Summer Programme 2021

Solutions to exercises from Michael Artin's *Algebra*

Satvik Saha
19MS154

Indian Institute of Science Education and Research, Kolkata, Mohanpur, West Bengal, 741246, India.

Chapter 1

Matrix Operations

1.4 Permutation Matrices

Exercise 1. Consider the permutation p defined by $1 \rightsquigarrow 3$, $2 \rightsquigarrow 1$, $3 \rightsquigarrow 4$, $4 \rightsquigarrow 2$.

(a) Find the associated permutation matrix P.

(b) Write p as a product of transpositions and evaluate the corresponding matrix product.

(c) Compute the sign of p.

Solution.

(a) The column P_i must be the standard basis vector $\boldsymbol{e}_{p(i)}$, so

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

(b) Check that $p = (1,3,4,2) = (1,2)(1,4)(1,3)$. This product is given by

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

(c) Since p is the product of an odd number of transpositions, its sign is -1. This is verified by calculating the determinant

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

Exercise 2. Prove that every permutation matrix is a product of transpositions.

Solution. Note that this is equivalent to stating that any ordered list can be sorted using transpositions.

The statement is trivially true for all 2×2 permutation matrices,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

the first being the identity and the second being a transposition itself. Suppose that any $n \times n$ permutation matrix is the product of transpositions. Use the fact that for square matrices A and B,

$$\begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} B & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} AB & 0 \\ 0 & 1 \end{bmatrix},$$

which means that if a permutation matrix $P = E_1 E_2 \dots E_k$, then

$$\begin{bmatrix} P & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} E_1 & 0 \\ 0 & 1 \end{bmatrix} \dots \begin{bmatrix} E_k & 0 \\ 0 & 1 \end{bmatrix}.$$

Now let Q be an arbitrary $(n+1) \times (n+1)$ permutation matrix. Let j be the index of the row of Q which is precisely $(0 \dots 0\, 1)$, and let E be the transposition matrix which interchanges the rows $j \leftrightarrow n+1$. Then,

$$EQ = \begin{bmatrix} Q' & 0 \\ 0 & 1 \end{bmatrix},$$

where Q' is an $n \times n$ permutation matrix. This is because Q' has exactly one 1 in each row and column, the remaining elements being 0. Multiply both sides by E, and use the fact that $E^2 = \mathbb{I}$. Now, Q' is a product of transpositions $E_1 \dots E_k$, so we finally have

$$Q = E \begin{bmatrix} Q' & 0 \\ 0 & 1 \end{bmatrix} = E \begin{bmatrix} E_1 & 0 \\ 0 & 1 \end{bmatrix} \dots \begin{bmatrix} E_k & 0 \\ 0 & 1 \end{bmatrix}.$$

Exercise 3. Prove that every matrix with a single 1 in each row and a single 1 in each column, the other entries being zero, is a permutation matrix.

Solution. Note that each column of such a matrix P must be a distinct standard basis vector $\boldsymbol{e}_k$, and we claim that this matrix represents the permutation p defined as $p(j) = k$, where $P_j = \boldsymbol{e}_k$ is the j^{th} column of P. Now, p is a bijection because every column j has one and exactly one 1 in the k^{th} row. This justifies that p is indeed a permutation. When P acts on a column vector $\boldsymbol{x}$, we have

$$P\boldsymbol{x} = P_1 x_1 + P_2 x_2 + \dots + P_n x_n = \boldsymbol{e}_{p(1)} x_1 + \boldsymbol{e}_{p(2)} x_2 + \dots + \boldsymbol{e}_{p(n)} x_n.$$

This means that

$$P \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_{p^{-1}(1)} \\ x_{p^{-1}(2)} \\ \vdots \\ x_{p^{-1}(n)} \end{bmatrix}.$$

Exercise 4. Let p be a permutation. Prove that $\operatorname{sign} p = \operatorname{sign} p^{-1}$.

Solution. This follows directly from the fact that $\det P^{-1} = 1/\det P$, and that $\det P = \pm 1$ so $\det P^{-1} = \det P$.

Exercise 5. Prove that the transpose of a permutation matrix P is its inverse.

Solution. Recall that $\det P = \pm 1$, so P is invertible. Write the permutation matrix P in terms of its columns,

$$P = \begin{bmatrix} | & | & \dots & | \\ \boldsymbol{e}_{p(1)} & \boldsymbol{e}_{p(2)} & \dots & \boldsymbol{e}_{p(n)} \\ | & | & \dots & | \end{bmatrix},$$

where p represents the corresponding permutation. Now note that the transpose can be written as

$$P = \begin{bmatrix} — \boldsymbol{e}_{p(1)}^t — \\ — \boldsymbol{e}_{p(2)}^t — \\ \vdots \\ — \boldsymbol{e}_{p(n)}^t — \end{bmatrix}.$$

Therefore, the ij^{th} element of the product P^tP is given by $\boldsymbol{e}_{p(i)}^t \boldsymbol{e}_{p(j)} = \delta_{p(i)p(j)} = \delta_{ij}$, meaning that $P^tP = \mathbb{I}$. We have used the fact that p is a bijection, so $p(i) = p(j)$ if and only if $i = j$. Thus, $P^{-1} = P^t$.

1.5 Cramer's Rule

Exercise 3. Let A be an $n \times n$ matrix with integer entries a_{ij}. Prove that A^{-1} has integer entries if and only if $\det A = \pm 1$.

Solution. First, suppose that $\det A = \pm 1$. If the entries of A^{-1} are b_{ij}, use

$$A^{-1} = \frac{1}{\det A} \operatorname{adj} A$$

to conclude that

$$b_{ij} = \frac{1}{\det A}(-1)^{i+j} \det A_{ji}.$$

Note that A_{ji} contains integer entries, hence its determinant must also be an integer via the complete expansion. Putting $\det A = \pm 1$ means that b_{ij} is always an integer.

Now suppose that A^{-1} has integer entries. Use $\det A = 1/\det A^{-1}$. Now both A and A^{-1} have integer entries, hence integer determinants, with $|\det A^{-1}| \geq 1$. This forces $\det A = \pm 1$.

Miscellaneous Problems

Exercise 2. Find a representation of the complex numbers by real 2 x 2 matrices which is compatible with addition and multiplication.

Solution. Consider the representation

$$z = a + ib \equiv \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Now, if $z = a + ib$, $w = c + id$, we have addition defined as

$$z + w \equiv \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & -b-d \\ b+d & a+c \end{bmatrix} \equiv (a+c) + i(b+d),$$

and multiplication as

$$zw \equiv \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{bmatrix} \equiv (ac-bd) + i(ad+bc).$$

Finally,

$$|z|^2 = z\overline{z} = a^2 + b^2 = \det \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Exercise 3. Find the Vandermonde determinant

$$\det A_n = \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{bmatrix}.$$

Solution. First look at the 2×2 case,

$$\det A_2 = \det \begin{bmatrix} 1 & 1 \\ a_1 & a_2 \end{bmatrix} = a_2 - a_1.$$

Now, look at the $n \times n$ case. Perform the row operations $R_k \to R_k - a_1 R_{k-1}$ for all rows $k = 2, \ldots, n$. This leaves the determinant unchanged, so

$$\det A_2 = \det \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & a_2 - a_1 & a_3 - a_1 & \cdots & a_n - a_1 \\ 0 & a_2(a_2 - a_1) & a_3(a_3 - a_1) & \cdots & a_n(a_n - a_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_2^{n-2}(a_2 - a_1) & a_3^{n-2}(a_3 - a_1) & \cdots & a_n^{n-2}(a_n - a_1) \end{bmatrix}.$$

Using expansion by minors on the first column, we have

$$\det A_2 = \det \begin{bmatrix} a_2 - a_1 & a_3 - a_1 & \cdots & a_n - a_1 \\ a_2(a_2 - a_1) & a_3(a_3 - a_1) & \cdots & a_n(a_n - a_1) \\ \vdots & \vdots & \ddots & \vdots \\ a_2^{n-2}(a_2 - a_1) & a_3^{n-2}(a_3 - a_1) & \cdots & a_n^{n-2}(a_n - a_1) \end{bmatrix}.$$

Factoring out $a_j - a_1$ from each j^{th} column gives

$$\det A_n = \prod_{j=2}^{n} (a_j - a_1) \times \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_2 & a_3 & \cdots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_2^{n-2} & a_3^{n-2} & \cdots & a_n^{n-2} \end{bmatrix}$$

Continuing in this fashion, we get

$$\det A_n = \prod_{j=2}^{n} (a_j - a_1) \times \prod_{j=3}^{n} (a_j - a_2) \times \cdots \times (a_{n-1} - a_n).$$

This can be written down concisely as

$$\det A_n = \prod_{1 \le i < j \le n}^{n} (a_j - a_i)$$

Exercise 4. Consider a general system $AX = B$ of m linear equations in n unknowns. If the coefficient matrix A has a left inverse A', a matrix such that $A'A = \mathbb{I}_n$, then we may try to solve the system as follows.

$$\begin{aligned} AX &= B, \\ A'AX &= A'B \\ X &= A'B. \end{aligned}$$

But when we try to check our work by running the solution backward, we get into trouble:

$$\begin{aligned} X &= A'B \\ AX &= AA'B \\ AX &\stackrel{?}{=} B. \end{aligned}$$

We seem to want A' to be a right inverse: $AA' = \mathbb{I}_n$, which isn't what was given. Explain.

Solution. In the case that $m > n$, note that the left inverse is not necessarily unique. An example is

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbb{I}_2,$$

irrespective of a and b. Hence, $X = A'B$ is not unique, but rather is dependent on our choice of A'. If we had started with

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} p \\ q \\ r \end{bmatrix}$$

then we would have written

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \end{bmatrix} \begin{bmatrix} p \\ q \\ r \end{bmatrix} = \begin{bmatrix} p + ar \\ q + br \end{bmatrix} = \begin{bmatrix} p \\ q \end{bmatrix} + r \begin{bmatrix} a \\ b \end{bmatrix}.$$

This means that the given argument is not sufficient to conclude $AA' = \mathbb{I}$.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \end{bmatrix} = \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 0 \end{bmatrix} \neq \mathbb{I}_3,$$

Note that this system is nonsense for $r \neq 0$ with no solutions, yet the left inverses A' do exist nonetheless. Here, $AX \neq B$ when $r \neq 0$, since

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} p + ar \\ q + ar \end{bmatrix} = \begin{bmatrix} p + ar \\ q + ar \\ 0 \end{bmatrix}.$$

In the case that $m < n$, A has no left inverse. Label the columns of A as A_i. Demanding $A'A = \mathbb{I}_n$ means that we want $A'A_i = \boldsymbol{e}_i$ for all $i = 1, \ldots, n$. Since the $m \times n$ matrix A has more columns than rows, its columns must be linearly dependent, so without loss of generality, write the first column A_1 as a non-trivial linear combination of the rest,

$$A_1 = a_2 A_2 + a_3 A_3 + \cdots + a_n A_n.$$

Multiplying by A' gives

$$A'A_1 = \boldsymbol{e}_1 = a_2 \boldsymbol{e}_2 + a_3 \boldsymbol{e}_3 + \cdots + a_n \boldsymbol{e}_n,$$

which is a contradiction since the basis vectors $\{\boldsymbol{e}_i\}$ are linearly independent.

In the case $m = n$, it is indeed true that A' is also a right inverse of A. Note that if A'' is a right inverse of A with $AA'' = \mathbb{I}_n$, then

$$A' = A'\mathbb{I}_n = A'(AA'') = (A'A)A'' = \mathbb{I}_n A'' = A''.$$

To justify that A'' exists, note that $A'A = \mathbb{I}_n$ gives $\det A' \det A = 1$, so $\det A \neq 0$. Thus, A has full rank and its range must be the full n dimensional vector space of column vectors. Multiplying by A, we have $AA'A = A$ or $(AA' - \mathbb{I}_n)A = 0$. Recall that the range of A is the entire vector space, so $(AA' - \mathbb{I}_n)\boldsymbol{x} = \mathbf{0}$ for all possible column vectors $\boldsymbol{x}$. This forces $AA' - \mathbb{I}_n = 0$, or $AA' = \mathbb{I}_n$.

Exercise 5.

(a) Let A be a real 2×2 matrix, and let A_1, A_2 be the rows of A. Let P be the parallelogram whose vertices are 0, A_1, A_2, $A_1 + A_2$. Prove that the area of P is the absolute value of the determinant $\det A$ by comparing the effect of and elementary row operation on the area and on $\det A$.

