Introduction to Abstract Algebra

Dhananjoy Dey

Indian Institute of Information Technology, Lucknow
ddey@iiitl.ac.in

July 19, 2021

Disclaimers

1

All the pictures used in this presentation are taken from freely available websites.

2

If there is a reference on a slide all of the information on that slide is attributable to that source whether quotation marks are used or not.

Outline

Outline

Group

Exercise

Solve the following equations:

1. $a + x = b$ & $y + a = b$

Group

Exercise

Solve the following equations:

1. $a + x = b$ & $y + a = b$
2. $a.x = b$ & $y.a = b$

Group

Exercise

Solve the following equations:

1. $a + x = b$ & $y + a = b$
2. $a.x = b$ & $y.a = b$

Solution

First, we try to solve $a + x = b$

$$\begin{aligned} a + x &= b \\ (-a) + (a + x) &= (-a) + b \end{aligned}$$

Group

Exercise

Solve the following equations:

1. $a + x = b$ & $y + a = b$
2. $a.x = b$ & $y.a = b$

Solution

First, we try to solve $a + x = b$

$$\begin{aligned} a + x &= b \\ (-a) + (a + x) &= (-a) + b \\ (-a + a) + x &= -a + b \end{aligned}$$

Group

Exercise

Solve the following equations:

1. $a + x = b$ & $y + a = b$
2. $a.x = b$ & $y.a = b$

Solution

First, we try to solve $a + x = b$

$$\begin{aligned} a + x &= b \\ (-a) + (a + x) &= (-a) + b \\ (-a + a) + x &= -a + b \\ 0 + x &= -a + b \\ x &= -a + b \end{aligned}$$

Binary Operation

Definition

Let X be a non-void set. Then a ***binary operation*** *in X is a function*

$$f : S\,(\subset X \times X) \to X.$$

Binary Operation

Definition

Let X be a non-void set. Then a ***binary operation*** *in X is a function*

$$f : S(\subset X \times X) \to X.$$

- Usually, the binary operation f is denoted by '$\circ$' or '$+$' or '$\cdot$' etc.
- If we use '$\circ$' is the binary operation, then $f(x, y)$ is denoted by $x \circ y$
- If $S = X \times X$, then we say that X is **closed** w.r.t. the binary operation

Set & Structure

Definition

A ***set*** *is a well defined collection of objects.*

Definition

An ***algebraic structure*** *is a set together with (a)some binary operation(s).*

Group

Definition

1. *Let G be a non-empty set with a binary operation $\circ$ defined on it. Then $(G, \circ)$ is said to be a* ***groupoid or magma*** *if $\circ$ is closed*
   i.e. if $\circ : G \times G \longrightarrow G$.
2. *A set G with an operation $\circ$ is said to be a* ***semigroup*** *if G is a groupoid and $\circ$ is associative.*
3. *A set G with an operation $\circ$ is said to be a* ***monoid*** *if G is a semigroup and $\exists$ an element $e \in G_m$ s/t $g.e = e.g = g \; \forall \; g \in G$.*
4. *For each $x \in G, \; \exists$ an element $y \in G$ s/t $y \circ x = x \circ y = e$.*
   Usually, y is denoted by x^{-1}.

If G satisfies all the above, it is said to be a ***Group****.*

If $x \circ y = y \circ x \; \forall \; x, y \in G$, G is called abelian or commutative group.

Group

Example

1. $(\mathbb{Z}, +)$
2. $(\mathbb{Q}, +), (\mathbb{Q} \setminus \{0\}, \cdot)$
3. $(\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$
4. $(\mathbb{Z}_n, +)$
5. $(\mathbb{Z}_p^*, \cdot)$
6. $(\{1, -1\}, \cdot)$
7. $(S_n, \circ)$

Group

Example (S_3)

Let us consider the following important example S_3 under composition of functions.

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Group

Example (S_3)

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Exercises

Exercise

1. *Give an example of a groupoid which is not a semigroup.*
2. *Give an example of a semigroup which is not a monoid.*
3. *Give an example of a monoid which is not a group.*
4. *Give an example of a semigroup which is not a group.*

Group

Theorem

Let $(G, \circ)$ be a group and e_ℓ be a left identity and for each $x \in G$, x_ℓ^{-1} denote the left inverse of x.

(i) *Then e_ℓ is the $!$ two sided identity in G.*

(ii) *x_ℓ^{-1} is the $!$ two sided inverse of x for each $x \in G$.*

Note:

(a) If e' is any identify whether left or right then $e' = e_\ell$.

(b) If y is any left or right inverse of x then $y = x_\ell^{-1}$.

Some Preliminary Lemmas

Lemma

If $(G, \cdot)$ *[*G*] is a group, then*

1. (i) *The identity element of* G *is* $!$.
2. (ii) *Every* $a \in G$ *has a* $!$ *inverse in* G.
3. (iii) *For every* $a \in G$, $(a^{-1})^{-1} = a$.
4. (iv) *For all* $a, b \in G$, $(a.b)^{-1} = b^{-1}.a^{-1}$

Some Preliminary Lemmas

Lemma

If $(G, \cdot)$ [G] is a group, then

(i) *The identity element of G is $!$.*

(ii) *Every $a \in G$ has a $!$ inverse in G.*

(iii) *For every $a \in G$, $(a^{-1})^{-1} = a$.*

(iv) *For all $a, b \in G$, $(a.b)^{-1} = b^{-1}.a^{-1}$*

Proof.

First, we assume that e & e' are two identities of G.
For every $a \in G$, $e.a = a$. So, $e.e' = e'$, assuming e as an identity element.
Similarly, for every $b \in G$, $b.e' = b$. So, $e.e' = e$, assuming e' as an identity element.
Thus, we have $e' = e.e' = e$, i.e., $e = e'$.

Some Preliminary Lemmas

Lemma

If $(G, \cdot)$ *[*G*] is a group, then*

1. (i) *The identity element of* G *is* $!$.
2. (ii) *Every* $a \in G$ *has a* $!$ *inverse in* G.
3. (iii) *For every* $a \in G$, $(a^{-1})^{-1} = a$.
4. (iv) *For all* $a, b \in G$, $(a.b)^{-1} = b^{-1}.a^{-1}$

Proof.

First, we assume that e & e' are two identities of G.
For every $a \in G$, $e.a = a$. So, $e.e' = e'$, assuming e as an identity element.
Similarly, for every $b \in G$, $b.e' = b$. So, $e.e' = e$, assuming e' as an identity element.
Thus, we have $e' = e.e' = e$, i.e., $e = e'$.

$$x = e.x = (b.a).x = b.(a.x) = b.(a.y) = (b.a).y = e.y = y$$

□

Some Preliminary Lemmas

Lemma

Let $(G, \circ)$ *be a group and* $c \in G$ *s/t* $c^2 = c$*. Then* $c = e$*, where* e *is the identity element of* G*.*

Some Preliminary Lemmas

Lemma

Let $(G, \circ)$ be a group and $c \in G$ s/t $c^2 = c$. Then $c = e$, where e is the identity element of G.

Proof.

$$\begin{aligned} \because c^2 &= c \\ \therefore c.c &= c \\ \Rightarrow c^{-1}.(c.c) &= c^{-1}.c \\ \Rightarrow (c^{-1}.c).c &= e \\ \Rightarrow e.c &= e \end{aligned}$$

Thus, $c = e$. □

Group

Cancellation Law

Let $(G, \circ)$ be a group. Then for each triplet $x, y, z \in G$

(i) $x \circ y = x \circ z \Rightarrow y = z$ (left cancellation law)

(ii) $y \circ x = z \circ x \Rightarrow y = z$ (right cancellation law)

Subgroup

Definition

A subset H of a group G is said to be a subgroup of G if H itself forms a group under the restricted binary operation in G.

Subgroup

Definition

A subset H of a group G is said to be a subgroup of G if H itself forms a group under the restricted binary operation in G.

Lemma

A non-empty subset H of the group G is a subgroup of G iff

(i) $a, b \in H \Rightarrow a.b \in H$;

(ii) $a \in H \Rightarrow a^{-1} \in H$.

Subgroup

Definition

A subset H of a group G is said to be a subgroup of G if H itself forms a group under the restricted binary operation in G.

Lemma

A non-empty subset H of the group G is a subgroup of G iff

(i) $a, b \in H \Rightarrow a.b \in H$;

(ii) $a \in H \Rightarrow a^{-1} \in H$.

Subgroup

Lemma

If $(\phi \neq)H \subset G$ *&* $\#H < \infty$ *and* H *is closed under multiplication, then* $H \leq G$.

Subgroup

Lemma

If $(\phi \neq)H \subset G$ & $\#H < \infty$ and H is closed under multiplication, then $H \leq G$.

Proof.

- We need to show that for any $a \in H$, $a^{-1} \in H$
- Suppose $a \in H$, thus, $a^2 = a.a \in H, a^3 = a^2.a \in H, \dots, a^m \in H$. [$\because H$ is closed]
- Thus, the infinite collection of elements $a, a^2, \dots, a^m, \dots$ must all $\in H$ which is a finite subset of G
- $\because H < \infty$, there will be some $r, s \in \mathbb{N}$, $a^r = a^s$. By cancellation law in G, $a^{r-s} = e$, assuming $r > s$.
- $\because (r - s - 1) \geq 0$, $a^{r-s-1} \in H$ and $a^{-1} = a^{r-s-1} \in H$.

□

Note: The lemma may not be true if H is not finite.

Subgroup

Lemma

If $(\phi \neq)H \subset G$ & $\#H < \infty$ and H is closed under multiplication, then $H \leq G$.

Proof.

- We need to show that for any $a \in H$, $a^{-1} \in H$
- Suppose $a \in H$, thus, $a^2 = a.a \in H, a^3 = a^2.a \in H, \ldots, a^m \in H$. [$\because H$ is closed]
- Thus, the infinite collection of elements $a, a^2, \ldots, a^m, \ldots$ must all $\in H$ which is a finite subset of G
- $\because H < \infty$, there will be some $r, s \in \mathbb{N}$, $a^r = a^s$. By cancellation law in G, $a^{r-s} = e$, assuming $r > s$.
- $\because (r - s - 1) \geq 0$, $a^{r-s-1} \in H$ and $a^{-1} = a^{r-s-1} \in H$.

□

Note: The lemma may not be true if H is not finite. $(\mathbb{N}, +)$ and $(\mathbb{Z}^*, \cdot)$

Subgroup

Example

1. $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$
2. $(\mathbb{Q}^*, \cdot) \leq (\mathbb{R}^*, \cdot)$
3. *Let* $G = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$*, where* $a, b, c, d \in \mathbb{R}$ *and* $ad - bc \neq 0$*.* G *is a group under matrix multiplication.*

   $H = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$*, and* $b \in \mathbb{R}$*. Then* $H \leq G$*.*

Subgroup

Proposition

Let $(G, \cdot)$ be a group and T be a non-void subset of G. Then the following are equivalent:

1. $T \leq G$
2. *For each* $x, y \in T$, $x \cdot y$ & $x^{-1} \in T$
3. *For each* $x, y \in T$, $x \cdot y^{-1} \in T$

Subgroup

Definition

Let G be a group and $S, T \subset G$. We then define

$$S \cdot T = \begin{cases} z \in G \mid z = x.y & for\ x \in S,\ \&\ y \in T \\ \phi, & if\ either\ S\ or\ T = \phi \end{cases}$$

$$S^{-1} = \begin{cases} z \in G, & z^{-1} \in S \\ \phi, & if\ S = \phi \end{cases}$$

Subgroup

Proposition

Let G *be a group and* T *be a non-void subset of* G*. Then the following are equivalent:*

1. $T \leq G$
2. $T \cdot T \subset T \;\&\; T^{-1} \subset T$
3. $T \cdot T^{-1} \subset T$

Subgroup

Proposition

Let G be a group and T be a non-void subset of G. Then the following are equivalent:

1. $T \leq G$
2. $T \cdot T \subset T$ & $T^{-1} \subset T$
3. $T \cdot T^{-1} \subset T$

Exercise

Let G be a group and H & $K \leq G$. Then $H \cdot K$ is a subgroup of G iff $H \cdot K = K \cdot H$.

Exercise

Let $\{T_\alpha, \alpha \in \lambda\}$ be a collection of subgroups of G. Then $\bigcap\{T_\alpha, \alpha \in \lambda\}$ is also a subgroup of G.

Subgroup

Solution

- *First, we assume that* $H.K = K.H$ *and we have to prove that* $H.K \leq G$*.*
- *Let* $u, v \in H.K$*. Then* $u = h_1.k_1 \ \& \ v = h_2.k_2$

$$u.v = (h_1k_1).(h_2k_2) = h_1(k_1.h_2)k_2$$

Now, $k_1h_2 \in KH = HK$ *and so* $\exists\ h', k'$ *s/t* $k_1h_2 = h'k'$*,* $h' \in H \ \& \ k' \in K$*.*

$$h_1(k_1.h_2)k_2 = h_1(h'k')k_2 = (h_1h').(k'k_2) = h_3k_3 \in HK,$$

$\because h_3 = h_1h' \in H$ *and* $k_3 = k'k_2 \in K$*.*

- $u^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK$
  $\Rightarrow \exists\ h_4 \ \& \ k_4 \ni k_1^{-1}h_1^{-1} = h_4k_4 \in HK$.

So, HK *is a subgroup of* G*.*

Subgroup

Solution

- *First, we assume that* $H.K = K.H$ *and we have to prove that* $H.K \leq G$.
- *Let* $u, v \in H.K$. *Then* $u = h_1.k_1 \ \& \ v = h_2.k_2$

$$u.v = (h_1k_1).(h_2k_2) = h_1(k_1.h_2)k_2$$

Now, $k_1h_2 \in KH = HK$ *and so* $\exists\, h', k'$ *s/t* $k_1h_2 = h'k'$, $h' \in H \ \& \ k' \in K$.

$$h_1(k_1.h_2)k_2 = h_1(h'k')k_2 = (h_1h').(k'k_2) = h_3k_3 \in HK,$$

$\because h_3 = h_1h' \in H$ *and* $k_3 = k'k_2 \in K$.

- $u^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK$
  $\Rightarrow \exists\, h_4 \ \& \ k_4 \ni k_1^{-1}h_1^{-1} = h_4k_4 \in HK$.

So, HK *is a subgroup of* G. *Converse part is an exercise.*

Subgroup generated by a subset

Let G be a group and S be a subset of G. Then there is a smallest[1] subgroup T of G containing S. Then T is said to be generated by S and is denoted by $\langle S \rangle$.

