamma^r (a)$ for all $r \geq 1$ then $\beta = \gamma$.*

(This result allows us to go from knowing what β and γ do to *one* element to knowing that they act identically on all elements, that is, they are the same permutation.)

Proof Let $a \in A$ be an element moved by both β and γ. A cycle can start at any point so we can start β at a and write

$$\beta = (a, a_1, a_{2,...}, a_m) \text{ where } a_i = \beta^i (a) \text{ for all } i \leq m \text{ and } \beta (a_m) = a. \quad (2)$$

Similarly, we can start γ at a with

$$\gamma = (a, b_1, b_2, ..., b_n) \text{ where } b_j = \gamma^j (a) \text{ for all } j \leq n \text{ and } \gamma (b_n) = a. \quad (3)$$

Without loss of generality assume $m \leq n$, (if not the case, relabel β as γ and γ as β.) Then from (2), for all $i \leq m$ we have

$$\begin{aligned} a_i &= \beta^i (a) = \gamma^i (a) \quad \text{by assumption in Theorem (with } r = i\text{)}, \\ &= b_i, \quad \text{by } (3), \end{aligned}$$

Thus we could write γ as $(a, a_1, a_2, ..., a_m, b_{m+1}, ..., b_n)$. But then

$$\begin{aligned} b_{m+1} &= \gamma^{m+1}(a) && \text{by } (3), \\ &= \beta^{m+1}(a) && \text{by assumption in Theorem } (r = m+1), \\ &= \beta(\beta^m(a)) = \beta(a_m) = a, && \text{by } (2). \end{aligned}$$

So the cycle in γ goes back to a. Thus n, the cycle length of γ, equals m. Hence γ and β contain the same elements and are the same length therefore $\gamma = \beta$. ■

Theorem 6 *A permutation on a finite set A can be expressed as a product of disjoint cycles* ***uniquely*** *apart from the order of the cycles.*

Proof Let

$$\pi = \alpha_1 \circ \alpha_2 \circ .... \circ \alpha_s = \beta_1 \circ \beta_2 \circ ... \circ \beta_t$$

be two factorizations into disjoint cycles. Proof is by induction on $n = \max(s, t)$.

1. **Base case** If $n = 1$ then $\pi = \alpha_1 = \beta_1$ and the two factorizations are identical.

2. **Inductive Step** Assume result true for $n = k$. So if $\alpha_1 \circ \alpha_2 \circ .... \circ \alpha_s = \beta_1 \circ \beta_2 \circ ... \circ \beta_t$ (disjoint cycles on each side) with $\max(s, t) = k$ then the β_i can be renumbered so $\alpha_i = \beta_i$ for all i, and in particular, $s = t$.

   Assume we have a permutation π that has two factorizations as above with $\max(s, t) = k + 1$.

   Let $a \in A$ be an element moved by β_t. By disjointedness a is unmoved by all $\beta_i, 1 \leq i \leq t - 1$. Thus for $r \geq 1$ we have

$$\begin{aligned} \pi^r(a) &= (\beta_1 \circ \beta_2 \circ ... \circ \beta_t)^r(a) \\ &= (\beta_1 \circ \beta_2 \circ ... \circ \beta_t) \circ (\beta_1 \circ \beta_2 \circ ... \circ \beta_t) \circ \cdots \circ (\beta_1 \circ \beta_2 \circ ... \circ \beta_t)(a) \\ &= \beta_t^r \circ \beta_{t-1}^r \circ ... \circ \beta_2^r \circ \beta_1^r(a), \quad \text{disjoint permutations commute,} \\ &= \beta_t^r \circ \beta_{t-1}^r \circ ... \circ \beta_2^r(a), \qquad \text{since } a \text{ is fixed by } \beta_1, \text{ and continue,} \\ &\vdots \\ &= \beta_t^r(a), \qquad \text{since } a \text{ is fixed by } \beta_{t-1}. \end{aligned}$$

Thus $\pi^r(a) = \beta_t^r(a)$ for all $r \geq 1$ (We cannot yet use the Lemma above since π need not be a cycle.)

Since a is moved by π it must be moved by some $\alpha_j, 1 \leq j \leq s$ and unmoved by all the other $\alpha_i, i \neq j$. By relabelling, we can assume that a is moved by α_s alone. By the same argument as for β we find that $\pi^r(a) = \alpha_s^r(a)$ for all $r \geq 1$.

Combine to get $\alpha_s^r(a) = \beta_t^r(a)$ for all $r \geq 1$. Since both α_s and β_t are cycles we can now apply the Lemma above and deduce $\alpha_s = \beta_t$. By the cancellation law we get

$$\alpha_1 \circ \alpha_2 \circ .... \circ \alpha_{s-1} = \beta_1 \circ \beta_2 \circ ... \circ \beta_{t-1}.$$

Now $\max(s-1, t-1) = \max(s,t) - 1 = k$ and we can use the inductive hypothesis to conclude that $s = t$ and, on relabelling the β_i, $\alpha_1 = \beta_1, ..., \alpha_{t-1} = \beta_{t-1}$.

