Groups

September-10-13 10:03 AM

A **binary operation** $*$ on a set S is a map
$*: S \times S \to S$

Write in infix. $S_1 * S_2 = S_3$ instead of $*(S_1, S_2) = S_3$

Group

A group G or $(G, \cdot)$ is a non-empty set endowed with a binary operation $\cdot$ satisfying the following properties:

1) Associativity
   $g \cdot (h \cdot k) = (g \cdot h) \cdot k \ \forall g, h, k \in G$
2) Identity
   $\exists e \in G$ s.t. $e \cdot g = g \cdot e = g \ \ \forall g \in G$
3) Inverse
   $\forall g \in G \ \ \exists g^{-1} \in G$ s.t. $g \cdot g^{-1} = g^{-1} g = e$

Remarks

- We will often write 1 for e
- Sometimes we will use $+$ as our binary operation, in which case we'll write 0 for e

Notation

$M_n(F) =$ all $n \times n$ matrices over the field F
$\mathrm{GL}_n(F) = \{A \in M_n(F) : \det A \neq 0\}$
$\mathrm{SL}_n(F) = \{A \in M_n(F) : \det A = 1\}$

Order

If $x \in G$, we say the **order** of x is the smallest natural number ≥ 1 n, if it exists, such that $x^n = 1 = e$
If no such x exists, we say that x has infinite order.

We write $o(x)$ for the order.
The order of G is just the size of G. i.e., order of $G = |G|$

Conjugates

If $x, y \in G$
Then $y^{-1}xy$ is called the conjugate of x
Fact:
x and $y^{-1}xy$ have the same order
Proof:
$x^n = 1 \Rightarrow (y^{-1}xy)^n = (y^{-1}xy) \ldots (y^{-1}xy) = y^{-1}x^n y = y^{-1}y = 1$

Abelian

A group G is abelian if
$g \cdot h = h \cdot g \ \ \forall g, h \in G$

Dihedral Groups

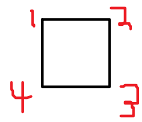
$D_n =$ group of symmetries of a regular n-gon
Let $\sigma =$ rotation by $\frac{2\pi}{n}$ radians
let $\tau =$ reflection about L (line through 1)

Relation

The rule $\tau \cdot \sigma \cdot \tau = \sigma^{-1} \Rightarrow \tau \cdot \sigma^i = \sigma^{-i} \cdot \tau$
is called a relation.
These relations show that any composition of $\sigma's$ and $\tau's$ can be written in one of the forms
$\sigma^i \cdot \tau$ or σ^i

Examples of Groups

1) $\mathbb{Z}, +$, identity $= 0$
2) Field, $+$
3) Let F be a field, let $F^* = F \setminus \{0\}$ then $(F^*, \cdot)$ is a group (with multiplication)
4) $n \times n$ invertible matrices over a field F with multiplication
   $\mathrm{GL}_n(F) = \{A \in M_n(F) : \det A \neq 0\}$
5) "Rubik's cube group"
6) Rotations/reflections that keep the shape of a square



   Can rotate by multiples of 90 degrees or reflect
7) S is a non-empty set
   $\mathrm{Aut}(S) = \{f : S \to S : f \text{ is 1-1 and onto}\}$
   binary operation $=$ composition
   - $f \circ g$

   inverse: $f = f^{-1}$
   $\mathrm{id} = \mathrm{id}(S) = S \ \ \forall s \in S$

8) $S^1 = \{e^{i\theta} : \theta \in [0, 2\pi)\}$
   binary operator $= \cdot$
   $e^{i\theta_1} \cdot e^{i\theta_2} = e^{i(\theta_1 + \theta_2 \bmod 2\pi)}$

Facts

For a group $(G, \cdot)$
1) Identity is unique
2) Inverses are unique
3) $(gh)^{-1} = h^{-1}g^{-1}$
4) Cancellation:
   $ax = ay \Rightarrow x = y$
   $xb = yb \Rightarrow x = y$

Why?
1) Suppose e_1 and e_2 are identities.
   $e_1 = e_1 \cdot e_2 = e_2$
2) Suppose g has two inverses h and k
   $h = h \cdot e = h \cdot (g \cdot k) = (h \cdot g) \cdot k = e \cdot k = k$
3) $(gh)h^{-1}g^{-1} = g(hh^{-1})g^{-1} = gg^{-1} = e$