(b) Prove an analogous result for $n \times n$ matrices.

Solution.

(a) First note that

$$\det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1,$$

which is consistent with the fact that the area of a unit square is 1. Now let a_{ij} be the elements of A. Perform the row operation which multiplies the top row by a_{11}, i.e. $R_1 \to a_{11}R_1$. We have

$$\det \begin{bmatrix} a_{11} & 0 \\ 0 & 1 \end{bmatrix} = a_{11}.$$

Now perform $R_1 \to R_1 + a_{12}R_2$. This gives

$$\det \begin{bmatrix} a_{11} & a_{12} \\ 0 & 1 \end{bmatrix} = a_{11}.$$

Next, perform $R_2 \to (a_{11}a_{22} - a_{12}a_{21})R_2$. This gives

$$\det \begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{11}a_{22} - a_{12}a_{21} \end{bmatrix} = (a_{11}a_{22} - a_{12}a_{21})a_{11}.$$

Next, perform $R_2 \to R_2 + a_{21}R_1$. This gives

$$\det \begin{bmatrix} a_{11} & a_{12} \\ a_{11}a_{21} & a_{11}a_{22} \end{bmatrix} = (a_{11}a_{22} - a_{12}a_{21})a_{11}.$$

Finally, perform $R_2 \to R_2/a_{11}$. This gives

$$\det A = \det \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Note that if $a_{11} = 0$, we could have interchanged the roles of a_{11} and a_{21} at the beginning by interchanging the rows of A. This would have given the same result, up to a sign which we are not interested in. If both a_{11} and a_{22} are zero, note that the two rows are linearly dependent, with one being a multiple of the other, so the parallelogram they form has zero area. Thus, we have shown that any matrix A representing a parallelogram with non-zero area can be obtained from the identity matrix $\mathbb{I}_2$ by performing elementary row operations.

Now, we consider the effect of these row operations on the area of a parallelogram with legs A_1 and A_2. Note that the operation $A_1 \to kA_1$ for some real scaling factor k has the effect of scaling the area by the same factor k. The operation of interchanging the

legs A_1 and A_2 has no effect on the area. The operation $A_1 \to A_1 + kA_2$ also has no effect on the area, because this has the effect of linearly shearing the parallelogram, in a manner parallel to the other leg A_2 which remains fixed. Thus, when we performed our row operations in the square to reach our parallelogram, our area transformed in precisely the same way as the unsigned determinant, which means that

$$\operatorname{area} A_{\parallel} = |\det A| = |a_{11}a_{22} - a_{12}a_{21}|.$$

(b) We use the fact that any square matrix A with non-zero determinant can be written as the product of row operations acting on the identity matrix $\mathbb{I}_n$, which represents the unit hypercube of hypervolume 1. The Gauss-Jordan elimination algorithm can be used to extract these operations. We see that all scaling operations will scale the hypervolume in the same way, all transpositions have no effect on the hypervolume, and all additions of linear combinations of other rows also have no effect, since they correspond to successive shearing of the hyperparallelopiped along a direction parallel to another leg. Thus, the area of the hypercube transformed in the same way as the unsigned determinant of A, so

$$\operatorname{hypervolume} A_{\parallel} = |\det A|.$$

Note that we are not interested in matrices with zero determinant, because such a matrix is not of full rank, hence its rows are linearly dependent. Thus, one of the legs of the corresponding hyperparallelopiped can be sheared until it is parallel to another, which immediately gives a zero hypervolume.

Exercise 6. 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) Prove uniqueness, that is, prove that there is at most one way to write A as a product.

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

(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.

Solution. We first show that the determinant of a triangular matrix is equal to the product of its diagonals. To see this, note that this holds for all 2×2 lower triangular matrices,

$$\det \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} = ad.$$

Next, suppose that this holds for all $n \times n$ lower triangular matrices. Using expansion of minors along the first row and our induction hypothesis on the minor A_{11}, compute

$$\det \begin{bmatrix} a_{11} & 0 & 0 & \cdots & a_{1n} \\ a_{21} & a_{22} & 0 & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{bmatrix} = a_{11} \det A_{11} + 0 + 0 + \cdots + 0 = a_{11}a_{22}a_{33} \cdots a_{nn}.$$

For upper triangular matrices, simply note that $\det U = \det U^t$, and U^t is lower triangular.

Now, we show that the inverse of a triangular matrix is also triangular of the same kind. Note that this holds for all invertible 2×2 matrices, with

$$\begin{bmatrix} a & 0 \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad} \begin{bmatrix} d & 0 \\ -c & a \end{bmatrix}.$$

Next, suppose that an invertible lower triangular matrix L has an inverse L^{-1}, whose columns are labelled $\boldsymbol{x}_j$. Since $LL^{-1} = \mathbb{I}_n$, we want

$$L\boldsymbol{x}_j = \boldsymbol{e}_j.$$

We claim that $(x_j)_i = 0$ for all $i < j$. To see this, note that the first $j-1$ rows expand to

$$\begin{aligned} 0 &= L_{11}x_{j1} \\ 0 &= L_{12}x_{j1} + L_{22}x_{j2} \\ &\vdots \quad \vdots \\ 0 &= L_{j-1,1}x_{j,j-1} + \cdots + L_{j-1,j-1}x_{j,j-1} \end{aligned}$$

All L_{ij} with $i < j$ are zero, and L_{ii} are non-zero since L is invertible hence $\det L \neq 0$. Thus, the first equation gives $x_{j1} = 0$, which when plugged into the second gives $x_{j2} = 0$, and so on up to $x_{j,j-1} = 0$. Hence, $L^{-1}_{ij} = 0$ for all $i < j$, making it a lower triangular matrix. In addition, the j^{th} row reads

$$1 = L_{j1}x_{j1} + \cdots + L_{j,j-1}x_{j,j-1} + L_{jj}x_{jj}.$$

All terms but the last one are 0, so the diagonal elements satisfy $L_{jj}L^{-1}_{jj} = 1$. Like before, for a lower triangular matrix U, use $(U^t)^{-1} = (U^{-1})^t$.

Finally, the product of two triangular matrices of the same kind give another triangular matrix of the same kind. Suppose that A and B are two lower triangular matrices. The ij^{th} element of their product AB is

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

Now, $a_{ik} = 0$ for all $i < k$ and $b_{ki} = 0$ for all $k < j$. Thus, when $i < j$, we have $c_{ij} = 0$, hence AB is also lower triangular. Furthermore, if all the diagonal entries $a_{ii} = b_{ii} = 1$, then the only term in the sum is $c_{ii} = a_{ii}b_{ii} = 1$, so the diagonal entries of C are all 1. Again for upper triangular matrices X, Y, use $(XY)^t = Y^tX^t$.

(a) Suppose that $A = LU = L'U'$ are two LU decompositions of A. Note that $\det A \neq 0$ from its invertibility, hence L, U, L', U' are all invertible. This gives

$$L^{-1}LU = L^{-1}L'U', \qquad U = L^{-1}L'U', \qquad U(U')^{-1} = L^{-1}L'.$$

Now, the left side is upper triangular while the right side is left triangular. Also, the left side has all 1's along its diagonal. This forces

$$U(U')^{-1} = \mathbb{I}_n = L^{-1}L', \qquad U = U', \quad L = L'.$$

(b) The elements of L and U can be obtained by brute force, solving the system $A = LU$ with $n(n+1)/2 + (n-1)n/2 = n^2$ unknowns.

(c) Note that after performing Gaussian elimination on an invertible matrix A, we are left with an upper triangular matrix U with 1's along its diagonal. Also, each elementary operation we performed can be represented by a lower triangular matrix. This is because all scaling matrices are diagonal, and in all cases where we added one row to another we always added higher row to ones lower down. Thus, the product of all these elementary matrices is a lower triangular matrix L, which means $LA = U$. This gives the desired decomposition, $A = L^{-1}U$.

However, we may have to exchange rows while performing the elimination process, which happens when one of the diagonal elements becomes zero. By performing this permutation of rows at the very end, we have actually decomposed $PLA = U$. The inverse of a permutation is another permutation, hence we have the desired decomposition $A = L^{-1}P^{-1}U$.

Exercise 7. Consider a system of n linear equations in n unknowns: $AX = B$, where A and B have *integer* entries. Prove or disprove the following.

(a) The system has a rational solution if $\det A \neq 0$.

(b) If the system has a rational solution, then it also has an integer solution.

Solution.

(a) If $\det A \neq 0$, then A is invertible. Since A has integer entries, its determinant is an integer and its adjoint has integer entries, which means that $A^{-1} = (\operatorname{adj} A)/\det A$ has rational entries. Also, B has integer entries so the solution $X = A^{-1}B$ must also be rational.

(b) This is false. Consider the system

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

This has the unique solution $x = y = \frac{1}{2}$.

Exercise 8. Let A, B be $m \times n$ and $n \times m$ matrices. Prove that $\mathbb{I}_m - AB$ is invertible if and only if $\mathbb{I}_n - BA$ is invertible.

Solution. Note that

$$B(\mathbb{I}_m - AB) = B - BAB = (\mathbb{I}_n - BA)B,$$
$$A(\mathbb{I}_n - BA) = A - ABA = (\mathbb{I}_m - AB)A.$$

Set $X = \mathbb{I}_m - AB$, $Y = \mathbb{I}_n - BA$, whence

$$BX = YB, \qquad AY = XA.$$

First suppose that X is invertible. If A is invertible, then $AY = XA$ gives $Y = A^{-1}XA$, so we can check that $Y^{-1} = A^{-1}X^{-1}A$.

$$(A^{-1}X^{-1}A)Y = A^{-1}X^{-1}A\,A^{-1}XA = \mathbb{I}_n.$$

If A is not invertible but B is invertible, then use $BX = YB$ to write $Y = BXB^{-1}$, so we can check that $Y^{-1} = BX^{-1}B^{-1}$.

$$(BX^{-1}B^{-1})Y = BX^{-1}B^{-1}\,BXB^{-1} = \mathbb{I}_n.$$

Now suppose that neither A nor B is invertible. Consider the products

$$(\mathbb{I}_n + BX^{-1}A)Y = Y + BX^{-1}AY = Y + BX^{-1}XA = Y + BA = \mathbb{I}_n,$$

$$Y(\mathbb{I}_n + BX^{-1}A) = Y + YBX^{-1}A = Y + BXX^{-1}A = Y + BA = \mathbb{I}_n.$$

Thus, $Y^{-1} = \mathbb{I}_n + BX^{-1}A$.

Chapter 2

Groups

2.1 The Definition of a Group

Exercise 1.

(a) Verify (1.17) and (1.18) by explicit computation.

(b) Make a multiplication table for S_3.

Solution.

(a) We see that

$$1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad x = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \qquad y = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Calculate

$$x^2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

$$xy = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

$$x^2y = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

These six matrices cover all possible permutations of the three rows.

(b)

$\times$	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^2	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

Exercise 2.

(a) Prove that $GL_n(\mathbb{R})$ is a group.

(b) Prove that S_n is a group.

Solution.

(a) We show that $GL_n(\mathbb{R})$ is a group under matrix multiplication. Note that if $\det A \neq 0$ and $\det B \neq 0$, then $\det AB = \det A \det B \neq 0$, so $GL_n(\mathbb{R})$ is closed under multiplication. This composition is also associative, by virtue of the associativity of matrix multiplication. The identity matrix $\mathbb{I}_n$ serves as the group identity, since $\mathbb{I}_n A = \mathbb{I}_n = A\mathbb{I}_n$ for all $A \in GL_n(\mathbb{R})$. Finally, all non-singular matrices are invertible, with the inverse also being non-singular, which means that every element $A \in GL_n(\mathbb{R})$ has an inverse $A^{-1} \in GL_n(\mathbb{R})$. Thus, $GL_n(\mathbb{R})$ forms a group.

(b) We show that S_n is a group under function composition. Note that each element S_n is a bijection $f\colon \{1,\dots,n\} \to \{1,\dots,n\}$. Since the composition of two bijections is also a bijection, we see that S_n is closed under composition. Also note that function composition is associative, with $(f \circ g) \circ h = g \circ (g \circ h)$. The identity map $\mathbb{I} \in S_n$ which maps each integer to itself serves as the identity element, since $\mathbb{I} \circ f = \mathbb{I} = f \circ \mathbb{I}$ for all $f \in S_n$. Finally, all bijections have an inverse which is also a bijection, hence every element $f \in S_n$ has n inverse $f^{-1} \in S_n$. Thus, S_n forms a group.

