

Unless otherwise indicated, the following exercises are from Michael Artin's *Algebra*, second edition. We write products of permutations using the right-to-left convention, and put $s_i = (i \ i + 1)$.

Chapter 1: Matrices

Section 1: The Basic Operations

Exercise 1.13

A square matrix A is *nilpotent* if $A^k = 0$ for some $k > 0$. Prove that if A is nilpotent, then $I + A$ is invertible. Do this by finding the inverse.

Solution

The key intuition is to apply the geometric series formula formally to matrices:

$$(I + A)^{-1} = I - A + A^2 - A^3 + \cdots .$$

In general, the infinite series on the right-hand side need not converge. However, since A is nilpotent, we can choose $k > 0$ such that $A^k = 0$. All powers of degree at least k then vanish, suggesting the finite sum

$$S = I - A + A^2 - A^3 + \cdots + (-1)^{k-1} A^{k-1}.$$

This is a finite geometric sum. Multiplying on either side gives

$$(I + A)S = S(I + A) = I + (-1)^{k-1} A^k = I.$$

Thus $I + A$ is invertible and

$$(I + A)^{-1} = I - A + A^2 - \cdots + (-1)^{k-1} A^{k-1}.$$

Miscellaneous Problems

Exercise M.10

Let A, B be $m \times n$ and $n \times m$ matrices. Prove that $I_m - AB$ is invertible if and only if $I_n - BA$ is invertible.

Solution

Suppose first that $I_m - AB$ is invertible. Using the same intuition as in the previous exercise, its inverse should formally be

$$I_m + AB + (AB)^2 + (AB)^3 + \cdots .$$

Multiplying this series by B on the left and A on the right, still formally, gives

$$BA + (BA)^2 + (BA)^3 + \cdots .$$

Adding I_n gives the formal geometric series for $(I_n - BA)^{-1}$. These series need not converge, but they suggest a formula that we can verify directly.

We first *define* $X = (I_m - AB)^{-1}$ and then consider

$$Y = I_n + BXA.$$

We claim this is the desired inverse of $I_n - BA$. Indeed,

$$\begin{aligned} (I_n - BA)Y &= I_n - BA + BXA - BABXA \\ &= I_n - BA + B(I_m - AB)XA = I_n, \end{aligned}$$

because $(I_m - AB)X = I_m$. Similarly,

$$\begin{aligned} Y(I_n - BA) &= I_n - BA + BXA - BXA BA \\ &= I_n - BA + BX(I_m - AB)A = I_n, \end{aligned}$$

because $X(I_m - AB) = I_m$. Therefore

$$(I_n - BA)^{-1} = I_n + B(I_m - AB)^{-1}A.$$

The converse follows by interchanging A and B (and m and n).

Chapter 2: Groups

Supplementary Problems: Permutations, Cycles, and Length

Exercise P.1

Let $p = [4, 1, 6, 2, 5, 3] \in S_6$.

- (a) Write p as a product of disjoint cycles.
- (b) List all inversions of p .
- (c) Compute $\text{inv}(p)$ and hence determine $\ell(p)$.
- (d) Express p as a product of exactly $\ell(p)$ simple transpositions.

Solution

- (a) Following the images of the entries gives

$$1 \mapsto 4 \mapsto 2 \mapsto 1, \quad 3 \mapsto 6 \mapsto 3, \quad 5 \mapsto 5.$$

Hence $p = (1\ 4\ 2)(3\ 6)$, with the fixed point 5 omitted.

- (b) An inversion is a pair (i, j) with $i < j$ and $p(i) > p(j)$. Reading from the one-line notation, the inversions are

$$(1, 2), (1, 4), (1, 6), (3, 4), (3, 5), (3, 6), (5, 6).$$

(c) There are seven inversions, so

$$\text{inv}(p) = 7 \quad \text{and hence} \quad \ell(p) = 7.$$

(d) Starting with the identity in one-line notation and successively swapping adjacent positions gives

$$\begin{aligned} [1, 2, 3, 4, 5, 6] &\xrightarrow{s_3} [1, 2, 4, 3, 5, 6] \xrightarrow{s_2} [1, 4, 2, 3, 5, 6] \xrightarrow{s_1} [4, 1, 2, 3, 5, 6] \\ &\xrightarrow{s_5} [4, 1, 2, 3, 6, 5] \xrightarrow{s_4} [4, 1, 2, 6, 3, 5] \xrightarrow{s_3} [4, 1, 6, 2, 3, 5] \\ &\xrightarrow{s_5} [4, 1, 6, 2, 5, 3]. \end{aligned}$$

Thus

$$p = s_3 s_2 s_1 s_5 s_4 s_3 s_5.$$

This expression has seven factors, so it is reduced.

