MTH4104 Introduction to Algebra

Alex Fink

Semester B, 2021

Cartesian product

Definition (1.1)

Let X and Y be any two sets.

We define their **Cartesian product** $X \times Y$ to be the set of all ordered pairs (x, y), with $x \in X$ and $y \in Y$;
that is, all ordered pairs which can be made using an element of X as first coordinate and an element of Y as second coordinate.

We write this as follows:

$$X \times Y = \{(x, y) : x \in X, y \in Y\}.$$

Cardinality of Cartesian product

Proposition (1.2)

Let X and Y be sets with $|X| = p$ and $|Y| = q$. Then

1. $|X \times Y| = pq$;
2. $|X^n| = p^n$.

Relations, formally

Definition (1.3)

A **relation** R on a set X is a subset of the Cartesian product $X^2 = X \times X$.
That is, it is a set of ordered pairs of elements of X.

Properties of relations

Definition (1.4)

Let R be a relation on a set X. We say that R is

reflexive if $(x, x) \in R$ for all $x \in X$;

symmetric if $(x, y) \in R$ implies that $(y, x) \in R$;

transitive if $(x, y) \in R$ and $(y, z) \in R$ together imply that $(x, z) \in R$.

An **equivalence relation** is a relation which is reflexive, symmetric, and transitive.

2016 exam, question 5

a. Give complete definitions of the terms
   a.1 **Cartesian product** of two sets;
   a.2 **relation** on a set;
   a.3 **equivalence relation** on a set.

b. Write down examples of:
   b.1 a relation which is transitive but not reflexive;
   b.2 an equivalence relation on $\{1, 2, 3, 4\}$ with exactly three equivalence classes.

c. Let X and Z be any two sets, and $f : X \to Z$ any function. Prove that

$$\{(x, y) \in X^2 : f(x) = f(y)\}$$

is an equivalence relation on X.

Partitions

Definition (1.5)

Let X be a set. A **partition** of X is a set P of subsets of X, whose elements are called its **parts**, having the following properties:

a. $\emptyset$ is not a part of P;
b. if A and B are distinct parts of P, then $A \cap B = \emptyset$;
c. The union of all parts of P is X.

Equivalence classes

Definition (1.6)

If R is an equivalence relation on the set X, then the sets

$$[x]_R = \{y \in X : (x, y) \in R\}$$

are called the **equivalence classes** of R.

The Equivalence Relation Theorem

Theorem (1.7)

a. *Let R be an equivalence relation on X. Then the sets $[x]_R$, for $x \in X$, form a partition of X.*
b. *Conversely, given any partition P of X, there is a unique equivalence relation R on X such that the parts of P are the same as the sets $[x]_R$ for $x \in X$, namely*

The Equivalence Relation Theorem

Theorem (1.7)

a. *Let R be an equivalence relation on X. Then the sets $[x]_R$, for $x \in X$, form a partition of X.*

b. *Conversely, given any partition P of X, there is a unique equivalence relation R on X such that the parts of P are the same as the sets $[x]_R$ for $x \in X$, namely*

$$R = \{(x, y) : x \text{ and } y \text{ lie in the same part of } P\}.$$

Which equivalence classes are equal?

Corollary (1.8)

Let R be an equivalence relation on a set X, and $x, y \in X$. Then $[x]_R = [y]_R$ if and only if xRy.

The division rule

Proposition (2.1)

Let a and b be integers, and assume that $b > 0$. Then there exist integers q and r such that

1. $a = bq + r$;
2. $0 \leq r < b$.

Moreover, q and r are unique.

The relation “divides”

Definition (2.2)

Let a and b be integers. Then a **divides** b if and only if there exists an integer c such that $b = ac$. The notation for “a divides b” is $a \mid b$.

2018 exam, question 2

a. Define what it means for $P = \{A_1, A_2, \ldots\}$ to be a **partition** of a set X.

b. Let $\mathcal{A}$ be a partition of X. Prove that

$$R = \{\, (x, y) \in X : \text{there exists } i \text{ such that } x \in A_i \text{ and } y \in A_i \,\}$$

is an equivalence relation on X.

c. Write down a partition of $\mathbb{Z}$ into three parts, exactly two of which are infinite.