Exercise 3. Let S be a set with an associative law of composition and with an identity element. Prove that the subset of S consisting of invertible elements is a group.

Solution. Let $S' \subset S$ be the set of all invertible elements of S. Note that by construction, composition in S' is associative. The identity element $e \in S$ must also belong to S', since $ee = e$, hence e is invertible with $e^{-1} = e$. This serves as an identity for all elements in S' as well. Also, all elements in S' are invertible, and their inverses must also be in S', because if $a^{-1} = b$, then $ba^{-1} = e = a^{-1}b$, so $b^{-1} = a$ making $b = a^{-1}$ invertible. Finally, S' is closed under composition, because the product of invertible elements is invertible, with $(ab)^{-1} = b^{-1}a^{-1}$. This means that S' is a group.

Exercise 4. Solve for y, given that $xyz^{-1}w = 1$ in a group.

Solution. Write

$$\begin{aligned} xyz^{-1}w &= 1, \\ xyz^{-1}ww^{-1} &= w^{-1}, \\ xyz^{-1} &= w^{-1}, \\ xyz^{-1}z &= w^{-1}z, \\ xy &= w^{-1}z, \\ x^{-1}xy &= x^{-1}w^{-1}z, \\ y &= x^{-1}w^{-1}z. \end{aligned}$$

Exercise 5. Assume that the equation $xyz = 1$ holds in a group G. Does it follow that $yzx = 1$? That $yxz = 1$?

Solution. We have $xyz = 1$, so

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

It is not necessarily true that $yxz = 1$. Consider the group S_3 as seen in Exercise 1. We have $(xy)(x)(y) = 1$, but $(x)(xy)(y) = x^2y^2 = x^2 \neq 1$.

Exercise 6. Write out all ways in which one can form a product of four elements a, b, c, d in the given order.

Solution.

$$(ab)(cd) \quad (a(bc))d \quad ((ab)c)d \quad a(b(cd)) \quad a((bc)d)$$

Exercise 7. Let S be any set. Prove that the law of composition defined by $ab = a$ is associative.

Solution. It is sufficient to show that $(ab)c = a(bc)$ for all $a, b, c \in S$. We have

$$(ab)c = ac = a, \qquad a(bc) = a.$$

Exercise 8. Give an example of 2×2 matrices such that $A^{-1}B \neq BA^{-1}$.

Solution. Consider

$$A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \qquad A^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Now,

$$A^{-1}B = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \qquad BA^{-1} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

Exercise 9. Show that if $ab = a$ in a group, then $b = 1$, and if $ab = 1$, then $b = a^{-1}$.

Solution. If $ab = a$, then

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

If $ab = 1$, then it suffices to show that $ba = 1$ to conclude $b = a^{-1}$.

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

Exercise 10. Let a, b be elements of a group G. Show that the equation $ax = b$ has a unique solution in G.

Solution. The existence of a solution is guaranteed by the inverse of a, namely $a^{-1} \in G$ such that $aa^{-1} = 1 = a^{-1}a$. Thus, $(a^{-1})ax = a^{-1}b$, hence $x = a^{-1}b$.

Now suppose that $ax = ay = b$. Again, left multiplying by a^{-1} gives $x = y$, guaranteeing that the solution is unique.

Exercise 11. Let G be a group, with multiplicative notation. We define an *opposite group* G° with law of composition $a \circ b$ as follows: The underlying set is the same as G, but the law of composition is the opposite; that is, we define $a \circ b = ba$. Prove that this defines a group.

Solution. The composition in G° is closed, since $a \circ b = ba \in G$ and G° shares all elements with G. Note that composition is associative in G, so for all $a, b, c \in G$,

$$c(ba) = (cb)a, \qquad (a \circ b) \circ c = a \circ (b \circ c).$$

This shows that composition is associative in G°. Next, the identity in G serves as the identity in G°, since for any $a \in G^\circ$,

$$1 \circ a = a1 = a = 1a = a \circ 1.$$

Each $a \in G$ has an inverse $a^{-1} \in G$, and this guarantees that each $a \in G^\circ$ has the same inverse $a^{-1} \in G^\circ$, since

$$a \circ a^{-1} = a^{-1}a = 1 = aa^{-1} = a^{-1} \circ a.$$

Thus, G° is a group.

2.2 Subgroups

Exercise 1. Determine the elements of the cyclic group generated by the matrix $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ explicitly.

Solution. Set

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad x = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}, \qquad x^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \qquad x^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},$$

$$x^4 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, \qquad x^5 = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}, \qquad x^6 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Therefore, the elements of the cyclic group generated by x are the matrices $\{1, x, x^2, x^3, x^4, x^5\}$. This group has order 6.

Exercise 2. Let a, b be elements of a group G. Assume that a has order 5 and that $a^3b = ba^3$. Prove that $ab = ba$.

Solution. We have $a^5 = 1$, therefore

$$ab = 1ab = a^5ab = a^6b = a^3(a^3b) = a^3(ba^3),$$

$$ba = ba1 = baa^5 = ba^6 = (ba^3)a^3 = (a^3b)a^3.$$

These are equal by associativity.

Exercise 3. Which of the following are subgroups?

(a) $GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$.

(b) $\{1, -1\} \subset \mathbb{R}^\times$.

(c) The set of positive integers in $\mathbb{Z}^+$.

(d) The set of positive reals in $\mathbb{R}^\times$.

(e) The set of all matrices $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, with $a \neq 0$, in $GL_2(\mathbb{R})$.

Solution. It can be shown that (a), (b), (d) meet the axioms required for a subgroup. In (c), the additive identity 0 is missing. In (e), the identity matrix $\mathbb{I}_2$ is missing (and none of the described matrices belong to $GL_2(\mathbb{R})$ in any case).

Exercise 4. Prove that a non-empty subset H of a group G is a subgroup if for all $x, y \in H$ the element xy^{-1} is also in H.

Solution. Since H is non-empty, we can pick $x \in H$. Then, $x \in H$ and $x \in H$, so $xx^{-1} = 1 \in H$. Next, for any $x \in H$, we have $1 \in H$ and $x \in H$, so $1x^{-1} = x^{-1} \in H$. Finally, for any $x, y \in H$, we have $x \in H$ and $y^{-1} \in H$, so $x(y^{-1})^{-1} = xy \in H$. This means that $H \subseteq G$ is a subgroup.

Exercise 5. An nth root of unity is a complex number z such that $z^n = 1$. Prove that the nth roots of unity form a cyclic subgroup of $\mathbb{C}^\times$ of order n.

Solution. Let the set of all nth roots of unity be G. First we have $1^n = 1$ so $1 \in G$. Next, if $x, y \in G$, then $x^n = y^n = 1$, so $(xy)^n = 1$, thus $xy \in G$. Finally, note that $x^{-1} = x^{n-1}$, because $xx^{n-1} = x^{n-1}x = x^n = 1$. To see that this is a cyclic subgroup, set $x = e^{1\pi i/n}$, then $G = \{1, x, \ldots, x^{n-1}\}$. There are no other elements of G, since the polynomial $x^n - 1$ has at most n distinct complex roots.

Exercise 6.

(a) Find generators and relations analogous to (2.13) for the Klein four group.

(b) Find all subgroups of the Klein four group.

Solution.

(a) Write

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad x = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad y = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad z = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

It can be verified that $x^2 = y^2 = z^2 = e$. Also, $xy = z = yx$, $xz = y = zx$, $yz = x = zy$. Thus, this group is abelian. Also, any two of x, y, z suffice to generate the third, and hence the entire Klein four group. Any one is not sufficient, since every element has order 2.

(b) The Klein four group has two trivial subgroups, namely $\{e\}$ and the whole group. Also, each of $\{e, x\}$, $\{e, y\}$, $\{e, z\}$ form a subgroup, since all of them contain the identity e, each element is their own inverse, and multiplication is closed. This gives a total of 5 subgroups.

Exercise 7. Let a and b be integers.

(a) Prove that the subset $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}^+$.

(b) Prove that a and $b + 7a$ generate the subgroup $a\mathbb{Z} + b\mathbb{Z}$.

Solution.

(a) We have

$$G = a\mathbb{Z} + b\mathbb{Z} = \{ar + bs : r, s \in \mathbb{Z}\}.$$

First note that $0 = a0 + b0 \in G$. Next, for any two elements $x, y \in G$, we can write $x = ar_1 + bs_1$ and $y = ar_2 + bs_2$ for integers r_1, r_2, s_1, s_2, so the sum $x + y = a(r_1 + r_2) + b(s_1 + s_2) \in G$. Finally, for $x = ar + bs \in G$, we have $-x = a(-r) + b(-s) \in G$, with $x + (-x) = 0$. This proves that G is a subgroup of $\mathbb{Z}^+$.

(b) Let H be the group generated by a and $b + 7a$. Note that a, $a + a = 2a$, $2a + a = 3a$, $\ldots$, $6a + a = 7a$, $\ldots$, $(n-1)a + a = na$ are all in H. Similarly, if $na \in H$, then $-na \in H$ for all positive integers n. Thus, $0 = a + (-a) \in H$, and $b = (b + 7a) + (-7a) \in H$. We repeat this process with b to see that $nb \in H$ for all integers n. Thus, $ar + bs \in H$ for all integers r and s, which means that $H \subseteq a\mathbb{Z} + b\mathbb{Z}$. On the other hand, for all $ar + bs \in a\mathbb{Z} + b\mathbb{Z}$, we have $ar + bs = a(1 - 7s) + (b + 7a)s \in H$, so $a\mathbb{Z} + b\mathbb{Z} \subseteq H$. This establishes that $H = a\mathbb{Z} + b\mathbb{Z}$.

Exercise 8. Make a multiplication table for the quaternion group H.

Solution. Use $i^2 = j^2 = k^2 = ijk = -1$, $ij = k$, $ji = i^3 j = -k$.

$\times$	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
1	-1	$-i$	$-j$	$-k$	1	i	j	k
i	$-i$	1	$-k$	j	i	-1	k	$-j$
j	$-j$	k	1	$-i$	j	$-k$	-1	i
k	$-k$	$-j$	i	1	k	j	$-i$	-1

Exercise 9. Let H be the subgroup generated by two elements a, b of a group G. Prove that if $ab = ba$, then H is an abelian group.

Solution. Since H is generated by a and b, every element in H can be written in the form

$$a^{m_1}b^{n_1}a^{m_2}b^{n_2}\dots a^{m_k}b^{n_k},$$

where $k \in \mathbb{N}$ and $m_i, n_i \in \mathbb{Z}$. First, we claim that every such element can be simplified to the form $a^m b^m$. To see this, note that since a and b commute, we have $ab(b^{-1}a^{-1}) = 1 = ba(a^{-1}b^{-1}) = ab(a^{-1}b^{-1})$, so cancelling ab gives $b^{-1}a^{-1} = a^{-1}b^{-1}$. Now, $ab = ba$ means $a = bab^{-1}$. Thus, for any positive power $a^m = ba^m b^{-1}$, and $a^{-m} = ba^{-m}b^{-1}$. Thus, $a^m b^n = ba^m b^{-1}b^n = ba^m b^{n-1}$. Repeating this another $n-1$ times gives $a^m b^n = b^n a^m$ for positive n. For negative n, simply note that $a^m = b^n(b^{-n}a^m) = b^n(a^m b^{-n})$, hence $a^m b^n = b^n a^m$. This means that the powers a^m and b^n commute. Thus, we can commute all powers b^{n_i} in our general expression to the right, yielding

$$a^{m_1+\dots+m_k}b^{n_1+\dots n_k} = a^m b^n.$$

Now pick arbitrary $x, y \in H$, and write $x = a^m b^n$, $y = a^r b^s$. Then,

$$xy = a^m b^n a^r b^s = a^m(b^n a^r)b^s = a^m a^r b^n b^s = a^{m+r}b^{n+s},$$

$$yx = a^r b^s a^m b^n = a^r(b^s a^m)b^n = a^r a^m b^s b^n = a^{m+r}b^{n+s}.$$

This gives $xy = yx$ for all $x, y \in H$, which means that H is abelian.

Exercise 10.

(a) Assume that an element x of a group has order rs. Find the order of x^r.

(b) Assuming that x has arbitrary order n, what is the order of x^r?

Solution. We first show that if x has order n and $x^m = 1$, then n divides m. Note that $n \le m$, since n is chosen to be the least natural number satisfying $x^n = 1$. Thus, use Euclid's Division Lemma to write $m = nq + r$ for integers $q > 0$, $0 \le r < n$. We now have

$$1 = x^m = x^{nq+r} = (x^n)^q x^r = x^r.$$

Since $r < n$, the only possibility is $r = 0$, hence $m = nq$, proving that n divides m.

