Advanced Algebra.

MA180-4.

Prof. Götz Pfeiffer

School of Mathematics, Statistics and Applied Mathematics
University of Galway

Semester 2 (2022/2023)

Outline

1. The Language of Mathematics: Logic and Sets.
   - Propositional Logic.
   - Valid Arguments.
   - Sets and Boolean Algebra.
   - Functions and Relations.
2. Examples of Algebraic Objects: Permutations and Polynomials.
   - Composition of Functions.
   - Permutations.
   - Polynomials.
   - Factorisation of Polynomials.
3. Mathematical Tools: Induction and Probability.
   - Mathematical Induction.
   - Probabilities and Sample Spaces
   - Some Probability Rules
   - Binomial Probability Distribution

References.


Norman L. Biggs.
Discrete Mathematics.
Oxford UP 2003.


Lindsay Childs.
A Concrete Introduction to Higher Algebra.
Springer 2000.


Douglas E. Ensley and J.Winston Crawley
Discrete Mathematics.
Wiley 2006.


Mark V. Lawson
Algebra & Geometry: An Introduction to University Mathematics
Taylor & Francis 2016

Introduction: Permutations and Polynomials.

- Certain **types of functions** occur frequently in **applications** and form examples of important **algebraic structures**.
- **Permutations** of a set correspond to **rearrangements** of its elements.
- In Computer Science, permutations are used in the study of **sorting** algorithms.
- The **product** of two permutations is a **composition** of functions.
- **Polynomials** are linear combinations of powers of an **indeterminate** x.
- Solving **polynomial equations** is a central problem in algebra.
- **Addition**, **multiplication** and **division** of polynomials share many properties with the corresponding operations on the **integers**.

Links: Permutations and Polynomials.

- http://en.wikipedia.org/wiki/Fifteen_puzzle
- http://en.wikipedia.org/wiki/Rubik's_Cube
- http://en.wikipedia.org/wiki/Function_composition
- http://en.wikipedia.org/wiki/Permutation
- http://en.wikipedia.org/wiki/Symmetric_group
- http://en.wikipedia.org/wiki/Cyclic_permutation
- http://en.wikipedia.org/wiki/Group_(mathematics)
- http://en.wikipedia.org/wiki/Ring_(mathematics)
- http://en.wikipedia.org/wiki/Field_(mathematics)
- http://en.wikipedia.org/wiki/Polynomial
- http://en.wikipedia.org/wiki/Polynomial_long_division
- http://en.wikipedia.org/wiki/Irreducible_polynomial
- http://mathworld.wolfram.com/IrreduciblePolynomial.html
- http://en.wikipedia.org/wiki/Fundamental_theorem_of_algebra
- http://www-history.mcs.st-andrews.ac.uk/Biographies/Gauss.html is a biography of the German mathematician **Carl Friedrich Gauss** (1777–1855).

Composition of Functions.

- The **composition** of relations $R \subseteq X \times Y$ and $S \subseteq Y \times Z$ is the relation $S \circ R$ from X to Z defined by $x(S \circ R)z$ if xRy and ySz for some $y \in Y$.
- The **composition** of functions $f\colon X \to Y$ and $g\colon Y \to Z$ is the function $g \circ f\colon X \to Z$ defined by $(g \circ f)(x) = g(f(x))$ for $x \in X$.

Theorem

*Composition of functions is **associative**:*
$(f \circ g) \circ h = f \circ (g \circ h)$.

Proof.

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$
$$= f((g \circ h)(x)) = (f \circ (g \circ h))(x). \qquad \square$$

- The composition of functions $f\colon X \to X$ and $g\colon X \to X$ is a function $g \circ f$ from the set X to itself.

Bijections and Inverse functions.

Example

Let X be a set. The **identity function** $\mathrm{id}_X : X \to X$, defined by $\mathrm{id}_X(x) = x$ for all $x \in X$, is a bijection.