Exercise P.2

Let $1 \leq a < b \leq n$, and let $\tau = (a \ b) \in S_n$.

- (a) Write τ in one-line notation.
- (b) Prove that $\text{inv}(\tau) = 2(b - a) - 1$.
- (c) Deduce that $\ell(\tau) = 2(b - a) - 1$.
- (d) Explain why two permutations with the same cycle type need not have the same Coxeter length.

Solution

(a) The transposition fixes every entry except a and b , so its one-line notation is

$$[1, \dots, a-1, b, a+1, \dots, b-1, a, b+1, \dots, n].$$

(b) The inversions involving position a are

$$(a, a+1), (a, a+2), \dots, (a, b),$$

giving $b - a$ inversions. The remaining inversions are

$$(a+1, b), (a+2, b), \dots, (b-1, b),$$

giving $b - a - 1$ more. All other pairs retain their natural order. Therefore

$$\text{inv}(\tau) = (b - a) + (b - a - 1) = 2(b - a) - 1.$$

(c) Since Coxeter length in S_n equals the number of inversions,

$$\ell(\tau) = 2(b - a) - 1.$$

- (d) All transpositions have the same cycle type, namely one 2-cycle and $n - 2$ fixed points, but their lengths depend on the distance between the exchanged positions. For example, when $n \geq 3$,

$$\ell((1\ 2)) = 1, \quad \ell((1\ n)) = 2n - 3.$$

Thus cycle type does not determine Coxeter length.

Section 3: Subgroups of the Additive Group of Integers

Exercise 3.3

- (a) Define the greatest common divisor of $\{a_1, \dots, a_n\}$. Prove that it exists and is an integer combination of the a_i .
- (b) If the greatest common divisor is d , prove that the greatest common divisor of $\{a_1/d, \dots, a_n/d\}$ is 1.

Solution

Assume the a_i are not all zero.

- (a) The greatest common divisor is the unique positive integer d such that

- (i) $d \mid a_i$ for every i , and
- (ii) every common divisor of the a_i divides d .

To prove existence, consider

$$H = \mathbb{Z}a_1 + \dots + \mathbb{Z}a_n = \{r_1a_1 + \dots + r_na_n : r_i \in \mathbb{Z}\}.$$

This is a nonzero subgroup of $\mathbb{Z}$, so $H = d\mathbb{Z}$ for a unique $d > 0$. Since $d \in H$, there are integers $r_1, \dots, r_n$ for which

$$d = r_1a_1 + \dots + r_na_n.$$

Also $a_i \in H = d\mathbb{Z}$, so $\mathbb{Z}a_i \subseteq \mathbb{Z}d$ and hence $d \mid a_i$ for every i . If c is any common divisor of the a_i , then c divides every integer combination of them, and therefore $c \mid d$. Hence this d is the gcd and is an integer combination of the a_i .

- (b) Put $a'_i = a_i/d$. Dividing the displayed Bézout identity by d gives

$$1 = r_1a'_1 + \dots + r_na'_n.$$

Any common divisor of the a'_i must divide the left-hand side, so the only positive common divisor is 1. Thus $\gcd(a_1/d, \dots, a_n/d) = 1$.

Section 4: Cyclic Groups

Exercise 4.3

Let $a, b \in G$. Prove that ab and ba have the same order.

Solution

The elements are conjugate, since

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

For every integer r , conjugation gives

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

Consequently $(ba)^r = 1$ if and only if $(ab)^r = 1$. Thus the least positive such r is the same for both elements; if no such r exists, both have infinite order. Hence ab and ba have the same order.

Exercise 4.7

Let $x, y \in G$. Assume that x , y , and xy each have order 2. Prove that $H = \{1, x, y, xy\}$ is a subgroup of G of order 4.