(a) Note that $(x^r)^s = x^{rs} = 1$, so the order of x^r divides s. Also, if the order of x^r were less then s, say $t < s$, then we would have $(x^r)^t = 1$, so $x^{rt} = 1$, with $rt < rs$. This would contradict the fact that rs is the order of x. Thus, the order of x^r must be s.

(b) We claim that the order of x^r is $m = n/\gcd(n, r)$. Write $\gcd(n, r) = d$, so $rm = nr/d = nk$ for some integer k since d divides r. Thus,

$$(x^r)^m = x^{rm} = x^{nk} = (x^n)^k = 1.$$

Suppose instead that the order of x^r is some $m' < m$. Then m' divides m, so $m = m'q$ for some integer $q > 1$. We have $1 = (x^r)^{m'} = x^{rm'}$, therefore n must divide rm', say $rm' = nk'$ for some integer k'. Now, $nk = rm = rm'q = nk'q$, so $k = k'q$. Recall that $n = md$, $r = kd$. Now we have found $n = m'(qd)$, $r = k'(qd)$, thus qd divides both n and r. However, $qd > d$, which contradicts the fact that any common factor of n and r must divide d. Hence, the order of x^r must be $m = n/d$.

Exercise 11. Prove that in any group the orders of ab and ba are equal.

Solution. Note that $ab = (b^{-1}b)ab = b^{-1}(ba)b$. It is easily seen by induction that $(ab)^n = b^{-1}(ba)^n b$ for all positive integers n. Therefore, if the order of ab is some integer n, $1 = (ab)^n = b^{-1}(ba)^n b$, hence $(ba)^n = bb^{-1} = 1$. Thus, the order of ba divides n. A similar argument using $(ba)^n = a^{-1}(ab)^n a$ shows that if the order of ba is n', then the order of ab divides n'. This forces $n = n'$ when either ab or ba has finite order.

Note that we shown that if the order of ab is finite, then the order of ba must be finite, and vice versa. This immediately implies that if the order of any one of ab or ba is infinite, then the order of the other must also be infinite. Hence, the order of ab and ba are always the same in any group.

Exercise 12. Describe all groups G which contain no proper subgroup.

Solution. Suppose that G has no proper subgroups, i.e. the only subgroups of G are $\{1\}$ and G. The trivial group of one element $\{1\}$ satisfies this. Otherwise, let G be a non-trivial group, with $x \in G$ such that $x \neq 1$. Then, the group generated by x, i.e. the group of elements $\{\dots x^{-2}, x^{-1}, 1, x, x^2, \dots\}$ is a subgroup of G. Since G has no proper subgroups, this forces this to be equal to G itself. Thus, G is a cyclic group.

Suppose that G has finite order, and furthermore suppose that this order is a composite number ab, where $a \geq b > 1$. Then, it can be shown that the group generated by x^a is a proper subgroup of G, with x not in this subgroup. Therefore, the order of G must be prime.

Suppose that G has infinite order. Now note that the group generated by x^2 is a proper subgroup of G, with x not in this subgroup. This is a contradiction, thus the order of G cannot be infinite.

Exercise 13. Prove that every subgroup of a cyclic group is cyclic.

Solution. Let G be a cyclic group generated by the single element x. If $x = 1$, then $G = \{1\}$, which has no proper subgroups. Otherwise, note that we can enumerate

$$G = \{\dots x^{-2}, x^{-1}, 1, x, x^2, \dots\}.$$

Let H be a proper subgroup of G, and let $y \in H$ be a non-trivial element. This means that $y \in G$, so we can write $y = x^k$ for some positive integer k (note that if k were negative, then $y^{-1} = x^{-k} \in H$ too, so use $-k$ instead). Suppose that we have chosen $w = x^m \in H$ such that m is the smallest possible, positive choice. This means that $m \leq k$, so using Euclid's Division Lemma, write $k = mq + r$ for $0 \leq r < m$. Thus, $x^k = (x^m)^q x^r = w^q x^r$, or $x^r = w^{-q}x^k$. Now, $w \in H$ means that all powers of w are also in H, hence $w^{-q} \in H$. This means that $w^{-q}x^k = x^r \in H$. However, recall that m was the smallest positive integer such that $x^m \in H$, which forces $r = 0$. Thus, for any $y \in H$, we see that $y = w^q$. This means that H is generated by the element $w = x^m$, which makes it a cyclic subgroup.

Exercise 14. Let G be a cyclic group of order n, and let r be an integer dividing n. Prove that G contains exactly one subgroup of order r.

Solution. Let G be generated by the element x, so $G = \{1, x, \dots, x^{n-1}\}$, and let H be a subgroup of order r, where $n = mr$ for some positive integer m. We claim that the subgroup generated by x^m is the only subgroup of order r. Note from the previous exercise that H must be cyclic, and thus is generated by some element $x^k \in G$. Thus, if we pick $y \in H$, we must have $y = x^{kq}$ for some non-negative integer q. Since H has order r, we require $y^r = 1$, i.e. $x^{kqr} = 1$. Now, x has order n, hence n must divide kqr, say $np = kqr$ for some positive integer p. Substitute $n = mr$, so $mp = kq$. Thus, $y = x^{kq} = x^{mp}$, so every element of H is a power of x^m. In other words, $H \subseteq \{1, x^m, \dots, x^{m(r-1)}\}$. Also note that H contains exactly r elements, and the right hand side also contains r elements since all x^{mp} are distinct. Thus, we must have an equality, which means that the only subgroup of G with order r is the one generated by x^m.

Exercise 15.

(a) In the definition of subgroup, the identity element in H is required to be the identity of G. One might require only that H have an identity element, not that it is the same as the identity in G. Show that if H has an identity at all, then it is the identity in G, so this definition would be equivalent to the one given.

(b) Show the analogous thing for inverses.

Solution.

(a) Let 1 be the identity element in G, and suppose that $1'$ is the identity element in H. Now, both $1' \in G$ and $1 \in G$, and we demand

$$1x = x \text{ for all } x \in G, \qquad 1'x = x \text{ for all } x \in H.$$

Combining these, we want

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

so the identity in H must be the same as the identity in G.

(b) Let $x \in H$, let y be its inverse in G, and let w be its inverse in H. We want

$$xy = 1 = yx, \qquad xw = 1 = wx.$$

Thus,

$$y = y1 = y(xw) = (yx)w = 1w = w,$$

so the inverse of x in G must be the same in H.

Exercise 16.

(a) Let G be a cyclic group of order 6. How many of its elements generate G?

(b) Answer the same question for cyclic groups of order 5, 8, and 10.

(c) How many elements of a cyclic group of order n are generators for that group?

Solution.

(a) Let $G = \{1, x, \ldots, x^5\}$. Then, the elements x and x^5 (2 elements) generate G. Note that x^2 and x^4 only generate $\{1, x^2, x^4\}$, and x^3 only generates $\{1, x^3\}$.

(b) Using the same notation as before, a cyclic group of order 5 is generated by x, x^2, x^3, x^4 (4 elements). A cyclic group of order 8 is generated by x, x^3, x^5, x^7 (4 elements). A cyclic group of order 10 is generated by x, x^3, x^7, x^9 (4 elements).

(c) A cyclic group of order n is generated by $\phi(n)$ elements, where the Euler totient function ϕ counts the number of positive integers less than n which are co-prime with n. This is because a cyclic group $G = \{1, \ldots, x^{n-1}\}$ of order n is generated by x^r precisely when $\gcd(n, r) = 1$. Recall from Exercise 14 that if the order of a cyclic group G is $n = ab$, then x^a generates a subgroup of order b. Thus, when $b > 1$, the generated subgroup is a proper subgroup. This means that whenever r divides n, x^r cannot generate the entire group G. Similarly, if r and n share a common factor $m > 1$, then m divides n so x^m cannot generate G, and neither can $x^r = x^{mk}$ for some integer k. This only leaves those x^r such that r and n have no common factors. If so, then we can choose integers p and q such that $\gcd(n, r) = 1 = np + rq$, so $x^1 = x^{np+rq} = (x^r)^q$. Thus, any element $x^m \in G$ can be expressed as $(x^r)^{mq}$, so x^r does indeed generate G.

Exercise 17. Prove that a group in which every element except the identity has order 2 is abelian.

Solution. Let G be such a group, and let $x, y \in G$. Note that since every element has order 2, we have $x^2 = y^2 = (xy)^2 = (yx)^2 = 1$. Also,

$$(xy)(yx) = xy^2x = x^2 = 1, \qquad (xy)(xy) = (xy)^2 = 1.$$

Equating and cancelling xy from the left gives $yx = xy$, showing that G is abelian.

Exercise 18.

(a) Prove that the elementary matrices of the first and third types suffice to generate $GL_n(\mathbb{R})$.

(b) The *special linear group* $SL_n(\mathbb{R})$ is the set of $n \times n$ matrices whose determinant is 1. Show that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

(c) Use row reduction to prove that the elementary matrices of the first type generate $SL_n(\mathbb{R})$. Do the 2×2 case first.

Solution.

(a) First, we show that elementary matrices of the second type, i.e. permutation matrices, can be generated by elementary matrices of the other two types, i.e. row adding and scaling. In order to transpose rows i and j, consider the following row operations: $R_i \to R_i + R_j$, $R_j \to R_i - R_j$, $R_i \to R_i - R_j$. This can be achieved using only row addition and scaling, hence any transposition matrix can be obtained by applying this to the identity matrix. Furthermore, any permutation matrix can be expressed as the product of transposition matrices. This proves that elementary matrices of the first and third types generate those of the second type. Now, if A is invertible, then the process of Gauss-Jordan elimination can be applied to reduce it to an identity matrix, hence $E_1 \cdots E_k A = \mathbb{I}$. This means that $A = E_k^{-1} \cdots E_1^{-1}$, hence any matrix in $GL_n(\mathbb{R})$ can be expressed as a product of elementary matrices. In addition, any product of elementary matrices is invertible, which means that the elementary matrices generate $GL_n(\mathbb{R})$.

(b) First note that the identity matrix $\mathbb{I}_n \in SL_n(\mathbb{R})$, since it has determinant 1. Using $\det AB = \det A \det B$, conclude that if $A, B \in SL_n(\mathbb{R})$, then $AB \in SL_n(\mathbb{R})$. Finally, use $\det A^{-1} = 1/\det A$ to conclude that if $A \in SL_n(\mathbb{R})$, then $A^{-1} \in SL_n(\mathbb{R})$. This proves that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

(c) Consider an arbitrary matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{R}),$$

where $ad - bc = 1$. Perform $R_1 \to R_1 - (b/d)R_2$ to get

$$\begin{bmatrix} a - bc/d & 0 \\ c & d \end{bmatrix}.$$

Note that $a - bc/d = 1/d$. Next, perform $R_2 \to R_2 - cdR_1$.

$$\begin{bmatrix} 1/d & 0 \\ 0 & d \end{bmatrix}.$$

Note that if $d = 0$, we could have performed analogous operations using b instead (both $b = d = 0$ is not possible, since we require $ad - bc = 1$). Now, perform $R_2 \to R_2 + dR_1$.

$$\begin{bmatrix} 1/d & 0 \\ 1 & d \end{bmatrix}.$$

Next, perform $R_1 \to R_1 - R_2/d$.

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

Next, perform $R_2 \to R_2 + dR_1$.

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

Finally, perform $R_1 \to R_1 + R_2$, $R_2 \to R_2 - R_1$, $R_1 \to R_1 + R_2$.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus, we have shown that any matrix in $SL_2(\mathbb{R})$ can be generated using only elementary matrices of the first type.

Analogously, consider some $A = [a_{ij}] \in SL_n(\mathbb{R})$. We have already seen that $R_i \to R_i + R_j$, $R_j \to R_j - R_i$, $R_i \to R_i + R_j$ transposes rows with a change of sign. Thus, transpose rows such that let $a_{11} \neq 0$ (if all $a_{1j} = 0$, then $\det A = 0$). Performing $R_i \to R_i - (a_{i1}/a_{11})R_1$ for all $i = 2, \dots, n$ makes sure that all elements except the first one are zero.