- If $f : X \to Y$ is a bijection there is a function $g : Y \to X$ defined by $g(y) = x$ if $f(x) = y$ (i.e., g maps $y \in Y$ to the unique $x \in X$ that f maps to y.)
- The function g is bijective as well and has the property that $g \circ f = \mathrm{id}_X$ (i.e., $g(f(x)) = x$ for all $x \in X$) and $f \circ g = \mathrm{id}_Y$ (i.e. $f(g(y)) = y$ for all $y \in Y$).
- This function g is **uniquely determined** by f and called the **inverse** of f.

Theorem

*A function has an **inverse** if and only if it is a **bijection**.*

Permutations.

- A **permutation** of a set X is a **bijection** from X to **itself**.
- Frequently, $X = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$.

Example ($X = \{1, 2, 3, 4, 5, 6\}$.)

The **relation** $\pi = \{(1,2), (2,5), (3,3), (4,6), (5,1), (6,4)\}$ on X is a **bijection**, which is written in **two-line-notation** as the **permutation** $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 6 & 1 & 4 \end{pmatrix}$.

- There are $n! = 1 \cdot 2 \cdots n$ permutations of X if $|X| = n$.
- The set S_n of all permutations of $X = \{1, 2, \ldots, n\}$ is called the **symmetric group** of degree n.

Example ($n = 3$.)

$S_3 = \{\binom{123}{123}, \binom{123}{213}, \binom{123}{321}, \binom{123}{132}, \binom{123}{231}, \binom{123}{312}\}$. $|S_3| = 3! = 6$.

Products of Permutations.

- The **product** $\sigma \circ \pi$ of $\pi, \sigma \in S_n$, defined by $(\sigma \circ \pi)(x) = \sigma(\pi(x))$, for $x \in X$, is a permutation.
- The **inverse** of $\pi = \binom{1 \cdots n}{\pi(1) \cdots \pi(n)}$ is the permutation $\pi^{-1} = \binom{\pi(1) \cdots \pi(n)}{1 \cdots n}$, since $\pi^{-1} \circ \pi = \mathrm{id}_X$.
- An m**-cycle** $(x_1, x_2, \ldots, x_m)$ permutes the m points $x_1, x_2, \ldots, x_m \in X$ cyclically.
- Each permutation is a product of **disjoint cycles**.

Example

$\pi = \binom{1\,2\,3\,4\,5\,6}{2\,5\,3\,6\,1\,4} = (1,2,5)(3)(4,6) = (1,2,5)(4,6)$.

- The **order** of a permutation π is the smallest $k \in \mathbb{N}$ such that $\pi^k = \pi \circ \pi \circ \cdots \circ \pi = \mathrm{id}_X$.
- An m-cycle has order m.
- The order of $\pi \in S_n$ is the lcm of its cycle lengths.

Write a Permutation as Disjoint Cycles.

Algorithm: Disjoint Cycles.

0. Consider all points $x \in \{1, 2, \ldots, n\}$ as "**unmarked**".
1. If all points are marked: STOP
   Otherwise, let x be the **smallest unmarked point**.
2. Determine its **cycle**

$$(x, \pi(x), \pi^2(x), \ldots)$$

   and mark all the points in the cycle.
3. **Go back** to step 1.

- Here $\pi^2 = \pi \circ \pi$, $\pi^k = \pi \circ \pi^{k-1}$.
- Given $\pi \in S_n$, what is the smallest $k \in \mathbb{N}$, such that $\pi^k = \mathrm{id}_X$?
- This k is called the **order** of π.

Products of Transpositions.

Examples

$(1,2)^{-1} = (1,2)$ and $(1,2)(2,3) = (1,2,3)$.

- A 2-cycle is called a **transposition**.
- Each n-cycle is a product of transpositions: $(x_1, x_2, \ldots, x_n) = (x_1, x_2)(x_2, x_3) \cdots (x_{n-1}, x_n)$.

Theorem (Librarian's Nightmare.)

Each permutation $\pi \in S_n$ is a product of transpositions

- $\pi \in S_n$ is called **even** (resp. **odd**) if it is a product of an even (resp. odd) number of transpositions.

Fact.