We can speak unambiguously about products
$g_1 g_2 g_3 = g_1(g_2 g_3) = (g_1 g_2) g_3$
holds for higher n

Example

$G = \left((\mathbb{Z}_{/7\mathbb{Z}})^*, \cdot\right)$
$(\square)^*$ means excluding zeros
What are the orders of
$[1] \to 1$
$[2] \to 3$
$[3] \to 6$
$[4] \to 4$
$[5] \to 6$
$[6] \to 2$

$G = \mathrm{SL}_2(\mathbb{R})$
Let $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$
What is the order of A? 6
$A^2 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$
$A^3 = A^2 A = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$
$A^6 = A^3 A^3 = I$
To find the order more easily, look at the eigenvalues. They should be roots of unity if the element has finite order.

Example

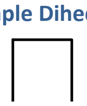
Let G be a group and suppose that every element of G has order 1 or 2.
Show that G is abelian

Proof

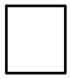
Let $g, h \in G$
Want to show $gh = hg$
We have $1 = (gh)^2 = ghgh \Rightarrow (gh)^{-1} = gh$
$(gh)^{-1} = h^{-1}g^{-1} = hg$
So $gh = hg \ \forall g, h \in G \Rightarrow G$ is abelian

Example Dihedral Group

$D_4 =$



Example Dihedral Group

$D_4 =$ 

$|D_4| = 8$
The vertex 1 can be in 4 places, and 2 can be in 2 places for each.

For D_n, what is $\tau \cdot \sigma \cdot \tau$
$\tau \cdot \sigma \cdot \tau = \sigma^{n-1} = \sigma^{-1}$
Notice that
σ has order n
τ has order 2
$\tau \cdot \sigma^i \cdot \tau = \sigma^{-1}$

Example

$\tau \cdot \sigma^2 \cdot \tau \cdot \sigma^3 \cdot \tau \cdot \tau = \sigma^{-2} \cdot \tau \cdot \tau \cdot \sigma^3 \cdot \tau = \sigma \cdot \tau \cdot \sigma = \sigma \cdot \sigma^{-1} \cdot \tau = \tau$

If we look at all elements in D_n formed by composing σ's and τ's we get $n + n = 2n$ elements. So $|D_n| \geq 2n$
Why are these all?
1 can go in n spots. for each, 2 can go in 2 spots. So $|D_n| \leq 2n$
$\Rightarrow |D_n| = 2n$

Symmetry

September-12-13 10:00 AM

D_n Dihedral group

A regular n-gon will be represented as a graph
$D_n = (V, E)$
$V = \{1,2,\dots,n\}$
$E = \{\{i,j\} : i,j \in V, \quad i - j \equiv \pm 1 \ (mod\ n)\}$

A symmetry of D_n is this setting is a map
$\phi: V \to V$ that is 1-1 and onto and preserves adjacency
$\{i,j\} \in E \Leftrightarrow \{\phi(i), \phi(j)\} \in E$

Lemma 1

Number of symmetries of D_n is $\leq 2n$

Lemma 2

The symmetries
$\{\sigma^i\}_{i=0}^{n-1}, \{\sigma^i \rho\}_{i=0}^{n-1}$
are $2n$ distinct symmetries

Presentation

We call
$\langle \rho, \sigma: \rho^2 = \sigma^n = \text{id}, \quad \rho\sigma = \sigma^{-1}\rho \rangle$
a presentation of D_n

Symmetry Groups

For $n \geq 1$
$S_n = \{\ \sigma: \{1,2,\dots,n\} \to \{1,2,\dots,n\}: \sigma \text{ is 1-1 and onto}\}$
Notice S_n is a group under composition
We technically should write "$\sigma \circ \tau$" but we'll write $\sigma\tau$

Note

Disjoint cycles permute

Proof of Lemma 1

$\exists \leq n$ choices for $\phi(1) \in \{1,2,\dots,n\}$
Say that $\phi(1) = i \in \{1,2,\dots,n\}$
Then $\phi(2) - i \equiv \pm 1 \ (\text{mod } n)$
There are ≤ 2 choices for n
Now by induction on $j = 3,\dots,n$, show that there is at most one choice for $\phi(j)$
So in total there are at most $2n$ symmetries.
■