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} - a_{12}a_{21}/a_{11} & \cdots & a_{2n} - a_{1n}a_{21}/a_{11} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} - a_{12}a_{n1}/a_{11} & \cdots & a_{nn} - a_{1n}a_{n1}/a_{11} \end{bmatrix}.$$

Now, note that the determinant of A is $a_{11} \det M_{11} \neq 0$, which means that the first column of M_{11} contains a non-zero element. We thus repeat the above process, transposing rows if necessary n times, finally giving us an upper triangular matrix. Relabel the entries as b_{ij}.

$$\begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{nn} \end{bmatrix}.$$

Note that $b_{11}b_{22} \dots b_{nn} = 1$. Thus, for each $j = n, n-1, \dots, 2$, perform $R_i \to R_i - (b_{ij}/b_{jj})R_j$ for all $i = 1, \dots, j-1$. This yields a diagonal matrix,

$$\begin{bmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{nn} \end{bmatrix}.$$

Now, look at the upper left 2×2 block. Performing $R_2 \to R_2 + R_1/b_{11}$, $R_1 \to R_1 - b_{11}R_2$, $R_2 \to R_2 + R_1/b_{11}$ yields

$$\begin{bmatrix} 0 & -b_{11}b_{22} & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{nn} \end{bmatrix}.$$

Performing our transposition with sign change yields

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & b_{11}b_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{nn} \end{bmatrix}.$$

Repeating this down the line, we see that $b_{11}b_{22}\dots b_{nn}$ bunches up at the lower right, but this is just 1, so we get the identity matrix. Thus, $SL_n(\mathbb{R})$ is generated by elementary matrices of the first type.

Exercise 19. Determine the number of elements of order 2 in the symmetric group S_4.

Solution. Use the notation $(a\ b\ c\ d)$ to denote a cycle $a \rightsquigarrow b$, $b \rightsquigarrow c$, $c \rightsquigarrow d$, $d \rightsquigarrow a$. Note that any transposition of two elements has order 2, hence all two-cycles

$$(1\ 2) \quad (1\ 3) \quad (1\ 4) \quad (2\ 3) \quad (2\ 4) \quad (3\ 4)$$

have order 2. If any two of them commute, then their product will also be of order 2 (Exercise 11), therefore the products of disjoint two-cycles

$$(1\ 2)(3\ 4) \quad (1\ 3)(2\ 4) \quad (1\ 4)(2\ 3)$$

also have order 2. This gives a total of 9 elements.

Exercise 20.

(a) Let a, b be elements of an abelian group of orders m, n respectively. What can you say about the order of their product ab?

(b) Show by example that the product of elements of finite order in a non-abelian group need not have finite order.

Solution.

(a) Set $d = \gcd(m, n)$. The order of ab will always divide $k = mn/d$. Note that in an abelian group,

$$(ab)^k = a^k b^k = a^{mn/d} b^{mn/d} = (a^m)^{n/d} (b^n)^{m/d} = 1.$$

Note that the order of ab is not always k. Consider $a = b = i \in \mathbb{C}^\times$, and note that the orders of a and b are 4. However, the order of their product $i^2 = -1$ is 2.

(b) Select the following elements from $GL_2(\mathbb{R})$.

$$A = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}.$$

Note that $A^2 = B^2 = \mathbb{I}_2$. However,

$$AB = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \qquad (AB)^2 = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}, \qquad (AB)^3 = \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}, \qquad \dots$$

In general for $n > 0$, we have

$$(AB)^n = \begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix}.$$

Thus, AB has infinite order.

Exercise 21. Prove that the set of elements of finite order in an abelian group is a subgroup.

Solution. Let G be abelian, and let H be the set of all elements with finite order. Note that $1 \in H$. Also, if a and b have finite order, so does ab by the previous exercise. Finally, if a has finite order n, then $a^n = 1$ forces $1 = a^{-n} = (a^{-1})^n$, hence a^{-1} has finite order n. Thus, H is a subgroup of G.

Exercise 22. Prove that the greatest common divisor of a and b, as defined in the text, can be obtained by factoring a and b into primes and collecting the common factors.

Solution. Suppose that

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \cdots, \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n} \cdots,$$

where p_i are the prime numbers, and α_i, β_i are non-negative integers. We have $\alpha_{i \geq M} = \beta_{i \geq N} = 0$ eventually, for a and b to be finite. Setting $\gamma_i = \min\{\alpha_i\, \beta_i\}$, we claim that the greatest common factor of a and b is

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n} \cdots.$$

First note that d divides both a and b, therefore d must divide $d' = \gcd(a, b)$. Write

$$d'/d = p_1^{\gamma_1'} p_2^{\gamma_2'} \cdots p_n^{\gamma_n'} \cdots.$$

Suppose that $\gamma_k' > 0$ for some k. This means that the power of p_k in d' is $\gamma_k + \gamma_k' > \min\{\alpha_k, \beta_k\}$. This means that d' cannot divide one or more of a and b, so $\gamma_i' = 0$ for all i. Thus, $d = d'$.

2.3 Isomorphisms

Exercise 1. Prove that the additive group $\mathbb{R}^+$ of real numbers is isomorphic to the multiplicative group P of positive reals.

Solution. We construct the isomorphism $\varphi\colon \mathbb{R}^+ \to P$, $x \mapsto e^x$. This is a homomorphism, because $\phi(0) = e^0 = 1$, and

$$\varphi(x + y) = e^{x+y} = e^x e^y = \varphi(x)\, \varphi(y).$$

This map is injective because for any $\varphi(x) = \varphi(y)$, we have $e^x = e^y$ or $e^{x-y} = 0$, hence $x - y = 0$ or $x = y$. This map is also surjective because $\varphi^{-1}(x) = \log(x)$ is well defined for all positive reals. Hence, φ is a bijection between $\mathbb{R}^+$ and P respecting their laws of composition, which proves that they are isomorphic.

Exercise 2. Prove that the elements ab and ba are conjugate elements in a group.

Solution. Note that

$$ab = (ab)aa^{-1} = a(ba)a^{-1}, \qquad ba = (ba)bb^{-1} = b(ab)b^{-1}.$$

Exercise 3. Let a, b be elements of a group G, and let $a' = bab^{-1}$. Prove that $a = a'$ is and only if a and b commute.

Solution. First, suppose that $a = a'$. This means that $a = baab^{-1}$, or $ab = ba$, hence a and b commute.

Next, suppose that a and b commute. Then, $a' = baab^{-1} = abb^{-1} = a$.

Exercise 4.

(a) Let $b' = aba^{-1}$. Prove that $b'^n = ab^n a^{-1}$.

(b) Prove that if $aba^{-1} = b^2$, then $a^3 ba^{-3} = b^8$.

Solution.

(a) The claim for $n \geq 1$ follows from induction. Note that the case $n = 1$ is true, and if it holds for some k with $b'^k = ab^k a^{-1}$, then

$$b'^{k+1} = b'^{k\prime} = (ab^k a^{-1})(aba^{-1}) = ab^k(a^{-1}a)ba^{-1} = ab^{k+1}a^{-1},$$

thus proving the claim for all $n \geq 1$. Now, for any $n \leq -1$, note that $b^{-n} = ab^{-n}a^{-1}$ by the first part, hence taking inverses gives $b^n = ab^n a^{-1}$. This establishes the formula for all $n \in \mathbb{Z}$.

(b) We have been given the rule $ab = b^2a$. Thus,

$$a^3ba^{-3} = a^2(ab)a^{-3} = a^2(b^2a)a^{-3} = a^2b^2a^{-2}.$$

Proceeding in this fashion, this is the same as

$$a(ab)ba^{-2} = a(b^2a)ba^{-2} = ab^2(ab)a^{-2} = ab^2(b^2a)a^{-2} = ab^4a^{-1}.$$

Finally, this is the same as

$$(ab)b^3a^{-1} = (b^2a)b^3a^{-1} = b^2(ab)b^2a^{-1} = b^2(b^2a)b^2a^{-1} =$$

$$b^4(ab)ba^{-1} = b^4(b^2a)ba^{-1} = b^6(ab)a^{-1} = b^6(b^2a)a^{-1} = b^8.$$

Alternatively, note that $b^2 = aba^{-1}$, so

$$b^8 = (b^2)^4 = ab^4a^{-1}, \qquad b^4 = (b^2)^2 = ab^2a^{-1}, \qquad b^2 = (b^2)^1 = aba^{-1}.$$

Substituting each of these into the equation above gives

$$b^8 = ab^4a^{-1} = a(ab^2a^{-1})a^{-1} = a(a(aba^{-1})a^{-1})a^{-1} = a^3ba^{-3}.$$

Exercise 5. Let $\varphi\colon G \to G'$ be an isomorphism of groups. Prove that the inverse function φ^{-1} is also an isomorphism.

Solution. First note that φ is a bijection, which means that φ^{-1} is also a bijection. Let $a', b' \in G'$ be arbitrary. We set $a = \varphi^{-1}(a')$, $b = \varphi^{-1}(b')$. Since

$$\varphi(ab) = \varphi(a)\varphi(b),$$

we have

$$\varphi(ab) = a'b', \qquad \varphi^{-1}(a')\varphi^{-1}(b') = ab = \varphi^{-1}(a'b').$$

This proves that $\varphi^{-1}\colon G' \to G$ is an isomorphism.

Exercise 6. Let $\varphi\colon G \to G'$ be an isomorphism of groups, let $x, y \in G$ and let $x' = \varphi(x)$ and $y' = \varphi(y)$.

(a) Prove that the orders of x and x' are equal.

(b) Prove that if $xyx = yxy$, then $x'y'x' = y'x'y'$.

(c) Prove that $\varphi(x^{-1}) = x'^{-1}$.

Solution. Recall that if e and e' are the identity elements in G and G' respectively, then $\varphi(e) = e'$. This is because $ee = e$, so $\varphi(e)\varphi(e) = \varphi(e)$, hence cancellation gives $\varphi(e) = e'$.

(a) Suppose that the orders of x and x' are m and n respectively, hence $x^m = e$ and $x'^n = e'$. Note that $\varphi(x^2) = \varphi(x)\varphi(x) = x'^2$, and by repeating this process, it can be shown that $\varphi(x^k) = x'^k$ for any $k \geq 1$. This means that if $x^m = e$, we have $x'^m = \varphi(x^m) = \varphi(e) = e'$, hence $m \geq n$. Also, φ^{-1} is also an isomorphism, so $x^n = \varphi^{-1}(x'^n) = \varphi^{-1}(e') = e$, hence $n \geq m$. Together, this implies that $m = n$.

Note that if m were infinite, this would force n to be infinite as well, and vice versa.

(b) Write

$$\varphi(xyx) = \varphi(xy)\varphi(x) = \varphi(x)\varphi(y)\varphi(x) = x'y'x'.$$

Similarly, $\varphi(yxy) = y'x'y'$. Equating the two gives the desired result.

(c) Use the fact that $xx^{-1} = e$, so $\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e) = e'$. This means $x'\varphi(x^{-1}) = e'$, which forces $\varphi(x^{-1}) = x'^{-1}$.

Exercise 9. Find an isomorphism from a group G to its opposite group G°.

Solution. Define $\varphi\colon G \to G^\circ$, $x \mapsto x^{-1}$. This is clearly a bijection because every element x has exactly one inverse. Observe that for any $x, y \in G$,

$$\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = \varphi(y)\varphi(x) = \varphi(x) \circ \varphi(y),$$

as desired. Recall the nature of composition $\circ$ in G°.

Exercise 10. Prove that the map $A \rightsquigarrow (A^t)^{-1}$ is an automorphism of $GL_n(\mathbb{R})$.

Solution. First note that this map is a bijection, because every matrix in $GL_n(\mathbb{R})$ has exactly one inverse, and every matrix in $GL_n(\mathbb{R})$ has exactly one transpose in $GL_n(\mathbb{R})$. Also observe that for $A, B \in GL_n(\mathbb{R})$,

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

which proves that the given map is an automorphism.

Exercise 11. Prove that the set $\mathrm{Aut}(G)$ of automorphisms of a group G forms a group, the law of composition being the composition of functions.

Solution. Note that the identity map is trivially an automorphism. The composition of functions is inherently associative, and the composition of two automorphisms is another automorphism - suppose that φ and ψ are automorphisms. Then, $\psi \circ \varphi$ is a bijection, with

$$(\psi \circ \varphi)(xy) = \psi(\varphi(xy)) = \psi(\varphi(x)\,\varphi(y)) = \psi(\varphi(x))\,\psi(\varphi(y)) = (\psi \circ \varphi)(x)\,(\psi \circ \varphi)(y).$$

Finally, the inverse of an automorphism is also an automorphism. This shows that $\mathrm{Aut}(G)$ forms a group.