Congruence modulo m

Definition (2.3)

We define a relation $\equiv_m$ on $\mathbb{Z}$, called **congruence mod** m, where m is a positive integer, as follows:

$$a \equiv_m b \text{ if and only if } b - a \text{ is a multiple of } m.$$

We read $a \equiv_m b$ are "a is congruent to b mod(ulo) m".

Some people write the relation $a \equiv_m b$ as $a \equiv b \pmod{m}$.

Congruence classes

Proposition (2.4)

The equivalence relation $\equiv_m$ *has exactly* m *equivalence classes, namely* $[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m$.

We call these **congruence classes** mod m.

Arithmetic with congruence classes

Definition (2.5)

We define addition, subtraction, and multiplication of congruence classes as follows:

$$\begin{aligned} [a]_m + [b]_m &:= [a+b]_m, \\ [a]_m - [b]_m &:= [a-b]_m, \\ [a]_m \cdot [b]_m &:= [a \cdot b]_m. \end{aligned}$$

Tables for $\mathbb{Z}_4$

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

$\cdot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

2018 exam, question 3

1. Define the divisibility relation $|$ on the set of natural numbers.
2. A relation R on a set X is said to be **antisymmetric** if the following condition holds:

   For all elements $a, b \in X$, if $a \mathrel{R} b$ and $b \mathrel{R} a$ both hold then $a = b$.

   Prove that $|$ is antisymmetric.
3. Define the **least common multiple** of two nonzero natural numbers.
4. Compute the least common multiple of $336 = 2^4 \cdot 3 \cdot 7$ and $180 = 2^2 \cdot 3^2 \cdot 5$. Include an explanation of your method.

Greatest common divisor

Definition (2.6)

Let a and b be nonnegative integers, not both zero.

A **common divisor** of a and b is a nonnegative integer d with the property that $d \mid a$ and $d \mid b$.

We call d the **greatest common divisor** if it is a common divisor, and if any other common divisor of a and b is smaller than d.

Least common multiple

Definition (2.7)

The positive integer m is a **common multiple** of a and b if both $a \mid m$ and $b \mid m$. It is the **least common multiple** if it is a common multiple which is smaller than any other common multiple.

Euclid's Algorithm

Algorithm

Input: Non-negative integers a, b.

Output: $\gcd(a, b)$.

Steps:

1. Put $b_0 = a$ and $b_1 = b$.
2. As long as the last number b_n found is non-zero, put $b_{n+1} = b_{n-1} \bmod b_n$.
3. When the last number b_n is zero, then the gcd is b_{n-1}.

Euclid's Algorithm extended

Theorem (2.9)

Let a and b be nonnegative integers, and $d = \gcd(a, b)$. Then there are integers x and y such that $d = xa + yb$. Moreover, x and y can be found from Euclid's algorithm.

What's going on in one step of Euclid's algorithm

Proposition (2.8)

$$\gcd(a, b) = \begin{cases} a & \text{if } b = 0, \\ \gcd(b, a \bmod b) & \text{if } b > 0. \end{cases}$$

Multiplicative inverses in $\mathbb{Z}_m$

Theorem (2.10)

The element $[a]_m$ of $\mathbb{Z}_m$ has a multiplicative inverse if and only if $\gcd(a, m) = 1$.

Multiplicative inverses in $\mathbb{Z}_m$

Theorem (2.10)

The element $[a]_m$ of $\mathbb{Z}_m$ has a multiplicative inverse if and only if $\gcd(a, m) = 1$.

Theorem (2.11)

Suppose that $m > 1$. The element $[a]_m$ of $\mathbb{Z}_m$ has no multiplicative inverse if and only if then there exists $b \not\equiv_m 0$ such that $[a]_m[b]_m = [0]_m$.

2019 resit exam, question 4

a. Write down the **multiplicative inverse law.** Pay attention to the quantifiers ("for all", "there exists") and other conditions in the law.

b. Use the Euclidean algorithm to show that $\gcd(45, 59) = 1$.

c. Carrying on from part (b), use the extended Euclidean algorithm to compute the multiplicative inverse of $[45]_{59}$ in $\mathbb{Z}_{59}$.

d. Find all solutions $x \in \mathbb{Z}_{31}$ to the equation

$$[16]_{31}\, x + [26]_{31} = [2]_{31}\, x + [3]_{31}\,.$$

Show your working. You are given that $[14]_{31}^{-1} = [20]_{31}$.

