Massachusetts Institute of Technology
6.5610: Applied Cryptography
Professor Srini Devadas

Handout R1
Feb 6, 2026
Kaiwen (Kevin) He

Recitation 1: Number Theory Background

1 Modular Arithmetic

Modular Arithmetic is a system of arithmetic within a finite set of integers, where numbers "wrap around" when reaching a certain number. For example,

$$2 \equiv 12 \equiv 22 \mod 10$$

Generally, for $n > 0$ and integers a and b, we can say that $a \equiv b \mod n$ if n divides $a - b$, also denoted as $n \mid a - b$.

2 Basic Operations

For addition, subtraction and multiplication, modular arithmetic operations are consistent with normal math. So for a, b, a', b' where $a \equiv a' \mod n$, $b \equiv b' \mod n$, we have the following:

- $a + b \equiv a' + b' \mod n$
- $a - b \equiv a' - b' \mod n$
- $a * b \equiv a' * b' \mod n$

Division is trickier and relies on the existence of multiplicative inverses. Given an integer a, a^{-1} is the multiplicative inverse of a modulo n if $a * a^{-1} \equiv 1 \mod n$.

Note that a only has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$. You will prove a special case of this fact in Problem Set 1.

On the other hand because for any non-zero element in modulo p where p is prime, there exists a multiplicative inverse so division works all the time. Other than the method of computing the multiplicative inverse, division in modular arithmetic works the same as normal division.

For example, $\frac{1}{2} + \frac{1}{3} = \frac{5}{6}$ over rationals. Considering modulo 7, we get $2^{-1} = 4, 3^{-1} = 5, 6^{-1} = 6$ so applying this to the fractional equation $1 * 4 + 1 * 5 \equiv 9 \equiv 5 * 6 \mod 7$.

3 Modular Exponentiation

Exponentiation works the same way as it does in normal math, i.e. repeated multiplication. The interesting part about exponentiation is how the value cycles as we go through the exponents.

For example, the powers of 2 and 6 appear as follows when simplified modulo 7:

2^1	2^2	2^3	2^4	2^5	2^6
2	4	1	2	4	1

6^1	6^2	6^3	6^4	6^5	6^6
6	1	6	1	6	1

In this case, 2 cycles every 3 elements. For any prime p and $a \neq 0 \pmod p$, $a^1, a^2, \ldots, a^{p-1}$ must cycle through some subset of the $p - 1$ possible non-zero residues modulo p. The length of the cycle is also called

the order, i.e. $\text{ord}_7(2) = 3$.

For any prime p, there exists some integer g such that $\text{ord}_p(g) = p - 1$. In other words, the cycle loops through all possible residues in some order. g is often referred to as a *primitive root* or a *generator* of p. For example, 3 is a generator modulo 7 since

3^0	3^1	3^2	3^3	3^4	3^5
1	3	2	6	4	5

4 Groups

The Diffie-Hellman key exchange protocol can be generalized to work with mathematical objects beyond integers modulo a prime, such as elliptic curves.[1] Both elliptic curves and modular multiplication fall under a common mathematical abstraction called a group, which we will define below.

A group is a set S equipped with a binary operation, commonly notated as addition with $+$, that satisfies the following properties:

1. The operation maps elements of the set into the set. Formally, for all $s_1, s_2 \in S$, $s_1 + s_2 \in S$.
2. There is an identity element, commonly notated 0. Formally, for all $s_1 \in S$, $s_1 + 0 = s_1$ and $0 + s_1 = s_1$.
3. Each element has an inverse. This means that there is another element that takes the result to the identity. Formally, for all $s_1 \in S$, there exists s_2 such that $s_1 + s_2 = 0$ and $s_2 + s_1 = 0$.
4. The order of operations does not matter (associativity). Formally, for all $s_1, s_2, s_3 \in S$, $(s_1 + s_2) + s_3 = s_1 + (s_2 + s_3)$.