Exercise 12. Let G be a group and let $\varphi\colon G \to G$ be the map $(x) = x^{-1}$.

(a) Prove that φ is bijective.

(b) Prove that φ is an automorphism if and only if G is abelian.

Solution. (a) The map φ is a bijection because every element x in G has a unique inverse.

(b) If G is abelian, note that

$$\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y).$$

If is to be an automorphism, we have

$$\varphi(x^{-1}y^{-1}) = (x^{-1}y^{-1})^{-1} = yx.$$

for all $x, y \in G$. We also demand

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

hence equating the two gives $xy = yx$, proving that G is abelian.

Exercise 13.

(a) Let G be a group of order 4. Prove that every element has order 1, 2, or 4.

(b) Classify groups of order 4 by considering the following cases.

(i) G contains an element of order 4.

(ii) Every element of G has order < 4.

Solution.

(a) Note that every $x \in G$ obeys $x^4 = 1$, so the order of every element of G must be either $1, 2, 3$ or 4. Suppose that $x^3 = 1$. Writing $x^3 = 1 = x^4$ gives $x = 1$. Thus, no element of G can have order 3.

In any group of n elements, observe that every element obeys $x^n = 1$. To see this, consider the set $\{1, x, \ldots, x^n\}$. All of these elements cannot be distinct since that would yield $n+1$ elements in a group of n elements. Thus, we have $x^p = x^q$ for some $0 \leq p < q \leq n$, giving $x^{q-p} = 1$, so the order of x is less than or equal to n. Suppose that x has order $m \leq q - p$; write $n = am + b$ for $0 \leq b < m$. Now, $x^n = (x^m)^a x^b = x^b$, so the minimality of m forces $b = 0$. This yields $x^n = 1$.

(b) Let the elements of G be $\{1, a, b, c\}$, where a, b, c are distinct. Suppose that a has order 4. Now, b and c must have order 2 or 4. Now, $a^2 \neq 1$ and $a^2 \neq a$, so without loss of generality set $a^2 = b$. Thus, $b^2 = a^4 = 1$, so b has order 2. We now have $a^{-1} \neq a$ since that would imply $a^2 = 1$, and also $a^{-1} \neq b$ because that would also give $a^{-2} = b^2 = 1$ hence $a^2 = 1$. Thus, $a^{-1} = c = a^3$, so c also has order 4. This means that G is the cyclic group $\{1, a, a^2, a^3\}$.

Now, suppose that no element has order 4. None of a, b, c can have order 1, hence each of them has order 2, with $a^2 = b^2 = c^2 = 1$. Examine ab, and note that $ab = b$ would imply $a = 1$, $ab = a$ would imply $b = 1$. This forces $ab = c$. The same argument also forces $ba = c$, and similarly $ac = ca = b$, $bc = cb = a$. Thus, G is the Klein four group $\{1, a, b, ab\}$.

Exercise 14. Determine the group of automorphisms of the following groups.

(a) $\mathbb{Z}^+$.

(b) A cyclic group of order 10.

(c) S_3.

Exercise 15. Show that the functions $f = 1/x$, $g = (x-1)/x$ generate a group of functions, the law of composition being composition of functions, which is isomorphic to the symmetric group S_3.

Solution. Observe that $f^2(x) = x$, $g^2(x) = ((x-1)/x - 1)/((x-1)/x) = -1/(x-1)$, $g^3(x) = -1/((x-1)/x - 1) = x$. This gives $fg(x) = (f \circ g)(x) = x/(x-1)$, and $fg^2(x) = (f \circ g^2)(x) = 1 - x$.

Next, $gf(x) = (1/x - 1)/(1/x) = 1 - x = fg^2(x)$, and $g^2 f(x) = ((1-x) - 1)/(1-x) = x/(1-x) = fg(x)$. This means that compositions like $fgfg = f(gf)g = f(fg^2)g = f^2g^3 = 1$. Thus, the elements f and g generate the elements $1, g, g^2, f, fg, fg^2$ which is closed under composition.

Our group consists of the functions $\{1, g, g^2, f, fg, fg^2\}$. The map from this set to S_3, defined as $f \rightsquigarrow (1\,2)$ and $g \rightsquigarrow (1\,2\,3)$ is thus an isomorphism, because it is bijective, and the multiplication table of our given elements is identical to that of S_3.

Exercise 16. Give an example of two isomorphic groups such that there is more than one isomorphism between them.

Solution. Recall that we constructed an isomorphism between the additive group $\mathbb{R}^+$ of real numbers and the multiplicative group P of positive reals, by considering the map $x \mapsto e^x$. Another isomorphism is defined by the map $x \mapsto e^{-x}$.

Note that this map is motivated by the fact that the reflection $\varphi\colon \mathbb{Z}^+ \to \mathbb{Z}^+$, $x \mapsto -x$ is an automorphism.

2.4 Homomorphisms

Exercise 1. Let G be a group, with law of composition written $x \# y$. Let H be a group with law of composition $u \circ v$. What is the condition for a map $\varphi\colon G \to H$ to be a homomorphism?

Solution. We demand that for all $x, y \in G$,

$$\varphi(x \# y) = \varphi(x) \circ \varphi(y).$$

Exercise 2. Let $\varphi\colon G \to G'$ be a group homomorphism. Prove that for any elements $a_1, \ldots, a_k$ of G,

$$\varphi(a_1 \cdots a_k) = \varphi(a_1) \cdots \varphi(a_k).$$

Solution. This follows from induction, the base case $k = 2$ following from the definition of a homomorphism. If this formula holds for some $n \geq 2$, then

$$\varphi(a_1 \cdots a_n a_{n+1}) = \varphi(a_1 \cdots a_n)\,\varphi(a_n) = \varphi(a_1) \cdots \varphi(a_n)\,\varphi(a_{n+1}).$$

Exercise 3. Prove that the kernel and image of a homomorphism are subgroups.

Solution. Let $\varphi\colon G \to H$ be a homomorphism. The kernel of φ is the set of all elements $x \in G$ such that $\varphi(x) = 1_H$. The image of φ is the set of all elements $u \in H$ such that $u = \varphi(x)$ for some $x \in G$. Denote the kernel as $K \subseteq G$, and the image as $I \subseteq H$. It suffices to show that $K < G$ and $I < H$ are subgroups.

Note that $1_G \in K$ because a homomorphism must send the identity of G to the identity of H. Note that $\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G)$, and cancellation gives $\varphi(1_G) = 1_H$. Next, if $x, y \in K$, then $\varphi(xy) = \varphi(x)\varphi(y) = 1_H 1_H = 1_H$, hence $xy \in K$. Finally, if $x \in K$, then $1_H = \varphi(1_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) = \varphi(x^{-1})$, so x^{-1} in K. Thus, the kernel of φ is a subgroup of G.

Note that $1_H \in I$, because $\varphi(1_G) = 1_H$. If $u, v \in I$, then $u = \varphi(x)$ and $v = \varphi(y)$ for some $x, y \in G$, so $uv = \varphi(x)\varphi(y) = \varphi(xy)$. This means that $uv \in I$. Finally, if $u \in I$ with $u = \varphi(x)$,

then $1_H = \varphi(1_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) = u\varphi(x^{-1})$, so $u^{-1} = \varphi(x^{-1})$ which means $u^{-1} \in I$. Thus the image of φ is a subgroup of H.

Exercise 4. Describe all homomorphisms $\varphi\colon \mathbb{Z}^+ \to \mathbb{Z}^+$, and determine which are injective, which are surjective, and which are isomorphisms.

Solution. Note that for any such homomorphism, $\varphi(0) = 0$. Since $\mathbb{Z}^+$ is generated by 1, the homomorphism φ is fully determined by $\varphi(1)$. For any $n > 0$, write $n = 1 + \cdots + 1$, hence $\varphi(n) = \varphi(1) + \cdots + \varphi(1) = n\varphi(1)$. Thus, $\varphi(0) = \varphi(n + (-n)) = \varphi(n) + \varphi(-n)$, so $\varphi(-n) = -\varphi(n) = -n\varphi(1)$.

If $\varphi(1) = 0$, then $\varphi(n = 0)$ for all n; this homomorphism is not injective, nor surjective. If $\varphi(1) = 1$ or $\varphi(1) = -1$, then $\varphi(n) = n$ or $\varphi(n) = -n$ respectively; these homomorphisms are isomorphisms, since they are both injective and surjective.

If $\varphi(1) > 1$, this homomorphism is injective, because if $\varphi(m) = \varphi(n)$, then $\varphi(m - n) = 0$ or $(m - n)\varphi(1) = 0$, which is possible only if $m - n = 0$. This is not surjective however, since there is no n such that $\varphi(n) = 1$. If $\varphi(n) = 1$, then note that $n\varphi(1) = 1$, which would require $\varphi(1) = 1/n \notin \mathbb{Z}$. The same applies whenever $\varphi(1) < -1$.

Exercise 5. Let G be an abelian group. Prove that the nth power map $\varphi\colon G \to G$ defined by $\varphi(x) = x^n$ is a homomorphism from G to itself.

Solution. Note that for any $x, y \in G$, we have

$$\varphi(xy) = (xy)^n = x^n y^n = \varphi(x)\,\varphi(y),$$

which shows that φ preserves the group structure, and is hence a homomorphism. Note that we have used the commutativity of elements in G to conclude that $(xy)^n = x^n y^n$.

Exercise 6. Let $f\colon \mathbb{R}^+ \to \mathbb{C}^\times$ be the map e^{ix}. Prove that f is a homomorphism, and determine its kernel and image.

Solution. For any $x, y \in \mathbb{R}$, note that

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

which establishes f as a homomorphism.

Note that the identity in $\mathbb{C}^\times$ is 1; the solutions of e^{ix} for real x are precisely $2\pi k$, for $k \in \mathbb{Z}$. This set forms the kernel of f. Also, f maps the interval $[0, 2\pi)$ precisely to the unit circle in $\mathbb{C}$, which thus forms the image of f. There are no other points in the image of f, since $|f(x)| = |e^{ix}| = 1$ for all real x.

Exercise 7. Prove that the absolute value map $|\ \ |\colon \mathbb{C}^\times \to \mathbb{R}^\times$ sending $\alpha \rightsquigarrow |\alpha|$ is a homomorphism, and determine its kernel and image.

Solution. For any $\alpha, \beta \in \mathbb{C}$, note that

$$|\alpha\beta| = |\alpha||\beta|,$$

which establishes the absolute value map as a homomorphism.

The pre-image of 1, the identity in $\mathbb{R}^\times$, is the unit circle in $\mathbb{C}$ described by $\{e^{ix}\colon x \in \mathbb{R}\}$. This is the kernel of the absolute value map. The image of this map is the entirety of $\mathbb{R}$, since $x = |x|$ for all $x \in \mathbb{R}$.

Exercise 8.

(a) Find all subgroups of S_3, and determine which are normal.

(b) Find all subgroups of the quaternion group, and determine which are normal.

Solution.

(a) Let x denote the transposition $(1\,2)$ and y denote the cycle $(1\,2\,3)$. The elements of S_3 are $1, x, y, xy, y^2, xy^2$, with $x^2 = 1$ and $y^3 = 1$. Now, x generates the subgroup $\{1, x\}$ and y or y^2 generate the subgroup $\{1, y, y^2\}$. Note that x and y together generate the whole of S_3. If a subgroup contains any of xy, xy^2 along with x, then $x(xy) = y$ and $x(xy^2) = y^2$ mean that y is also in the subgroup, hence the subgroup is S_3 itself. Similarly, if a subgroup contains any of xy, xy^2 along with y, then $(xy)yy = x$ and $(xy^2)y = x$ mean that y is also in the subgroup, again forcing the subgroup to be S_3. Also note that xy generates the subgroup $\{1, xy\}$ and xy^2 generates the subgroup $\{1, xy^2\}$. If a subgroup contains both xy and xy^2, then it also contains $(xy)^{-1} = y^2x$ hence $(y^2x)(xy^2) = y$ and $(xy^2)y = x$, which forces it to be equal to S_3. Thus, we have found all subgroups of S_3, namely $\{1\}$, $\{1, x\}$, $\{1, xy\}$, $\{1, xy^2\}$, $\{1, y, y^2\}$, and S_3.