Hence the result is true if $\max(s,t) = k+1$. Thus by induction the result holds for all permutations. ■

Theorem 7 *The order of a cycle is equal to its length.*

Proof Let σ be a cycle on A. Let d be the order of σ, so $\sigma^d = 1_A$ and let ℓ be the length of σ.

We will show that $d = \ell$ by showing that $d \geq \ell$ and $d \leq \ell$.

Let $a_0 \in A$ be chosen as an element moved by σ. Recall that we can write the cycle starting with any element moved by it. Hence

$$\sigma = \left(a_0, \sigma(a_0), \sigma^2(a_0), ..., \sigma^{\ell-1}(a_0)\right).$$

From this we see that

$$\begin{aligned} \sigma(a_0) &\neq a_0, \\ \sigma(a_0) &\neq a_0, \\ &\vdots \\ \sigma^{\ell-1}(a_0) &\neq a_0, \\ \sigma^{\ell}(a_0) &= a_0. \end{aligned}$$

Proof that $d \geq \ell$. From the definition of d as $\sigma^d = 1_A$ we have $\sigma^d(a_0) = a_0$ for the element chosen above. Yet, from the above list we see that

$$\sigma^d(a_0) = a_0 \neq \sigma^j(a_0)$$

for any $0 \leq j \leq \ell - 1$. In other words, $d \neq j$ for any $0 \leq j \leq \ell - 1$. Hence $d \geq \ell$.

Proof that $d \leq \ell$. Let $b \in A$ be given. There are two cases.

Case (i) If b is moved by σ, then b occurs in the cycle seen above,

$$\left(a_0, \sigma(a_0), \sigma^2(a_0), ..., \sigma^{\ell-1}(a_0)\right),$$

i.e. $b = \sigma^j(a_0)$ for some $0 \leq j \leq \ell - 1$. Consider

$$\begin{aligned} \sigma^\ell(b) &= \sigma^\ell\left(\sigma^j(a_0)\right) = \sigma^{\ell+j}(a_0) = \sigma^{j+\ell}(a_0) \\ &= \sigma^j\left(\sigma^\ell(a_0)\right) = \sigma^j(a_0), \quad \text{see last line in above list,} \\ &= b \quad \text{since } b = \sigma^j(a_0). \end{aligned}$$

Thus $\sigma^\ell(b) = b$.

Case (ii) The second case is b fixed by σ. But then trivially b is fixed by σ^ℓ, i.e. $\sigma^\ell(b) = b$.

In both cases i) and ii) we get $\sigma^\ell(b) = b$.

True for all $b \in A$ means that $\sigma^\ell = 1_A$.

But d is the order of σ so, by Lemma, $d|\ell$. In particular, $d \leq \ell$.

Combine $d \geq \ell$ and $d \leq \ell$ from (a) and (b) to deduce $d = \ell$. ■

Theorem 8 *Suppose that $\pi = \pi_1 \circ \pi_2$ is a decomposition into a product of two disjoint permutations then the order of π is the least common multiple of the orders of π_1 and π_2.*

Proof Let d be the order of π. Let d_1 be the order of π_1 and d_2 the order of π_2. Set $f = \text{lcm}(d_1, d_2)$.

We will show $d = f$ by showing that $d \leq f$ and $d \geq f$.

Proof that $d \leq f$.

From the definition of $f = \operatorname{lcm}(d_1, d_2)$ we have $d_1|f$ and $d_2|f$ which in turn mean there exist integers a_1 and a_2 such that $f = a_1 d_1$ and $f = a_2 d_2$. Then

$$\begin{aligned}
\pi^f &= (\pi_1 \circ \pi_2)^f \\
&= (\pi_1 \circ \pi_2) \circ (\pi_1 \circ \pi_2) \circ ... \circ (\pi_1 \circ \pi_2) \\
&= \pi_1^f \circ \pi_2^f \qquad \text{reordering allowed since } \pi_1 \text{ and } \pi_2 \text{ disjoint,} \\
&= \pi_1^{a_1 d_1} \circ \pi_2^{a_2 d_2} \\
&= \left(\pi_1^{d_1}\right)^{a_1} \circ \left(\pi_2^{d_2}\right)^{a_2} \\
&= (1_A)^{a_1} \circ (1_A)^{a_2}, \\
&= 1_A.
\end{aligned}$$

That is $\pi^f = 1_A$. But the order of π is d so, by the Lemma, $d|f$. In particular, $d \leq f$.

Proof that $d \geq f$.

Let $a \in A$ be given. There are two cases.

(i) **Suppose a is moved by π_1.** But then a is fixed by π_2 since the two cycles are disjoint. Recalling that d is the order of π we start from

$$\begin{aligned}
a &= \pi^d(a) = (\pi_1 \circ \pi_2)^d (a) \\
&= \left(\pi_1^d \circ \pi_2^d\right)(a), \quad \text{reordering allowed since } \pi_1 \text{ and } \pi_2 \text{ are disjoint,} \\
&= \pi_1^d\left(\pi_2^d(a)\right), \quad \text{by definition of composition,} \\
&= \pi_1^d(a) \quad \text{since } a \text{ is fixed by } \pi_2 \text{ and thus by } \pi_2^d.
\end{aligned}$$

Thus $\pi_1^d(a) = a$.