Operations

Definition (3.1)

A (binary) **operation** on a set X is a function whose domain is $X \times X$ and whose codomain is X.

Rings and fields

Definition (3.2)

A **ring** is a set R that comes with two operations on R, **addition** (written $+$) and **multiplication** (written $\cdot$), which satisfies the following **axioms**: [. . .]

Definition (3.3)

A **field** is defined to be a ring satisfying the following additional axioms: [. . .]

[See the next slide for the axioms.]

Ring axioms: black. Field axioms: black and blue.

	Additive	Multiplicative
Closure	$\forall a, b \in R$: $a + b \in R$	$\forall a, b \in R$: $ab \in R$
Associative	$\forall a, b, c \in R$: $a + (b + c) = (a + b) + c$	$\forall a, b, c \in R$: $a(bc) = (ab)c$
Identity	$\exists 0 \in R$: $\forall a \in R$: $a + 0 = 0 + a = a$	$\exists 1 \in R$: $\forall a \in R$: $a1 = 1a = a$
Inverse	$\forall a \in R$: $\exists b \in R$: $a + b = b + a = 0$ (notation: $b = -a$)	$\forall a \in R \setminus \{0\}$: $\exists b \in R$: $ab = ba = 1$ (notation: $b = a^{-1}$)
Commutative	$\forall a, b \in R$: $a + b = b + a$	$\forall a, b \in R$: $ab = ba$
Distributive	**left**: $\forall a, b, c \in R$: $a(b + c) = ab + ac$ **right**: $\forall a, b, c \in R$: $(b + c)a = ba + ca$	
Nontrivial	$1 \neq 0$	

Special kinds of rings

Definitions

Let R be a ring.

- R is a **ring with identity** if it satisfies the multiplicative identity law.
- R is a **skewfield** if it is a ring with identity and also satisfies the multiplicative inverse and nontriviality laws.
- R is a **commutative ring** if it satisfies the multiplicative commutative law.

Define addition and multiplication operations on the set $U = \mathbb{R}^2$ by

$$(a, b) + (c, d) = (a + c,\ b + d),$$
$$(a, b) \cdot (c, d) = (ac,\ ad + bc).$$

a. Name the multiplicative identity element in U, and prove the multiplicative identity law.
b. Prove that, if $a \neq 0$, then (a, b) has a multiplicative inverse in U.

Uniqueness of identities and inverses

Proposition (3.10)

In a ring R,

a. *there is a unique zero element;*
b. *any element has a unique additive inverse.*

Uniqueness of identities and inverses

Proposition (3.10)

In a ring R,

a. *there is a unique zero element;*
b. *any element has a unique additive inverse.*

Proposition (3.11)

Let R be a ring.

a. *If R has a multiplicative identity, then this identity is unique.*
b. *If $a \in R$ has a multiplicative inverse, then this inverse is unique.*

The cancellation property

Proposition (3.12)

Let R be a ring and $a, b, c \in R$. If $a + b = a + c$, then $b = c$.

The cancellation property

Proposition (3.12)

Let R be a ring and $a, b, c \in R$. If $a + b = a + c$, then $b = c$.

Proposition

Let R be a skewfield and $a, b, c \in R$ with $a \neq 0$. If $ab = ac$, then $b = c$.

Multiplying by zero

Proposition (3.13)

Let R be a ring. For any element $a \in R$, we have $0a = a0 = 0$.

Associativity with more than three elements

Proposition (3.14)

Let $\diamond$ be an operation on a set X which satisfies the associative law. Then the value of the expression

$$a_1 \diamond a_2 \diamond \cdots \diamond a_n$$

is the same, whatever (legal) way $n - 2$ pairs of brackets are inserted.

2017 exam, question 5

a. Let R be a ring. Define what it means for R to be
   a.1 a **commutative ring**;
   a.2 a **skewfield**.

   Give the full statement of any axioms you invoke.

b. Let R be a ring. Prove from the axioms that $a \cdot 0 = 0$ for any $a \in R$.

c. Let R be a ring, and $a \in R$ an element such that $a^2 = 0$. Must it be true that $a = 0$? Justify your answer.