Theorem

Let G be a group and S be a non-void subset of G. Then $\langle S \rangle$ consists of all finite product of the form

$$x_1.x_2.\dots.x_n, \; for \; n \in \mathbb{N} \; \& \; x_i \in S \cup S^{-1}.$$

[1] T is the smallest in the following sense:
if H is a subgroup and $S \subset H$ then $T \subset H$

Subgroup generated by a subset

Let G be a group and S be a subset of G. Then there is a smallest[1] subgroup T of G containing S. Then T is said to be generated by S and is denoted by $\langle S \rangle$.

Theorem

Let G be a group and S be a non-void subset of G. Then $\langle S \rangle$ consists of all finite product of the form

$$x_1.x_2.\ldots.x_n,\ for\ n \in \mathbb{N}\ \&\ x_i \in S \cup S^{-1}.$$

Theorem

If G is an abelian group and $(\phi \neq)S \subset G$, then $\langle S \rangle$ consists of all elements of the form $x_1^{r_1}.x_2^{r_2}.\ldots.x_k^{r_k}$, $x_i \neq x_j, r_i \in \mathbb{Z}$.

[1] T is the smallest in the following sense: if H is a subgroup and $S \subset H$ then $T \subset H$

Cyclic Group

Theorem

Let G be a group and $a \in G$. Then $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and is the smallest subgroup of G that contains a.

Cyclic Group

Theorem

Let G be a group and $a \in G$. Then $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and is the smallest subgroup of G that contains a.

Definition

1. *Let G be a group and $a \in G$. Then the smallest subgroup $H = \{a^n \mid n \in \mathbb{Z}\}$ of G which contains a is called the cyclic subgroup of G generated by a.*
2. *An element $a \in G$ generates G and is a generator for G if $\langle a \rangle = G$.*
3. *A group G is cyclic if there is some element $a \in G$ that generates G.*

Subgroup

Notation:

- a^n under multiplication $a^n = \overbrace{a.a.\cdots.a}^{n-times}$
- a^n under addition $a^n = n.a = \underbrace{a + a + \cdots + a}_{n-times}$
- $a.b^{-1}$ under addition

Subgroup

Notation:

- a^n under multiplication $a^n = \overbrace{a.a.\cdots .a}^{n-times}$
- a^n under addition $a^n = n.a = \underbrace{a + a + \cdots + a}_{n-times}$
- $a.b^{-1}$ under addition $a - b$

Group

Definition

1. *A group G is finite if $|G|$ or $\# G$ is finite. The number of elements in a finite group is called its order.*
2. *A group G is cyclic if $\exists\ \alpha \in G$ s/t for each $\beta \in G\ \exists$ integer i with $\beta = \alpha^i$. Such an element α is called a generator of G.*
3. *Let $\alpha \in G$. The order of α is defined to be the least positive integer t s/t $\alpha^t = e$, provided that such an integer exists. If such a t does not exist, then the order of α is defined to be ∞.*

Subgroup

Example

1. *Consider the multiplicative group* $\mathbb{Z}_{19}^{*} = \{1, 2, \cdots, 18\}$ *of order 18.*

Subgroup	Generators	Order
$(\{1\}, \cdot)$	1	1
$(\{1, 18\}, \cdot)$	18	2
$(\{1, 7, 11\}, \cdot)$	7, 11	3
$(\{1, 7, 8, 11, 12, 18\}, \cdot)$	8, 12	6
$(\{1, 4, 5, 6, 7, 9, 11, 16, 17\}, \cdot)$	4, 5, 6, 9, 16, 17	9
$(\mathbb{Z}_{19}^{*}, \cdot)$	2, 3, 10, 13, 14, 15	18

2. *Consider the multiplicative group* $(\mathbb{Z}_{26}^{*}, \cdot)$

Coset

Definition

*Let G be a group and $H \leq G$. For $a, b \in G$, we say that a is **congruent to** $b \mod H$, i.e., $a \equiv b \mod H$ if $a.b^{-1} \in H$.*

Lemma

The relation $a \equiv b \mod H$ is an equivalence relation.

Definition

If $H \leq G, a \in G$, then

$$Ha = \{ha \mid h \in H\} \ [aH = \{ah \mid h \in H\}].$$

Ha is called a right [left] coset of H in G.

Coset

Lemma

If $H \leq G$, then

$$Ha = \{x \in G \mid a \equiv x \mod H\}$$

Coset

Lemma

If $H \leq G$, then

$$Ha = \{x \in G \mid a \equiv x \mod H\}$$

Proof.

Let $[a] = \{x \in G \mid a \equiv x \mod H\}$. First, we prove that $Ha \subset [a]$.
If $h \in H$, $ha \in H$. Now we see $a(ha)^{-1} = a(a^{-1}h^{-1}) = h^{-1} \in H$, $\because H \leq G$.
By definition of congruence, $ha \in [a]$ for every $h \in H$ and so $Ha \subset [a]$.

Next we assume that $x \in [a]$. Thus $ax^{-1} \in H$, so $(ax^{-1})^{-1} = xa^{-1} \in H$, i.e., $xa^{-1} = h$ for some $h \in H$.
$(xa^{-1})a = ha \Rightarrow x = ha$.
Thus, $[a] \subset Ha$.

Thus, we have $[a] = Ha$.

Coset

Lemma

If $H \leq G$, then

$$Ha = \{x \in G \mid a \equiv x \mod H\}$$

Proof.

Let $[a] = \{x \in G \mid a \equiv x \mod H\}$. First, we prove that $Ha \subset [a]$.
If $h \in H$, $ha \in H$. Now we see $a(ha)^{-1} = a(a^{-1}h^{-1}) = h^{-1} \in H, \because H \leq G$.
By definition of congruence, $ha \in [a]$ for every $h \in H$ and so $Ha \subset [a]$.

Next we assume that $x \in [a]$. Thus $ax^{-1} \in H$, so $(ax^{-1})^{-1} = xa^{-1} \in H$, i.e., $xa^{-1} = h$ for some $h \in H$.
$(xa^{-1})a = ha \Rightarrow x = ha$.
Thus, $[a] \subset Ha$.

Thus, we have $[a] = Ha$. □

Thus, any 2 right cosets of H in G are either identical or have no element in common.

Coset

Exercise

Prove that there exists a bijection $f : aH \to Hb$ *and hence there exists a bijection from* $aH \leftrightarrow bH$*, for any* $a, b \in G$.

Coset

Exercise

Prove that there exists a bijection $f : aH \to Hb$ and hence there exists a bijection from $aH \leftrightarrow bH$, for any $a, b \in G$.

Solution

Hint:

- $f : aH \to Hb$ given by $u \mapsto a^{-1}ub$
- *Prove that f is injective as well as onto.*

Coset

Exercise

Prove that there exists a bijection $f : aH \to Hb$ and hence there exists a bijection from $aH \leftrightarrow bH$, for any $a, b \in G$.

Solution

Hint:

- $f : aH \to Hb$ given by $u \mapsto a^{-1}ub$
- *Prove that f is injective as well as onto.*
- *By taking $b = e$, there is a bijection $f_a : aH \to H$.*
- *So, there is a bijection $f_b : bH \to H$.*
- *Then $f_b^{-1} \circ f_a : aH \to bH$ is a bijection.*

Coset

Proposition

Let G be a group and $H \leq G$ & $a, b \in G$. The following are equivalent:

i) $a.H = b.H$

ii) $a^{-1}b \in H$ [or $b^{-1}a \in H$]

iii) $a \in b.H$ [or $b \in a.H$]

Coset

Proposition

Let G be a group and $H \leq G$ & $a, b \in G$. The following are equivalent:

i) $a.H = b.H$
ii) $a^{-1}b \in H$ [or $b^{-1}a \in H$]
iii) $a \in b.H$ [or $b \in a.H$]

Proof.

Hint:

- $(i) \Rightarrow (ii)$
  $b \in bH = aH$. So, $\exists\, h \in H \ni b = ah$
- $(ii) \Rightarrow (iii)$
  $b^{-1}a \in H \Rightarrow \exists\, h \in H \ni b^{-1}a = h$
- $(iii) \Rightarrow (i)$
  $\because a \in bH \therefore a = bh_0$, for some $h_0 \in H$. Now, PT $aH \subset bH$ & $bH \subset aH$

□

Coset

Theorem

Let G be a group and $H \leq G$. For each $a \in G$,

- i) $a \in aH$
- ii) *For any pair $a, b \in G$, either $aH = bH$ or $aH \cap bH = \phi$*
- iii) $\bigcup\{aH \ni a \in G\} = G$
- iv) $\{aH \ni a \in G\}$ *is a partition of G.*

Coset

Theorem

Lagrange's Theorem: *If* G *is a finite group &* $H \leq G$ *, then*

$$\#H \mid \#G \; [or \;\; \circ(H) \mid \circ(G)]$$

Hence, if $a \in G$*, the order of* a *divides* $\#G$*.*

Coset

Theorem

Lagrange's Theorem: *If G is a finite group & $H \leq G$, then*

$$\#H \mid \#G \; [or \;\; \circ(H) \mid \circ(G)]$$

Hence, if $a \in G$, the order of a divides $\#G$.

Proof.

- Let $x_1H, x_2H, \ldots$ be the set of distinct left cosets of H in G
- $\bigcup_{i=1}^{k} x_iH = G$ and $x_iH \cap x_jH = \phi$ for $i \neq j$
- $\because |x_iH| = |H| = m$ (say)
- $\therefore |G| = \sum_{i=1}^{k} |x_iH| = \sum_{i=1}^{k} m = mk = n$ (say)

$$\#H \mid \#G$$

□

Subgroup

Corollary

1. *Let* $(G, \cdot)$ *be a finite group of order* p*, where* p *is a prime. Then* G *is cyclic and hence abelian.*
2. *Let* $(G, \cdot)$ *be a finite group and* $x \in G$ *be an arbitrary element. Then* $order\ of\ x$ *is a divisor of* $order\ of\ G$*.*
3. *Let* p *be a prime number and* $\gcd(a, p) = 1$*, where* $a \in \mathbb{N}$*. Then* $a^{p-1} \equiv 1 \mod p$*.*
4. *Let* p *be prime. Then* $(p-1)! \equiv -1 \mod p$*.*

Subgroup

Proof.

- We know that $(\mathbb{Z}_p^*, \cdot)$ is a group of order $p - 1$.
- Show that the only element of order 2 in $\mathbb{Z}_p^*$ is

Subgroup

Proof.

- We know that $(\mathbb{Z}_p^*, \cdot)$ is a group of order $p-1$.
- Show that the only element of order 2 in $\mathbb{Z}_p^*$ is $p-1$

Subgroup

Proof.

- We know that $(\mathbb{Z}_p^*, \cdot)$ is a group of order $p-1$.
- Show that the only element of order 2 in $\mathbb{Z}_p^*$ is $p-1$
- Consider

$$2.3\ldots(p-2) = 1,$$

$\because$ none of these elements are self inverse.

- Thus, we have

$$\begin{aligned}(p-2)! &\equiv 1 \mod p\\ (p-1)! &\equiv (p-1) \mod p\\ &\equiv -1 \mod p\end{aligned}$$

Cyclic Group

Theorem

Every subgroup H of a cyclic group G is also cyclic.

In fact, if G is a cyclic group of order n, then for each positive divisor d of n, G contains exactly one subgroup of order d.

- Let $\langle a \rangle = G$.
- If H is $\{e\}$, then there is nothing to prove. So, we assume $H \neq \{e\}$.
- Then $\exists\ u \in H \ni u \neq e$
- We have now 2 cases:

Case-1: G is infinite cyclic group

- $\exists\ n_0 \ni u = a^{n_0}$.
- $\because u \in H \Rightarrow u^{-1} \in H$ as $H \leq G$
- Let $T = \{n \in \mathbb{N}\ :\ n > 0,\ a^n \in H\}$
- $T \neq \phi$

Cyclic Group

Theorem

Every subgroup H of a cyclic group G is also cyclic.

In fact, if G is a cyclic group of order n, then for each positive divisor d of n, G contains exactly one subgroup of order d.

- Let $\langle a \rangle = G$.
- If H is $\{e\}$, then there is nothing to prove. So, we assume $H \neq \{e\}$.
- Then $\exists\ u \in H \ni u \neq e$
- We have now 2 cases:

Case-1: G is infinite cyclic group

- $\exists\ n_0 \ni u = a^{n_0}$.
- $\because u \in H \Rightarrow u^{-1} \in H$ as $H \leq G$
- Let $T = \{n \in \mathbb{N}\ :\ n > 0,\ a^n \in H\}$
- $T \neq \phi$ as $n_0\ or\ -n_0 \in T$

Cyclic Group

Case-1: G is infinite cyclic group

- $\because \mathbb{N}$ is well-ordered, $\therefore T$ has a least element, say k_0.
- Then $a^{k_0} \in H$ and $1 \leq n < k_0, a^n \notin H$
- Again, let M be a cyclic group generated by a^{k_0}
- Then $\because a^{k_0} \in H$ and H is a subgroup, $M \subset H$
- Now, let $v \in H$. Then $v = a^m$ for $m \in \mathbb{Z}$

  $m = qk_0 + r$, where $0 \leq r < k_0$
- Now, $a^m \in H$ and $a^{qk_0} = (a^{k_0})^q \in H$
  So, $a^{m-qk_0} \in H \Rightarrow a^r \in H$
- By minimal property of k_o we must have $r = 0$. So $m = qk_0$
- Then, $a^m = (a^{k_0})^q \in M$. Then $H \subset M \Rightarrow M = H$.

Thus, H is a cyclic subgroup generated by a^{k_0}.

Cyclic Group

Case-2: G is finite cyclic group of order m

- Then $G = \{e, a, a^2, \dots a^{m-1}\}$.
- Let $T = \{r \in \mathbb{N} \ : \ a^r \in H, \ 1 \leq r \leq m-1\}$
- Then $T \neq \phi \ \because H \neq \phi$.
- Let k_0 be the minimum value of r, s/t $a^r \in H$.
- $a^{k_0} \in H$.
- Then by above H is cyclic subgroup generated by a^{k_0}.

Cyclic Group

Example

1. $(\mathbb{Z}, +)$ *and* $(\mathbb{Z}_n, +)$ *are cyclic groups*
2. $(\mathbb{Z} \times \mathbb{Z}, +)$ *is not cyclic group. However, it is finitely generated.*

Cyclic Group

Example

1. $(\mathbb{Z}, +)$ *and* $(\mathbb{Z}_n, +)$ *are cyclic groups*
2. $(\mathbb{Z} \times \mathbb{Z}, +)$ *is not cyclic group. However, it is finitely generated.* $S = \{(1, 0), (0, 1)\}$ *generates* $\mathbb{Z} \times \mathbb{Z}$
3. $(\mathbb{Q}, +)$ & $(Q^*, \cdot)$ *are not finitely generated.*

Homomorphism

Definition

Let $(G_1, \cdot)$ *and* $(G_2, \cdot)$ *be groups and* $f : G_1 \to G_2$ *be a function. Then*

1. f *is said to be a homomorphism iff for each* $a, b \in G_1$,
$$f(a.b) = f(a).f(b).$$
2. *A homomorphism* f *is said to be monomorphism (epimorphism) iff* f *is injective (surjective).*
3. *A homomorphism* f *is said to be isomorphism iff* f *is both monomorphism and an epimorphism.*

Homomorphism

Proposition

Let G_1, G_2, G_3 *be groups and* $f : G_1 \to G_2$ & $g : G_2 \to G_3$ *be homomorphisms.*

Then $g \circ f : G_1 \to G_3$ *is also a homomorphism.*

Further, $g \circ f$ *is a monomorphism (epimorphism) if* g & f *are both injective (surjrctive).*

Thus, in particular if f & g *are isomorphisms, so is* $g \circ f$.