(ii) **In the second case a is fixed by π_1.** Trivially it is then fixed by π_1^d, i.e. $\pi_1^d(a) = a$.

So in both cases i) and ii) we have $\pi_1^d(a) = a$. True for all $a \in A$ means that $\pi_1^d = 1_A$. But d_1 is the order of π_1 and so, by the Lemma, $d_1|d$.

Repeat the argument, replacing π_1 by π_2 and vice-versa to get $\pi_2^d = 1_A$ and thus $d_2|d$. (Student must do this.)

Thus $d_1|d$ and $d_2|d$, in which case, d is *a* common multiple of d_1 and d_2. Yet f is the *least* of all such common multiples, hence $f \leq d$.

Combine $d \leq f$ and $f \leq d$ from (a) and (b) to get $d = f$. ■

Theorem 9 *Suppose that*

$$\pi = \pi_1 \circ \pi_2 \circ .... \circ \pi_m$$

is a decomposition into a product of disjoint permutations, then the order of π *is the least common multiple of the orders of the permutations* $\pi_1, \pi_2, ..., \pi_m$.

Proof by induction on m.

If $m = 2$ then the result holds by a previous Theorem.

Assume result holds for $m = k$. Let π have a decomposition into $k+1$ disjoint permutations, $\pi_1 \circ \pi_2 \circ .... \circ \pi_{k+1}$, and let o_i =order(π_i).

By the induction hypothesis the order of $\pi_1 \circ \pi_2 \circ .... \circ \pi_k$ equals lcm $(o_1, o_2, ..., o_k)$. The earlier Theorem on the order of the composition of *two* disjoint permutations means that the order of $(\pi_1 \circ \pi_2 \circ .... \circ \pi_k) \circ \pi_{k+1}$ equals

$$\operatorname{lcm}(\operatorname{lcm}(o_1, o_2, ..., o_k), o_{k+1}) = \operatorname{lcm}(o_1, o_2, ..., o_k, o_{k+1})$$

as required. ■

(I leave it to the student to check that for $a, b, c \in \mathbb{Z}$, $\operatorname{lcm}(\operatorname{lcm}(a, b), c) = \operatorname{lcm}(a, b, c)$.)

Appendix to the Appendix

We have seen that we can build all permutations out of cycles. But there are other possible building blocks.

Definition 10 *A* ***transposition*** *is a cycle of length 2.*

Example $(2,3) \in S_5$ is a transposition.

Example In S_5 we have $(2,3,4) = (3,4) \circ (2,4)$, i.e. we have written a permutation as a product of transpositions. This decomposition is not unique, for example $(2,3,4) = (3,4,2) = (4,2) \circ (3,2)$ and the sets of transpositions $\{(4,2),(3,2)\}$, $\{(3,4),(2,4)\}$ are different. But we do have a general result.

Theorem 11 *Every cycle is a product of transpositions.*

Proof Simply check that

$$(a_1, a_2, ..., a_r) = (a_{r-1}, a_r) \circ (a_{r-2}, a_r) \circ ... \circ (a_2, a_r) \circ (a_1, a_r).$$

■

Corollary 12 *Every permutation can be written as a product of transpositions.*

Proof Every permutation can be written as a product of cycles, and every cycle is a product of transpositions. ■

Example (i) In S_7 we have

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 6 & 2 & 1 & 5 & 4 \end{pmatrix} &= (1,3,6,5) \circ (2,7,4) \\ &= (6,5) \circ (3,5) \circ (1,5) \circ (7,4) \circ (2,4). \end{aligned}$$

This decomposition is neither unique or disjoint.

(ii) In S_4

$$(1,2,3,4) = (1,4) \circ (1,3) \circ (1,2) = (1,4) \circ (2,3) \circ (1,3).$$

(iii) In S_4,

$$\begin{aligned} (1,2,3) &= (1,3)(1,2) \\ &= (1,3)(4,2)(1,2)(1,4) \\ &= (1,3)(4,2)(1,2)(1,4)(2,3)(2,3), \end{aligned}$$

it might not seem unreasonable that the parity of number of factor (i.e. odd or even) is the same for all factorizations. We do not pursue this further.

Positive powers

Definition 13 *For $m \in \mathbb{Z}, m \geq 1$, and $g \in G$ define positive powers inductively by*

$$g^m = g * g^{m-1},$$

with $g^0 = e$, the identity.

Theorem 14

$$g^m * g^n = g^{m+n} \text{ and } (g^m)^n = g^{mn}.$$

Proof i) By induction on $m+n$. If $m+n=0$ then $m=n=0$ so the result states $1_A * 1_A = 1_A$ which is true.

Assume result is true if $m+n=k$. Assume $m+n=k+1$. If $m=0$ then the result is $1_A * g^n = g^{0+n}$ which is true.