Polynomials

Definition (4.1)

Let R be a ring. Let x be a variable.
A **polynomial in x with coefficients in R** is an expression

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

where $a_0, a_1, \ldots, a_{n-1}, a_n$ are elements of R. They are the **coefficients** of f.
The set of all such polynomials will be denoted by $R[x]$.

Degree

Definition (4.2)

The **degree** of a nonzero polynomial is the largest integer n for which its coefficient of x^n is non-zero.

Names for polynomials of low degree:

deg 0	deg 1	deg 2	deg 3	deg 4	deg 5	deg 6
constant	**linear**	**quadratic**	**cubic**	**quartic**	**quintic**	**sextic**

Properties of polynomial rings

Theorem (4.3)

If R is a ring, then so is $R[x]$.
If R is a ring with identity, then so is $R[x]$.
If R is commutative, then so is $R[x]$.

Properties of polynomial rings

Theorem (4.3)

If R is a ring, then so is $R[x]$.
If R is a ring with identity, then so is $R[x]$.
If R is commutative, then so is $R[x]$.

Proposition (4.4)

If R is a ring, then $R[x]$ is not a skewfield.

a. Let R be a ring. Give the definition of a **polynomial in x with coefficients in R**.

b. Define the **degree** of a polynomial.

c. Let $f(x)$ and $g(x)$ be nonzero polynomials in $\mathbb{R}[x]$, of degrees m and n, respectively. Prove that $\deg(f(x)\,g(x)) = m + n$.

d. Give a counterexample to the multiplicative inverse law for the ring $\mathbb{R}[x]$ of polynomials in x with real coefficients. Explain why your counterexample works.

Polynomial division when the divisor is linear

Proposition (4.6)

Let K be a field. Let $f \in K[x]$ and $\alpha \in K$. Then there exist $q \in K[x]$ and $r \in K$ such that

$$f = (x - \alpha) \cdot q + r.$$

Polynomial division when the divisor is linear

Proposition (4.6)

Let K be a field. Let $f \in K[x]$ and $\alpha \in K$. Then there exist $q \in K[x]$ and $r \in K$ such that

$$f = (x - \alpha) \cdot q + r.$$

Corollary (4.7)

The remainder obtained when dividing f by $x - \alpha$ is $f(\alpha)$.

In particular, α is a root of f if and only if the polynomial $x - \alpha$ is a factor of f.

Repeated roots

Definition (4.8)

Let k be a nonnegative integer. An element $\alpha \in K$ is a **root of multiplicity** k of the polynomial $f \in K[x]$ if $(x - \alpha)^k$ is a factor of f, but $(x - \alpha)^{k+1}$ is not.

Repeated roots

Definition (4.8)

Let k be a nonnegative integer. An element $\alpha \in K$ is a **root of multiplicity** k of the polynomial $f \in K[x]$ if $(x - \alpha)^k$ is a factor of f, but $(x - \alpha)^{k+1}$ is not.

Theorem (Fundamental Theorem of Algebra with multiplicities)

Let $n \geq 1$, and let $a_0, a_1, \cdots, a_{n-1}, a_n$ be complex numbers, where $a_n \neq 0$. The polynomial

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$$

has exactly n roots in $\mathbb{C}$, counted with multiplicity.

The polynomial division rule

Theorem (4.10)

Let K be a field. Let f and g be two polynomials in $K[x]$, with $g \neq 0$. Then there exist a quotient q and a remainder r in $K[x]$ such that

- $f = gq + r$;
- *either $r = 0$ or the degree of r is smaller than the degree of g.*

2019 exam, question 1

Let $f, g \in \mathbb{R}[x]$ be polynomials, with $\deg g > 0$.

a. The **division rule for polynomials** states that f can be divided by g to produce a quotient q and remainder r. Write down the two conclusions that the division rule states about q and r.
b. How do we tell, from q and r, whether g **divides** f?
c. Suppose that $\deg f = 8$, and $(x-1)^3$ divides f. What can be said about the multiplicity of $x = 1$ as a solution of $f(x) = 0$?

Properties of matrix rings

Theorem (5.1)

If R is a ring, then so is $M_n(R)$.
If R is a ring with identity, then so is $M_n(R)$.