4.1 Examples of groups

A common example of a group is the integers modulo n, for some number n. For example, let's consider the integers mod 4 with the operation of addition. There are 4 elements in the set S: $\{0, 1, 2, 3\}$. The operation of addition maps the elements in the following way:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

This looks a lot like a multiplication table and is referred to as a Cayley table for a group. Is there another group with 4 elements?

$\oplus$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

This group is formed by the exclusive or operator on 2 bits. We can notice some patterns about groups

[1] In fact, real-world Internet protocols like TLS (essentially the `s` in `https`) and SSH almost exclusively use elliptic curves to perform the Diffie-Hellman key exchange for performance reasons.

- The element 0 appears in every row and column, because every element has an inverse.
- No value repeats in any row or column. If it did then we would have $x + y_1 = x + y_2$, but this means $y_1 = y_2$.
- Every value appears in every row and column. As there are no repeats and only 4 values, they all must appear.

What other groups of 4 elements are there? We can consider a group where we rotate a square. The group operation is to apply the rotations consecutively

	0	90	180	270
0	0	90	180	270
90	90	180	270	0
180	180	270	0	90
270	270	0	90	180

If this looks like a familiar pattern, you're right. This group is actually the same as $\mathbb{Z}_4$, but all the elements have different "names." This is called an isomporphism.

We can also consider the group made by reflections of a non-square rectangle. We can flip over the vertical and horizontal axes. To close the group, we also need to consider flipping over both axis.

	nothing	horizontal	vertical	both
nothing	nothing	horizontal	vertical	both
horizontal	horizontal	nothing	both	vertical
vertical	vertical	both	nothing	horizontal
both	both	vertical	horizontal	nothing

This group is isomorphic to the XOR group we saw above. In fact, there are only 2 commutative groups with 4 elements. A commutative group is one where the operator also satisfies $a + b = b + a$. This can be proven precisely (the fundamental theorem of finite Abelian groups), but it has to do with the fact that 4 can only be factored as $4 * 1$ and $2 * 2$.

4.2 Generators, order

The behavior of a group can be analyzed by looking at the order of the group elements. The order of an element is the number of times an element has to be added to itself to get the identity, where the order of the identity element is 1.

For example, in $\mathbb{Z}_4$,

- $0 = 0$, order 1
- $1 + 1 + 1 + 1 = 0$, order 4
- $2 + 2 = 0$, order 2
- $3 + 3 + 3 + 3 = 0$, order 4

In the XOR group, which I will call K_4. Because of isomorphism, you can also call it D_2 or $\mathbb{Z}_2^2$ and many other names.

- $00 = 00$, order 1
- $01 \oplus 01 = 00$, order 2
- $10 \oplus 10 = 00$, order 2

- $11 \oplus 11 = 00$, order 2

How do we know that an element eventually reaches the identity? Pigeonhole principle - if must eventually reach a duplicate element after $|S|$ additions. Let this duplicate element appear for the first time after k_1 and k_2 additions, where $k_1 < k_2$ without loss of generality. Then, we can subtract x k_1 times from both sides. We get $0 = x(k_2 - k_1)$. This means that adding x to itself $k_2 - k_1$ times results in the identity, and therefore every element eventually reaches the identity, and in no more that $|S|$ times (we need $|S|$ elements for pigeonhole.

If there is an element of order $|S|$, it is called a generator. Notice that $\mathbb{Z}_4$ has 2 generators (1 and 3) but K_4 has no generators, so not all groups have generators. The number of generators in $\mathbb{Z}_n$ can be found by the totient function $\phi(n)$, which counts the number of relatively prime numbers from 1 to $n-1$. The reason 2 is not a generator is because 2 and 4 share a common factor, 2, and so we only iterate through even numbers (multiples of 2) and not all of the numbers in the group. We can calculate the value of the totient function as follows: for each prime factor p of n, $1/p$ of the numbers will share this factor. For example, with $n = 10$