So assume $m \geq 1$. Then

$$\begin{aligned} g^m * g^n &= \left(g * g^{m-1}\right) * g^n \quad \text{by definition of } g^m, \\ &= g * \left(g^{m-1} * g^n\right) \quad \text{by associativity} \\ &= g * g^{m-1+n} \quad \text{by inductive hypothesis} \\ &= g^{m+n} \quad \text{by definition of powers.} \end{aligned}$$

Thus the result holds when $m+n=k+1$ and thus for all values of $m+n$, i.e. all $m, n \geq 0$.

ii) By induction on n, so here the proposition we will prove true for all $n \geq 0$ is that

$$(g^m)^n = g^{mn} \text{ for all } m \geq 0.$$

If $n=0$ then the result states $(g^m)^0 = g^0 = 1_A$ for all $m \geq 0$, which is true.

Assume the result is true for $n=k$. Assume that $n=k+1$. Then

$$\begin{aligned} (g^m)^{k+1} &= g^m * (g^m)^k \quad \text{by definition of } k+1\text{-st power} \\ &= g^m * g^{mk} \quad \text{by inductive hypothesis} \\ &= g^{m+mk} \quad \text{by part i,} \\ &= g^{m(k+1)}, \end{aligned}$$

for all $m \geq 0$. Thus the result holds for $n=k+1$ and thus, by induction, for all $n \geq 0$. ■

Negative powers

Definition 15 *For $m \in \mathbb{Z}$, and $g \in G$ define*

$$g^m = \left(g^{-1}\right)^{-m},$$

i.e. the positive power of the inverse.

Elementary consequences of the Group axioms:

Theorem 16 *Let $(G, *)$ be a group.*

i) For $a, x, y \in G$ if $x * a = y * a$ then $x = y$ (a cancellation result),

ii) For $a, x, y \in G$ if $a * x = a * y$ then $x = y$ (a cancellation result),

iii) $e^{-1} = e$, where e is the identity,

iv) For all $x \in G, \left(x^{-1}\right)^{-1} = x$,

v) For all $x, y \in G, (x * y)^{-1} = y^{-1} * x^{-1}$,

vi) For $x_1, x_2, ..., x_n \in G$,

$$(x_1 * x_2 * ... * x_n)^{-1} = x_n^{-1} * ... * x_2^{-1} * x_1^{-1},$$

vii) For $m, n \in \mathbb{Z}$ and $g \in G$, $g^m * g^n = g^{m+n}$ and $(g^n)^m = g^{nm}$.

Proof (i)

$$\begin{aligned} x * a = y * a &\Rightarrow (x * a) * a^{-1} = (y * a) * a^{-1} \\ &\Rightarrow x * \left(a * a^{-1}\right) = y * \left(a * a^{-1}\right) \quad \text{by associativity,} \\ &\Rightarrow x * e = y * e \quad \text{definition of inverses,} \\ &\Rightarrow x = y. \end{aligned}$$

(ii)

$$\begin{aligned} a * x = a * y &\Rightarrow a^{-1} * (a * x) = a^{-1} * (a * y) \\ &\Rightarrow \left(a^{-1} * a\right) * x = \left(a^{-1} * a\right) * y \quad \text{by associativity,} \\ &\Rightarrow e * x = e * y \quad \text{definition of inverses,} \\ &\Rightarrow x = y. \end{aligned}$$

(iii)

$$\begin{aligned} e^{-1} &= e^{-1} * e \quad \text{since } e \text{ is the identity,} \\ &= e \quad \text{since } e^{-1} \text{ is the inverse of } e. \end{aligned}$$

(iv) By definition $\left(x^{-1}\right)^{-1}$ is the inverse of x^{-1}. Yet $x^{-1} * x = x * x^{-1} = e$ means that x is *also* the inverse of x^{-1}. We know that the inverse of an element is *unique,* hence $\left(x^{-1}\right)^{-1} = x$ as required.

(v) By definition $(x * y)^{-1}$ is the inverse of $x * y$. Yet

$$\begin{aligned} (x * y) * \left(y^{-1} * x^{-1}\right) &= \left((x * y) * y^{-1}\right) * x^{-1} \quad \text{by associativity,} \\ &= \left(x * \left(y * y^{-1}\right)\right) * x^{-1} \quad \text{again by associativity,} \\ &= (x * e) * x^{-1} \\ &= x * x^{-1} = e. \end{aligned}$$

Similarly, $(y^{-1} * x^{-1}) * (x * y) = e$. So $y^{-1} * x^{-1}$ is *also* an inverse of $x * y$. We know that the inverse of an element is *unique,* hence $(x * y)^{-1} = y^{-1} * x^{-1}$ as required.

(vi) Use induction based on

$$\begin{aligned} (x_1 * x_2 * ... * x_n)^{-1} &= ((x_1 * x_2 * ... * x_{n-1}) * x_n)^{-1} \\ &= x_n^{-1} * (x_1 * ... * x_{n-1})^{-1}, \end{aligned}$$

having used part (v).