Properties of matrix rings

Theorem (5.1)

If R is a ring, then so is $M_n(R)$.
If R is a ring with identity, then so is $M_n(R)$.

Proposition (5.2)

If R is a ring in which not all products of two elements equal zero, and $n \geq 2$, then $M_n(R)$ is neither a commutative ring nor a skewfield.

Permutations

Definition (6.1)

A **permutation** of a set X is a function $f : X \to X$ which is a bijection (one-to-one and onto).

Permutations

Definition (6.1)

A **permutation** of a set X is a function $f : X \to X$ which is a bijection (one-to-one and onto).

S_n is the set of permutations of $\{1, \ldots, n\}$.

Permutations

Definition (6.1)

A **permutation** of a set X is a function $f : X \to X$ which is a bijection (one-to-one and onto).

S_n is the set of permutations of $\{1, \ldots, n\}$.

Proposition (6.2)

$|S_n| = n!$.

Composition, inverses

Proposition (6.3)

If f and g are elements of S_n, then the composite function $f \circ g$ is in S_n as well.

Composition, inverses

Proposition (6.3)

If f and g are elements of S_n, then the composite function $f \circ g$ is in S_n as well.

Proposition (6.4)

If $f \in S_n$, then the inverse function f^{-1} exists and is an element of S_n as well.

Cycles

Theorem (6.5)

Any permutation can be written as a composition of disjoint cycles. The representation is unique, up to the facts that:

- *the cycles can be written in any order;*
- *each cycle can be started at any point;*
- *cycles of length 1 can be left out.*

Cycles

Theorem (6.5)

Any permutation can be written as a composition of disjoint cycles. The representation is unique, up to the facts that:

- *the cycles can be written in any order;*
- *each cycle can be started at any point;*
- *cycles of length 1 can be left out.*

Definition

The **order** of the element $g \in S_n$ is the smallest positive number k for which $\underbrace{g \circ \cdots \circ g}_{k \text{ times}} = e$.

Cycles

Theorem (6.5)

Any permutation can be written as a composition of disjoint cycles. The representation is unique, up to the facts that:

- *the cycles can be written in any order;*
- *each cycle can be started at any point;*
- *cycles of length 1 can be left out.*

Definition

The **order** of the element $g \in S_n$ is the smallest positive number k for which $\underbrace{g \circ \cdots \circ g}_{k \text{ times}} = e$.

Proposition (6.6)

The order of a permutation is the least common multiple of the lengths of the cycles in its disjoint cycle representation.

Let f be the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 6 & 1 & 5 & 4 & 9 & 10 & 8 & 2 & 3 \end{pmatrix} \in S_{10},$$

given in two-line notation.

a. Write f in cycle notation.

b. Let g be the permutation $(2\ 4\ 10\ 7\ 5\ 8\ 9)(3\ 6) \in S_{10}$. Compute $g \circ f \circ g^{-1}$, and write your answer in cycle notation.

c. What is the order of f? Show your working.

Groups

Definition (7.1)

A **group** is a set G with an operation $\diamond$ on G satisfying the following axioms:

Closure law: for all $a, b \in G$, we have $a \diamond b \in G$.

Associative law: for all $a, b, c \in G$, we have $a \diamond (b \diamond c) = (a \diamond b) \diamond c$.

Identity law: there is an element $e \in G$ (called the *identity*) such that $a \diamond e = e \diamond a = a$ for any $a \in G$.

Inverse law: for all $a \in G$, there exists $b \in G$ such that $a \diamond b = b \diamond a = e$, where e is the identity. The element b is called the *inverse* of a, written a^*.

If in addition the following law holds:

Commutative law: for all $a, b \in G$ we have $a \diamond b = b \diamond a$

then G is called an **abelian group**.

Examples of groups we've already seen

Theorem (7.2)

Let R be a ring. Take $G = R$, with operation $+$. Then G is an abelian group.

Examples of groups we've already seen

Theorem (7.2)

Let R be a ring. Take $G = R$, with operation $+$. Then G is an abelian group.

Theorem (7.3)

The set S_n of all permutations of $\{1, \ldots, n\}$, with the operation of composition, is a group.