x	0	1	2	3	4	5	6	7	8	9
x mod 2	0	1	0	1	0	1	0	1	0	1
x mod 5	0	1	2	3	4	0	1	2	3	4

Exactly half of the numbers from 0 to 10 are even - because they are either 0 or 1 mod 2. Exactly one fifth of the numbers from 0 to 10 are multiples of 5 - because they cycle through $0, 1, 2, 3, 4$ repeatedly. Therefore, the number of integers relatively prime to 10 is $10 * (1/2) * (4/5) = 4$ and there are 4 generators - $1, 3, 7, 9$ which we can see are the only numbers that do not share a factor with 10.

5 Rings, Fields

A ring is a commutative group equipped with an additional operation, commonly referred to as multiplication.

1. All the properties of a group must be satisfied.
2. There exists a multiplicative identity, denoted 1 such that for all $s \in S$, $s * 1 = s = 1 * s$.
3. Multiplication is also associative: for all $s_1, s_2, s_3 \in S$, $(s_1 * s_2) * s_3 = s_1 * (s_2 * s_3)$.
4. Multiplication is also commutative: for all $s_1, s_2 \in S$, $(s_1 * s_2) = (s_2 * s_1)$.
5. Addition and multiplication follow the distributive law. For all $s_1, s_2, s_3 \in S$, $s_1 * (s_2 + s_3) = s_1 * s_2 + s_1 * s_3$ and $(s_1 + s_2) * s_3 = s_1 * s_3 + s_2 * s_3$.

A field is a ring with one additional property—a multiplicative inverse for every element (except 0) exists.

1. All the properties of a ring must be satisfied.
2. Each element (except for the additive identity) has a multiplicative inverse. For all $s_1 \in S \neq 0$, there exists s_2 such that $s_1 * s_2 = 1 = s_2 * s_1$.

5.1 Examples of rings

The simplest example of a ring is the integers $\mathbb{Z}$, which is not a field (2 has no inverse). The rational, real, and complex numbers $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields. We give more examples below:

5.1.1 Integers modulo an integer

Let's consider the integers modulo 4. We can build a multiplication table:

$*$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

This is a ring but not a field, because there is no element x such that $2 * x = 1 \pmod 4$.

5.1.2 Integers modulo a prime

The integers mod a prime number are a field. Since every element has a multiplicative inverse, we can define another group, the multiplicative group, over these elements. For the integers mod p, this is a group where the operation is multiplication! Let's consider the integers mod 5, rather than mod 4.

$*$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Note that although 0 does not have a multiplicative inverse, it does not matter. Each of the other elements now has an inverse - an element where it multiplies to 1. It is common to consider the multiplicative group of a field - the elements other than 0. Several notations can be used for this, we will denote this as $\mathbb{Z}_5^\times$.

$*$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

But $\mathbb{Z}_5^\times$ has 4 elements, and we already listed out all the groups with 4 elements. This means $\mathbb{Z}_5^\times$ must be the same group with the number renamed somehow. Specifically, $\mathbb{Z}_5^\times$ isomorphic to $\mathbb{Z}_4$. To see why, consider writing each number in terms of the generator 2.

$*$	2^0	2^1	2^3	2^2
2^0	2^0	2^1	2^3	2^2
2^1	2^1	2^2	2^0	2^3
2^3	2^3	2^0	2^2	2^1
2^2	2^2	2^3	2^1	2^0

The second and third columns have been swapped, but this is the same as the Cayley table for $\mathbb{Z}_4$. In fact, any of the generators of $\mathbb{Z}_5^\times$ work. We could even do multiplication with addition if you had a function called log that performed this isomorphism such that $\log(a) + \log(b) = \log(ab)$.

5.2 Polynomial rings

For any ring R, the set of univariate polynomials with coefficients in R form a ring denoted $R[x]$, under the usual polynomial addition and multiplication operations.