Also, if f *is isomorphism from* $G_1 \to G_2$*, then* $f^{-1} : G_2 \to G_1$ *is also an isomorphism.*

Homomorphism

Proposition

Let G_1, G_2, G_3 be groups and $f : G_1 \to G_2$ & $g : G_2 \to G_3$ be homomorphisms.

Then $g \circ f : G_1 \to G_3$ is also a homomorphism.

Further, $g \circ f$ is a monomorphism (epimorphism) if g & f are both injective (surjrctive).

Thus, in particular if f & g are isomorphisms, so is $g \circ f$.

Also, if f is isomorphism from $G_1 \to G_2$, then $f^{-1} : G_2 \to G_1$ is also an isomorphism.

Note: Let C be collections of groups. Define $G_1 \sim G_2$ $(G_i \in C)$ iff $\exists$ an isomorphism $f : G_1 \to G_2$. Verify that $\sim$ is an equivalence relation.

Homomorphism

Proposition

Let G_1, G_2, G_3 be groups and $f : G_1 \to G_2$ & $g : G_2 \to G_3$ be homomorphisms.

Then $g \circ f : G_1 \to G_3$ is also a homomorphism.

Further, $g \circ f$ is a monomorphism (epimorphism) if g & f are both injective (surjrctive).

Thus, in particular if f & g are isomorphisms, so is $g \circ f$.

Also, if f is isomorphism from $G_1 \to G_2$, then $f^{-1} : G_2 \to G_1$ is also an isomorphism.

Note: Let C be collections of groups. Define $G_1 \sim G_2$ $(G_i \in C)$ iff $\exists$ an isomorphism $f : G_1 \to G_2$. Verify that $\sim$ is an equivalence relation.

Two isomorphic groups are absolutely indistinguishable. The main problem of group theory is to decide whether to given groups are isomorphic or not

Homomorphism

Exercise

Let P be the set of all polynomials with integer coefficient. Then $(P, +)$ is a abelian group. Show that $(P, +)$ is isomorphic to $(\mathbb{Q}^*, \cdot)$. [$(P, +) \cong (\mathbb{Q}^*, \cdot)$]

Homomorphism

Exercise

Let P be the set of all polynomials with integer coefficient. Then $(P,+)$ is a abelian group. Show that $(P,+)$ is isomorphic to $(\mathbb{Q}^*,\cdot)$. [$(P,+)\cong(\mathbb{Q}^*,\cdot)$]

Solution

- *Let $\{p_n\}_{n=0}^{\infty}$ be the set of all primes enumerated as*

$$p_0 < p_1 < p_2 < \cdots$$

- *Now, we define $f:(P,+)\to(\mathbb{Q}^*,\cdot)$ as follows:*
  for $p(x)\in P$, with $p(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$

$$f(p(x)) = p_0^{a_0}.p_1^{a_1}.p_2^{a_2}\ldots p_n^{a_n}$$

- *Show that f is an isomorphism.*

Detailed Study of Cyclic Group

Theorem

Let $(G, \cdot)$ be a cyclic group[a]. Then

(i) $(G, \cdot) \cong (\mathbb{Z}, +)$ *iff* G *is infinite*

(ii) $(G, \cdot) \cong (\mathbb{Z}_n, +)$ *iff* G *is finite and* $|G| = n$.

[a] This is the complete characterization theorem for cyclic group

Detailed Study of Cyclic Group

Theorem

Let $(G, \cdot)$ be a cyclic group[a]. Then

1. $(G, \cdot) \cong (\mathbb{Z}, +)$ *iff* G *is infinite*
2. $(G, \cdot) \cong (\mathbb{Z}_n, +)$ *iff* G *is finite and* $|G| = n$.

[a] This is the complete characterization theorem for cyclic group

Proof.

Let G be a cylic group generated by a. Then $G = \{a^n \ : \ n \in \mathbb{Z}\}$. Then two cases can arise

Case-1: $a^n \neq a^m$ for $n \neq m$

Consider the function $f : (\mathbb{Z}, +) \to (G, \cdot)$ given by $m \mapsto a^m$

Case-2: $\exists\, n, m \in \mathbb{Z} \ni a^n = a^m$

Consider the function $f : (\mathbb{Z}_n, +) \to (G, \cdot)$ given by $\bar{m} \mapsto a^{\bar{m}}$

□

Cyclic Group

Exercise

1. *Let* G *be a group.*
   - (a) *If the order of* $a \in G$ *is* t, *then the order of* a^k *is* $\frac{t}{gcd(t,k)}$.
   - (b) *If* G *is a cyclic group of order* n & $d \mid n$, *then* G *has exactly* $\phi(d)$ *elements of order* d. *In particular,* G *has* $\phi(n)$ *generators.*
2. *Let* G_1, G_2 *be cyclic group of order* m, n *respectively and* $\gcd(m,n) = 1$. *Then* $G_1 \times G_2$ *is a cyclic group of order* mn.

   If $\gcd(m,n) \neq 1$, $G_1 \times G_2$ *is never cyclic.*

Normal Subgroup

Definition

If $H \leq G$, the index of H in G is the number of distinct right (or left) cosets of H in G.

We denote it by $i_G(H)$. In case G is a finite group,

$$i_G(H) = \frac{\circ(G)}{\circ(H)}.$$

Normal Subgroup

Definition

If $H \leq G$, the index of H in G is the number of distinct right (or left) cosets of H in G.

We denote it by $i_G(H)$. In case G is a finite group,

$$i_G(H) = \frac{\circ(G)}{\circ(H)}.$$

Definition

Let G be a group and H be a subgroup of G. Then H is said to be a normal [or invariant] subgroup of G iff for each $x \in G$, $xH = Hx$. [$H \trianglelefteq G$]

Normal Subgroup

Definition

If $H \leq G$, the index of H in G is the number of distinct right (or left) cosets of H in G.

We denote it by $i_G(H)$. In case G is a finite group,

$$i_G(H) = \frac{\circ(G)}{\circ(H)}.$$

Definition

Let G be a group and H be a subgroup of G. Then H is said to be a normal [or invariant] subgroup of G iff for each $x \in G$, $xH = Hx$. [$H \trianglelefteq G$]

If G is abelian, then every subgroup is normal.

Normal Subgroup

- If G is non-abelian, it may happen that $aH \neq Ha$ for some $a \in G$.
- Consider the group $(S_3, \circ)$

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

- Let

$$H = \left\{ \rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \& a = \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Quotient Group

Theorem

Let G be a group and H be a normal subgroup of G. Then the G/H of left cosets of H in G is a group under operation of set product.

Proof.

Hint:

- Let xH & $yH \in G/H$. Prove that $(xH)(yH) \in G/H$
- The element $H = eH$ is the identity element of G/H
- Prove that $x^{-1}H$ is the inverse of xH

□

Definition

The G/H is called the quotient group of G by the normal subgroup H.

Quotient Group

Exercise

Let $(\mathbb{Z}, +)$ *be the additive group of integers. Any subgroup of* $\mathbb{Z}$ *is of the form* $n\mathbb{Z}$ *for* $n \in \mathbb{Z}^+$. *Then* $n\mathbb{Z}$ *is a normal subgroup.*

Show that $(\mathbb{Z}/n\mathbb{Z}, +) = (\mathbb{Z}_n, +)$.

Proposition

Let $(G_1, \cdot), (G_2, \cdot)$ *be two groups and* $f : G_1 \to G_2$ *be a homomorphism. Then*

(i) $f(e_1) = e_2$, *where* e_1, e_2 *are the identities of* G_1, G_2 *respectively.*

(ii) *For each* $x \in G_1$, $f(x^{-1}) = (f(x))^{-1}$

(iii) *If* $T \leq G_1$, $f(T) \leq G_2$

First Isomorphism Theorem

Theorem

Let G_1 & G_2 *be two groups and* $f : G_1 \to G_2$ *be a homomorphism.*

Let $K = \{x \in G_1 \ : \ f(x) = e_2\}$ *denote the kernel of* f

Then,

(i) $K \trianglelefteq G_1$

(ii) *The quotient group* G_1/K *is isomorphic to image of* $f = f(G_1)(\subset G_2)$ *under the following map*

$$\tilde{f} : G_1/K \to G_2 \; defined \; by \; \tilde{f}(xK) = f(x)$$

Second Isomorphism Theorem

Theorem

Let $(G, \cdot)$ *be a group and* H & $K \leq G$ *of which* $K \trianglelefteq G$.

Then,

(i) $H.K \leq G$

(ii) $H \cap K \trianglelefteq H$.

(iii) $H.K/K \cong H/H \cap K$

Third Isomorphism Theorem

Theorem

Let $(G, \cdot)$ *be a group and* $H \ \& \ K \trianglelefteq G$ *s/t* $K \subset H$.

Then the quotients groups $G/K, G/H,$ *and* H/K *are defined and* H/K *is a normal subgroup of* G/K *and further*

$$G/H \cong (G/K)/(H/K)$$

Outline

Rings

Definition

A ***ring*** $(R, +, \cdot)$ *is a set* R *with 2 binary operations addition* $+$ *and multiplication* $\cdot$ *defined on* R *s/t the following conditions are satisfied:*

1. (i) $(R, +)$ *is an abelian group*
2. (ii) *multiplication* $\cdot$ *is associative*
3. (iii) *For all* $a, b, c \in R$ *the* ***left distributive law***

$$a.(b + c) = (a.b) + (a.c)$$

and ***right distributive law***

$$(a + b).c = (a.c) + (b.c) \; hold$$

Rings

Definition

1. *If a ring* R *contains the identity element* 1 *w.r.t. to multiplication, i.e.,* $1.a = a.1 = a \; \forall \; a \in R$*, then we shall describe* R *as a ring with unit element or ring with identity.*
2. *If the multiplication* $\cdot$ *is commutative on* R*, i.e.,* $a.b = b.a \; \forall \; a, b \in R$*, then we call* R *is a commutative ring.*
3. *If* R *satisfied both the above conditions, the we say* R *is a commutative ring with identity.*

Rings

Example

1. $R = (\mathbb{Z}, +, \cdot)$ – *the set of integers under the usual rules of addition and multiplication forms a ring.* R *is commutative ring with identity*[a].
2. R *is the set of even integers under the usual rules of addition and multiplication forms a ring.* R *is commutative ring but has no identity element.*
3. *For* $n \geq 1$, *the set* $\mathbb{Z}_n$ *under modular addition and modular multiplication forms a ring.*
   - (a) *For* $n = 6$, *the set* $\mathbb{Z}_6$ *under modular addition and modular multiplication forms a ring.*
   - (b) *For* $n = 7$, *the set* $\mathbb{Z}_7$ *under modular addition and modular multiplication forms a ring.*

[a] Hilbert first introduced the term **ring**

Rings

Example

4 *The set* $\mathbb{Q}$ *of rational numbers under the usual rules of addition and multiplication forms a ring.*

5 *The set* $\mathbb{R}$ *of real numbers under the usual rules of addition and multiplication forms a ring.*

6 *The set* $\mathbb{C}$ *of complex numbers under the usual rules of addition and multiplication forms a ring.*

7 *Let* $M_n(R)$ *be the collection of all* $n \times n$ *matrices having elements of* R*. Then* $M_n(R)$ *forms a non-commutative ring with matrix addition and matrix multiplication*

(a) $M_n(\mathbb{Z}), M_n(\mathbb{Q}), M_n(\mathbb{R}),\ \&\ M_n(\mathbb{C})$ *form rings under matrix addition and matrix multiplication*

Rings

Example (Ring of Quaternions)

Let Q be the sent of all symbols of the form $\alpha_0 + \alpha_1.i + \alpha_2.j + \alpha_3.k$, where all $\alpha_i \in \mathbb{R}$ and

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Let $\alpha, \beta \in Q$ and $\alpha = \alpha_0 + \alpha_1.i + \alpha_2.j + \alpha_3.k$ and $\beta = \beta_0 + \beta_1.i + \beta_2.j + \beta_3.k$.

We define

$\alpha = \beta \iff \alpha_i = \beta_i \;\; for\ i = 0, 1, 2, 3.$

$\alpha + \beta = (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1).i + (\alpha_2 + \beta_2).j + (\alpha_3 + \beta_3).k$

$$\alpha.\beta = (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)i + (\alpha_0\beta_2 - \alpha_1\beta_3 + \alpha_2\beta_0 + \alpha_3\beta_1)j + (\alpha_0\beta_3 + \alpha_1\beta_2 - \alpha_2\beta_1 + \alpha_3\beta_0)k$$

Q forms a non-commutative ring under the operations defined above.

Rings

Definition

1. *If* R *is a commutative ring and* $a(\neq 0) \in R$, *then* a *is said to be a zero-divisor, if* $\exists\ b \in R$ *and* $b \neq 0$ *s/t* $a.b = 0$.

Rings

Definition

1. *If R is a commutative ring and $a(\neq 0) \in R$, then a is said to be a zero-divisor, if $\exists\ b \in R$ and $b \neq 0$ s/t $a.b = 0$.*

   For example in $\mathbb{Z}_6$, $2, 3, 4$ are zero-divisors.

2. *A commutative ring is an integral domain if it has no zero-divisors.*

Rings

Definition

1. *If R is a commutative ring and $a(\neq 0) \in R$, then a is said to be a zero-divisor, if $\exists\, b \in R$ and $b \neq 0$ s/t $a.b = 0$.*

   For example in $\mathbb{Z}_6$, $2, 3, 4$ are zero-divisors.

2. *A commutative ring is an integral domain if it has no zero-divisors.*

   For example, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ & $\mathbb{Z}_7$ are integral domains.

3. *A ring is said to be a division ring (or skew field) if its non-zero elements form a group under multiplication.*

Rings

Definition

1. *If R is a commutative ring and $a(\neq 0) \in R$, then a is said to be a zero-divisor, if $\exists\ b \in R$ and $b \neq 0$ s/t $a.b = 0$.*

   For example in $\mathbb{Z}_6$, $2, 3, 4$ are zero-divisors.