(vii) *Proof of* $g^m * g^n = g^{m+n}$: This is done in cases.

- If $m \geq 1, n \geq 1$ the result has been seen earlier.
- If either $m = 0$ or $n = 0$, use the fact that $g^0 = e$, the identity.
- If $m \leq -1$ and $n \leq -1$ write $m = -r, n = -t$ when, by the definition for negative powers,

$$\begin{aligned} g^m * g^n &= \left(g^{-1}\right)^r * \left(g^{-1}\right)^s \\ &= \left(g^{-1}\right)^{r+s} \quad \text{by the result for } \textit{positive} \text{ powers,} \\ &= g^{-(r+s)} = g^{m+n}. \end{aligned}$$

- If $m \leq -1$ and $n \geq 1$ then $g^m * g^n = \left(g^{-1}\right)^r * g^n$, with $r = -m \geq 1$. Here $\left(g^{-1}\right)^r = g^{-1} * \left(g^{-1}\right)^{r-1}$ and $g^n = g * g^{n-1}$ by the iterative definition of a positive power. But by the index law for *positive* powers for g^{-1} we have $g^{-1} * \left(g^{-1}\right)^{r-1} = \left(g^{-1}\right)^{r-1} * g^{-1}$. So we can combine as in

$$\begin{aligned}
\left(g^{-1}\right)^r * g^n &= \left(\left(g^{-1}\right)^{r-1} * g^{-1}\right) * \left(g * g^{n-1}\right) \\
&\qquad \text{by definition of } r\text{-th and } n\text{-}th \text{ powers,} \\
&= \left(\left(\left(g^{-1}\right)^{r-1} * g^{-1}\right) * g\right) * g^{n-1} \\
&\qquad \text{by associativity,} \\
&= \left(\left(g^{-1}\right)^{r-1} * \left(g^{-1} * g\right)\right) * g^{n-1} \\
&\qquad \text{by associativity,} \\
&= \left(\left(g^{-1}\right)^{r-1} * e\right) * g^{n-1} \\
&= \left(g^{-1}\right)^{r-1} * g^{n-1}.
\end{aligned}$$

Continue, to get $\left(g^{-1}\right)^{r-n}$, if $r \geq n$, or g^{n-r} otherwise. In both cases the end result is $g^{n-r} = g^{n+m}$ since $m = -r$.

- If $m \geq 1$ and $n \leq -1$ then $g^m * g^n = g^m * \left(g^{-1}\right)^s$ with $s = -n \geq 1$. The result follows similarly.

In all cases we have $g^m * g^n = g^{m+n}$.

Proof of $\left(g^n\right)^m = g^{mn}$: This is done in cases.

- If $m \geq 1, n \geq 1$ the result has been seen earlier.
- If either $m = 0$ or $n = 0$, both sides are equal to the identity.
- If $n \geq 1$ and $m \leq -1$ write $m = -r$. Then

$$\begin{aligned}
\left(g^n\right)^m &= \left(g^n\right)^{-r} = \left(\left(g^n\right)^{-1}\right)^r \quad \text{by definition of negative exponent,} \\
&= \left(\left(g^{-1}\right)^n\right)^r, \quad \text{by part (vi) of this Theorem,} \\
&= \left(g^{-1}\right)^{nr} \quad \text{by this result for positive exponents,} \\
&= g^{-nr} \quad \text{by definition of negative exponent,} \\
&= g^{nm}.
\end{aligned}$$

- If $n \leq -1$ and $m \geq 1$ write $n = -s$. Then

$$\begin{aligned} (g^n)^m &= \left(g^{-s}\right)^m = \left(\left(g^{-1}\right)^s\right)^m \qquad \text{by definition of negative exponent,} \\ &= \left(g^{-1}\right)^{sm} \qquad \text{by this result for positive exponents,} \\ &= g^{-sm} \qquad \text{by definition of negative exponent,} \\ &= g^{nm}. \end{aligned}$$

- If $n \leq -1$ and $m \leq -1$ then

$$\begin{aligned} (g^n)^m &= \left(g^{-s}\right)^{-r} = \left(\left(\left(g^{-1}\right)^s\right)^{-1}\right)^r \text{ by definition of negative exponent,} \\ &= \left(\left((g^s)^{-1}\right)^{-1}\right)^r \qquad \text{by part (vi) of this Theorem,} \\ &= (g^s)^r \qquad \text{by part (iv) of this Theorem,} \\ &= g^{sr} \qquad \text{by this result for positive exponents,} \\ &= g^{mn} \qquad \text{since } mn = rs. \end{aligned}$$

Hence in all cases $(g^n)^m = g^{mn}$. ■

Rings

Definition 17 *A **ring** is a non-empty set R along with two binary operations on R, addition $+$ and multiplication $\times$, such that*

1. *$(R, +)$ is an abelian group,*
2. *R is closed under multiplication,*
3. *multiplication is associative on R,*
4. *For all a, b and $c \in R$ we have*

$$\begin{aligned} a \times (b + c) &= a \times b + a \times c \\ (b + c) \times a &= b \times a + c \times a. \end{aligned}$$

These are called the ***Distributive laws***, we are "distributing" the a throughout the terms of the bracket. These laws are important in that they combine both operations, $+$ and $-$.