5.2.1 Detour: factoring and irreducibility

Similar to the special case of integers, we can define a more generalized notion of factoring for a large class of rings[2], which includes (but is not limited to) $\mathbb{Z}$ and $K[x]$ when K is a field. The *prime* elements are often called irreducible, which is formally defined as a non-zero element with no inverse and cannot be written as a product of two non-invertible elements. For univariate polynomials in a field, a nonzero polynomial in $K[x]$ is invertible if and only if it is a constant polynomial, so you can replace "invertible" with "constant".

Note that whether a polynomial is irreducible depends on the ring. For example, $x^2 + 1$ is reducible in $\mathbb{C}[x]$ as it factors into $(x - i)(x + i)$, but is irreducible in $\mathbb{R}[x]$ or $\mathbb{Q}[x]$ since it has no real roots.

5.2.2 Detour: ideals and quotient rings

Similar to modular arithmetic over the integers, we can generalize modular arithmetic over polynomials. The abstract algebra terminology for the modulus is an "ideal", and taking a ring R modulo an ideal I yields another quotient ring R/I. The simplest type of ideals are principal ideals, where (a) denotes the ideal defined by arithmetic modulo a ring element $a \in R$. Our focus is on rings where the only ideals are principal ideals[3], which again include most familiar rings like $\mathbb{Z}$ and $K[x]$ when K is a field.

For example, $\mathbb{Z}/(3\mathbb{Z})$ denotes the ring of integers modulo 3, $\mathbb{Z}[x]/(x^2 + 1)$ denotes the ring of integers modulo the irreducible polynomial $x^2 + 1$.

5.3 The Galois field of size 4

This field extends the XOR group K_4 we saw earlier. However, multiplication in this group is not repeated addition! This group interprets the elements of K_4 as polynomials with coefficients in $\mathbb{Z}_2$—the coefficients are either 0 or 1 and $1 + 1 = 0$. So for example $(x + 1) + x = 2x + 1 = 0x + 1 = 1$, and this corresponds to XOR-ing 11 with 10 to get 01. Specifically, multiplication is defined by

1. Interpret each bit as the coefficient of a polynomial. So 10 is $1x + 0$, 11 is $1x + 1$, 01 is $0x + 1$ and 0 is $0x + 0$.

2. Multiply the polynomials modulo $x^2 + x + 1$ and take each coefficient mod 2.

The multiplication table for this group looks like this:

$*$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

In fact, this can be generalized to all finite fields. The field of order p^k can be constructed by considering a degree-k polynomial with coefficients in $\mathbb{Z}_p$ (so the trivial p^1 case is just the field $\mathbb{Z}_p$!). The multiplication is taken modulo an irreducible polynomial—a k degree polynomial that doesn't factor over the field $\mathbb{Z}_p$. It's a bit outside of group theory, but the choice of $x^2 + x + 1$ is in fact forced for a field of 4 elements. $x^2 + 1$ factors as $(x + 1)(x + 1) = x^2 + 2x + 1 = x^2 + 1 \pmod 2$, and $x^2 + x$ and x^2 clearly factor.

6 Appendix: Notations for Problem Set 1

Notice that we define f_λ as an element of a family of one way functions, instead of f just being a OWF.

[2] called unique factorization domains (UFD)

[3] called a principal ideal domain (PID), a subclass of UFDs.

$\Pr[\texttt{statement}: \texttt{conditions}]$	The probability of the statement given the conditions.
$f_\lambda(x)$	The one way function λ evaluated at x.
$x \xleftarrow{R} \{0,1\}^\lambda$	x is a random λ-bit string.
$A(f_\lambda(x))$	The adversary runs an algorithm given $f_\lambda(x)$ as input.
$\mu(\lambda)$	A negligible function. For example, $2^{-\lambda}$ and $2^{-\lambda/2}$ are negligible, but λ^{-100} is not. For a polynomial adversary, a negligible advantage is often used in theoretical definitions.