Last time we constructed two symmetries:
σ, ρ
$\phi(i) \equiv i + 1 \ (\text{mod } n)$
$\rho(1) = 1, \rho(2) = n, \dots$ (reflection)

Proof of Lemma 2

First, if $\sigma^i = \sigma^j$ for $i \neq j, 0 \leq i,j \leq n-1$
Applying σ^{-i} gives $\sigma^{-i} \circ \sigma^i = \sigma^{-i} \circ \sigma^j \Rightarrow id = \sigma^{j-i}$ rotation clockwise by $\frac{2\pi(j-i)}{n} \pm id$
$1 \neq \sigma^{j-i}(1) = 1 + i - i \ (\text{mod } n)$

Similarly, if $i \neq j, 0 \leq i,j \leq n-1$
$\Rightarrow \sigma^i \rho \neq \sigma^j \rho$ since $\sigma^i \neq \sigma^j$ we can cancel ρ
Finally, if $\sigma^i = \sigma^j \rho$
$\Rightarrow \sigma^{-j+i} = \rho$
$\Rightarrow \sigma^{-j+i}(1) = \rho(1)$
$\Rightarrow 1 + i - j \ (\text{mod } n) == 1$
$\Rightarrow i = j \Rightarrow \rho = id$, contradiction.

Remarks

1) This shows that $|D_n| = 2n$
2) This shows that D_n is **generated** as a group by ρ and σ. This means that **every** element of D_n can be expressed as a finite composition (product in group) of elements from $\{\rho, \rho^{-1}, \sigma, \sigma^{-1}\}$
3) The group structure can be completely understood via the relations $\rho^2 = id; \ \ \rho^n = id; \ \ \sigma\rho = \rho\sigma^{-1}$

Question

Show that D_n is not abelian for $n \geq 3$

Answer

$\rho\sigma = \sigma^{-1}\rho$. If D_n were abelian, then we would have
$\rho\sigma = \sigma\rho \Rightarrow \sigma^{-1}\rho = \sigma\rho \Rightarrow \sigma^{-1} = \sigma \Rightarrow \sigma^2 = \text{id}$
$\sigma^2 \neq \text{id}$ for $n \geq 3$

D_2 is abelian
$D_2 = \langle \rho, \sigma : \rho^2 = \sigma^2 = \text{id}, \rho\sigma = \sigma\rho \rangle$
We will see later that
$D_2 \cong \mathbb{Z}_{/2\mathbb{Z}} \times \mathbb{Z}_{\backslash 2\mathbb{Z}}$

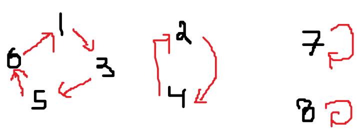
Notes on Symmetry Groups

- $|S_n| = n!$
- Two ways of representing **permutations**

Example $n = 8$

1 2 3 4 5 6 7 8
σ:
1 2 3 4 5 6 7 8

Or could represent in **disjoint cycle notation**



- Representations:
  1) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 2 & 6 & 1 & 7 & 8 \end{pmatrix}$
  2) Disjoint cycle notation: (1 3 5 6)(2 4)(7)(8)
     Or omit 1-cycles: (1 3 5 6)(2 4)

- Disjoint Cycles Permute

Proof

$i_1, \dots, i_s, j_1, \dots, j_t \in \{1,\dots,n\}$ are pairwise distinct
Let $\sigma = (i_1, \dots, i_s) \leftarrow$ this means that if $k \notin \{i_1,\dots,i_s\} \Rightarrow \sigma(k) = k$
Let $\tau = (j_1, \dots, j_t)$
Define $i_{s+1} \coloneqq i_1, \ j_{t+1} \coloneqq j_1$
Look at $\sigma \circ \tau(k) = \begin{cases} i_{a+1} & \text{if } k = i_a \\ j_{b+1} & \text{if } k = j_b \\ k & \text{otherwise} \end{cases} = \tau \circ \sigma(k)$