2. *A commutative ring is an integral domain if it has no zero-divisors.*

   For example, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ & $\mathbb{Z}_7$ are integral domains.

3. *A ring is said to be a division ring (or skew field) if its non-zero elements form a group under multiplication.*

   For example, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and ring of quaternions Q are division rings

Rings & Fields

Definition

The characteristic of an integral domain R is defined as the smallest positive integer m s/t $m.a = 0$ for all $a \in R$.

The characteristic of an integral domain R is defined 0, if we don't have such m.

Definition

A field is a commutative division ring.

*A **field** $(F, +, \cdot)$ satisfies the following conditions:*

(i) $(F, +)$ *is an abelian group*

(ii) $(F \setminus \{0\}, \cdot)$ *is also an abelian group*

(iii) *For all $a, b, c \in F$ the **distributive law***

$$a.(b + c) = (a.b) + (a.c) \;\; hold$$

Rings

Lemma

If R is a ring, then for all $a, b \in R$

- (i) $a.0 = 0.a = 0$
- (ii) $a(-b) = (-a)b = -(ab)$
- (iii) $(-a)(-b) = ab$

If, in addition, R has an identity element 1, then

- (iv) $(-1)a = -a$
- (v) $(-1)(-1) = 1$

Rings & Fields

Lemma

A finite integral domain is a field.

Rings & Fields

Lemma

A finite integral domain is a field.

Proof.

- Let D be a finite integral domain.
- To prove D is a field we must show:
  - $\exists\ 1 \in D$ s/t $a.1 = a\ \forall\ a \in D$
  - For every $a \neq 0 \in D,\ \exists\ b \in D$ s/t $a.b = 1$

Rings & Fields

Lemma

A finite integral domain is a field.

Proof.

- Let D be a finite integral domain.
- To prove D is a field we must show:
  - $\exists\ 1 \in D$ s/t $a.1 = a\ \forall\ a \in D$
  - For every $a \neq 0 \in D,\ \exists\ b \in D$ s/t $a.b = 1$
- Let $x_1, x_2, \ldots x_n$ be all the elements of D, and $a \neq 0 \in D$.
- Consider the elements $x_1 a, x_2 a, \ldots x_n a \in D$.
- **Claim:** they are all distinct!

Rings & Fields

Lemma

A finite integral domain is a field.

Proof.

- Let D be a finite integral domain.
- To prove D is a field we must show:
  - $\exists\ 1 \in D$ s/t $a.1 = a\ \forall\ a \in D$
  - For every $a \neq 0 \in D,\ \exists\ b \in D$ s/t $a.b = 1$
- Let $x_1, x_2, \dots x_n$ be all the elements of D, and $a \neq 0 \in D$.
- Consider the elements $x_1 a, x_2 a, \dots x_n a \in D$.
- **Claim:** they are all distinct!
- By the pigeonhole principle, $\exists\ i_0$ for which we will have $x_{i_0} a = a$.
- Prove that x_{i_0} is the multiplicative identity, i.e., for any $y \in D,\ y.x_{i_0} = y$

□

Rings & Fields

Corollary

If p is a prime number, then $\mathbb{Z}_p$ is a field.

Rings & Fields

Corollary

If p is a prime number, then $\mathbb{Z}_p$ is a field.

Note: $\mathbb{Z}_n$ never forms a field if n is composite

Exercise

If D is an integral domain and D is of finite characteristic, prove that the characteristic of D is a prime number.

Rings

Example

Let R be a ring and x be an indeterminate. The polynomial ring $R[x]$ is defined to be the set of all formal sums $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$, where $a_i \in R$ are called the coefficients of x^i rsp.

Given two polynomials $f(x) = \sum_{i=0}^{n} a_i x^i$ & $g(x) = \sum_{i=0}^{m} b_i x^i \in R[x]$

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i,$$

where we have implicitly assumed that $m \leq n$ and we set $b_i = 0$, for $i > m$ and

$$f(x).g(x) = \sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_{i-j} b_j x^i \right)$$

$R[x]$ becomes a ring, with 0 given as the polynomial with zero coefficients.
If R has identity, $1 \neq 0$ then $R[x]$ has identity, $1 \neq 0, 1$ is the polynomial whose constant coefficient is 1 and other terms are 0.

Rings

Example

Solve $x^2 - 5x + 6 = 0$ *in* Z_{12}.

Rings

Example

Solve $x^2 - 5x + 6 = 0$ *in* Z_{12}.

Solution

$$x^2 - 5x + 6 = (x-2)(x-3) =$$

Rings

Example

Solve $x^2 - 5x + 6 = 0$ *in* Z_{12}.

Solution

$$x^2 - 5x + 6 = (x-2)(x-3) = (x+10)(x+9) = 0$$

$$2.6 = 6.2 = 3.4 = 4.3 = 3.8 = 8.3 = 4.6 = 6.4 = 4.9 = 9.4$$
$$= 6.6 = 6.8 = 8.6 = 6.10 = 10.6 = 8.9 = 9.8 = 0$$

Rings

Example

Solve $x^2 - 5x + 6 = 0$ *in* Z_{12}.

Solution

$$x^2 - 5x + 6 = (x-2)(x-3) = (x+10)(x+9) = 0$$

$$2.6 = 6.2 = 3.4 = 4.3 = 3.8 = 8.3 = 4.6 = 6.4 = 4.9 = 9.4$$
$$= 6.6 = 6.8 = 8.6 = 6.10 = 10.6 = 8.9 = 9.8 = 0$$

Exercise

1. *Find all the solution of the equation* $x^2 + 2x + 4 = 0$ *in* $\mathbb{Z}_6$
2. *Solve the equation* $3x = 2$ *in* $\mathbb{Z}_{23}$

Applications to $ax \equiv b \mod m$

Theorem

Let $m \in \mathbb{N}$ *and* $a \in \mathbb{Z}_m$ *s/t* $\gcd(a, m) = 1$. *For each* $b \in \mathbb{Z}_m$, *the equation* $ax = b$ *has unique solution in* $\mathbb{Z}_m$.

Applications to $ax \equiv b \mod m$

Theorem

Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}_m$ s/t $\gcd(a, m) = 1$. For each $b \in \mathbb{Z}_m$, the equation $ax = b$ has unique solution in $\mathbb{Z}_m$.

Theorem

Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}_m$. Let $d = \gcd(a, m)$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ iff $d \mid b$. When $d \mid b$, the equation has exactly d solutions in $\mathbb{Z}_m$.

Applications to $ax \equiv b \mod m$

Theorem

Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}_m$ s/t $\gcd(a, m) = 1$. For each $b \in \mathbb{Z}_m$, the equation $ax = b$ has unique solution in $\mathbb{Z}_m$.

Theorem

Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}_m$. Let $d = \gcd(a, m)$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ iff $d \mid b$. When $d \mid b$, the equation has exactly d solutions in $\mathbb{Z}_m$.

Proof.

- Let $s \in \mathbb{Z}_m$ be a solution of the equation $ax = b$ in $\mathbb{Z}_m$
- $as - b = qm$ in $\mathbb{Z}$

  $b = as - qm$

  $d \mid (as - qm)$
- Thus, a solution s can exist only if $d \mid b$

□

Applications to $ax \equiv b \mod m$

Theorem

Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}_m$. Let $d = \gcd(a, m)$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ iff $d \mid b$. When $d \mid b$, the equation has exactly d solutions in $\mathbb{Z}_m$.

Applications to $ax \equiv b \mod m$

Theorem

Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}_m$. Let $d = \gcd(a, m)$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ iff $d \mid b$. When $d \mid b$, the equation has exactly d solutions in $\mathbb{Z}_m$.

Proof.

- Suppose $d \mid b$, $\Rightarrow b = b_1 d$
- $\because \gcd(a, m) = d, \therefore a = a_1 d \ \& \ m = m_1 d$
- Then the equation $ax = b$ in $\mathbb{Z}_m$ can be written as $ax - b = qm$ in $\mathbb{Z}$
- $ax - b = qm \Rightarrow d(a_1 x - b_1) = dqm_1$
- Now, $m \mid (ax - b) \iff m_1 \mid (a_1 x - b_1)$
- Thus the solution s of $ax = b$ in $\mathbb{Z}_m$ are precisely the solution of $a_1 x = b_1$ in $\mathbb{Z}_{m_1}$
- Now, $s \in \mathbb{Z}_{m_1}$ is the $!$ solution of $a_1 x = b_1$ in $\mathbb{Z}_{m_1}$
- The numbers $\in \mathbb{Z}_m$ that reduces to $s \mod m_1$

$$s, s + m_1, s + 2m_1, \ldots, s + (d - 1)m_1$$

Applications to $ax \equiv b \mod m$

Theorem

Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}_m$. Let $d = \gcd(a, m)$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ iff $d \mid b$. When $d \mid b$, the equation has exactly d solutions in $\mathbb{Z}_m$.

Proof.

- Suppose $d \mid b$, $\Rightarrow b = b_1 d$
- $\because \gcd(a, m) = d, \therefore a = a_1 d \;\&\; m = m_1 d$
- Then the equation $ax = b$ in $\mathbb{Z}_m$ can be written as $ax - b = qm$ in $\mathbb{Z}$
- $ax - b = qm \Rightarrow d(a_1 x - b_1) = dqm_1$
- Now, $m \mid (ax - b) \iff m_1 \mid (a_1 x - b_1)$
- Thus the solution s of $ax = b$ in $\mathbb{Z}_m$ are precisely the solution of $a_1 x = b_1$ in $\mathbb{Z}_{m_1}$
- Now, $s \in \mathbb{Z}_{m_1}$ is the $!$ solution of $a_1 x = b_1$ in $\mathbb{Z}_{m_1}$
- The numbers $\in \mathbb{Z}_m$ that reduces to $s \mod m_1$

$$s, s + m_1, s + 2m_1, \ldots, s + (d-1)m_1$$

Thus, there are exactly d solutions of the equation in $\mathbb{Z}_m$.

□

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An **affine cipher :**

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$p_i \mapsto (a.p_i + b) \mod 26.$$

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An **affine cipher :**

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$p_i \mapsto (a.p_i + b) \mod 26.$$

Example

- *Encrypt* ***COLLEGE*** *using* $a = 5$ *and* $b = 4$
- *Convert* ***C O L L E G E*** *in numeric form*

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An **affine cipher :**

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$

$$p_i \mapsto (a.p_i + b) \mod 26.$$

Example

- *Encrypt* ***COLLEGE*** *using* $a = 5$ *and* $b = 4$
- *Convert* ***C O L L E G E*** *in numeric form*

$$2\ 14\ 11\ 11\ 4\ 6\ 4$$

- *Apply the affine function*

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An **affine cipher :**

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$p_i \mapsto (a.p_i + b) \mod 26.$$

Example

- *Encrypt* ***COLLEGE*** *using* $a = 5$ *and* $b = 4$
- *Convert* ***C O L L E G E*** *in numeric form*

$$2\ 14\ 11\ 11\ 4\ 6\ 4$$

- *Apply the affine function* *14 22 7 7 24 8 24*
- *Cipher text is*

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An **affine cipher :**

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$p_i \mapsto (a.p_i + b) \mod 26.$$

Example

- *Encrypt* ***COLLEGE*** *using* $a = 5$ *and* $b = 4$
- *Convert* ***C O L L E G E*** *in numeric form*

$$2\ 14\ 11\ 11\ 4\ 6\ 4$$

- *Apply the affine function* *14 22 7 7 24 8 24*
- *Cipher text is* ***OWHHYIY***

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An affine cipher is a simple substitution where

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x \mapsto (a.x + b) \mod 26.$$

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An affine cipher is a simple substitution where

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x \mapsto (a.x + b) \mod 26.$$

Exercise

1. *Let* $f_{(a,b)}$ & $f_{(c,d)}$ *be two affine ciphers s/t*

$$f_{(a,b)}(x) \equiv (a.x + b) \mod 26$$
$$f_{(c,d)}(x) \equiv (c.x + d) \mod 26$$

Is $f_{(c,d)} \circ f_{(a,b)}$ *a stronger encryption scheme than* $f_{(a,b)}$*?*

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An affine cipher is a simple substitution where

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$

$$x \mapsto (a.x + b) \mod 26.$$

Exercise

1. *Let* $f_{(a,b)}$ & $f_{(c,d)}$ *be two affine ciphers s/t*

$$f_{(a,b)}(x) \equiv (a.x + b) \mod 26$$

$$f_{(c,d)}(x) \equiv (c.x + d) \mod 26$$

   Is $f_{(c,d)} \circ f_{(a,b)}$ *a stronger encryption scheme than* $f_{(a,b)}$*?*

2. *How many functions of type* $f_{(a,b)}$ *are there for affine cipher in* $\mathbb{Z}26$*?*

Rings

Theorem

In the ring $\mathbb{Z}_n$, the zero-divisors are precisely those non-zero elements that are not relatively prime to n.

Corollary

If p is prime, then $\mathbb{Z}_p$ has no zero-divisor

Theorem

The cancellation laws holds in a ring R iff R has no zero-divisor.

Homomorphism

Definition

A mapping ϕ from the ring R into the ring R' is said to be a homomorphism if

1. (i) $\phi(a+b) = \phi(a) + \phi(b)$
2. (ii) $\phi(a.b) = \phi(a).\phi(b)$

Definition

A mapping ϕ from the ring R into the ring R' is said to be a isomorphism if ϕ is a homomorphism as well as one-to-one and onto.

Homomorphism

Lemma

If ϕ is a homomorphism of R into R', then

(i) $\phi(0) = 0$

(ii) $\phi(-a) = -\phi(a)\ \forall\ a \in R$

Homomorphism

Lemma

If ϕ is a homomorphism of R into R', then

(i) $\phi(0) = 0$

(ii) $\phi(-a) = -\phi(a)\ \forall\ a \in R$

Definition

If ϕ is a homomorphism of R into R' then the kernel of phi, $I(\phi)$, is the set of all elements $a \in R$ s/t $\phi(a) = 0$, the zero-element of R'.

Homomorphism

Lemma

If ϕ is a homomorphism of R into R' with kernel $I(\phi)$, then

(i) *$I(\phi)$ is a subgroup of R under addition.*

(ii) *If $a \in I(\phi)$ and $r \in R$ then both $a.r, r.a \in I(\phi)$.*

Homomorphism

Lemma

If ϕ is a homomorphism of R into R' with kernel $I(\phi)$, then

- (i) $I(\phi)$ *is a subgroup of* R *under addition.*
- (ii) *If* $a \in I(\phi)$ *and* $r \in R$ *then both* $a.r, r.a \in I(\phi)$.

