University of Warwick
Department of Mathematics

MA136

Introduction to Abstract Algebra

Cem Yilmaz

July 14, 2022

Contents

1 Requirements

1.1 Functions

Theorem 1.1. *A function is invertible iff it is a bijection*

Proof. We know that if $f(x_1) = f(x_2)$, then $x_1 = x_2$ in a bijective function, as it is injective. Similarly, from subjectivity, we know that for $y \in Y$ for $f : X \to Y$, there exists $f(x) = y$. As it is an iff statement, we are required that the proof works in both direction. We first begin with the fact that $f : X \to Y$ is bijective $\implies f$ is invertible.
Suppose that f is invertible, i.e., $\exists g : Y \to X$ such that $f \circ g(y) = y \ \forall y \in Y$ and $g \circ f(x) = x \ \forall x \in X$. Suppose two elements $x_1, x_2 \in X$ and let us consider $f(x_1)$ and $f(x_2)$. Apply g where

$$\begin{aligned}
&\implies g(f(x_1)) = g(f(x_2)) \\
&\implies g \circ f(x_1) = g \circ f(x_2) \\
&\implies x_1 = x_2 \text{ f is injective}
\end{aligned}$$

that is, injectivity follows from the definition of invertible. Now, we show surjectivity. Let $y \in Y$. We know

$$\begin{aligned}
f \circ g(y) &= y \\
\implies f(g(y)) &= y
\end{aligned}$$

Since $g(y) \in X$, f is surjective. In other words, since $g(y)$ is $g : Y \to X$, we show that a unique x mapping does exist. Now, we show that bijectivity implies invertibility also.
Suppose f is a bijective. We need to show that we can construct g such that

$$\begin{gathered}
g : Y \to X \\
f \circ g(y) = y \ \forall y \in Y \\
g \circ f(x) = x \ \forall x \in X
\end{gathered}$$

Let $y \in Y$. Since f is injective and surjective, there exists a unique $x \in X$ such that $f(x) = y$. This gives $g : Y \to X$. Let $y \in Y$ and consider $f \circ g(y) = f(g(y))$. By definition of g, it follows that

$$f(g(y)) = y$$

Similarly, we consider $x \in X$ and $g \circ f(x) = g(f(x))$. We obtain $g(f(x)) = x$. □

1.2 Matrices

Let m, n be positive integers. An $m \times n$ matrix (or a matrix of size or order $m \times n$) is a rectangular array consisting of mn numbers arranged in m rows and n columns. The elements are denoted a_{ij} where i is the row and j is the column. The notation for sets of matrices is denoted by $M_{m \times n}(\mathbb{R})$, this is the set of $m \times n$ matrices with entries in $\mathbb{R}$. The addition, subtraction and scalar multiplication is defined in matrices. Whilst addition and subtraction are trivial, the multiplication is to be defined. Let $A = (a_{ij})_{m \times n}$ and $B = (b_{ij})_{n \times p}$, we define the product AB to be the matrix $C = (c_{ij})_{m \times p}$ such that

$$c_{ij} = a_{i1}b_{i1} + a_{i2}b_{2i} + \ldots + a_{in}b_{nj}$$

In other words, multiply the first matrix's row element by corresponding column element. Similarly, we can transform matrices through a function such that

$$T_A \begin{bmatrix} x \\ y \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

for $T_A : \mathbb{R}^2 \to \mathbb{R}^2$. That is, it is something that takes in $\mathbb{R}^2$ and gives back in $\mathbb{R}^2$.Note that these transformations can also be bijective, injective and surjective. For example,

$$\begin{aligned}
T_A \mathbb{R}^2 &\to \mathbb{R}^2 \\
T_A(x, y) &= \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + 2y \\ 3x + 6y \end{bmatrix}
\end{aligned}$$

Note that this is not surjective as for $x = 0$ and $y = 0$ we obtain $(0, 0)$ and similarly for $(-2, 1)$ we also obtain $(0, 0)$. It is also not injective as something such as $(1, 4)$ would not have a solution for x, y as the solutions of this transformation lie on $y = 3x$.

Theorem 1.2. *A matrix $A_{2\times 2}$ is invertible if and only if $ad - bc \neq 0$. Then, the inverse is*

$$A^{-1} = \frac{1}{ad - bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Proof. Let us begin from left to right. We assume A is invertible. This implies the existence of a matrix

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix}$$

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore the matrix

$$\begin{bmatrix} ax + cy & bx + dy \\ az + cw & bz + dw \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Hence $ax + cy = 1$, $bx + dy = 0$, $az + cw = 0$ and $bz + dw = 1$. Solving these equations we obtain

$$\begin{aligned} adx + cdy &= d \\ bcx + dcy &= 0 \text{ from multiplying second equation by } c \\ x(ad - bc) &= d \text{ by substitution} \end{aligned}$$

Then, we obtain the second equation

$$\begin{aligned} bax + bcy &= b \text{ by multiplying first equation by } b \\ abx + ady &= 0 \text{ by multiplying second equation by } a \\ -(ad - bc)y &= b \text{ by substituting both} \end{aligned}$$