- The order of a cycle $(i_1, i_2, \dots, i_s)$ is s
- The order of a set of disjoint cycles is the LCM of the orders of the individual cycles
  If $\sigma = \sigma_1 \cdot \dots \cdot \sigma_k, \sigma_1, \dots, \sigma_k$ disjoint cycles of length $l_1, \dots, l_k$, respectively
  Then $\sigma^n = (\sigma_1 \cdots \sigma_k)^n = \sigma_1^n \cdot \sigma_2^n \cdot \dots \cdot \sigma_k^n$
  If $n = lcm(d_1, \dots, d_k) \Rightarrow \sigma_1^n = \sigma_2^n = \dots = \sigma_k^n = \text{id} \Rightarrow \sigma_1^n \cdots \sigma_k^n = \text{id}$
  Show in assignment that $o(\sigma_1 \cdots \sigma_k)$ divides $\text{lcm}(d_1, \dots, d_k)$

But if $1 \leq m = o(\sigma_1, \dots, \sigma_k) < \text{lcm}(d_1, \dots, d_k)$
$\Rightarrow \exists\ i$ such that d_i does not divide m
Then $\sigma_i^m \neq 1$ and since all the cycles are disjoint, suppose $\sigma_i = \left(a_1, \dots, a_{d_i}\right)$
then $\exists j, 1 \leq j \leq d_i$ such that $\sigma_i^m\left(a_j\right) \neq a_j$
$\tau\left(a_j\right) = \sigma_1^m \cdots \sigma_i^m \cdots \sigma_k^m\left(a_j\right) = \sigma_i^m\left(a_j\right) \neq a_j$ so $\tau \neq \text{id}$

Linear Groups

September-12-13 11:00 AM

Field

A field is a set $\neq \emptyset$ with two binary operations $+$ and $\cdot$ such that $(F,+)$ is an abelian group with identity 0 and $(F\backslash\{0\},\cdot)$ is an abelian group with identity 1.
Furthermore, $(a+b)\cdot x = a\cdot x + b\cdot x$

Note

$(\mathbb{Z}\backslash\{0\},\cdot)$ is not a group because $2^{-1} \notin \mathbb{Z}\backslash\{0\}$

$\mathbb{Z}_p = \{[0],\dots,[p-1]\}$ where p is a prime.

Questions

What is the order of $\mathrm{GL}_2(\mathbb{Z}_2)$?

$\begin{pmatrix}\{[0],[1]\} & \{[0],[1]\} \\ \{[0],[1]\} & \{[0],[1]\}\end{pmatrix}$, $\quad |\mathrm{GL}_2(\mathbb{Z}_2)| \leq 16$

$\mathrm{GL}_2(\mathbb{Z}_2) = \left\{\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}, \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}, \begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\1 & 1\end{pmatrix}\right\}$

So $|\mathrm{GL}_2(\mathbb{Z}_2)| = 6$

What is the size of $\mathrm{GL}_n(\mathbb{Z}_p)$

If $n=1$, Answer is $p-1$

In general, the answer is

$(p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1})$

Proof

An $n\times n$ matrix $A = (\vec{v}_1 \quad \vec{v}_2 \quad \cdots \quad \vec{v}_n)$ is invertible $\Leftrightarrow$ columns are linearly independent.

Choose columns one by one, maintaining linear independence.

There are p^n-1 ways of choosing $\vec{v}_1$ (all but $\mathbf{0}$)

For $\vec{v}_2$, can pick anything that is not in $\mathrm{span}(\{\vec{v}_1\})$

span$(\{\vec{v}_1\})$ consists of the p scalar multiples of $\vec{v}_1$, so there are p^n-p choices for $\vec{v}_2$

In general, can pick any $\vec{v}_i$ that is not in $\mathrm{span}(\{\vec{v}_1,\dots,\vec{v}_{i-1}\})$

Since $\vec{v}_1,\dots,\vec{v}_{i-1}$ are all linearly independent, $|\mathrm{span}(\{\vec{v}_1,\dots,\vec{v}_{i-1}\})| = p^{i-1}$

So there are $p^n - p^i$ choices for $\vec{v}_i$

Quaternion Group

Group Q_8 of order 8

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

$i^2 = j^2 = k^2 = -1$

$ij = k, ji = -k$

Note: -1 commutes

What is jk?