Note that we **don't** demand that $(R, \times)$ is a group. Non-zero elements in R may fail to have inverses. Even more basic, there may not be a multiplicative identity! And we also **don't** demand that multiplication is commutative.

Example 18 *of rings:*

i) $(\mathbb{Z}, +, \times)$ is the first example of a ring. From that we can go to a finite ring $(\mathbb{Z}_m, +, \times)$.

ii) The set of $n \times n$ matrices with real coefficients, $(M_n(\mathbb{R}), +, \times)$, is a ring. We have a multiplicative identity, the identity matrix, but not every matrix has an inverse. Also this ring is non-commutative.

The interest in rings lies in how the two operations interact with each other. We saw before, in the section on primes, that if we ask additive questions about multiplicative objects, primes, we get questions, such as Goldbach's Conjecture, that have withstood attack for hundreds of years.

In the case of a general ring we have the ***additive*** identity 0. What would we expect of the *multiplication* $0 \times a$ for $a \in R$? Unsurprisingly

Lemma 19 *For all $a \in R$ we have $0 \times a = 0$.*

Proof Let $a \in R$ be given. Since 0 is the additive identity, we have $0+0=0$. Then

$$\begin{aligned}
(0+0) \times a &= 0 \times a \\
0 \times a + 0 \times a &= 0 \times a, \quad \text{by distributive law,} \\
0 \times a &= 0, \quad \text{on adding } -(0 \times a) \text{ to both sides.}
\end{aligned}$$

Since the distributive law is the only axiom to contain both operations, + and × it is no surprise we have to use it in the proof above. ■

Again, -1 is the **additive** inverse of 1 as is $-a$ for any element of R. But are $-a$ and $-1 \times a$ the same? Unsurprisingly we have

Lemma 20 *For all $a \in R$ we have $-1 \times a = -a$.*

Proof Let $a \in R$ be given. Start from $1 + (-1) = 0$. Then

$$\begin{aligned}
(1+(-1)) \times a &= 0 \times a = 0 \quad \text{by result above,} \\
1 \times a + (-1) \times a &= 0 \quad \text{by distributive law,} \\
a + (-1) \times a &= 0 \quad \text{since 1 is the multiplicative identity,} \\
-a + (a + (-1) \times a) &= -a + 0 \quad \text{adding } -a \text{ to both side,} \\
(-a + a) + (-1) \times a &= -a, \quad \text{by associativity on LHS and 0 identity on RHS,} \\
0 + (-1) \times a &= -a, \\
(-1) \times a &= -a,
\end{aligned}$$

What we can see here is that because we have only a few axioms defining a ring, the proof of something quite familiar, is surprisingly long. We increase the number of axioms in the next section.

Fields

Definition 21 *A **field** $(F,+,\times)$, is a non-empty set F along with two binary operations on F, addition $+$ and multiplication $\times$, such that satisfies*

i) $(F,+,\times)$ *is a ring,*

ii) multiplication is commutative on F*,*

iii) There is a multiplicative identity in F*,*

iv) Every non-zero element of F *has a multiplicative inverse.*

The interest in fields comes from the fact that many of a our familiar arithmetic structures are fields.

Example 22 *of fields:*

i) $(\mathbb{R},+,\times),(\mathbb{C},+,\times)$ *and* $(\mathbb{Q},+,\times)$ *are infinite fields,*

ii) $(\mathbb{Z}_p,+_p,\times_p)$ *for* p *a prime, is an example of a finite field.*

But note that $(\mathbb{Z}_m,+_m,\times_m)$ is **not** a field if m not prime.

Something for future years: $(\mathbb{R},+,\times),(\mathbb{C},+,\times)$ and $(\mathbb{Q},+,\times)$ satisfy the axioms of a field and so, to this extent, are the same. But what further properties do they satisfy that show they are different?

On $(\mathbb{R},+,\times)$ and $(\mathbb{Q},+,\times)$ we can define an order relation $a<b$ with properties such that if $a<b$ then $a+c<b+c$ and if $a<b$ and $b<c$ then $a<c$. It can be shown that no such relation exists on $(\mathbb{C},+,\times)$. Hence $(\mathbb{C},+,\times)$ is different to both $(\mathbb{R},+,\times)$ and $(\mathbb{Q},+,\times)$.

But are $(\mathbb{R},+,\times)$ and $(\mathbb{Q},+,\times)$ different? From the first half of the course you know they are different, $\mathbb{R}$ is uncountable while $\mathbb{Q}$ is countable. But here I want to mention another difference. Consider the *sequence* of rational numbers $1, 1.4, 1.41, 1.414, 1.4142, 1.41421, ...$, which gets arbitrarily close (*converges to*) the limit $\sqrt{2}$. Unfortunately, $\sqrt{2}\notin\mathbb{Q}$. So, in $(\mathbb{Q},+,\times)$ it is not true that all convergent sequences converge. But it can be shown that in $(\mathbb{R},+,\times)$ all convergent sequences converge. These ideas take us away from algebra and into areas of analysis.