A permutation $\pi \in S_n$ is either even or odd, **but not both**.

Groups.

- The symmetric group S_n is an example of a **group**.
- In general, a group is defined by **axioms**.

Definition

A **group** is a set G, together with a **binary operation** $\star\colon G \times G \to G$ such that:

(G1) **Associative:** $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$.

(G2) **Identity:** There exists an element $e \in G$ such that $a \star e = a$ and $e \star a = a$ for all $a \in G$.

(G3) **Inverse:** For each $a \in G$ there exists an element $a' \in G$ such that $a \star a' = e$ and $a' \star a = e$.

Examples

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n^*, \cdot)$, $(\{\pm 1\}, \cdot)$, ...
- The set of invertible 2×2-matrices over $\mathbb{Q}$.
- $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$, $(P(S), \cup)$, $(P(S), \cap)$ are **not groups**.

Rings.

- A group $(G, \star)$ is **abelian** (or **commutative**) if $a \star b = b \star a$ for all $a, b \in G$.

Definition

A **ring** is a set R together with binary operations $+$ **and** $\star\colon R \times R \to R$ such that $(R, +)$ is an abelian group and:

(R1) $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in R$.

(R2) There exists an element $e \in R$ such that $a \star e = a$ and $e \star a = a$ for all $a \in R$.

(R3) $a \star (b + c) = a \star b + a \star c$ and $(a + b) \star c = a \star c + b \star c$ for all $a, b, c \in R$.

- A ring $(R, +, \star)$ is called **commutative** if $a \star b = b \star a$ for all $a, b \in R$.

Examples

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_m$, ..., the set of **all** 2×2-matrices over $\mathbb{Q}$.

Polynomials are like Numbers.

Definition

Suppose R is a commutative ring. A **polynomial** over R is an expression of the form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

$$= a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n = \sum_{i=0}^{n} a_i x^i.$$

for some integer $n \geqslant 0$, with **coefficients** $a_0, a_1, \ldots, a_n \in R$ (e.g. $R = \mathbb{R}$ or $R = \mathbb{Z}_m$)

- Two polynomials are **equal** if they have the **same coefficent** at every power of x.
- A polynomial $p(x)$ defines a **polynomial function** $R \to R$ by the rule $a \mapsto p(a)$.

Distinct polynomials can define the same function.

Rings of Polynomials.

- The set of all polynomials over R is denoted by $R[x]$.
- Polynomials can be **added**:

$$\left(\sum a_i x^i\right) + \left(\sum b_i x^i\right) = \sum (a_i + b_i) x^i.$$

- Polynomials can be **multiplied**:

$$\begin{aligned}\left(\sum a_i x^i\right)\left(\sum b_i x^i\right) &= \sum_j \sum_k a_j b_k x^{j+k} \\ &= \sum_i \left(\sum_{j+k=i} a_j b_k\right) x^i.\end{aligned}$$

- $R[x]$ is a **commutative ring**.

Quotients and Roots of Polynomials.

- Suppose that F is a **field**, i.e., a commutative ring F, where each $a \in F \setminus \{0\}$ has an inverse.

Examples

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields, $\mathbb{Z}$ is not. $\mathbb{Z}_m$ is a field if m is a prime.

Theorem (Division Theorem)

*Let $f, g \in F[x]$ be polynomials with $g \neq 0$. Then there exist unique polynomials $q \in F[x]$ (the **quotient**) and $r \in F[x]$ (the **remainder**) with $\deg r < \deg g$ such that $f = gq + r$.*

Theorem (Remainder Theorem)

For any polynomial $f(x) \in F[x]$ and $a \in F$, the value $f(a)$ is the remainder of $f(x)$ upon division by $x - a$.

Theorem (Root Theorem)

*The number $a \in F$ is a **root** of $f(x) \in F[x]$ if and only if the polynomial $x - a$ is a **factor** of $f(x)$.*

Greatest Common Divisors.

- **Euclid's Algorithm** can be used to compute the **gcd** of two polynomials f and g.