$ji = -k \Rightarrow j^2 i = -jk \Rightarrow -i = jk \Rightarrow jk = i$

$ik = (jk)k = jk^2 = -j$

$ki = -j$

Concrete representation

$Q_2 \subseteq GL_2(\mathbb{C})$

$1 \mapsto \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$

$-1 \mapsto \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$

$i \mapsto \begin{pmatrix}i & 0\\0 & -i\end{pmatrix}$

$j \mapsto \begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}$

$k \mapsto \begin{pmatrix}0 & i\\i & 0\end{pmatrix}$

Homomorphism

September-17-13 10:01 AM

Homomorphism

Let G, H be two groups.
A map $\phi: G \to H$ is called a **homomorphism** if
$\phi(gh) = \phi(g)\phi(h)\ \forall g, h \Rightarrow \phi(e_G) = e_H$

If $\phi: G \to H$ is a homomorphism and ϕ is 1-1 and onto then ϕ is called an **isomorphism**. Can be written $G \approx H$
If $\phi: G \to G$ is an isomorphism, we can also call it an **automorphism** of G.

Circle Group

$S^1 = \{e^{i\theta} : \theta \in [0, 2\pi)\}$
$e^{i\theta} \cdot e^{i\psi} = e^{i(\theta+\psi \bmod 2\pi)}$

Proposition

Let G, H be groups and let $\phi: G \to H$ be a homomorphism.

1) If G is abelian and ϕ is onto then H is abelian;
2) If H is abelian and ϕ is 1-1 then G is abelian.
3) If ϕ is an isomorphism then G is abelian $\Leftrightarrow$ H is abelian.

Homomorphisms

Why does $\phi(e_G) = e_H$?
$e_H\phi(g) = \phi(g) = \phi(e_G g) = \phi(e_G)\phi(g)$
$\therefore e_H = \phi(e_g)$ (cancel)

Also, $\phi(g^{-1}) = \phi(g)^{-1}\ \forall g \in G$
Why? $e_H = \phi(e_g) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$
$\Rightarrow \phi(g)^{-1}e_H = \phi(g)^{-1} = \phi(g^{-1})$

Example 1

Trivial homomorphism
$\phi: G \to H$
$\phi(g) = e_H\ \forall g \in G$

Example 2

$\phi: G \to G$
$\phi(g) = g\ \forall g$

Example 3

$G = \left\{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z}\right\}$
$\phi: G \to (\mathbb{Z}, +)$
$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mapsto n$
$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix}$

Example

If $G\&H$ are groups, we can make the direct product $G \times H$ into a group by declaring
$e_{G\times H} = (e_G, e_H)$
$(g_1, h_1) \cdot (g_2, h_2) = (g_1g_2, h_1h_2)$

a) Then G is isomorphic to $\{(g, e_H) : g \in G\}$
b) $G \times H \approx H \times G$
   $(g, h) \mapsto (h, g)$

Example

$D_3 \approx S_3 \approx \mathrm{GL}_2(\mathbb{Z}_2) \not\approx \mathbb{Z}_2 \times \mathbb{Z}_3$

Example

Let $(\mathbb{R}_{>0}, \cdot) = \{x \in \mathbb{R} : x > 0\}$
This is a group under multiplication with identity 1
Let $\mathbb{C}^* = \{$All nonzero complex numbers under multiplication$\}$

Claim

$\mathbb{C}^* \approx (\mathbb{R}_{>0}, \cdot) \times S^1$

Proof

If $z \in \mathbb{C}$ then we can write z uniquely as $\phi(z) = re^{i\theta}$ is 1-1 and onto
$z = re^{i\theta}, r > 0, \theta \in [0, 2\pi)$

Example

$(\mathbb{R}_{>0}, \cdot) \approx (\mathbb{R}, +)$, $\quad x \cdot y \to \log(xy) = \log(x) + \log(y)$
$x \mapsto \log(x)$

So $\mathbb{C}^* \approx \mathbb{R} \times S^1$

Remark

Isomorphism is an equivalence relation

1) $G \approx G$
2) $G \approx H \Rightarrow H \approx G$
3) $G \approx H \,\&\, H \approx K \Rightarrow G \approx K$
   $\phi: G \to H, \quad \psi: H \to K \Rightarrow \psi \circ \phi: G \to K$