Consider the subgroup $\{1, x\}$. Note that $yxy^{-1} = yxy^2 = (xy^2)y^2 = xy \notin \{1, x\}$. Similarly for the other subgroups of order 2, $y(xy)y^{-1} = yxyy^2 = yx = xy^2$, and $y(xy^2)y^{-1} = yxy = xy^2y = x$. Thus, none of these are normal subgroups. Looking at $\{1, y, y^2\}$, consider the homomorphism $\varphi\colon S_3 \to S_3$ defined by $\varphi(x) = x$, $\varphi(y) = 1$. This gives $\varphi(y^2) = 1$, $\varphi(xy) = x$, $\varphi(xy^2) = x$, hence $\{1, y, y^2\}$ is the kernel of the homomorphism φ, making it a normal subgroup. This is the only normal subgroup besides $\{1\}$ and S_3.

(b) The quaternion group contains the elements $1, i, j, k, -1, -i, -j, -k$. The only non-trivial subgroups are $\{1, -1\}$, $\{1, i, -1, -i\}$, $\{1, j, -1, -j\}$ and $\{1, k, -1, -k\}$. This is because any two other elements like i and j can generate the third, $ij = k$. The subgroup $\{1, -1\}$ is normal since $x(-1)x^{-1} = -xx^{-1} = -1$ for all other choices of x. It suffices to show that $\{1, i, -1, -i\}$ is normal to prove that all the subgroups are normal. We can check that $jij^{-1} = ji(-j) = -jij = -jk = -i$, $kik^{-1} = ki(-k) = -kik = -k(-j) = -i$, which is sufficient to show that $\{1, i, -1, -i\}$ is normal.

Exercise 9.

(a) Prove that the composition $\varphi \circ \psi$ of two homomorphisms φ, ψ is a homomorphism.

(b) Describe the kernel of $\varphi \circ \psi$.

Solution.

(a) Note that for all elements x, y, we have

$$(\varphi \circ \psi)(xy) = \varphi(\psi(x)\psi(y)) = \varphi(\psi(x))\varphi(\psi(y)) = (\varphi \circ \psi)(x)\,(\varphi \circ \psi)(y).$$

(b) The kernel of $\varphi \circ \psi$ is by definition $\psi^{-1}(\varphi^{-1}(1))$, where 1 is the identity in the image of $\varphi \circ \psi$. This contains the kernel of ψ, since $\psi(x) = 1 \implies \varphi(\psi(x)) = 1$.

Exercise 10. Let $\varphi\colon G \to G'$ be a group homomorphism. Prove that $\varphi(x) = \varphi(y)$ if and only if $xy^{-1} \in \ker\varphi$.

Solution. Recall that $\varphi(y^{-1}) = \varphi(y)^{-1}$. Suppose that $\varphi(x) = \varphi(y)$. Then, $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(y)\varphi(y)^{-1} = 1$, so $xy^{-1} \in \ker\varphi$.

Next, suppose that $xy^{-1} \in \ker\varphi$, i.e. $\varphi(xy^{-1}) = 1$. This gives $\varphi(x)\varphi(y)^{-1} = 1$, hence $\varphi(x) = \varphi(y)$.

Exercise 11. Let G, H be cyclic groups, generated by the elements x, y. Determine the condition on the orders m, n of x and y so that the map sending $x^i \rightsquigarrow y^i$ is a group homomorphism.

Solution. Note that $x^m = 1$, hence $x^i = x^{i+km}$ for all integers k. We want $y^i = \varphi(x^i) = \varphi(x^{i+m}) = y^{i+m}$, hence $1 = y^m$. This means that the order of y must divide m, hence $n \mid m$ is a necessary condition for our map to be well-defined.

We claim that φ is now a homomorphism. Given any $x^p, x^q \in G$, we see that $\varphi(x^p x^q) = \varphi(x^{p+q}) = y^{p+q} = y^p y^q = \varphi(x^p)\varphi(x^q)$. These operations are well-defined since there is a unique element $y^j \in H$ such that $y^j = y^{p+q}$, namely when $j = p + q \pmod n$.

Exercise 12. Prove that the $n \times n$ block matrices M which have the block form

$$\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$$

with $A \in GL_r(\mathbb{R})$ and $D \in GL_{n-r}(\mathbb{R})$ form a subgroup P of $GL_n(\mathbb{R})$, and the map $P \to GL_r(\mathbb{R})$ sending $M \rightsquigarrow A$ is a homomorphism. What is it's kernel?

Solution. Note that multiplication of such block matrices is closed, with

$$\begin{bmatrix} A_1 & B_1 \\ 0 & D_1 \end{bmatrix} \begin{bmatrix} A_2 & B_2 \\ 0 & D_2 \end{bmatrix} = \begin{bmatrix} A_1A_2 & A_1B_2 + B_1D_2 \\ 0 & D_1D_2 \end{bmatrix}.$$

The identity matrix $\mathbb{I}_n \in P$, since it is of the required block form ($A = \mathbb{I}_r$, $D = \mathbb{I}_{n-r}$, $B = 0$). Because A and D are invertible, note that

$$\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}^{-1} = \begin{bmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{bmatrix},$$

which can be checked by

$$\begin{bmatrix} A & B \\ 0 & D \end{bmatrix} \begin{bmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{bmatrix} = \begin{bmatrix} AA^{-1} & A(-A^{-1}BD^{-1}) + B(D^{-1}) \\ 0 & DD^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus, P forms a subgroup of $GL_n(\mathbb{R})$. Labelling the matrices M_A, where A is the top left block, we see that the map sends

$$M_X \rightsquigarrow X, \qquad M_Y \rightsquigarrow Y, \qquad M_X M_Y \rightsquigarrow XY$$

since the top left block obeys the usual multiplication in $GL_r(\mathbb{R})$. This shows that this map is a homomorphism. Its kernel is the pre-image of $\mathbb{I}_r$, which is the set of matrices $M_A \in P$ such that $A = \mathbb{I}_r$.

Exercise 13.

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

(b) Prove that a subgroup H of G is normal if and only if $gHg^{-1} = H$ for all $g \in G$.

Solution.

(a) Note that the identity $1 \in G$ is present in H, hence $g1g^{-1} = 1 \in gHg^{-1}$. Next, multiplication of elements in closed in the conjugate subgroup, because for any $h_1, h_2 \in H$, we have

$$(gh_1g^{-1})(gh_2g^{-1}) = gh_1(g^{-1}g)h_2g^{-1} = g(h_1h_2)g^{-1},$$

and $h_1h_2 \in H$. Finally, for any $h \in H$, we have $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$, with $h^{-1} \in H$. Thus, gHg^{-1} is indeed a subgroup of G.

(b) Suppose that H is a normal subgroup. For any $ghg^{-1} \in G$ with $h \in H$, we must have $ghg^{-1} \in H$ by definition. Also for any $h \in H$, we must have $ghg^{-1} \in H$, hence $gHg^{-1} = H$.

Suppose that $gHg^{-1} = H$ for every $g \in G$. This means that given $h \in H$, we have $ghg^{-1} \in H$, hence H must be a normal subgroup.

Exercise 14. Let N be a normal subgroup of G, and let $g \in G$, $n \in N$. Prove that $g^{-1}ng \in N$.

Solution. Note that we must have $gng^{-1} \in N$ for every choice of $g \in G$. Thus, choose $g^{-1} \in G$, whence $(g^{-1})n(g^{-1})^{-1} = g^{-1}ng \in N$.

Exercise 15. Let φ and ψ be two homomorphisms from a group G to another group G', and let $H \subset G$ be the subset $\{x \in G \colon \phi(x) = \psi(x)\}$. Prove or disprove: H is a subgroup of G.

Solution. Note that a homomorphism must map the identity to the identity, so $(1) = 1' = \psi(1)$ gives $1 \in H$. If $x, y \in H$, then $\varphi(x) = \psi(x)$ and $\varphi(y) = \psi(y)$, so $\varphi(xy) = \varphi(x)\varphi(y) = \psi(x)\psi(y) = \psi(xy)$ giving $xy \in H$. Finally, if $x \in H$ with $\varphi(x) = \psi(x)$, we have $\varphi(x^{-1}) = \varphi(x)^{-1} = \psi(x)^{-1} = \psi(x^{-1})$, so $x^{-1} \in H$. Thus, H forms a subgroup of G.

Exercise 16. Let $\varphi \colon G \to G'$ be a group homomorphism, and let $x \in G$ be an element of order r. What can you say about the order of $\varphi(x)$?

Solution. Note that the order of $\varphi(x)$ is at most r, since

$$\varphi(x)^r = \varphi(x^r) = \varphi(1) = 1.$$

Furthermore, if the order of $\varphi(x)$ is r', we must have $r' \mid r$. Write $r = ar' + b$ for $0 \leq b < r'$, whence

$$1 = \varphi(x^r) = \varphi(x^{ar'+b}) = \varphi(x^a)^{r'}\varphi(x)^b = \varphi(x)^b.$$

The minimality of r' forces $b = 0$, hence $r = ar'$.

Exercise 17. Prove that the center of a group is a normal subgroup.

Solution. Recall that the center H of a group G is the set of elements $x \in G$ such that $xg = gx$ for all $g \in G$. This forms a subgroup of G since $1 \in H$, $(xy)g = x(yg) = x(gy) = (xg)y = g(xy)$ hence $xy \in H$ if $x, y \in H$, and $xg = gx$ implies $gx^{-1} = x^{-1}g$ hence $x^{-1} \in H$ if $x \in H$. Furthermore, H is a normal subgroup since H is abelian. Note that given any $x \in H$ and $g \in G$, we have $gxg^{-1} = xgg^{-1} = x \in H$.

Exercise 18. Prove that the center of $GL_n(\mathbb{R})$ is the subgroup $Z = \{cI \colon c \in \mathbb{R}, c \neq 0\}$.

Solution. Note that for each element $cI \in Z$, we indeed observe that

$$(cI)A = cA = Ac = (AI)c = A(cI)$$

for every choice of $A \in GL_n(\mathbb{R})$. Suppose that B commutes with every matrix in $GL_n(\mathbb{R})$, i.e. $BA = AB$ for all $A \in GL_n(\mathbb{R})$. Let E_{ij} be the matrix with 1 in the i, jth entry and zeroes everywhere else, and note that the product BE_{ij} is a matrix with its jth column equal to the ith column of B and with zeroes everywhere else. Similarly, $E_{ij}B$ is the matrix whose ith row is the jth row of B, and with zeroes everywhere else. Now, $I + E_{ij} \in GL_n(\mathbb{R})$, so by demanding $B(I + E_{ij}) = (I + E_{ij})B$, we want $BE_{ij} = E_{ij}B$, which forces $b_{jj} = b_{ii}$, with the remaining entries $b_{ki} = 0$ and $b_{jk} = 0$ for the remaining choices of k. Repeating this for every pair $1 \leq i < j \leq n$, we conclude that all the diagonal entries b_{ii} are equal, and all off-diagonal entries of B are zero. Thus, B must be of the form $b_{11}I = cI$.

Exercise 19. Prove that if a group contains exactly one element of order 2, then that element is in the center of the group.

Solution. Let x be the only element of order 2 in the group G, i.e. $x^2 = 1$ hence $x = x^{-1}$. Suppose that for some $g \in G$, we have $xg \neq gx$, i.e. $xgx^{-1}g^{-1} = y \neq 1$. Then we have $xy = x^{-1}y = gx^{-1}g^{-1}$, hence $(xy)^2 = gx^{-2}g^{-1} = gg^{-1} = 1$. Since x is the only element of order 2, either $xy = 1$ or $xy = x$. The former implies that $y = x^{-1} = x$, hence $xgx^{-1}g^{-1} = x \implies gx^{-1}g^{-1} = 1 \implies x = 1$, a contradiction. The latter implies that $y = 1$, another contradiction. Thus, we must have $xg = gx$ for all $g \in G$, which means that x is in the center of G.

Exercise 20. Consider the set U of real 3×3 matrices of the form

$$\begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}.$$

(a) Prove that U is a subgroup of $SL_3(\mathbb{R})$.

(b) Prove or disprove: U is normal.

(c) Determine the center of U.

Solution.

(a) See Chapter 1, Miscellaneous Problems, Exercise 6.

(b) Consider

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

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Thus, this particular conjugate does not belong to U, which means that U is not a normal subgroup of $SL_3(\mathbb{R})$.

(c) Note that a general product of matrices in U looks like

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

Thus, for this product to commute for fixed a, b, c, we require $ac' = a'c$ for all choices of a' and c'. This immediately gives $a = c = 0$, and this is sufficient. The center of U is the set of all matrices of the form

$$\begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Exercise 21. Prove by giving an explicit example that $GL_2(\mathbb{R})$ is not a normal subgroup of $GL_2(\mathbb{C})$.

Solution. Consider

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

Exercise 22. Let $\varphi\colon G \to G'$ be a surjective homomorphism.