Then we can further obtain the equations

$$\begin{aligned} (ad - bc)w &= a \\ -(ad - bc)z &= c \end{aligned}$$

using further algebra. If $ad - bc = 0$, then $a = b = c = d = 0$. This means that A is the zero matrix and $A = \underline{0}$, which is not invertible. Therefore, $ad - bc \neq 0$. Hence

$$\begin{aligned} x &= \frac{d}{ad - bc} \\ y &= \frac{-b}{ad - bc} \\ w &= \frac{a}{ad - bc} \\ z &= \frac{-c}{ad - bc} \\ \begin{bmatrix} x & y \\ z & w \end{bmatrix} &= \frac{1}{ad - bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \end{aligned}$$

Now, RHS to LHS, suppose $ad - bc \neq 0$. Then, let

$$A^{-1} = \frac{1}{ad - bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Then,

$$
\begin{aligned}
A^{-1}A &= \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} \\
&= \frac{1}{ad-bc}\begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\end{aligned}
$$

Similar steps follow for AA^{-1}. Therefore, we have the result in both directions. $\square$

As an exercise, let A be a 2×2 matrix where

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

Let

$$u = \begin{bmatrix} a \\ c \end{bmatrix} \qquad v = \begin{bmatrix} b \\ d \end{bmatrix}$$

Show that $|det(A)|$ is the area of the parallelogram with adjacent sides u and v.
Lastly, we can create a composition of transformations. Suppose two matrices $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ and $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$. This gives rise to two functions $T_A : \mathbb{R}^2 \to \mathbb{R}^2$ and $T_B : \mathbb{R}^2 \to \mathbb{R}^2$. Now,

$$T_B\left(T_A\begin{bmatrix} x \\ y \end{bmatrix}\right) = B\left(A\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}\left(\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}\right)$$

Would be the same as if we start to multiply wherever. In other words, for $(AB)C = A(BC)$ holds true for $A = m \times n$, $B = n \times p$ and $C = p \times q$ matrix. Matrix multiplication is associative.

2 Elements of Abstract Algebra

2.1 Binary operation

Definition 2.1. Binary operation - let S be a set. A binary operation on S is a rule by which any two elements of S can be combined to give another element of S. We are giving to use the symbol $\star$ for binary operation. Given $s_1, s_2 \in S$ we have a further element $s_1 \star s_2 \in S$.

Example 2.1. Example binary operations

Let $S = \mathbb{R}$ and $\star = +$. Then, $x + y \in \mathbb{R}$ indeed, which is an example of a binary operation. However, note that $\mathbb{N}, -$ is not a binary operation as $5 - 7 = -2$ and $-2 \notin \mathbb{N}$.

We can also denote the set of all polynomials using the notation

$$
\begin{gathered}
\mathbb{R}[x] \\
\mathbb{C}[x] \\
\mathbb{Q}[x] \\
\mathbb{Z}[x]
\end{gathered}
$$

These would denote the set of all polynomials whose coefficients follow the set in the notation. Note that addition and subtraction on polynomials is a binary operation.
Note that composition of functions is not a binary operation. For example, $f : A \to B$ and $g : B \to C$ then $g \circ f : A \to C$ is not a binary operation due to difference in set mappings.

2.2 Commutativity

Definition 2.2. Let S be a set and $\star$ a binary operation. We say that the binary operation $\star$ is commutative on S if

$$a \star b = b \star a$$

for all $a, b \in S$

Example 2.2. Examples of commutativity

For example, $\mathbb{R}, +$ is commutative

2.3 Associativity

Definition 2.3. We say that a binary operation $\star$ is associative on S if

$$(a \star b) \star c = a \star (b \star c)$$

for all $a, b, c \in S$. I.e., bracketing doesn't matter as long as we keep the same order and this is called the general associativity theorem.

Example 2.3. Examples of associativity

For example, $\mathbb{R}, +$ is also associative

2.4 Groups

Definition 2.4. A group is a pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G, such that the following four properties hold:

1. closure - $\forall a, b \in G$, $a \star b \in G$.
2. associativity - $\forall a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$
3. existence of identity element - $\exists e. \forall a \in G, a \star e = e \star a = a$
4. existence of inverse - $\forall a \in G, \exists b \in G. a \star b = b \star a = e$

Definition 2.5. A group is called Abelian if it is a group and follows

1. commutative - $\forall a, b \in G, a \star b = b \star a$

Example 2.4. Example of Groups

Some example groups are:

1. $(\mathbb{R}, +)$

We can also form groups of the same binary operation by picking only specific elements. I.e.,

Definition 2.6. A subgroup is a group with the same binary operation $\star$ but it uses the specific set X where $X \subseteq G$.