Example ($f = x^5 + 1$, $g = x^2 + 1$; $F = \mathbb{Z}_3 = \{0, 1, 2\}$)

- $x^5 + 1 = (x^2 + 1)(x^3 + 2x) + (x + 1)$.
- $x^2 + 1 = (x + 1)(x + 2) + 2$.
- $\gcd(f, g) = 2 = 2 \cdot 1$.

- **Note:** The gcd is determined only up to units in F.

Example ($f = x^3 + 2x^2 + 2$, $g = x^2 + 2x + 1$ over $\mathbb{Z}_3$)

- $x^3 + 2x^2 + 2 = (x^2 + 2x + 1)x + (2x + 2)$.
- $x^2 + 2x + 1 = (2x + 2)(2x + 2) + 0$.
- $\gcd(f, g) = 2x + 2 = 2 \cdot (x + 1)$.

- $\gcd(f, g)$ can be computed without factoring f or g.

Irreducible Polynomials.

- Recall that, if $f \in F[x]$ then $\deg f \leqslant 0$ if and only if f is a constant polynomial, i.e. $f \in F$.
- A polynomial $p \in F[x]$ is **irreducible** if $\deg p > 0$ and if $p = fg$ for polynomials $f, g \in F[x]$ implies that either $\deg f = 0$ or $\deg g = 0$.
- Any nonzero polynomial $f \in F[x]$ is either irreducible or it is a **product** of **irreducible polynomials**.

Theorem

Let $f \in F[x]$. If $f = p_1 p_2 \cdots p_s$ and $f = q_1 q_2 \cdots q_t$ are two factorizations of f into a product of irreducible polynomials, then $s = t$, and up to rearranging the factors, $q_i = \alpha_i p_i$ for some $\alpha_i \in F$, $i = 1, \ldots, s$.

- Thus the factorization of a polynomial f into a product of irreducible polynomials is essentially **unique**.

Examples of Irreducible Polynomials.

- $f(x) = x - r \in F[x]$ for any $r \in F$ is irreducible.
- $f(x) = x^2 + bx + c \in \mathbb{R}[x]$ is irreducible if $b^2 - 4c < 0$.

Theorem (Fundamental Theorem of Algebra)

If $f(x) \in \mathbb{C}[x]$ is a polynomial of degree $n > 0$ then $f(x)$ has a root in $\mathbb{C}$.

- Consequently, no polynomial $f \in \mathbb{C}[x]$ with $\deg f > 1$ is irreducible.
- No polynomial $f \in \mathbb{R}[x]$ with $\deg f > 2$ is irreducible.

Proof.

Suppose $\deg f > 2$. By the Fundamental Theorem, $f(x)$ has a complex root $\alpha \in \mathbb{C}$. Note that $\overline{f(x)} = f(\overline{x})$. $f(\alpha) = 0$ implies $f(\overline{\alpha}) = \overline{f(\alpha)} = \overline{0} = 0$. Hence both $(x - \alpha)$ and $(x - \overline{\alpha})$ are factors of $f(x)$. Suppose $\alpha = a + b\,i$. Then $(x - \alpha)(x - \overline{\alpha}) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$ is an irreducible factor of $f(x)$. □

Summary: Permutations and Polynomials.

- **Composition** of functions is **associative**.
- A **permutation** is a bijection from a set to itself.
- A permutation is a product of **disjoint cycles**.
- The cycle lengths determine the **order** of a permutation.
- A permutation has **sign** $(-1)^{\ell}$ if it is a product of ℓ **transpositions**.
- The permutations of the set $\{1, \ldots, n\}$ form the **symmetric group** S_n with **composition** as product.
- The **polynomials** over a **commutative ring** R form a **commutative ring** $R[x]$.
- **Quotients** and **remainders** of polynomials are computed by **long division**.
- A polynomial over a **field** is a product of **irreducible** polynomials in an essentially **unique** way.
- Every irreducible polynomial $f \in \mathbb{C}[x]$ has degree 1.
- An irreducible polynomial $f \in \mathbb{R}[x]$ has $\deg f \leqslant 2$.