Proof of Proposition

3 follows from 1&2

1) Assuming G is abelian and ϕ is onto.
   Let $h_1, h_2 \in H$. $\exists g_1, g_2$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$
   $h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2) = \phi(g_2g_1) = \phi(g_2)\phi(g_1) = h_2h_1$
2) Assuming H is abelian and ϕ is 1-1.
   Let $g_1, g_2 \in G$. Consider $\phi(g_1g_2) = \phi(g_1)\phi(g_2) = \phi(g_2)\phi(g_1) = \phi(g_2g_1)$
   $\because \phi$ is 1-1, $g_1g_2 = g_2g_1 \therefore G$ is abelian

Group Actions

September-17-13 10:52 AM

Group Actions

- G is a group
- X is a nonempty set

A **group action** of G on X is a map $G \times X \to X$

$(g, x) = x'$, write $gx = x'$

such that if $g_1, g_2 \in G, x \in X$

1) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$
2) $1 \cdot x = x \; \forall x \in X$

Symmetric Group acting on X

Given a set X, we let

$S_X = \{f: X \to X : f \text{ is 1-1 and onto}\}$

Then S_X is a group under $\circ$

Theorem

Let G be a group acting on a nonempty set X.

Then there is a homomorphism

$\phi: G \to S_X$

given by $\phi(g)(x) = g \cdot x$ for $g \in G, x \in X$

Moreover, ϕ is 1-1 $\Leftrightarrow \{g : g \cdot x = x \; \forall x \in X\} = \{1\}$

and in this case we say that the action is **faithful**.

Group Actions

Example 1

Trivial action

$g \cdot x = x \; \forall g \in G, x \in X$

Example 2

S_n actions on $\{1, 2, \dots, n\}$

Rule $\sigma \in S_n, \sigma: \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$

$\sigma \cdot i = \sigma(i)$

$(\sigma \cdot \tau) \cdot i = \sigma \circ \tau(i) = \sigma(\tau(i)) = \sigma \cdot (\tau \cdot i)$

Example 3

S_n acts on $\mathcal{P}(\{1, 2, \dots, n\})$ = power set of $\{1, 2, \dots, n\}$ = all subsets of $\{1, 2, \dots, n\}$

via the rule, $\sigma \cdot \emptyset = \emptyset$

$\sigma \cdot \{i_1, \dots, i_k\} = \{\sigma(i_1), \dots, \sigma(i_k)\}$

Example 4

D_n acts on $\{1, 2, \dots, n\}$

look at image of vertex i under symmetry

Example 5: Matrix multiplication

$\mathrm{GL}_n(\mathbb{F})$ acts on $X = \mathbb{F}^n = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} : x_1, \dots, x_n \in \mathbb{F} \right\}$

via left multiplication

$A \cdot \vec{v} = (A\vec{v})$

Example 6

$G, X = G$

$g \cdot x = gx$ (multiplication in the group)

Example 7

$X = G$

$g \cdot x = gxg^{-1}$ (conjugation)

Properties:

$1 \cdot x = 1x1^{-1} = x$

$g_1 \cdot (g_2 \cdot x) = g_1 \cdot (g_2 x g_2^{-1}) = g_1 g_2 x g_2^{-1} g_1^{-1} = (g_1 g_2) x (g_1 g_2)^{-1} = (g_1 g_2) \cdot x$

Note

If G is a group and $g \in G$ then conjugation by g is an automorphism of G

i.e. the map $\Phi_g: G \to G, \; x \mapsto gxg^{-1}$ is an automorphism

To see that Φ_g is an automorphism note that

$\Phi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \Phi_g(x)\Phi_g(y)$

Notice that $\Phi_{g^{-1}} \circ \Phi_g(x) = \Phi_{g^{-1}}(gxg^{-1}) = g^{-1}gxg^{-1}g = x = \mathrm{id}(x)$

& $\Phi_g \circ \Phi_{g^{-1}} = \mathrm{id}$ so Φ_g is an automorphism.