More examples of binary operations and groups.

Example 23 *of binary operations not seen in course:*

- *$S = M_n(\mathbb{R})$, the set of $n \times n$ matrices with real entries, with a binary operation of either matrix addition or matrix multiplication.*
- *Let X be any non-empty set, $S = \mathcal{P}(X)$, the power set of X, with a binary operation of either $\cap$ or $\cup$.*
- *Let Ω be a non-empty set and S the set of **all** functions $\Omega \to \Omega$ along with $\circ$, composition of functions.*

Example 24 ***Not*** *a binary operation:*

- *If $S = \mathbb{N}$ then subtraction $-$ is not a binary operation since $1 - 2 \notin \mathbb{N}$.*
- *If $S = \mathbb{Q}$ then $a * b = a/b$ is not a binary operation since $1 * 0$ has no meaning.*

Example of binary operations not seen in course: Want to take the time to define sets of polynomials.

Definition 25 *For a set F, a **polynomial over F with variable** x is of the form*

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0,$$

where $a_n, a_{n-1}, ..., a_1, a_0 \in F$.

*The a_i, $0 \leq i \leq n$ are the **coefficients** of the polynomial.*

*If x^n is the largest power of x appearing in the polynomial then n is the **degree** of the polynomial, $a_n x^n$ is the **leading term** and a_n is the **leading coefficient**.*

The collection of all polynomials with one variable x and with coefficients from F will be denoted by $F[x]$. (Note the square brackets.)

Note that $0 \in F[x]$, being $... + 0x^2 + 0x + 0$, but it is **not** said to have a degree, though some books give it degree -1 or even $-\infty$.

Example 26

$$\begin{aligned} 3x^2 + 5x - 1 &\in \mathbb{Z}[x], \\ x^2 - \pi &\in \mathbb{R}[x], \\ \tfrac{3}{7}x^3 - \tfrac{5}{12}x^2 + x &\in \mathbb{Q}[x], \\ 5x^4 + x + 2 &\in \mathbb{Z}_7[x]. \end{aligned}$$

If we can add and multiply numbers in the set F then we can add and multiply the polynomials in $F[x]$.

Example 27 *i) In $\mathbb{Z}[x]$ the sum of $3x^2+5x-1$ and $5x^3-3x^2+2x+1$ is*

$$\begin{array}{rl} & \left(\qquad 3x^2+5x-1\right) \\ + & \left(5x^3-3x^2+2x+1\right) \\ = & 5x^3 \qquad\qquad +7x. \end{array}$$

ii) Addition in $\mathbb{Z}_3[x]$. The sum of $2x^3+2x^2+x+1$ and x^3+2x^2+2 is

$$\begin{array}{rl} & 2x^3+2x^2+x+1 \\ + & \left(x^3+2x^2 \qquad +2\right) \\ = & \qquad\quad x^2+x, \end{array}$$

iii) In $\mathbb{Z}[x]$ the product of x^2+2x+3 and x^2+4 is

$$\begin{array}{rcl} \left(x^2+2x+3\right)\left(x^2+4\right) & = & \qquad\qquad 3x^2 \qquad +12 \\ & & \qquad +2x^3 \qquad +8x \\ & & +x^4 \qquad +4x^2 \\ & = & x^4+2x^3+7x^2+8x+12 \end{array}$$

iv) Multiplication in $\mathbb{Z}_2[x]$. The product of x^3+x+1 and x^2+x+1 is

$$\begin{array}{rcl} \left(x^3+x+1\right)\left(x^2+x+1\right) & = & x^5+x^4+x^3 \\ & & \qquad\qquad +x^3+x^2+x \\ & & \qquad\qquad\qquad +x^2+x+1 \\ & = & x^5+x^4 \qquad\qquad\qquad\qquad +1. \end{array}$$

using $2 \equiv 0 \bmod 2$. Thus $+$ and $\times$ are binary operations on $\mathbb{Z}[x]$ and $\mathbb{Z}_m[x]$.

Aside The results of Chapters 1-3, on arithmetic, congruencies and congruence classes can be given for either $\mathbb{Z}[x]$, $\mathbb{Z}_m[x]$ in place of $\mathbb{Z}$. This is because we can talk of one polynomial dividing another.

Definition 28 *If $f, g \in F[x]$, we say that g **divides** f if there exists $h \in F[x]$ such that $f = gh$.*

Example 29 *In $\mathbb{Z}[x]$, $x-1$ divides x^3-2x^2+1 since*

$$x^3-2x^2+1=(x-1)\left(x^2-x-1\right).$$

In $\mathbb{Z}_2[x]$, $x+1$ divides x^3+1 since

$$x^3+1=(x+1)\left(x^2+x+1\right).$$

We could then talk of greatest common divisors (greatest in terms of degree) and linear combinations. Or we could talk about congruencies, saying $f(x)\equiv g(x) \bmod h(x)$ iff $h(x)$ divides $f(x)-g(x)$ and congruence classes. We could then construct new "algebraic structures" by defining addition and multiplication on these congruence classes of polynomials. *This is something for future years.*

End of aside

Example 30 *of identity. In $(\mathcal{P}(X),\cap)$ the identity is X since $X\cap C=C\cap X=C$ for all $C\in\mathcal{P}(X)$.*

Question Do we always have identities?