7 Acknowledgement

Material based on recitations from previous iterations of the class, including a handout by Deep Gupta as well as other TAs. Many thanks to whoever worked on those material.

Recitation 1:

Number Theory Review + Basic Abstract Algebra

Kaiwen (Kevin) He

Review: modular arithmetic

- Arithmetic where numbers wrap around after reaching a number m, called the modulus

Ex. $m = 12$, $11 + 2 = 13 \equiv 1 \pmod{12}$

"2 hours after 11 am is 1 pm."

$11 - 13 = -2 \equiv 10 \pmod{12}$

"13 hours before 11 am is 10 pm."

$2 \cdot 8 \equiv 4 \pmod{12}$

Abstract algebra

- A framework to generalize mathematical structures like integers modulo n.

Abstract algebra

- A framework to generalize mathematical structures like integers modulo n.
- Why abstract algebra?
  - Proofs about abstract structures generalize to all instantiations.

Abstract algebra

- A framework to generalize mathematical structures like integers modulo n.
- Why abstract algebra?
  - Proofs about abstract structures generalize to all instantiations.
  - Proofs are often simpler after ignoring many "implementation details".

Abstract algebra

- A framework to generalize mathematical structures like integers modulo n.
- Why abstract algebra?
  - Proofs about abstract structures generalize to all instantiations.
  - Proofs are often simpler after ignoring many "implementation details".
  - Allows generalizing the same cryptosystems to diverse mathematical structures
    - Diffie-Hellman key exchange was originally over integers mod p, but now works over elliptic curves as well
      ↑ in fact, more efficient to compute.

Groups

A group is a set S equipped w/ an operation $+$ that satisfies the following props:

Closure: $\forall\, a, b \in S,\ a + b \in S$ $\quad (+ : S \times S \to S)$

Groups

A group is a set S equipped w/ an operation $+$ that satisfies the following props:

Closure: $\forall\, a, b \in S,\ a+b \in S$

Identity: $\exists\, e \in S$ s.t. $\forall\, s \in S,\ s+e = s$

(We usually denote e as the digit 0)

Groups

A group is a set S equipped w/ an operation $+$ that satisfies the following props:

Closure: $\forall\, a, b \in S,\ a+b \in S$

Identity: $\exists\, e \in S$ s.t. $\forall\, s \in S,\ s+e = s$

(We usually denote e as the digit 0)

Inverses: $\forall\, a \in S,\ \exists\, b \in S$ s.t. $a+b = 0$

(We denote b as $-a$)

Groups

A group is a set S equipped w/ an operation $+$ that satisfies the following props:

Closure: $\forall\, a, b \in S,\ a+b \in S$

Identity: $\exists\, e \in S$ s.t. $\forall\, s \in S,\ s+e = s$

(We usually denote e as the digit 0)

Inverses: $\forall\, a \in S,\ \exists\, b \in S$ s.t. $a+b = 0$

(We denote b as $-a$)

Associativity: $\forall\, a, b, c \in S,\ (a+b)+c = a+(b+c)$

Groups (alternate notation)

A group is a set S equipped w/ an operation $\cdot$ that satisfies the following props:

Sometimes denoted ab.

Closure: $\forall\, a, b \in S,\ a \cdot b \in S$

Identity: $\exists\, e \in S$ s.t. $\forall\, s \in S,\ s \cdot e = s$

(We usually denote e as the digit 1)

Inverses: $\forall\, a \in S,\ \exists\, b \in S$ s.t. $a \cdot b = 1$

(We denote b as a^{-1})

Associativity: $\forall\, a, b, c \in S,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$

Groups

A group is a set S equipped w/ an operation $+$ that satisfies the following:

Closure: $\forall a, b \in S$, $a + b \in S$

Identity: $\exists e \in S$ s.t. $\forall s \in S$, $s + e = s$

(We usually denote e as the digit 0)

Inverses: $\forall a \in S$, $\exists b \in S$ s.t. $a + b = 0$

(We denote b as $-a$)

Associativity: $\forall a, b, c \in S$, $(a+b)+c = a+(b+c)$

Focus of this recitation:

Abelian Groups

Groups w/ an additional property:

Commutativity: $\forall a, b \in S$,

$a + b = b + a$

Examples of groups

Can someone (who have not seen this) give an example of a group?