Proof of Theorem

Let $g, h \in G$

We want to show that $\phi(gh) = \phi(g)\phi(h)$

Let $x \in X$, then

$\phi(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot (\phi(h)(x)) = \phi(g)(\phi(h)(x)) = \phi(g) \circ \phi(h)(x)$

So $\phi(gh) = \phi(g) \circ \phi(h) \therefore \phi$ is a homomorphism

If $T = \{g: g \cdot x = x \; \forall x \in X\} \supsetneq \{1\}$

$\exists g \neq 1$ But $x = \phi(g)(x) = \phi(1)(x) \; \forall x \in X$

$\Rightarrow \phi(g) = \phi(1) \Rightarrow \phi$ is not 1-1

If ϕ is not 1-1 $\Rightarrow \exists g, h \in G$ such that $\phi(g) = \phi(h)$and $g \neq h$

So $\phi(gh^{-1}) = \phi(g) \cdot \phi(h)^{-1} = \mathrm{id}$

$\Rightarrow gh^{-1} \cdot x = x \forall x \in X \Rightarrow gh^{-1} \neq 1, gh^{-1} \in T$

■

Claim

$\mathrm{GL}_2(\mathbb{Z}_2) \approx S_3$

$\mathrm{GL}_2(\mathbb{Z}_2)$ acts on $\left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\} \subseteq \mathbb{Z}_2^2$ but can exclude $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ since it is always mapped to itself.

So we get a homomorphism $\phi: \mathrm{GL}_2(\mathbb{Z}_2) \to S_X \approx S_3$

Why is ϕ 1-1? If $A \in \mathrm{GL}_2(\mathbb{Z}_2)$ is s.t. $Ax = x \; \forall x \in X$

$\Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ & $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \Rightarrow A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = I$

So ϕ is 1-1

Since $|S_3| = |\mathrm{GL}_2(\mathbb{Z}_2)| = 6$, ϕ is onto

$\therefore$ it is an isomorphism

Orbits

September-19-13 10:01 AM

Orbit

Suppose that G is a group acting on a set X. Then given $x \in X$, call the set
$\{gx : g \in G\} \subseteq X$ the orbit of x and denote it O_x

Proposition

Let $G \hookrightarrow X$ "G acts on X"
If $x_1, x_2 \in X$ then either $O_{x_1} = O_{x_2}$ or $O_{x_1} \cap O_{x_2} = \emptyset$

This says that X is partitioned into a disjoint union of orbits.

Subgroups

Let G be a group, we say that a subset $H \subseteq G$ is a subgroup if it is closed under taking products and inverses (operations from G)

i.e. $h_1 h_2 \in H \Rightarrow h_1 h_2 \in H$
$h_1 \in H \Rightarrow h_1^{-1} \in H$

Lagrange's Theorem

Let G be a finite group and let H be a subgroup of G. "$H \leq G$"
Then $|H|$ divides $|G|$.

Corollary (Fermat's Little Theorem)

If p is prime and $a \not\equiv 0 \pmod p$
$\Rightarrow a^{p-1} \equiv 1 \pmod p$

Coset

In the case that $H \leq G$ and $H \hookrightarrow G$ by left multiplication we usually write Hx for O_x and call it the right coset Hx.

Then $G = Hx_1 \cup Hx_2 \cup \cdots \cup Hx_d$ if $|G| < \infty$
In general, any group G is a disjoint union of cosets but the number could be infinite if G is infinite.

A symmetric argument shows that G is a disjoint union of left cosets, xH

We write $[G:H]$ for the number of distinct left cosets = number of distinct right cosets = $\frac{|G|}{|H|}$ if $|G|, |H| < \infty$
$[G:H]$ - "Index of H in G"

Cyclic Groups

A group G is cyclic if it can be generated by one element.
In terms of generators & relations:
$G = \langle x \mid x^n = 1 \rangle$ for some $n \geq 1$
or
$G = \langle x \rangle \cong \mathbb{Z}$

Proposition

If G is cyclic then either $G \cong \mathbb{Z}_n$ for some $n \geq 1$ or $G \cong \mathbb{Z}$

Theorem

Let G be a cyclic group and let $H \leq G$. Then H is cyclic.