Example

Let $J(\sqrt{2})$ *be all real numbers of the form* $m + n\sqrt{2}$ *where* $m, n \in \mathbb{Z}$; $J(\sqrt{2})$ *forms a ring under the usual addition andmultiplication of real numbers. (Verify!)*

Define $\phi : J(\sqrt{2}) \to J(\sqrt{2})$ *by*

$$\phi(m + n\sqrt{2}) = m - n\sqrt{2}.$$

ϕ *is a homomorphism of* $J(\sqrt{2})$ *onto* $J(\sqrt{2})$ *and its kernel* $I(\phi)$, *consists only of 0. (Verify!)*

Ideals and Quotient Rings

Definition

A non-empty subset I of R is said to be a (two-sided) ideal of R if

(i) *I is a subgroup of R under addition.*

(ii) *For every $u \in I$ and $r \in R$, both $ur, \ \& \ ru \in I$.*

Ideals and Quotient Rings

Lemma

If I is an ideal of the ring R, then R/I is a ring and is a homomorphic image of R.

Ideals and Quotient Rings

Lemma

If I is an ideal of the ring R, then R/I is a ring and is a homomorphic image of R.

Proof.

Hint:

- R/I is the set of all the distinct cosets of I in R
- R/I consists of all the cosets $a + I$, where $a \in R$.
- R/I is automatically a group under addition $(a + I) + (b + I) = (a + b) + I$.
- Define the multiplication in R/I as $(a + I)(b + I) = ab + I$
- Define homomorphism $\phi : R \to R/I$ by $\phi(a) = a + I$ for every $a \in R$.
- Prove that kernel of ϕ is exactly I.

□

Ideals and Quotient Rings

Lemma

If I is an ideal of the ring R, then R/I is a ring and is a homomorphic image of R.

Proof.

Hint:

- R/I is the set of all the distinct cosets of I in R
- R/I consists of all the cosets $a+I$, where $a \in R$.
- R/I is automatically a group under addition $(a+I)+(b+I)=(a+b)+I$.
- Define the multiplication in R/I as $(a+I)(b+I)=ab+I$
- Define homomorphism $\phi : R \to R/I$ by $\phi(a)=a+I$ for every $a \in R$.
- Prove that kernel of ϕ is exactly I.

□

If R is commutative then so is R/I. If R has the identity element 1, then R/I has the identity $1+I$

Ideals and Quotient Rings

Theorem

Let R, R' be rings and ϕ be a homomorphism of R onto R' with kernel I. Then R' is isomorphic to R/I.

Moreover, there is a one-to-one correspondence between the set of ideals of R' and the set of ideals of R which contain I.

This correspondence can be achieved by associating with an ideal I' in R' the ideal I in R is defined by $I = \{x \in R \mid \phi(x) \in I'\}$. R/I is isomorphic to R'/I'.

Ideals and Quotient Rings

Lemma

Let R be a commutative ring with identity whose only ideals are (0) and R itself. Then R is a field.

Ideals and Quotient Rings

Lemma

Let R be a commutative ring with identity whose only ideals are (0) and R itself. Then R is a field.

Proof.

- Suppose that $a \neq 0$ is in R. Consider the set $Ra = \{xa \mid x \in R\}$.
- **Claim:** Ra is an ideal of R.
- Ra is an additive subgroup of R.
- If $r \in R,\ u \in Ra,\ ru = r(r_1a) = (rr_1)a \in Ra$. Ra is an ideal of R.
- $Ra = (0)$ *or* $Ra = R$. $\because 0 \neq a = 1a \in Ra,\ Ra \neq (0)$; thus, we have $Ra = R$.
- $\because 1 \in R$ so, it can be realized as a multiple of a; $\exists\ b \in R$ s/t $ba = 1$.

□

Ideals and Quotient Rings

Definition

*An ideal $M \neq R$ in a ring R is said to be a **maximal ideal** of R if whenever U is an ideal of R s/t $M \subset U \subset R$, then either $R = U$ or $M = U$.*

Ideals and Quotient Rings

Definition

An ideal $M \neq R$ in a ring R is said to be a ***maximal ideal*** *of R if whenever U is an ideal of R s/t $M \subset U \subset R$,then either $R = U$ or $M = U$.*

Exercise

Let $R = \mathbb{Z}$ be the ring of integers, and let U be an ideal of R. $\because U \leq R$ we know that $U = n_0\mathbb{Z}$; we write this as $U = (n_0)$. What values of n_0 lead to maximal ideals?

Ideals and Quotient Rings

Solution

- *First, we assume* p *is prime* $\Rightarrow P = (p)$ *is a maximal ideal of* R.
  - *If* U *is an ideal of* R *and* $P \subset U$, *then* $U = (n_0)$ *for some integer* n_0
  - $\because p \in P \subset U, p = mn_0$ for some $m \in \mathbb{Z}$
    $\because p$ is a prime $\Rightarrow n_0 = 1$ or $n_0 = p$
  - *If* $n_0 = p$, *then* $P \subset U = (n_0) \subset P, \Rightarrow U = P$
  - *If* $n_0 = 1$,*then* $1 \in U$, *hence* $r = 1r \in U \forall\ r \in R$ *whence* $U = R$

Ideals and Quotient Rings

Solution

- *Now, we assume $M = (n_0)$ is a maximal ideal of $R \Rightarrow n_0$ must be prime.*
  - ***Claim:** n_0 must be a prime*
  - *If $n_0 = ab$, where $a, b \in \mathbb{N}$, then $U = (a) \supset M$, hence $U = R$ or $U = M$.*
    - *If $U = R$, then $a = 1 \Rightarrow n_0$ is prime*
    - *If $U = M$, then $a \in M$ and so $a = rn_0$ for some integer r,*
      $\because$ every element of M is a multiple of n_0
    - *But then $n_0 = ab = rn_0b, \Rightarrow rb = 1$, so that $b = 1, n_0 = a$.*
      Thus, n_0 is a prime number.

Ideals and Quotient Rings

Example (Maximal Ideal)

Let R *be the ring of all the real-valued, continuous functions on the closed unit interval* $[0, 1]$.

Let

$$M = \{f(x) \in R \mid f(1/2) = 0\}.$$

M *is certainly an ideal of R. Moreover, it is a maximal ideal of* R.

Ideals and Quotient Rings

Theorem

If R is a commutative ring with identity and M is an ideal of R, then M is a maximal ideal of $R \iff R/M$ is a field.

Ideals and Quotient Rings

Theorem

If R is a commutative ring with identity and M is an ideal of R, then M is a maximal ideal of $R \iff R/M$ is a field.

Proof.

- Suppose, first, R/M is a field.
  - $\because R/M$ is a field its only ideals are (0) and R/M itself.
  - There is a one-to-one correspondence between the set of ideals of R/M and the set of ideals of R which contain M.
  - The ideal M of R corresponds to the ideal (0) of R/M whereas the ideal R of R corresponds to the ideal R/M of R/M in this one-to-one mapping.
  - Thus there is no ideal between M and R other than these two, whence M is a maximal ideal.

□

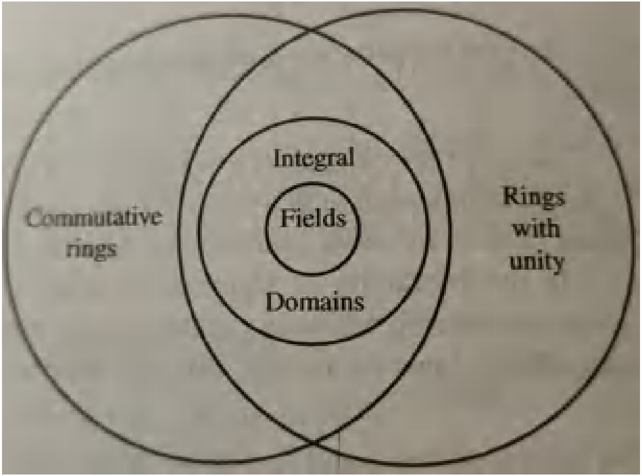
Ideals and Quotient Rings

Proof.

- Now, assume that M is a maximal ideal of R
  - $\because$ M is a maximal ideal of R, R/M has only (0) and itself as ideals.
  - Furthermore R/M is commutative with identity element since R enjoys both these properties.
  - By the lemma, we can say that R/M is a field.

$\square$

Ideals and Quotient Rings



The Field of Quotients of an ID

Definition

*A ring R can be **imbedded** in a ring R' if there is an isomorphism*[a] *of R into R'.*

*R' will be called an **over-ring** or **extension** of R if R can be imbedded in R'.*

---

[a] If R & R' have identity element, then this isomorphism takes 1 onto 1'.

The Field of Quotients of an ID

Definition

A ring R can be ***imbedded*** *in a ring R' if there is an isomorphism*[a] *of R into R'.*

R' will be called an ***over-ring*** *or* ***extension*** *of R if R can be imbedded in R'.*

[a] If R & R' have identity element, then this isomorphism takes 1 onto 1'.

- Let D be our integral domain. Let a/b denotes all quotients where $a, b \in D$ and $b \neq 0$
- Define:
  - $\frac{a}{b} = \frac{c}{d} \iff ad = bc$
  - $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
  - $\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}$

The Field of Quotients of an ID

- $\mathcal{M} = \{(a, b) \mid a, b \in D \;\&\; b \neq 0\}$
- Define a relation on $\mathcal{M}$ as follows:

$$(a, b) \sim (c, d) \iff ad = bc.$$

- Prove that $\sim$ is an equivalence relation on $\mathcal{M}$
- Let $[a, b]$ be the equivalence class in $\mathcal{M}$ of (a, b).
- Let F be the set of all such equivalence classes $[a, b]$ where $a, b \in D$ and $b \neq 0$.
- Prove that F is a field where

$$[a, b]^{-1} = [b, a], \because \; a \neq 0$$

The Field of Quotients of an ID

Theorem

Every integral domain can be imbedded in a field.

Euclidean Rings

Definition

An integral domain R *is said to be a* *Euclidean ring* *if for every* $a \neq 0$ *in* R *there is defined a non-negative integer* $d(a)$ *s/t*

(i) $\forall\ a, b \in R$, both non-zero, $d(a) \leq d(ab)$.

(ii) For any $a, b \in R$, both non-zero, $\exists\ q, r \in R$ s/t $a = qb + r$ where either $r = 0$ or $d(r) < d(b)$.

Euclidean Rings

Definition

An integral domain R is said to be a Euclidean ring if for every $a \neq 0$ in R there is defined a non-negative integer $d(a)$ s/t

1. (i) $\forall\ a, b \in R$, *both non-zero,* $d(a) \leq d(ab)$.
2. (ii) *For any* $a, b \in R$, *both non-zero,* $\exists\ q, r \in R$ *s/t* $a = qb + r$ *where either* $r = 0$ *or* $d(r) < d(b)$.

Note:

- We do not assign a value to $d(0)$.
- $d(a) =$ absolute value of a acts as the required function.

Euclidean Rings

Theorem

Let R be a Euclidean ring and let A be an ideal of R. Then $\exists\ a_0 \in A$ s/t A consists exactly of all a_0x as x ranges over R.

Euclidean Rings

Theorem

Let R be a Euclidean ring and let A be an ideal of R. Then $\exists\ a_0 \in A$ s/t A consists exactly of all a_0x as x ranges over R.

Proof.

- If A just consists of the element 0, put $a_0 = 0$
- Thus, we assume that there is an $a \neq 0$ in A.
- Pick an $a_0 \in A$ s/t $d(a_o)$ is minimal.
- $\because a \in A$, by the properties of Euclidean rings there exist $q, r \in R$ s/t $a = qa_0 + r$ where $r = 0$ or $d(r) < d(a_0)$.
- $\because a_0 \in A$ and A is an ideal of $R, qa_0 \in A$.

  $\Rightarrow a - qa_0 \in A$; but $r = a - qa_0$, whence $r \in A$.
- If $r \neq 0$ then $d(r) < d(a_0)$, giving us an element $r \in A$ whose d-value is smaller than that of a_0, in contradiction to our choice of $a_0 \in A$ of minimal d-value.

□

Euclidean Rings

Definition

An integral domain R with identity is a ***principal ideal ring*** *if every ideal A in R is of the form $A = (a)$ for some $a \in R$, where the notation $(a) = \{xa \mid x \in R\}$ to represent the ideal of all multiples of a.*

Euclidean Rings

Definition

An integral domain R with identity is a ***principal ideal ring*** *if every ideal A in R is of the form $A = (a)$ for some $a \in R$, where the notation $(a) = \{xa \mid x \in R\}$ to represent the ideal of all multiples of a.*

Exercise

A Euclidean ring possesses the identity element.

Euclidean Rings

Definition

An integral domain R with identity is a ***principal ideal ring*** *if every ideal A in R is of the form $A = (a)$ for some $a \in R$, where the notation $(a) = \{xa \mid x \in R\}$ to represent the ideal of all multiples of a.*

Exercise

A Euclidean ring possesses the identity element.

Definition

If $a \neq 0$ and b are in a commutative ring R then a is said to divide b if $\exists$ a $c \in R$ s/t $b = ac$. We shall use the symbol $a \mid b$ to represent the fact that a divides b and $a \nmid b$ to mean that a does not divide b.

Euclidean Rings

Definition

If $a, b \in R$ *then* $d \in R$ *is said to be a greatest common divisor of* a *and* b *if*

(i) $d \mid a$ & $d \mid b$.

(ii) *Whenever* $c \mid a$ *and* $c \mid b$ *then* $c \mid d$.

Euclidean Rings

Definition

If $a, b \in R$ then $d \in R$ is said to be a greatest common divisor of a and b if

1. (i) $d \mid a \;\&\; d \mid b$.
2. (ii) *Whenever $c \mid a$ and $c \mid b$ then $c \mid d$.*

Lemma

Let R be a Euclidean ring. Then any two elements $a \;\&\; b \in R$ have a greatest common divisor d. Moreover $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.

Euclidean Rings

Proof.

- Let $A = \{ra + sb \ : \ r, s \in R\}$
- Prove that A is an ideal of R.
- Since A is an ideal of R, $\therefore A$ is principle ideal ring.
- $\exists\, d \in A$ s/t every element in A is a multiple of d.
- $\because R$ is a Euclidean ring, R contains identity.
- Thus, $a = 1.a + 0.b \in A, \ b = 0.a + 1.b \in A$
- They are both multiples of d, whence $d \mid a \ \& \ d \mid b$.
- Finally, suppose that $c \mid a \ \& \ c \mid b$; then $c \mid \lambda a + \mu b = d$.

□

Euclidean Rings

Definition

Let R be a commutative ring with identity. An element $a \in R$ is a ***unit*** *in R if $\exists$ an element $b \in R$ s/t $ab = 1$.*

Do not confuse a ***unit*** *with a* ***unit element****. A unit in a ring is an element whose inverse is also in the ring.*

Exercise

Let R be an integral domain with identity and suppose that for $a, b \in R$ both $a \mid b, \ \& \ b \mid a$. Then $a = ub$, where u is a unit in R.