(a) Assume that G is cyclic. Prove that G' is cyclic.

(b) Assume that G is abelian. Prove that G' is abelian.

Solution.

(a) Let G be generated by the element x. For every element $u \in G'$, we must have $u = \varphi(x^r)$ for some $r \in \mathbb{Z}$ because of the surjectivity of φ. Thus, every $u \in G'$ is of the form $u = \varphi(x)^r$, which means that G' is a cyclic group generated by $\varphi(x)$.

(b) For any $u, v \in G'$, we must have $u = \varphi(x)$ and $v = \varphi(y)$ for some $x, y \in G$. Then, $uv = \varphi(x)\varphi(y) = \varphi(xy) = \varphi(yx) = \varphi(y)\varphi(x) = vu$, which shows that G' is abelian.

Exercise 23. Let $\varphi\colon G \to G'$ be a surjective homomorphism, and let N be a normal subgroup of G. Prove that $\varphi(N)$ is a normal subgroup of G'.

Solution. Let $u \in \varphi(N)$ be fixed, and let $v \in G'$ be arbitrary. We find $x \in N$, $y \in G$ such that $u = \varphi(x)$, $v = \varphi(y)$. Since $x \in N$ is part of a normal subgroup, we have $yxy^{-1} \in N$, hence $\varphi(yxy^{-1}) \in \varphi(N)$. However, $\varphi(yxy^{-1}) = vuv^{-1} \in \varphi(N)$, which shows that $\varphi(N)$ is a normal subgroup of G'.

2.5 Equivalence Relations and Partitions

Exercise 1. Prove that the non-empty fibres of a map form a partition of the domain.

Solution. Consider a map $f\colon X \to Y$, and without loss of generality let f be surjective (if not, substitute $\operatorname{im} Y$ for Y). We wish to show that for any two $u, v \in Y$ such that $u \neq v$, the pre-images $f^{-1}(u)$ and $f^{-1}(v)$ are disjoint. Suppose these two sets had a common element x; this would imply $f(x) = u$ and $f(x) = v$ simultaneously, which is absurd. Furthermore, every $x \in X$ belongs to the fibre $f^{-1}(f(x))$ by construction, which means that the non-empty fibres of the map f partition the domain X.

Exercise 2. Let S be a set of groups. Prove that the relation $G \sim H$ if G is isomorphic to H is an equivalence relation in S.

Solution. Note that $\sim$ is reflexive, since every group is isomorphic to itself via the identity map. The relation $\sim$ is also symmetric because if $G \sim H$, there is an isomorphism $\varphi\colon G \to H$ whose inverse $\phi^{-1}\colon H \to G$ is also an isomorphism hence $H \sim G$. Finally, if $G_1 \sim G_2$ and $G_2 \sim G_3$, there exist isomorphisms $\varphi\colon G_1 \to G_2$ and $\psi\colon G_2 \to G_3$, whence the map $\psi\circ\colon G_1 \to G_3$ is an isomorphism giving $G_1 \sim G_3$, making $\sim$ transitive. Thus, $\sim$ is an equivalence relation in S.

Exercise 3. Determine the number of equivalence relations on a set of 5 elements.

Solution. It can be shown that any partition $\{A_i\}$ of a set defines an equivalence relation, namely $x \sim y$ if x and y belong to the same set A_i. Additionally, every equivalence relation defines a partition of its set, which means that there is a one-to-one correspondence between partitions and equivalence relations. There are 52 partitions of a set of 5 elements, which means that there are 52 possible equivalence relations.

Exercise 4. Is the intersection $R \cap R'$ of two equivalence relations $R, R' \subset S \times S$ an equivalence relation? Is the union?

Solution. Yes, the intersection $T = R \cap R'$ is an equivalence relation. Note that xTx because xRx and $xR'x$, xTy means that xRy and $xR'y$ which means yRx and $yR'x$, giving yTx. Finally, if xTy and yTz, that means that xRy and $xR'y$, yRz and $yR'z$, which together give xRz and $xR'z$ giving xTz. This proves that T is an equivalence relation.

No, the union $R \cup R'$ is not necessarily an equivalence relation. Consider the relations on $S = \{1, 2, 3\}$, where

$$R = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}, \qquad R' = \{(1,1), (2,2), (3,3), (2,3), (3,2)\}.$$

It is clear that both R and R' are equivalence relation. Their union

$$R \cup R' = \{(1,1), (2,2), (3,3), (1,2), (2,1), (2,3), (3,2)\}$$

is not however, since it contains $(1,2)$ and $(2,3)$, but not $(1,3)$.

Exercise 5. Let H be a subgroup of a group G. Prove that the relation defined by the rule $a \sim b$ if $b^{-1}a \in H$ is an equivalence relation on G.

Solution. For any $a \in G$, we have $a^{-1}a = 1 \in H$ so $a \sim a$. For any $a, b \in G$, if $a \sim b$ i.e. $b^{-1}a \in H$, its inverse $a^{-1}b \in H$ i.e. $b \sim a$. Finally, if for $a, b, c \in G$ we have $a \sim b$ and $b \sim c$, i.e. $b^{-1}a \in H$ and $c^{-1}b \in H$, we have the product $(c^{-1}b)(b^{-1}a) = c^{-1}a \in H$ so $c \sim a$.

Exercise 6.

(a) Prove that the relation x conjugate to y in a group G is an equivalence relation on G.

(b) Describe the elements a whose conjugacy class (equivalence class) consists of the element a alone.

Solution.

(a) Note that every element is self conjugate via $x = 1x1$. If x is conjugate with y, we have $x = gyg^{-1}$ for some $g \in G$, hence $y = g^{-1}xg = (g^{-1})x(g^{-1})^{-1}$ so y is conjugate with y. Finally, if x is conjugate with y and y is conjugate with z, we have $x = gyg^{-1}$ and $y = hzh^{-1}$ for some $g, h \in G$, which gives $x = g(hzh^{-1})g^{-1} = (gh)x(gh)^{-1}$, hence x is conjugate with z.

(b) Suppose that the conjugacy class of a contains only a. This means that the only element b such that $a = gbg^{-1}$ for some $g \in G$, i.e. $b = g^{-1}ag$, is a itself. Thus, the quantity $g^{-1}ag = a$ for all $g \in G$, i.e. $ag = ga$ for all $g \in G$, i.e. a is in the center of G.

Exercise 7. Let R be the relation on the set $\mathbb{R}$ of real numbers. We may view R as a subset of the (x, y) plane. Explain the geometric meaning of the reflexive and symmetric properties.

Solution. Reflexivity forces every pair $(x, x) \in R$, hence the diagonal line $x = y$ must be present in R. Symmetry forces $(y, x) \in R$ whenever $(x, y) \in R$, which means that R has a reflection symmetry about the $x = y$ line.

Exercise 8. With each of the following subsets R of the (x, y) plane, determine which of the axioms (5.2) are satisfied and whether or not R is an equivalence relation on the set $\mathbb{R}$ of real numbers.

(a) $R = \{(s, s) \colon s \in \mathbb{R}\}$.

(b) $R =$ empty set.

(c) $R =$ locus $\{y = 0\}$.

(d) $R = \text{locus}\,\{xy + 1 = 0\}$.

(e) $R = \text{locus}\,\{x^2y - xy^2 - x + y = 0\}$.

(f) $R = \text{locus}\,\{x^2 - xy + 2x - 2y = 0\}$.

Solution.

(a) All three axioms are satisfied, R being the 'discrete' relation where every element is related only to itself.

(b) Symmetry and transitivity are vacuously satisfied, reflexivity is not.

(c) Only transitivity is (trivially) satisfied. Note that $(1,1) \notin R$, $(1,0) \in R$ but $(0,1) \notin R$. Also, every element is only related to 0, which means that the only configuration of xRy and yRz is $xR0$ and $0R0$.

(d) Only symmetry is satisfied. Note that $1 \cdot 1 + 1 = 2 \neq 0$, and both $(1,-1) \in R$ and $(-1,1) \in R$, yet $(1,1) \notin R$.

(e) All three axioms are satisfied. Clearly, $(x,x) \in \mathbb{R}$ for all $x \in R$, whenever $(x,y) \in R$ we have $x^2y - xy^2 = x - y$, hence $y^2x - x^2y = y - x$ so $(y,x) \in R$. Rewrite our condition as $xy(x-y) - (x-y) = 0$ or $(xy-1)(x-y) = 0$. Thus, xRy if $x = y$ or $xy = 1$. Suppose that xRy and yRz. We may have $x = y = z$, or $x = y$ and $yz = 1$ hence $xz = 1$, $xy = 1$ and $y = z$ hence $xz = 1$, or $xy = 1$ and $yz = 1$, whence $x = z$. In all cases, xRz.

(f) Only symmetry is satisfied. Clearly $(x,x) \in R$ for all $x \in \mathbb{R}$. Note that our condition can be written as $x(x-y) + 2(x-y) = 0$, or $(x+2)(x-y) = 0$. This gives xRy whenever $x = -2$ or $x = y$. Thus, $(-2,0) \in R$ but $(0,-2) \notin R$. Now, if xRy and yRz, we may have $x = -2$ and $y = -2$, or $x = -2$ and $y = z$, or $x = y$ and $y = -2$ hence $x = -2$, or $x = y$ and $y = z$ hence $x = z$. In all cases, xRz.

Exercise 9. Describe the smallest equivalence relation on the set of real numbers which contains the line $x - y = 1$ in the (x,y) plane, and sketch it.

Solution. Reflexivity demands that we include the line $x = y$, symmetry demands that we include the line $y - x = 1$. Now, for all $x \in \mathbb{R}$, we have $(x-1,x) \in R$ and $(x,x+1) \in R$, so transitivity demands $(x-1,x+2) \in R$ which is equivalent to saying that $(x,x+2) \in R$ for all $x \in \mathbb{R}$. By repeating this process arbitrarily many times and employing symmetry, we see that $(x,x+n) \in R$ for all $x \in \mathbb{R}$ and $n \in \mathbb{Z}$. This gives

$$R = \text{locus}\,\{x - y = n \colon n \in \mathbb{Z}\}.$$

This consists of all lines with slope 1 which cut the axes at integral points.

Exercise 10. Draw the fibres of the map from the (x,z) plane to the y axis defined by the map $y = zx$.

Solution. Denote the map $f \colon \mathbb{R}^2 \to \mathbb{R}$, $(x,z) \mapsto xz$. Fixing $y \in R$, we see that $f^{-1}(y)$ is the collection of points (x,z) such that $xz = y$, i.e. a rectangular hyperbola.

Exercise 11. Work out rules, obtained from the rules on the integers, for addition and multiplication on the set (5.8).

Solution. The required rules are those of addition and multiplication in the field $\mathbb{Z}_2$. Note that given any two elements $x, y \in \bar{0}$, we have $x + y = \bar{0}$ because the sum of even numbers is even. Similarly, the sum of an even number and an odd number is odd, and the sum of

two odd numbers is even. This ensures that it makes sense to define $\bar{0} + \bar{0} = \bar{1} + \bar{1} = \bar{0}$, and $\bar{0} + \bar{1} = \bar{1} + \bar{0} = \bar{1}$. Similarly, the product of an even number with any other number is even, and the product of two odd numbers is odd. Thus, we can define $\bar{0} \cdot \bar{0} = \bar{0} \cdot \bar{1} = \bar{1} \cdot \bar{0} = \bar{0}$, and $\bar{1} \cdot \bar{1} = \bar{1}$.

Exercise 12. Prove that the cosets (5.14) are the fibres of the map φ.

Solution. Recall that we defined the group homomorphism $\varphi\colon G \to G'$ with kernel N, and described the cosets

$$aN := \{g \in G\colon g = an \text{ for some } n \in N\}.$$

Suppose that $b \in \operatorname{im}\varphi$. This means that $b = \varphi(a)$ for at least one $a \in G$. We claim that the fibre $\varphi^{-1}(b) = aN$. To see this, note that if $x \in \varphi^{-1}(b)$, then $\varphi(x) = b = \varphi(a)$, hence $\varphi(a^{-1}x) = 1$ so $a^{-1}x \in N$. Thus, $x = a(a^{-1}x) \in aN$. Next, pick $x \in aN$, i.e. $x = an$ where $\varphi(n) = 1$. Thus, $\varphi(x) = \varphi(an) = \varphi(a)\varphi(n) = b$, hence $x \in \varphi^{-1}(b)$. Together, we have shown that the coset aN is precisely the fibre of $\varphi(a)$.