Examples of groups

1. The integers $\mathbb{Z}$ under addition. (denoted $\mathbb{Z}^+$)

Q: Is $\mathbb{Z}$ under multiplication also a group? Why / why not?

Examples of groups

1. The integers $\mathbb{Z}$ under addition. (denoted $\mathbb{Z}^+$)

   Q: Is $\mathbb{Z}$ under multiplication also a group? Why / why not?

   No, 2 has no inverse in $\mathbb{Z}$ ($1/2 \notin \mathbb{Z}$)

2. The integers $\{0, 1, \ldots, m\}$ under additions modulo m. (denoted $\mathbb{Z}_m$ or $\mathbb{Z}/m$)

   For example, in $\mathbb{Z}_4$, $2 + 3 = 1$, $-3 = 1$

Examples of groups

1. The integers $\mathbb{Z}$ under addition. (denoted $\mathbb{Z}^+$)

   Q: Is $\mathbb{Z}$ under multiplication also a group? Why / why not?

   No, 2 has no inverse in $\mathbb{Z}$. ($1/2 \notin \mathbb{Z}$)

2. The integers $\{0, 1, \ldots, m\}$ under additions modulo m. (denoted $\mathbb{Z}_m$ or $\mathbb{Z}/m$)

   For example, in $\mathbb{Z}_4$, $2 + 3 = 1$, $-3 = 1$

3. The integers $\{1, \ldots, p\}$ under multiplications modulo a prime p. ($\mathbb{Z}_p^\times$)

Examples of groups

1. The integers $\mathbb{Z}$ under addition. (denoted $\mathbb{Z}^+$)

Q: Is $\mathbb{Z}$ under multiplication also a group? Why / why not?

No, 2 has no inverse in $\mathbb{Z}$. ($1/2 \notin \mathbb{Z}$)

2. The integers $\{0, 1, \ldots, m\}$ under additions modulo m. (denoted $\mathbb{Z}_m$ or $\mathbb{Z}/m$)

For example, in $\mathbb{Z}_4$, $2 + 3 = 1$, $-3 = 1$

3. The integers $\{1, \ldots, p\}$ under multiplications modulo a prime p. ($\mathbb{Z}_p^\times$)

$\mathbb{Z}_5^\times$:

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$1^{-1} = 1$

$2^{-1} = 3$

$3^{-1} = 2$

$4^{-1} = 4$

Examples of groups

1. The integers $\mathbb{Z}$ under addition. (denoted $\mathbb{Z}^+$)

Q: Is $\mathbb{Z}$ under multiplication also a group? Why / why not?

No, 2 has no inverse in $\mathbb{Z}$. ($1/2 \notin \mathbb{Z}$)

2. The integers $\{0, 1, \ldots, m\}$ under additions modulo m. (denoted $\mathbb{Z}_m$ or $\mathbb{Z}/m$)

For example, in $\mathbb{Z}_4$, $2 + 3 = 1$, $-3 = 1$

3. The integers $\{1, \ldots, p\}$ under multiplications modulo a prime p. ($\mathbb{Z}_p^\times$)

$\mathbb{Z}_5^\times$:

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$1^{-1} = 1$

$2^{-1} = 3$

$3^{-1} = 2$

$4^{-1} = 4$

Pset 1:

3a) Prove $\mathbb{Z}_p^\times$ is a group for all primes p.

3b) Show that primality is necessary, i.e., $\mathbb{Z}_m^\times$ is NOT a group for composite m.