Definition

Let R be a commutative ring with identity. Two elements $a \ \& \ b \in R$ are said to be associates if $b = ua$ for some unit $u \in R$.

Euclidean Rings

Definition

In the Euclidean ring R a nonunit π is said to be a prime element of R if whenever $\pi = ab$, where $a, b \in R$, then one of a or b is a unit in R.

Lemma

Let R be a Euclidean ring. Then every element in R is either a unit in R or can be written as the product of a finite number of prime elements of R.

Definition

In the Euclidean ring R, a & $b \in R$ are said to be relatively prime if $\gcd(a, b)$ is a unit of R.

Euclidean Rings

Lemma

Let R be a Euclidean ring. Suppose that for $a, b, c \in R,\ a \mid bc$ but $\gcd(a, b) = 1$. Then $a \mid c$.

Lemma

If π is a prime element in the Euclidean ring R and $\pi \mid ab$ where $a, b \in R$ then π divides at least one of a or b.

Theorem (Unique Factorization Theorem)

Let R be a Euclidean ring and $a \neq 0$ a nonunit in R. Suppose that

$$a = \pi_1 \pi_2 \ldots \pi_n = \pi'_1 \pi'_2 \ldots \pi'_m,$$

where the π_i & π'_j are prime elements of R. Then $n = m$ and each $\pi_i,\ 1 \leq i \leq n$ is an associate of some $\pi'_j,\ 1 \leq j \leq m$ and conversely each π'_k is an associate of some π_q.

Euclidean Rings

Lemma

Let R *be a Euclidean ring. Suppose that for* $a, b, c \in R,\ a \mid bc$ *but* $\gcd(a, b) = 1$*. Then* $a \mid c$*.*

Lemma

If π *is a prime element in the Euclidean ring* R *and* $\pi \mid ab$ *where* $a, b \in R$ *then* π *divides at least one of* a *or* b*.*

Theorem (Unique Factorization Theorem)

Let R *be a Euclidean ring and* $a \neq 0$ *a nonunit in* R*. Suppose that*

$$a = \pi_1 \pi_2 \ldots \pi_n = \pi'_1 \pi'_2 \ldots \pi'_m,$$

where the π_i & π'_j *are prime elements of* R*. Then* $n = m$ *and each* $\pi_i,\ 1 \leq i \leq n$ *is an associate of some* $\pi'_j,\ 1 \leq j \leq m$ *and conversely each* π'_k *is an associate of some* π_q*.*

Euclidean Rings

Every nonzero element in a Euclidean ring R can be uniquely written (up to associates) as a product of prime elements or is a unit in R.

Euclidean Rings

Every nonzero element in a Euclidean ring R can be uniquely written (up to associates) as a product of prime elements or is a unit in R.

Lemma

The ideal $A = (a_0)$ is a maximal ideal of the Euclidean ring R iff a_0 is a prime element of R.

Polynomial Rings

- Let F be a field. By the ring of polynomials in the indeterminate, x, denoted by $F[x]$,

$$F[x] = \{a_0 + a_1 x + \ldots + a_n x^n, \; : \; n \in \mathbb{N} \;\&\; a_i \in \mathbb{F}, \; for\; 0 \leq i \leq n\}.$$

Exercise

$F[x]$ is an integral domain, when F is a field (integral domain)

Theorem

$F[x]$ is a Euclidean ring, when F is a field (Euclidean domain)

Polynomial Rings

Lemma

$F[x]$ is a principal ideal ring, when F is a field

Lemma

Given two polynomials $f(x), g(x) \in F[x]$ and let $d(x) = \gcd(f(x), g(x))$. Then $d(x)$ can be expressed as

$$d(x) = \lambda(x)f(x) + \mu(x)g(x).$$

Polynomial Rings

Lemma

$F[x]$ is a principal ideal ring, when F is a field

Lemma

Given two polynomials $f(x), g(x) \in F[x]$ and let $d(x) = \gcd(f(x), g(x))$. Then $d(x)$ can be expressed as

$$d(x) = \lambda(x)f(x) + \mu(x)g(x).$$

Definition

A polynomial $p(x) \in F[x]$ is said to be irreducible over F if whenever $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$, then one of $a(x)$ or $b(x)$ has degree 0 (i.e., is a constant).

Polynomial Rings

Lemma

Any polynomial in $F[x]$ can be written in a unique manner as a product of irreducible polynomials in $F[x]$.

Lemma

The ideal $A = (p(x))$ in $F[x]$ is a ***maximal ideal*** *iff $p(x)$ is irreducible over F.*

Polynomial Rings

Lemma

Any polynomial in $F[x]$ can be written in a unique manner as a product of irreducible polynomials in $F[x]$.

Lemma

*The ideal $A = (p(x))$ in $F[x]$ is a **maximal ideal** iff $p(x)$ is irreducible over F.*

Definition

The polynomial $f(x) = a_0 + a_1x + \ldots + a_nx^n$, where the $a_0, a_1, a_2, \ldots,$ are integers is said to be primitive if the greatest common divisor of $a_0, a_1, \ldots, a_n$ is 1.

Polynomial Rings

Definition

The content of the polynomial $f(x) = a_0 + a_1x + \ldots + a_nx^n$, where the a_i's are $\in \mathbb{Z}$, is the greatest common divisor of the integers $a_0, a_1, \ldots, a_n$.

Theorem

If the primitive polynomial $f(x)$ can be factored as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients.

Polynomial Rings

Definition

The content of the polynomial $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, where the a_i's are $\in \mathbb{Z}$, is the greatest common divisor of the integers $a_0, a_1, \ldots, a_n$.

Theorem

If the primitive polynomial $f(x)$ can be factored as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients.

Definition

A polynomial is said to be integer monic if all its coefficients are integers and its highest coefficient is 1.

Polynomial Rings

Theorem (THE EISENSTEIN CRITERION)

Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ *be a polynomial with integer coefficients. Suppose that for some prime number* $p, p \nmid a_n, p \mid a_0, p \mid a_1, p \mid a_2, \ldots, p \mid a_{n-1}, p^2 \nmid a_0$*. Then* $f(x)$ *is irreducible over the rationals.*

Polynomial Rings

Lemma

If R is an integral domain, then so is $R[x]$.

Polynomial Rings

Lemma

If R is an integral domain, then so is $R[x]$.

Definition

An element a which is not a unit in R will be called irreducible (or a prime element[a]) if, whenever $a = bc$ with $b, c \in R$, then one of b or c must be a unit in R.

[a] in case of R is a UFD

Polynomial Rings

Definition

An integral domain, R, with identity element is a unique factorization domain (UFD) if any nonzero element in R is either a unit or can be written as the product of a finite number of irreducible elements of R and the the decomposition is unique up to the order and associates of the irreducible elements.

Polynomial Rings

Definition

An integral domain, R, with identity element is a unique factorization domain (UFD) if any nonzero element in R is either a unit or can be written as the product of a finite number of irreducible elements of R and the the decomposition is unique up to the order and associates of the irreducible elements.

Lemma

If R is a unique factorization domain and if $a, b \in R$, then a and b have a greatest common divisor $(a, b) \in R$.

Polynomial Rings

Lemma

If R is a unique factorization domain, then the product of two primitive polynomials in $R[x]$ is again a primitive polynomial in $R[x]$.

Lemma

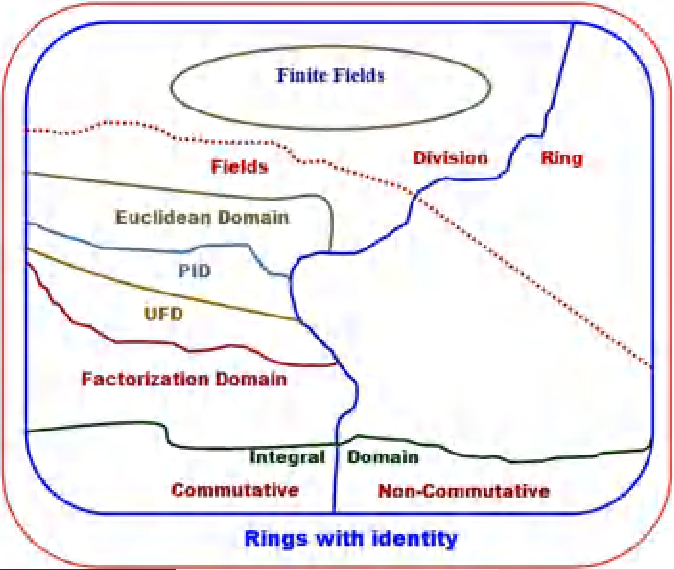
If R is a unique factorization domain and if $p(x)$ is a primitive polynomial in $R[x]$, then it can be factored in a unique way as the product of irreducible elements in $R[x]$.

Polynomial Rings

Theorem

If R is a unique factorization domain, then so is $R[x]$.

Ring Structure



Outline

Vector Spaces

Definition

A non-empty set $\mathbf{V}$ *is said to be a vector space over a field* $\mathbb{F}$, *is denoted by* $(\mathbf{V}, +, \cdot, \mathbb{F})$ *if* $\mathbf{V}$ *is an abelian group under an operation which we denote by* $+$, *and if for every* $\alpha \in \mathbb{F},\ v \in \mathbf{V}$ *there is defined an element, written* $\alpha v \in \mathbf{V}$ *subject to*

(i) $\alpha.(v + w) = \alpha.v + \alpha.w$;

(ii) $(\alpha + \beta).v = \alpha.v + \beta.v$;

(iii) $\alpha.(\beta.v) = (\alpha.\beta).v$;

(iv) $1.v = v$;

or all $\alpha, \beta \in \mathbb{F},\ v, w \in \mathbf{V}$ *(where the* 1 *represents the identity element of* $\mathbb{F}$ *under multiplication).*

Linear Independence and Bases

Definition

If $\mathbf{V}$ is a vector space over $\mathbb{F}$ and if $v_1, \ldots, v_n \in \mathbf{V}$ then any element of the form

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n,$$

*where the $\alpha_i \in \mathbb{F}$, is a **linear combination** of $v_1, \ldots, v_n$ over $\mathbb{F}$.*

Linear Independence and Bases

Definition

If $\mathbf{V}$ is a vector space over $\mathbb{F}$ and if $v_1, \ldots, v_n \in \mathbf{V}$ then any element of the form

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n,$$

*where the $\alpha_i \in \mathbb{F}$, is a **linear combination** of $v_1, \ldots, v_n$ over $\mathbb{F}$.*

Definition

*If S is a nonempty subset of the vector space $\mathbf{V}$, then $L(S)$, the **linear span** of S, is the set of all linear combinations of finite sets of elements of S.*

Linear Independence and Bases

Lemma

$L(S)$ *is a subspace of* $\mathbf{V}$.

Linear Independence and Bases

Lemma

$L(S)$ *is a subspace of* $\mathbf{V}$.

Definition

If $\mathbf{V}$ *is a vector space and if* $v_1, \ldots, v_n$ *are in* $\mathbf{V}$*, we say that they are* ***linearly dependent*** *over* $\mathbb{F}$ *if there exist elements* $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$*, not all of them* *0**, s/t*

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n = 0.$$

If the vectors $v_1, \ldots, v_n$ *are not linearly dependent over* $\mathbb{F}$*, they are said to be* ***linearly independent*** *over* $\mathbb{F}$.

Linear Independence and Bases

Lemma

If $v_1, \ldots, v_n \in \mathbf{V}$ are linearly independent, then every element in their linear span has a ! representation in the form $\lambda_1 v_1 + \ldots + \lambda_n v_n$ with the $\lambda_i \in \mathbb{F}$.

Theorem

If $v_1, \ldots, v_n$ are in $\mathbf{V}$ then either they are linearly independent or some v_k is a linear combination of the preceding ones, $v_1, \ldots, v_{k-1}$.

Corollary

If $\mathbf{V}$ is a finite-dimensional vector space, then it contains a finite set $v_1, \ldots, v_n$ of linearly independent elements whose linear span is $\mathbf{V}$.

Linear Independence and Bases

Definition

A subset S o f a vector space $\mathbf{V}$ is called a ***basis*** *of $\mathbf{V}$ if S consists of linearly independent elements*[a] *and $\mathbf{V} = L(S)$.*

[a] Any finite number of elements in S is linearly independent

Corollary

If $\mathbf{V}$ is a finite-dimensional vector space and if $u_1, \ldots, u_m$ span $\mathbf{V}$ then some subset of $u_1, \ldots, u_m$ forms a basis of $\mathbf{V}$.

Corollary

If $\mathbf{V}$ is finite-dimensional over $\mathbb{F}$ then any two bases of $\mathbf{V}$ have the same number of elements.

Linear Independence and Bases

Corollary

If $\mathbf{V}$ is finite-dimensional over $\mathbb{F}$ then $\mathbf{V}$ is isomorphic to $\mathbb{F}^{(n)}$ for a unique integer n; in fact, n is the number of elements in any basis of $\mathbf{V}$ over $\mathbb{F}$.

Definition

The integer n in the above Corollary is called the ***dimension*** *of $\mathbf{V}$ over $\mathbb{F}$.*

Outline

Field Extension

Definition

If $\mathbb{K}$ is a subfield of a field $\mathbb{M}$, then $\mathbb{M}$ is called an ***extension of the field*** *$\mathbb{K}$.*

Definition

Let $\mathbb{M}$ be an extension of a field $\mathbb{K}$. An element $u \in \mathbb{M}$ is said to be ***algebraic*** *over $\mathbb{K}$ if u satisfies a polynomial over $\mathbb{K}$ i.e., if elements $c_0, c_1, \ldots, c_n$ not all zero exit in $\mathbb{K}$ such that*

$$c_0 + c_1.u + \ldots + c_n.u^n = 0.$$

Field Extension

Definition

*An element of $\mathbb{M}$ which is not algebraic is said to be **transcendental** over $\mathbb{K}$.*

Definition

*An extension of a field $\mathbb{K}$ is called an **algebraic extension** if every member of it is algebraic over $\mathbb{K}$. Otherwise if $\exists$ a single element in the extension which is transcendental over $\mathbb{K}$, the extension is called a **transcendental** extension of $\mathbb{K}$.*

Extension as a Vector Space

- An extension $\mathbb{M}$ of a field $\mathbb{K}$ can be looked upon as a vector space over $\mathbb{K}$.

Extension as a Vector Space

- An extension $\mathbb{M}$ of a field $\mathbb{K}$ can be looked upon as a vector space over $\mathbb{K}$.
- $\because$ $\mathbb{M}$ is a field, $\therefore$ it is already an additive commutative group.
- Now the product of an element of $\mathbb{K}$ and an element of an element of $\mathbb{M}$ is a product of two elements of $\mathbb{M}$ and is therefore an element of $\mathbb{M}$.
- Hence, $\mathbb{M}$ is a vector space over $\mathbb{K}$.