Examples of groups we've already seen

Theorem (7.2)

Let R be a ring. Take $G = R$, with operation $+$. Then G is an abelian group.

Theorem (7.3)

The set S_n of all permutations of $\{1, \ldots, n\}$, with the operation of composition, is a group.

Proposition (7.4)

S_n is an abelian group if $n \leq 2$, and is non-abelian if $n \geq 3$.

Some notations for groups

Notation	Operation	Identity	Inverse
General	$a \diamond b$	e	a^*
Multiplicative	ab or $a \cdot b$	1	a^{-1}
Additive	$a + b$	0	$-a$

Etcetera.

Elementary properties of groups

Proposition (7.5)

Let G be a group.

a. *The identity of G is unique.*
b. *Each element has a unique inverse.*
c. *For any $a, b \in G$, we have $(a \diamond b)^* = b^* \diamond a^*$.*
d. *Cancellation law: if $a \diamond b = a \diamond c$ then $b = c$.*

Units

Let R be a ring with identity element 1.

Definition (7.6)

An element $u \in R$ is called a **unit** if there is an element $v \in R$ such that $uv = vu = 1$.

The element v is called the **inverse** of u, written u^{-1}.

Units

Let R be a ring with identity element 1.

Definition (7.6)

An element $u \in R$ is called a **unit** if there is an element $v \in R$ such that $uv = vu = 1$.

The element v is called the **inverse** of u, written u^{-1}.

Proposition (7.7)

a. *If R satisfies the nontrivial law, then 0 is not a unit.*
b. *1 is a unit; its inverse is 1.*
c. *If u is a unit, then so is u^{-1}; its inverse is u.*
d. *If u and v are units, then so is uv; its inverse is $v^{-1}u^{-1}$.*

The group of units

If R is a ring with identity, we let $R^\times$ denote the set of units of R, with the operation of multiplication in R.

Theorem (7.8)

$R^\times$ is a group.

We name $R^\times$ the **group of units** of R.

Subgroups

Definition (7.9)

Let $(G, \diamond)$ be a group, and H a sub*set* of G. We say that H is a **subgroup** of G if H, with the same operation $\diamond$ is itself a group.

Subgroups

Definition (7.9)

Let $(G, \diamond)$ be a group, and H a sub*set* of G. We say that H is a **subgroup** of G if H, with the same operation $\diamond$ is itself a group.

Proposition (7.10)

A non-empty subset H of a group $(G, \diamond)$ is a subgroup if and only if, for all $h_1, h_2 \in H$, we have $h_1 \diamond h_2^* \in H$.

Subgroups

Definition (7.9)

Let $(G, \diamond)$ be a group, and H a sub*set* of G. We say that H is a **subgroup** of G if H, with the same operation $\diamond$ is itself a group.

Proposition (7.10)

A non-empty subset H of a group $(G, \diamond)$ is a subgroup if and only if, for all $h_1, h_2 \in H$, we have $h_1 \diamond h_2^* \in H$.

Theorem (Lagrange's Theorem, 7.11)

Let G be a finite group, and H a subgroup of G. Then $|H|$ divides $|G|$.

Extra question 7.2.1

Write down every possible Cayley table of a group whose set of elements is $\{a, b, c\}$.

a. Define what it means for a set G with a binary operation $*$ to be a **group**, including the statements of every axiom you cite.

b. Let

$$S = \{a + b\mathrm{i} \in \mathbb{C} : a, b \in \mathbb{R}, a^2 + b^2 = 1\}$$

be the set of all complex numbers of modulus 1. Prove that S is a subgroup of the multiplicative group $\mathbb{C}^\times$.

Variant of Extra 2.6.4 (solving equations in $\mathbb{Z}_p$)

Find all $X, Y \in \mathbb{Z}_{13}$ that satisfy the simultaneous system of linear equations

$$\begin{aligned} [5]_{13}\, X + [2]_{13}\, Y &= [6]_{13} \\ [4]_{13}\, X + \phantom{[2]_{13}}\, Y &= [2]_{13}. \end{aligned}$$

CW week 12 Q4 (subgroup proofs)

Let S be the set of all complex numbers of modulus 1. Prove that S is a subgroup of the multiplicative group $\mathbb{C}^\times$.