Rings

A ring is a set R equipped w/ two operators $+, \cdot$ s.t.

① R is an abelian group under addition $+$ (identity: 0, inverse of x is $-x$)

② R satisfy all abelian group properties <u>except inverse</u> under multiplication $\cdot$.
(identity: 1)

③ Distributive law:

$$a \cdot (b+c) = a \cdot b + a \cdot c$$

Rings

A ring is a set R equipped w/ two operators $+, \cdot$ s.t.

① R is an abelian group under addition $+$ (identity: 0, inverse of x is $-x$)

② R satisfy all abelian group properties <u>except inverse</u> under multiplication $\cdot$.
(identity: 1)

③ Distributive law:

$$a \cdot (b+c) = a \cdot b + a \cdot c$$

<u>Examples:</u>

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under the usual $+, \cdot$
2. The integers mod m ($\mathbb{Z}_m$)
   (this time, any positive integer m would work)
3. the ring of polynomials w/ coefficients in ring R: $R[x]$.

Rings

A ring is a set R equipped w/ two operations $+, \cdot$ s.t.

① R is an abelian group under addition $+$ (identity: 0, inverse of x is $-x$)

② R satisfy all abelian group properties except inverse under multiplication $\cdot$.
(identity: 1)

③ Distributive law:

$$a \cdot (b+c) = a \cdot b + a \cdot c$$

Fields are rings where the nonzero elements form a group under multiplication

Q: Which of the examples are fields? Under what conditions?

Examples:

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under the usual $+, \cdot$
2. The integers mod m ($\mathbb{Z}_m$)
   (this time, any positive integer m would work)
3. The ring of polynomials $f(x)$ w/ coefficients in ring R: $R[x]$.

Rings

A ring is a set R equipped w/ two operations $+, \cdot$ s.t.

① R is an abelian group under addition $+$ (identity: 0, inverse of x is $-x$)

② R satisfy all abelian group properties except inverse under multiplication $\cdot$.
(identity: 1)

③ Distributive law:

$$a \cdot (b+c) = a \cdot b + a \cdot c$$

Fields are rings where the nonzero elements form a group under multiplication

Q: Which of the examples are fields? Under what conditions?

Examples of fields

1. ~~$\mathbb{Z}$~~, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ under the usual $+, \cdot$

2. The integers mod prime n ($\mathbb{Z}_n$)

3. The field of rational functions in x.

e.g., $\dfrac{x^2+x+1}{x+5}$

Quotient rings

- Generalizing modular arithmetic to an arbitrary ring:

  $R/(m)$ denotes the ring R modulo an element $m \in R$.

Quotient rings

- Generalizing modular arithmetic to an arbitrary ring:

  $R/(m)$ denotes the ring R modulo an element $m \in R$.

- Example: $\mathbb{Z}[x]/(x^2+1)$

$$(2x+3)(5x+7)$$

$$= 10x^2 + 29x + 21$$

$$= 29x + 11 \qquad (\text{mod } x^2+1)$$

Quotient rings

- Generalizing modular arithmetic to an arbitrary ring:

  $R/(m)$ denotes the ring R modulo an element $m \in R$.

- When is $R/(m)$ a field?
  - Special case we saw (and you will prove in Pset 1):

    When $R = \mathbb{Z}$, $R/(m)$ is a field iff m is prime.

$$\mathbb{Z}[x]/(x^2+1)$$

$$(2x+3)(5x+7)$$

$$= 10x^2 + 29x + 21$$

$$= 29x + 11 \qquad (\text{mod } x^2+1)$$

Quotient rings

- Generalizing modular arithmetic to an arbitrary ring:

  $R/(m)$ denotes the ring R modulo an element $m \in R$.

- When is $R/(m)$ a field?