Definition

If $\mathbb{M}$ is an extension of a field $\mathbb{K}$, then $\mathbb{M}$ may be looked upon as a vector space over $\mathbb{K}$. The dimension of this vector space is called the ***degree of the extension****, and is denoted by $[\mathbb{M} : \mathbb{K}]$.*

Extension as a Vector Space

Theorem (Paul Halmos)

Any finite extension of a field is an algebraic extension of the field.

Extension as a Vector Space

Theorem (Paul Halmos)

Any finite extension of a field is an algebraic extension of the field.

Proof.

- Let $\mathbb{M}$ be a finite extension of a field $\mathbb{K}$ and $[\mathbb{M} : \mathbb{K}] = n$.
- Then for any $u \in \mathbb{M}$, the $(n+1)$ elements $1, u, \ldots, u^n$ must be linearly dependent over $\mathbb{K}$.
- Hence, elements $c_0, c_1, \ldots, c_n$, not all zero exists in $\mathbb{K}$ such that

$$c_0.1 + c_1.u + \cdots + c_n u^n = 0.$$

- This shows that u is an algebraic over $\mathbb{K}$; but u was an arbitrary element of $\mathbb{M}$.
- Thus, it is proved that $\mathbb{M}$ is an algebraic extension of $\mathbb{K}$.

□

Extension as a Vector Space

Exercise

If $\mathbb{M}$ *is an extension of a field* $\mathbb{K}$ *and* $[\mathbb{M} : \mathbb{K}] = 1$, *show that* $\mathbb{M} = \mathbb{K}$.

Extension as a Vector Space

Exercise

If $\mathbb{M}$ *is an extension of a field* $\mathbb{K}$ *and* $[\mathbb{M} : \mathbb{K}] = 1$, *show that* $\mathbb{M} = \mathbb{K}$.

Solution

- $\because [\mathbb{M} : \mathbb{K}] = 1, \therefore$ *for any* $u \in \mathbb{M},\ 1\ \&\ u$ *must be linearly dependent over* $\mathbb{K}$.
- *Hence,* $\exists\ c_0\ \&\ c_1$ *not both zero in* $\mathbb{K}$ *s/t* $c_0.1 + c_1.u = 0$
  Clearly $c_1 \neq 0$, *[*$\because c_1 = 0$ *gives* $c_0 = 0$ *]*
- *Now,* $\because [\mathbb{M} : \mathbb{K}] = 1$ *is finite,* $\therefore$ *every elements of* $\mathbb{M}$ *is algebraic.*
- $\because \mathbb{K}$ *is a field and* $c_1 \neq 0, \therefore c_1^{-1}$ *exists in* $\mathbb{K}$.
- *Now from above equation we see that* $u = -c_1^{-1}c_0 \in \mathbb{K}$ *[*$\because\ \mathbb{K}$ *is a field]*
- $\because u$ *is arbitrary, therefore* $\mathbb{M} \subseteq \mathbb{K}$ *and* $\because \mathbb{M}$ *is an extension of a field* $\mathbb{K}$, $\therefore \mathbb{K} \subseteq \mathbb{M}$.
  Hence we have $\mathbb{M} = \mathbb{K}$.

Extension as a Vector Space

Theorem (Transitivity of Finite Extensions)

If $\mathbb{B}, \mathbb{C}$ & $\mathbb{D}$ *are 3 fields s/t* $\mathbb{B}$ *is a finite extension of* $\mathbb{C}$ *and* $\mathbb{C}$ *is finite extension of* $\mathbb{D}$, *then* $\mathbb{B}$ *is finite extension of* $\mathbb{D}$, *and* $[\mathbb{B} : \mathbb{D}] = [\mathbb{B} : \mathbb{C}] \times [\mathbb{C} : \mathbb{D}]$.

Extension as a Vector Space

Theorem (Transitivity of Finite Extensions)

If $\mathbb{B}, \mathbb{C}$ & $\mathbb{D}$ are 3 fields s/t $\mathbb{B}$ is a finite extension of $\mathbb{C}$ and $\mathbb{C}$ is finite extension of $\mathbb{D}$, then $\mathbb{B}$ is finite extension of $\mathbb{D}$, and $[\mathbb{B} : \mathbb{D}] = [\mathbb{B} : \mathbb{C}] \times [\mathbb{C} : \mathbb{D}]$.

Proof.

- Let $[\mathbb{B} : \mathbb{C}] = m$ & $[\mathbb{C} : \mathbb{D}] = n$. Let $\{u_1, \ldots, u_m\}$ be a basis of $\mathbb{B}$ over $\mathbb{C}$ & $\{v_1, \ldots, v_n\}$ be a basis of $\mathbb{C}$ over $\mathbb{D}$.
- Then any $t \in \mathbb{B}$ is of the form $t = \sum_{i=1}^{n} b_i u_i$, for certain elements $b_1, \ldots, b_m \in C$.
- $\because b_1, \ldots, b_m \in \mathbb{C}$ each of them is a linear combination of $\{v_1, \ldots, v_n\}$ with coefficient from $\mathbb{D}$.
- Let $b_i = \sum_{j=1}^{n} c_{ij} v_j$, where c_{ij}'s $\in \mathbb{D}$. But then $t = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} c_{ij} v_j \right) u_i = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} v_j u_i$

□

Extension as a Vector Space

Proof.

- This shows that the mn elements $v_j u_i$ generate $\mathbb{B}$ over $\mathbb{D}$.
- We show that these elements are independent over $\mathbb{D}$. For this, let $\sum_{i=1}^{m}\sum_{j=1}^{n} d_{ij}v_j u_i = 0$. This can be written as $\sum_{i=1}^{m}\left(\sum_{j=1}^{n} d_{ij}v_j\right)u_i = 0$.
- Since u vectors are independent over $\mathbb{C}$ we get $\sum_{j=1}^{n} d_{ij}v_j = 0$, for $1 \le i \le m$.
- However, v vectors are independent over $\mathbb{D}$ we get $d_{ij} = 0$, for $1 \le i \le m$ & $1 \le j \le n$.
- Hence, the mn vectors $v_j u_i$ are indeed independent over $\mathbb{D}$ showing that these vectors form a basis of $\mathbb{B}$ over $\mathbb{D}$.
- Hence, $[\mathbb{B} : \mathbb{D}] = mn$ and thus $[\mathbb{B} : \mathbb{D}] = [\mathbb{B} : \mathbb{C}] \times [\mathbb{C} : \mathbb{D}]$.

□

Extension as a Vector Space

Exercise

If $\mathbb{B}$ is a finite extension of a field $\mathbb{D}$ and $\mathbb{C}$ is a field intermediate between $\mathbb{B}$ and $\mathbb{D}$, show that $\mathbb{B}$ is a finite extension of $\mathbb{C}$ and $\mathbb{C}$ is a finite extension of $\mathbb{D}$.

Corollary

If $[\mathbb{B} : \mathbb{C}] = p$, a prime number then there cannot be any field properly in between $\mathbb{B}$ and $\mathbb{C}$.

Exercise

1. *If $\mathbb{B}$ and $\mathbb{C}$ are finite extension of a field $\mathbb{D}$ and $\mathbb{D} \subset \mathbb{C} \subset \mathbb{B}$, then show that $\mathbb{B}$ is a finite extension of $\mathbb{D}$.*
2. *If $\mathbb{B}$ is a finite extension of a field $\mathbb{D}$ and $\mathbb{C}$ is a subfield of $\mathbb{B}$ then show that $[\mathbb{C} : \mathbb{D}]$ divides $[\mathbb{B} : \mathbb{D}]$*
3. *The field of complex numbers $\mathbb{C}$ is a finite extension of degree 2 over the real field $\mathbb{R}$.*

Adjunction

- Let $\mathbb{M}$ be an extension of a field $\mathbb{K}$ and let $G \subset \mathbb{M}$.
- Then the intersection of all subfields of $\mathbb{M}$ containing $\mathbb{K}$ and G is the smallest subfield of $\mathbb{M}$ containing $\mathbb{K}$ and G.
- This subfield is denoted by $\mathbb{K}(G)$ and is called the subfield of $\mathbb{M}$ obtained from $\mathbb{K}$ by the **adjunction** of the subset G or simply '$\mathbb{K}$ adjunction G'.
- If G is a finite set equal to $\{a_1, \ldots, a_n\}$ then $\mathbb{K}(G)$ is also written as $\mathbb{K}(a_1, \ldots, a_n)$.

Adjunction

Theorem

If $\mathbb{M}$ is a finite extension of a field $\mathbb{K}$, then $\mathbb{M}$ can be obtained by adjoining a finite number of elements $u_1, \ldots, u_m$ to $\mathbb{K}$ so that $\mathbb{M} = \mathbb{K}(u_1, \ldots, u_m)$ where $u_1, \ldots, u_m$ are algebraic over $\mathbb{K}$.

Adjunction

Theorem

If $\mathbb{M}$ is a finite extension of a field $\mathbb{K}$, then $\mathbb{M}$ can be obtained by adjoining a finite number of elements $u_1, \ldots, u_m$ to $\mathbb{K}$ so that $\mathbb{M} = \mathbb{K}(u_1, \ldots, u_m)$ where $u_1, \ldots, u_m$ are algebraic over $\mathbb{K}$.

Proof.

- $\because$ $\mathbb{M}$ is a finite extension of $\mathbb{K}$ each element of $\mathbb{M}$ is algebraic over $\mathbb{K}$.
- If $\mathbb{M} = \mathbb{K}$ the theorem is vacuously true.
- If $\mathbb{M} \neq \mathbb{K}$ then $\exists$ at least one element $u_1 \in \mathbb{M} \setminus \mathbb{K}$. If $\mathbb{M} = \mathbb{K}(u_1)$ the theorem is proved.
- If $\mathbb{M} \neq \mathbb{K}(u_1)$, $\exists$ at least one element $u_2 \in \mathbb{M} \setminus \mathbb{K}(u_1)$. If $\mathbb{M} = \mathbb{K}(u_1, u_2)$ the theorem is proved.
- If not, we carry on the process and after a finite number of steps we shall arrive at an extension $\mathbb{K}(u_1, \ldots, u_m)$ s/t $\mathbb{M} = \mathbb{K}(u_1, \ldots, u_m)$. $\because$ at each step we arrive at proper extension of the previous one and thus an extension ≥ 2; but $\mathbb{M}$ is of finite degree over $\mathbb{K}$.

Adjunction

Definition

Let $\mathbb{M}$ be an extension of a field $\mathbb{K}$ and u be any element of $\mathbb{M}$. Then the field $\mathbb{K}(u)$ obtained from $\mathbb{K}$ by adjunction of the single element u is called a ***simple extension of*** $\mathbb{K}$.

The extension is called a ***simple algebraic extension*** *or a* ***simple transcendental extension*** *according as u is algebraic or transcendental over $\mathbb{K}$.*

Definition

Let $\mathbb{M}$ be an extension of a field $\mathbb{K}$ and $u \in \mathbb{M}$ be algebraic over $\mathbb{K}$. Then the monic polynomial of the least degree over $\mathbb{K}$ satisfied by u is called the ***minimal polynomial*** *of u over $\mathbb{K}$. If $f(x)$ is the minimal polynomial of u over $\mathbb{K}$, then degree of $(f(x))$ is also called the degree of u over $\mathbb{K}$, written as $deg(u)$ over $\mathbb{K}$.*

Adjunction

Exercise

If p is a prime and $\mathbb{Q}$ the rational field, then show that $\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p} \;:\; a, b \in \mathbb{Q}\}$

Adjunction

Exercise

If p is a prime and $\mathbb{Q}$ the rational field, then show that $\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p} \ : \ a, b \in \mathbb{Q}\}$

Solution

- *Let* $\alpha = \sqrt{p}$. *Then* $\alpha^2 = p$ *i.e.,* $\alpha^2 - p = 0$.
- *Thus,* $\alpha = \sqrt{p}$ *satisfies the polynomial* $x^2 - p$ *over* $\mathbb{Q}$. *But* $\sqrt{p}$ *can't satisfy a polynomial of degree* < 2 *i.e., a polynomial of degree 1 over* $\mathbb{Q} \because \sqrt{p} \notin \mathbb{Q}$.
- *Hence,* $deg \sqrt{p}$ *over* $\mathbb{Q} = 2$.
- *Thus,* $\{1, \sqrt{p}\}$ *forms a basis of* $\mathbb{Q}(\sqrt{p})$ *over* $\mathbb{Q}$.
- *Hence, any number of* $\mathbb{Q}(\sqrt{p})$ *is of the form* $a.1 + b.\sqrt{p}$ *where* $a, b \in \mathbb{Q}$.

Adjunction

Exercise

Find the inverse of $5u + 6$ as a polynomial in u over the rationals given that the minimal polynomial of u over the rationals is $x^2 + 7x - 11$.

Adjunction

Exercise

Find the inverse of $5u + 6$ as a polynomial in u over the rationals given that the minimal polynomial of u over the rationals is $x^2 + 7x - 11$.

Solution

We have $u^2 + 7u - 11 = 0$ *or* $u^2 = -7u + 11$.
Let $au + b$ *be the required inverse of* $5u + 6$.
We must have
$$\begin{aligned} 1 &= (5u + 6)(au + b) \\ &= 5au^2 + (6a + 5b)u + 6b \\ &= 5a(-7u + 11) + (6a + 5b)u + 6b \\ &= (-29a + 5b)u + (55a + 6b) \end{aligned}$$
So, we have $-29a + 5b = 0 \quad \& \quad 55a + 6b = 1$
Therefore the required inverse is $\frac{5}{449}u + \frac{29}{449}$

Algebraic Closure

Definition

Let $\mathbb{M}$ be an extension of a field $\mathbb{K}$. Then the set $\mathbb{E}$ of all elements of $\mathbb{M}$ which are algebraic over $\mathbb{K}$ is a subfield of $\mathbb{M}$ containing $\mathbb{K}$. This field $\mathbb{E}$ is called the ***algebraic closure*** *of $\mathbb{K}$ in $\mathbb{M}$.*

Definition

Let $\mathbb{K}$ be any field. Then an algebraic extension $\bar{\mathbb{K}}$ is said to be ***algebraic closure*** *iff $\bar{\mathbb{K}}$ is algebrically closed over $\mathbb{K}$.*

Note 1: If $\mathbb{F}$ is an algebraically closed field, then the algebraic closure of $\mathbb{F}$ is $\mathbb{F}$ itself.

Note 2: (**Fundamental Theorem of Algebra**) The complex field $\mathbb{C}$ is algebraically closed.

Finite Fields

- A **finite field** is a field $\mathbb{F}$ which contains a finite number of elements.

Finite Fields

- A **finite field** is a field $\mathbb{F}$ which contains a finite number of elements.
- If $\mathbb{F}$ is a finite field, then $\mathbb{F}$ contains p^m elements for some prime p and integer $m \geq 1$.