Solution

Because $x^2 = y^2 = (xy)^2 = 1$, each of x, y, xy is its own inverse. Moreover,

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

so x and y commute. It follows that every product of powers of x and y reduces to one of

$$1, \quad x, \quad y, \quad xy.$$

Thus $H = \langle x, y \rangle$ and is a subgroup. The four displayed elements are distinct: x, y, xy are not 1 because each has order 2; $x = y$ would imply $xy = x^2 = 1$; and $xy = x$ or $xy = y$ would imply respectively $y = 1$ or $x = 1$. Hence $|H| = 4$.

Section 5: Homomorphisms

Exercise 5.3

Let U be the group of invertible upper triangular matrices $A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, and define $\varphi: U \rightarrow \mathbb{R}^\times$ by $\varphi(A) = a^2$. Prove that φ is a homomorphism, and determine its kernel and image.

Solution

For

$$A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}, \quad C = \begin{bmatrix} c & e \\ 0 & f \end{bmatrix} \in U,$$

the upper-left entry of AC is ac . Therefore

$$\varphi(AC) = (ac)^2 = a^2 c^2 = \varphi(A) \varphi(C),$$

so φ is a homomorphism. Since an upper triangular matrix is invertible exactly when $a, d \neq 0$,

$$\ker \varphi = \left\{ \begin{bmatrix} \varepsilon & b \\ 0 & d \end{bmatrix} : \varepsilon \in \{1, -1\}, \quad b \in \mathbb{R}, \quad d \in \mathbb{R}^\times \right\}.$$

Every value a^2 is positive, so $\text{im } \varphi \subseteq \mathbb{R}_{>0}$. Conversely, if $r > 0$, then

$$\varphi\left(\begin{bmatrix} \sqrt{r} & 0 \\ 0 & 1 \end{bmatrix}\right) = r.$$

Hence $\text{im } \varphi = \mathbb{R}_{>0}$.

Exercise 5.6

Determine the center of $\text{GL}_n(\mathbb{R})$.

Solution

Every nonzero scalar matrix commutes with every matrix, so $\{\lambda I_n : \lambda \in \mathbb{R}^\times\}$ lies in the center. Conversely, let $A = (a_{pq})$ be central. For $i \neq j$, the elementary matrix $T_{ij} = I_n + E_{ij}$ is invertible. From $AT_{ij} = T_{ij}A$ we get $AE_{ij} = E_{ij}A$. Entrywise this says

$$a_{pi} \delta_{jq} = \delta_{pi} a_{jq} \quad \text{for all } p, q.$$

Taking $q = j$ and $p \neq i$ gives $a_{pi} = 0$, so column i has no off-diagonal entries. Taking $p = i$ and $q \neq j$ gives $a_{jq} = 0$, so row j has no off-diagonal entries. Finally, taking $(p, q) = (i, j)$ gives $a_{ii} = a_{jj}$. As $i \neq j$ were arbitrary, A is diagonal and all its diagonal entries are equal. Since A is invertible, this common entry is nonzero. Therefore

$$Z(\text{GL}_n(\mathbb{R})) = \{\lambda I_n : \lambda \in \mathbb{R}^\times\}.$$

(For $n = 1$, the same conclusion is immediate.)

Section 6: Isomorphisms

Exercise 6.7

Let $H \leq G$ and let $g \in G$. Prove that $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is a subgroup of G .

Solution

The set is nonempty because $g1g^{-1} = 1$. If $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$ belong to gHg^{-1} , then

$$xy^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1} = g(h_1h_2^{-1})g^{-1}.$$

Since $h_1h_2^{-1} \in H$, we have $xy^{-1} \in gHg^{-1}$. The subgroup test now shows that $gHg^{-1} \leq G$.

Exercise 6.11

Let $a \in G$. Prove that if $\{1, a\}$ is a normal subgroup of G , then a lies in the center of G .

Solution

If $a = 1$, the conclusion is immediate. Otherwise, let $g \in G$. Normality gives

$$gag^{-1} \in \{1, a\}.$$

Conjugation is injective, so $gag^{-1} \neq 1$ because $a \neq 1$. Consequently $gag^{-1} = a$, and hence $ga = ag$. This holds for every $g \in G$, so $a \in Z(G)$.