Example 31 *Let $2\mathbb{Z}$ be the set of even integers. The product of two even integers is even so $\times$ is a binary operation on $2\mathbb{Z}$. Yet there is no identity in $(2\mathbb{Z},\times)$* ***because 1 is not even****.*

In $(\mathbb{Z},-)$ we have a right identity, $n-0=n$, but no left identity (the left identity won't be 0 since $0-n=-n\neq n$ when $n\neq 0$ and no other possible value for the left identity will work).

Question Do we always have inverses?

Example 32 *In $(M_2(\mathbb{R}),\times)$ not every non-zero matrix here has an inverse, for example*

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

Example 33 *of semigroups. (X is a non-empty set)*

$$(\mathbb{Z},\times),\ (\mathbb{Z}_n,+),\ (\mathbb{Z}_n,\times),\ (\mathbb{N},+),\ (2\mathbb{Z},\times),\ (\mathcal{P}(X),\cap),\ (\mathcal{P}(X),\cup),$$
$$(S_n,\circ),\ (\mathbb{Z}[x],+),(\mathbb{Z}[x],\times),(\mathbb{Z}_n[x],+)\quad \textit{and}\quad (\mathbb{Z}_n[x],\times).$$

Definition 34 *An important subset of $(M_2(\mathbb{R}), \times)$ is the collection of matrices that have an inverse, i.e. are invertible. Such matrices have a non-zero determinant.*

$$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0 \right\}.$$

Here GL stands for ***General Linear***. So again we have “thrown away” the elements with no inverse.

Example 35 *In $(M_2(\mathbb{R}), \times)$ let*

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Then

$$(ab)^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}.$$

But

$$a^2b^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}.$$

So we don't necessarily have $a^2 * b^2 = (a * b)^2$.

Example 36 $(\mathbb{Z}, +)$ *is an additive group.*

Verification

G1 If $m, n \in \mathbb{Z}$ then $m + n \in \mathbb{Z}$,

G2 If $m, n, p \in \mathbb{Z}$ then $(m + n) + p = m + (n + p)$,

G3 We have $0 \in \mathbb{Z}$ and for all $n \in \mathbb{Z}$, $n + 0 = 0 + n = n$,

G4 For any $n \in \mathbb{Z}$ we have $-n \in \mathbb{Z}$ and $n + (-n) = (-n) + n = 0$.

Thus $(\mathbb{Z}, +)$ is an additive group with identity 0 and the inverse of n is $-n$. ■

Example 37 $(\mathbb{Z}_m, +_m)$ *is an additive group.*

Verification We know $(\mathbb{Z}_m, +)$ is a semigroup. So only need note that $[0]_m$ is the identity and, for $[a]_m \in \mathbb{Z}_m$, the inverse is $[-a]_m = [m - a]_m$.

■

Example 38 $(M_n(\mathbb{R}), +)$ $(\mathbb{Z}[x], +)$ *and* $(\mathbb{Z}_m[x], +)$ *are further examples of additive groups. In such groups the identity is normally denoted by 0.*

Example 39 $(\{i, -1, -i, 1\}, \times)$, *where* $i^2 = -1$, *is a multiplicative group.*

Verification From the table

$\times$	1	i	$-i$	-1
1	1	i	$-i$	-1
i	i	-1	1	$-i$
$-i$	$-i$	1	-1	i
-1	-1	$-i$	i	1

we see that G1, G3 (with $e = 1$) and G4 (with $1^{-1} = 1$, $i^{-1} = -i$, $(-1)^{-1} = -1$ and $(-i)^{-1} = i$) are all satisfied. G2 holds since multiplication of complex numbers is associative. ■

Example 40 *Other multiplicative groups are* $(\mathbb{C} \setminus \{0\}, \times)$, $(\mathbb{Q} \setminus \{0\}, \times)$, *and* $(\mathbb{Z}_p^*, \times_p)$.

Question for students. Why are $(M_n(\mathbb{R}), \times)$ $(\mathbb{Z}[x], \times)$ and $(\mathbb{Z}_m[x], \times)$ not multiplicative groups?

Note In the theory of groups a general group is normally written with a multiplicative operation.

In multiplicative groups the identity is normally denoted by 1, *id* or I. Note that I say "normally".

Example 41 $(\{2, 4, 6, 8\}, \times_{10})$.

$\times_{10}$	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

From the table we see that the identity is 6. Also $2^{-1} = 8, 4^{-1} = 4, 6^{-1} = 6$ and $8^{-1} = 2$.