Finite Fields

- A **finite field** is a field $\mathbb{F}$ which contains a finite number of elements.
- If $\mathbb{F}$ is a finite field, then $\mathbb{F}$ contains p^m elements for some prime p and integer $m \geq 1$.
- For every prime power order p^m, there is a $!$ finite field of order p^m. This field is denoted by $\mathbb{F}_{p^m}$, or sometimes by $GF(p^m)$.

Finite Fields

- A **finite field** is a field $\mathbb{F}$ which contains a finite number of elements.
- If $\mathbb{F}$ is a finite field, then $\mathbb{F}$ contains p^m elements for some prime p and integer $m \geq 1$.
- For every prime power order p^m, there is a $!$ finite field of order p^m. This field is denoted by $\mathbb{F}_{p^m}$, or sometimes by $GF(p^m)$.
- For $m = 1$, $\mathbb{F}_p$ or $GF(p)$ is a field. If p is a prime then $\mathbb{Z}_p$ is a field.

$$\mathbb{F}_p \cong GF(p) \cong \mathbb{Z}_p.$$

Finite Fields

- Let $\mathbb{F}_q$ be a finite field of order $q = p^m$.
  - Then every subfield of $\mathbb{F}_q$ has order p^n, for some n which is a positive divisor of m.
  - Conversely, if n is a positive divisor of m, then there is exactly one subfield of $\mathbb{F}_q$ of order p^n.

Finite Fields

- Let $\mathbb{F}_q$ be a finite field of order $q = p^m$.
  - Then every subfield of $\mathbb{F}_q$ has order p^n, for some n which is a positive divisor of m.
  - Conversely, if n is a positive divisor of m, then there is exactly one subfield of $\mathbb{F}_q$ of order p^n.
- The non-zero elements of $\mathbb{F}_q$ form a group under multiplication called the **multiplicative group** of $\mathbb{F}_q$, denoted by $\mathbb{F}_q^*$.

Finite Fields

- Let $\mathbb{F}_q$ be a finite field of order $q = p^m$.
  - Then every subfield of $\mathbb{F}_q$ has order p^n, for some n which is a positive divisor of m.
  - Conversely, if n is a positive divisor of m, then there is exactly one subfield of $\mathbb{F}_q$ of order p^n.
- The non-zero elements of $\mathbb{F}_q$ form a group under multiplication called the **multiplicative group** of $\mathbb{F}_q$, denoted by $\mathbb{F}_q^*$.
- $\mathbb{F}_q^*$ is a cyclic group of order $q - 1$. Hence $a^q = a, \ \forall \ a \in \mathbb{F}_q$.

Finite Fields

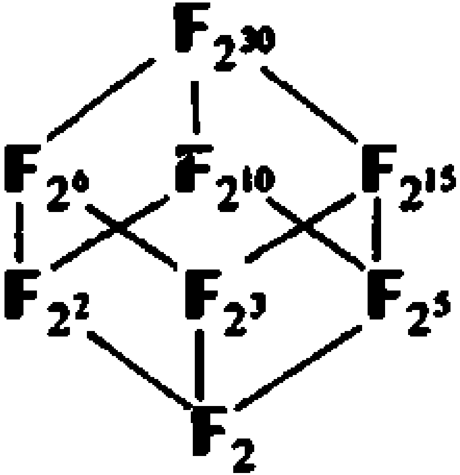
- Let $\mathbb{F}_q$ be a finite field of order $q = p^m$.
  - Then every subfield of $\mathbb{F}_q$ has order p^n, for some n which is a positive divisor of m.
  - Conversely, if n is a positive divisor of m, then there is exactly one subfield of $\mathbb{F}_q$ of order p^n.
- The non-zero elements of $\mathbb{F}_q$ form a group under multiplication called the **multiplicative group** of $\mathbb{F}_q$, denoted by $\mathbb{F}_q^*$.
- $\mathbb{F}_q^*$ is a cyclic group of order $q - 1$. Hence $a^q = a, \ \forall \ a \in \mathbb{F}_q$.
- A generator of the cyclic group $\mathbb{F}_q^*$ is called a **primitive element** or **generator** of $\mathbb{F}_q$.

Finite Fields

Subfields of $\mathbb{F}_{2^{30}}$ and their relation:

Finite Fields

Subfields of $\mathbb{F}_{2^{30}}$ and their relation:

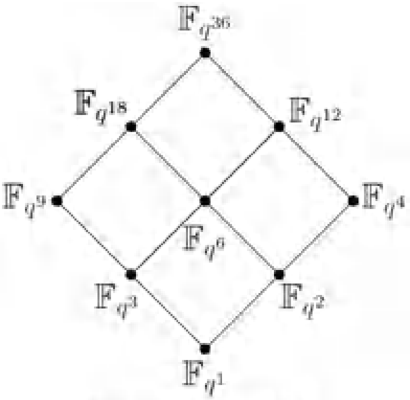


Finite Fields

Subfields of $\mathbb{F}_{q^{36}}$ and their relation:

Finite Fields

Subfields of $\mathbb{F}_{q^{36}}$ and their relation:



The subfields of $\mathbb{F}_{q^{36}}$

Construction of Finite Field of Order p^m

Construction of Finite Field of Order p^m

- First select an irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree m.
- The ideal $< f(x) >$ is

Construction of Finite Field of Order p^m

- First select an irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree m.
- The ideal $< f(x) >$ is a maximal ideal.
- Then $Z_p[x]/ < f(x) >$ is a

Construction of Finite Field of Order p^m

- First select an irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree m.
- The ideal $< f(x) >$ is a maximal ideal.
- Then $Z_p[x]/ < f(x) >$ is a finite field of order p^m.
- For each $m \geq 1$, $\exists$ a monic irreducible polynomial of degree m over $\mathbb{Z}_p$.

  Hence, every finite field has a polynomial basis representation.

Construction of Finite Field of Order p^m

Theorem

The number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n is given by

$$\frac{1}{n}\sum_{d|n}\mu(d)q^{n/d},$$

where μ is Möbius function.

Construction of Finite Field of Order p^m

Theorem

The number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n is given by

$$\frac{1}{n}\sum_{d|n}\mu(d)q^{n/d},$$

where μ is Möbius function.

Definition

TheMöbius function μ is the function on $\mathbb{N}$ defined by

$$\mu(n) = \begin{cases} 1 & if\ n = 1, \\ (-1)^k & if\ n\ is\ the\ product\ of\ k\ distinct\ primes, \\ 0 & if\ n\ is\ divisible\ by\ square\ of\ a\ prime. \end{cases}$$

Construction of Finite Field of Order 2^4

(i) First consider α is a root of the irreducible polynomial $x^4 + x + 1$ over $GF(2)$

(ii) $\alpha^4 + \alpha + 1 = 0 \Rightarrow \alpha^4 = \alpha + 1$

Construction of Finite Field of Order 2^4

(i) First consider α is a root of the irreducible polynomial $x^4 + x + 1$ over $GF(2)$

(ii) $\alpha^4 + \alpha + 1 = 0 \Rightarrow \alpha^4 = \alpha + 1$

$\alpha^0 = 1$	$\alpha^1 = \alpha$	$\alpha^2 = \alpha^2$	$\alpha^3 = \alpha^3$
$\alpha^4 = \alpha + 1$	$\alpha^5 = \alpha^2 + \alpha$	$\alpha^6 = \alpha^3 + \alpha^2$	$\alpha^7 = \alpha^3 + \alpha + 1$
$\alpha^8 = \alpha^2 + 1$	$\alpha^9 = \alpha^3 + \alpha$	$\alpha^{10} = \alpha^2 + \alpha + 1$	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha^{13} = \alpha^3 + \alpha^2 + 1$	$\alpha^{14} = \alpha^3 + 1$	$\alpha^{15} = 1$

Construction of Finite Field of Order 2^4

(i) First consider α is a root of the irreducible polynomial $x^4 + x + 1$ over $GF(2)$

(ii) $\alpha^4 + \alpha + 1 = 0 \Rightarrow \alpha^4 = \alpha + 1$

$\alpha^0 = 1$	$\alpha^1 = \alpha$	$\alpha^2 = \alpha^2$	$\alpha^3 = \alpha^3$
$\alpha^4 = \alpha + 1$	$\alpha^5 = \alpha^2 + \alpha$	$\alpha^6 = \alpha^3 + \alpha^2$	$\alpha^7 = \alpha^3 + \alpha + 1$
$\alpha^8 = \alpha^2 + 1$	$\alpha^9 = \alpha^3 + \alpha$	$\alpha^{10} = \alpha^2 + \alpha + 1$	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha^{13} = \alpha^3 + \alpha^2 + 1$	$\alpha^{14} = \alpha^3 + 1$	$\alpha^{15} = 1$

(iii) Now Consider the irreducible polynomial $x^4 + x^3 + x^2 + x + 1$ or $x^4 + x^3 + 1$ over $GF(2)$.

Computing Multiplicative Inverses in $\mathbb{F}_{p^m}$

Algorithm

Input: a non-zero polynomial $g(x) \in \mathbb{F}_{p^m}$[a].

Output: $g(x)^{-1} \in \mathbb{F}_{p^m}$.

Computing Multiplicative Inverses in $\mathbb{F}_{p^m}$

Algorithm

Input: a non-zero polynomial $g(x) \in \mathbb{F}_{p^m}$[a].

Output: $g(x)^{-1} \in \mathbb{F}_{p^m}$.

1. Use the extended Euclidean algorithm for polynomials to find 2 polynomials $s(x)$ & $t(x) \in \mathbb{Z}_p[x]$ s/t

$$s(x)g(x) + t(x)f(x) = 1.$$

Computing Multiplicative Inverses in $\mathbb{F}_{p^m}$

Algorithm

Input: a non-zero polynomial $g(x) \in \mathbb{F}_{p^m}$[a].

Output: $g(x)^{-1} \in \mathbb{F}_{p^m}$.

1. Use the extended Euclidean algorithm for polynomials to find 2 polynomials $s(x)$ & $t(x) \in \mathbb{Z}_p[x]$ s/t
$$s(x)g(x) + t(x)f(x) = 1.$$
2. *Return*($s(x)$).

[a] The elements of the field $\mathbb{F}_{p^m}$ are represented as $\mathbb{Z}_p[x]/ < f(x) >$, where $f(x) \in \mathbb{Z}_p[x]$ is an irreducible polynomial of degree m over $\mathbb{Z}_p$.

Finite Fields

Definition

An irreducible polynomial $f \in \mathbb{Z}_p[x]$ *of degree* m *is called a* ***primitive polynomial*** *if* α *is a generator of* $\mathbb{F}^*_{p^m}$*, the multiplicative group of all the non-zero elements in* $\mathbb{F}_{p^m} = \mathbb{Z}_p[x]/ < f(x) >$*, where* α *is a root of the polynomial* $f(x)$ *over its extension field.*

Finite Fields

Definition

An irreducible polynomial $f \in \mathbb{Z}_p[x]$ *of degree* m *is called a* ***primitive polynomial*** *if* α *is a generator of* $\mathbb{F}^*_{p^m}$*, the multiplicative group of all the non-zero elements in* $\mathbb{F}_{p^m} = \mathbb{Z}_p[x]/ < f(x) >$*, where* α *is a root of the polynomial* $f(x)$ *over its extension field.*

- The irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree m is a primitive polynomial iff $f(x) \mid x^k - 1$ for $k = p^m - 1$ and for no smaller positive integer k.

Finite Fields

Definition

An irreducible polynomial $f \in \mathbb{Z}_p[x]$ of degree m is called a ***primitive polynomial*** *if α is a generator of $\mathbb{F}^*_{p^m}$, the multiplicative group of all the non-zero elements in $\mathbb{F}_{p^m} = \mathbb{Z}_p[x]/ < f(x) >$, where α is a root of the polynomial $f(x)$ over its extension field.*

- The irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree m is a primitive polynomial iff $f(x) \mid x^k - 1$ for $k = p^m - 1$ and for no smaller positive integer k.
- For each $m \geq 1$, $\exists$ a monic primitive polynomial of degree m over $\mathbb{Z}_p$. In fact, there are precisely $\frac{\phi(p^m-1)}{m}$ such polynomials.

Example

- **Addition (in the field $GF(2^8)$)**

  The sum of two elements is the polynomial with coefficients that are given by the sum modulo 2 of the coefficients of the two terms.

Example

- **Addition (in the field $GF(2^8)$)**

  The sum of two elements is the polynomial with coefficients that are given by the sum modulo 2 of the coefficients of the two terms.

Example

$$57 + 83 = ?$$

Example

- **Addition (in the field $GF(2^8)$)**

  The sum of two elements is the polynomial with coefficients that are given by the sum modulo 2 of the coefficients of the two terms.

Example

$$57 + 83 = ?$$

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2 = D4$$

Example

- **Multiplication**
  Multiplication in $GF(2^8)$ corresponds with multiplication of polynomials modulo an irreducible polynomial over $GF(2)$ of degree 8. For Rijndael, the inventors selected the following irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1 \text{ or } 11B.$$

Example

- **Multiplication**
  Multiplication in $GF(2^8)$ corresponds with multiplication of polynomials modulo an irreducible polynomial over $GF(2)$ of degree 8. For Rijndael, the inventors selected the following irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1 \ or \ 11B.$$

Example

$$57 \times 83 = ?$$

Example

- **Multiplication**
  Multiplication in $GF(2^8)$ corresponds with multiplication of polynomials modulo an irreducible polynomial over $GF(2)$ of degree 8. For Rijndael, the inventors selected the following irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1 \ or \ 11B.$$

Example

$$57 \times 83 = ?$$

$$(x^6 + x^4 + x^2 + x + 1) \times (x^7 + x + 1)$$

$$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$

Example

- **Multiplication**
  Multiplication in $GF(2^8)$ corresponds with multiplication of polynomials modulo an irreducible polynomial over $GF(2)$ of degree 8. For Rijndael, the inventors selected the following irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1 \; or \; 11B.$$

Example

$$57 \times 83 = ?$$

$$(x^6 + x^4 + x^2 + x + 1) \times (x^7 + x + 1)$$

$$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$

$$x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \; mod \; m(x)$$

$$= x^7 + x^6 + 1 = C1$$

References

- John B. Fraleigh,
  A First Course in Abstract Algebra, Pearson, 2014.
- I. N. Herstein,
  Topics in Algebra, John Wiley & Sons, 1975.
- Alko R. Meijer,
  Algebra for Cryptologists, Springer, 2016.
- Gerard O'Regan,
  Guide to Discrete Mathematics: An Accessible Introduction to the History, Theory, Logic and Applications, Springer 2016.

The End

Thanks a lot for your attention!