We get something of the kind

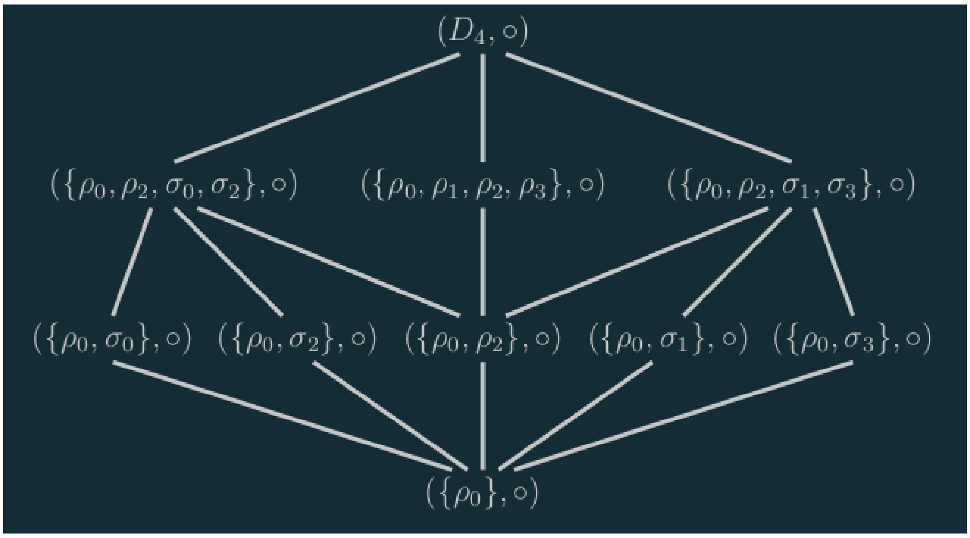

Figure 1: Subgroup

Furthermore,

Theorem 2.1. *Uniqueness of the identity element. Let $(G, \star)$ be a group. Then $(G, \star)$ has a unique identity element.*

Proof. Let $a \in G$. Suppose $b, b' \in G$ which are both inverses to a. Then,

$$\begin{aligned} b \star a = a \star b = e \\ b' \star a = a \star b' = e \\ b = b \star e = b \star (a \star b') \\ b = (b \star a) \star b' = b = e \star b' \\ b = b' \end{aligned}$$

□

Theorem 2.2. *Inverse of an inverse. Let G be a group and $a \in G$. Then*

$$(a^{-1})^{-1} = a$$

Proof. Let $a \in G$. Need to show a is the inverse of a^{-1}. This means that $a^{-1}a = aa^{-1} = e$. Hence

$$(a^{-1})^{-1}$$

□

Theorem 2.3. *Inverse of a product. Let G be a group and $a, b \in G$. Then,*

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

Proof. $b^{-1}a^{-1}$ is the inverse of ab.

$$\begin{aligned} (ab)(b^{-1}a^{-1}) & abb^{-1}a^{-1} \\ & = a1a^{-1} \\ & = aa^{-1} \\ & = 1 \end{aligned}$$

□

Theorem 2.4. *Properties of power notation. Let G be a group and let $a \in G$. Then*

1. *$a^n \in G$ for all $n \in \mathbb{Z}$.*

2. *If $n \in \mathbb{Z}$ then $(a^{-1})^n = (a^n)^{-1} = a^{-n}$*

3. *Moreover, if m, n are integers then $(a^m)^n = a^{mn}$ and $a^m a^n = a^{m+n}$*

4. *Further, if the group G is abelian, $a, b \in G$ and n is an integer then $(ab)^n = a^n b^n$*

Proof for 1

Proof. $a^0 = 1$, true for $n = 0$. Suppose $n > 0$, $n \in \mathbb{Z}$. For $n = 1$, $a^n = a$ and indeed $a \in G$. Assume true if $n = k$, $k > 0$, $k \in \mathbb{Z}$. Consider

$$a^{k+1} = a^k a$$

Certainly $a^k a \in G$ as $a \in G$ and $a^k \in G$ by assumption. Suppose $n < 0$, $n \in \mathbb{Z}$. We know

$$a^n = (a^{-n})^{-1}$$

As $-n > 0$ by earlier, we know $a^{-n} \in G \implies (a^{-n})^{-1} \in G$. □

Proof for 2

Proof. If $n = 0$, $(a^{-1})^0 = (a^0)^{-1} = a^{-0}$ Indeed, all of these are equal to the identity e. If $n > 0$, $n \in \mathbb{Z}$, we consider $a^n(a^{-1})^n$:

$$\begin{aligned} a^n(a^{-1})^n &= \underbrace{aa\ldots a}_{n}\underbrace{a^{-1}a^{-1}\ldots a^{-1}}_{n} \\ a^n(a^{-1})^n &= \underbrace{11\ldots 1}_{n} \\ a^{-n} &= (a^n)^{-1} \end{aligned}$$

Suppose $n < 0$ and $n \in \mathbb{Z}$. Suppose $a^n(a^{-1})^n$:

$$\begin{aligned} a^n(a^{-1})^n &= (a^{-n})^{-1}\left((a^{-1})^{-n}\right)^{-1} \\ &= (a^{-1})^{-n}\left((a^{-1})^{-1}\right)^{-n} \\ &= (a^{-1})^{-n}a^{-n} \\ &= \underbrace{aa\ldots a}_{n}\underbrace{a^{-1}a^{-1}\ldots a^{-1}}_{n} \end{aligned}$$

□

Proof for 3