  - Special case we saw (and you will prove in Pset 1):
    When $R = \mathbb{Z}$, $R/(m)$ is a field iff m is prime.
  - General case is complicated for general rings R,* so we focus on $R = K[x]$ where K is a field

In this case, $K[x]/(f(x))$ is a field if $f(x)$ is an irreducible polynomial.

$\mathbb{Z}[x]/(x^2+1)$

$(2x+3)(5x+7)$

$= 10x^2 + 29x + 21$

$= 29x + 11$ (mod x^2+1)

*: $R/(m)$ is a field $\Leftrightarrow$ (m) is a maximal ideal.

Irreducible polynomials

A polynomial $f(x) \in K[x]$ is irreducible if

1) $f(x)$ is not the constant or zero polynomial

2) $f(x)$ cannot be factored into two non-constant polynomials.

Irreducible polynomials

A polynomial $f(x) \in K[x]$ is irreducible if

1) $f(x)$ is not the constant or zero polynomial
2) $f(x)$ cannot be factored into two non-constant polynomials.

Examples

$2x+3$ in $\mathbb{R}[x]$

(in general, degree 1 poly over any $K[x]$)

Non-examples

Irreducible polynomials

A polynomial $f(x) \in K[x]$ is irreducible if

1) $f(x)$ is not the constant or zero polynomial

2) $f(x)$ cannot be factored into two non-constant polynomials.

Examples

$2x+3$ in $\mathbb{R}[x]$

(in general, degree 1 poly over any $K[x]$)

x^2+1 in $\mathbb{R}[x]$

Non-examples

x^2+2x+1 in $\mathbb{R}[x]$

$(x^2+2x+1 = (x+1)^2)$

Irreducible polynomials

A polynomial $f(x) \in K[x]$ is irreducible if

1) $f(x)$ is not the constant or zero polynomial

2) $f(x)$ cannot be factored into two non-constant polynomials.

Examples

$2x+3$ in $\mathbb{R}[x]$

(in general, degree 1 poly over any $K[x]$)

x^2+1 in $\mathbb{R}[x]$

Non-examples

x^2+2x+1 in $\mathbb{R}[x]$

$(x^2+2x+1 = (x+1)^2)$

x^2+1 in $\mathbb{C}[x]$ $\quad (x^2+1 = (x-i)\cdot(x+i))$

⚠ Whether a polynomial is irreducible depends on the field!

The Galois field of size 4 : $\mathbb{F}_4$

$$\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2+x+1)$$

> Recall: $K[x]/(f(x))$ is a field if $f(x)$ is an irreducible polynomial.

$f(x) = x^2+x+1$ is irreducible over $\mathbb{Z}_2[x]$:

$f(0) = 1 \neq 0$

$f(1) = 1 \neq 0$

$\Rightarrow \nexists\, a, b$ s.t. $(x-a)(x-b) = x^2+x+1$

The Galois field of size 4 : $\mathbb{F}_4$

$$\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2+x+1)$$

> Recall: $K[x]/(f(x))$ is a field if $f(x)$ is an irreducible polynomial.

$f(x) = x^2+x+1$ is irreducible over $\mathbb{Z}_2[x]$:

$f(0) = 1 \neq 0$
$f(1) = 1 \neq 0$

$\Rightarrow \nexists\, a, b$ s.t. $(x-a)(x-b) = x^2+x+1$

Multiplication table:

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

General Galois fields

$\mathbb{F}_{p^k}$, a field of size p^k, can be constructed as

$$\mathbb{Z}_p[x] / f(x)$$

where $f(x)$ is an irreducible polynomial (over $\mathbb{Z}_p[x]$) of degree k.

General Galois fields

$\mathbb{F}_{p^k}$, a field of size p^k, can be constructed as

$$\mathbb{Z}_p[x] / f(x)$$

where $f(x)$ is an irreducible polynomial (over $\mathbb{Z}_p[x]$) of degree k.

In PSET 1 3c), you will construct $\mathbb{F}_{3^2}$ as an exercise.

Thank You!

Any Questions?