Orbit Examples

Example 1

S_n acting on $\{1, 2, \ldots, n\}$
Then $O_i = \{1, 2, \ldots, n\}$

Example 2

Look at S_3 acting on itself by conjugation
$g \cdot x = gxg^{-1}$
What is $O_{(12)}$

S_3	$g \cdot (12)$
id	$\text{id} \cdot (12) = (12)$
(12)	$(12) \cdot (12) = (12)(12)(12)^{-1} = (1\ 2)$
(23)	$(23) \cdot (12) = (23)(12)(23)^{-1} = (1\ 3)$
(13)	$(13) \cdot (12) = (13)(12)(13)^{-1} = (1)(2\ 3)$
$(1\ 2\ 3)$	$(1\ 2\ 3) \cdot (1\ 2) = (1\ 2\ 3)(1\ 2)(1\ 2\ 3)^{-1} = (1)(2\ 3)$
$(1\ 3\ 2)$	$(1\ 3\ 2) \cdot (1\ 2) = (1\ 3\ 2)(1\ 2)(1\ 3\ 2)^{-1} = (1\ 3)(2)$

$O_{(12)} = \{(1\ 2), (1\ 3), (2\ 3)\}$

Proof of Proposition

Let $x_1, x_2 \in X$ and suppose $O_{x_1} \cap O_{x_2} \neq \emptyset$
Then $\exists y \in X$ s.t. $y = g_1 \cdot x_1$ & $y = g_2 \cdot x_2$, $g_1, g_2 \in G$
We will show that $O_{x_1} \subseteq O_{x_2}$ and by symmetry $O_{x_2} \subseteq O_{x_1} \Rightarrow O_{x_1} = O_{x_2}$

Let $z \in O_{x_1}$
Then $z = h \cdot x_1$ for some $h \in G$
$z = (hg_1^{-1}g_2) \cdot x_1 = (hg_1^{-1})(g_1 x_1) = (hg_1^{-1})y = (hg_1^{-1}g_2) \cdot x_2 \in O_{x_2}$
So $O_{x_1} \subseteq O_{x_2}$
■

Example Subgroups

Example 1

$G = \mathbb{Z}, +$
$H = 2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$

Example 2

$G = D_n = \langle \rho, \tau \mid \rho^2 = \tau^n = \text{id}, \quad \rho\tau = \tau\rho \rangle$
$H = \{1, \rho, \rho^2, \ldots, \rho^n\}$

Example 3

$G = V$ a vector space
$H = W$, a subspace of V is a subgroup

Example: General Linear Group

$G = \text{GL}_n(\mathbb{R}) = \{\text{all non-invertible real matrices}\}$
$H = \text{SL}_n(\mathbb{R}) = \{A \in \text{GL}_n \mid \det(A) = 1\}$

Proof of Lagrange's Theorem

Let H act on $X = G$ via left-multiplication: $h \cdot x = hx \in G$, $x \in G$
If $x \in G$, what is O_x?
$O_x = \{h \cdot x : h \in H\}$. What is $|O_x|$? $|O_x| = |H|$. Why?
$H \leftrightarrow O_x$ by $h \rightsquigarrow h \cdot x$ is 1-1 and onto (since h has an inverse).

We know that G is a disjoint union of orbits. Let's say there are d disjoint orbits making up G.
Each orbit has size $|H|$ so $|G| = d|H|$. ■

Proof of Fermat's Little Theorem

Let $G = \mathbb{Z}_p^* = \{[1], [2], \ldots, [p-1], \cdot\} = (\mathbb{Z}_p \setminus \{[0]\}, \ \cdot)$
If $a \in \mathbb{Z}$ and $a \not\equiv 0 \pmod p$ then $[a] \in \mathbb{Z}_p^*$

Let $m = \text{order}([a])$ in $\mathbb{Z}_p$
Then $H := \{[1], [a], \ldots, [a^{m-1}]\}$ is a subgroup of $\mathbb{Z}_p^*$
Then $|H| = m$ and $|G| = |\mathbb{Z}_p^*| = p - 1$
so $(p-1) = md$ for some $d \geq 1$
Then $[a^{p-1}] = [a^{md}] = [(a^m)^d] = [1^d] = [1] \Rightarrow a^{p-1} \equiv 1 \pmod p$

Example

$G = S_4$
$H \approx S_3, \qquad H = \{\sigma \in S_4 : \sigma(4) = 4\}$
$H \leq G$

Find a set of left coset representations.
$S_4 = H\sigma_1 \cup H\sigma_2 \cup H\sigma_3 \cup H\sigma_4$
$\sigma_1 = \text{id}, \qquad H\sigma_1 = H$
$\sigma_2 = (1\ 4), \qquad H\sigma_2 = H(2\ 1)$
$\sigma_3 = (2\ 4)$
$\sigma_4 = (3\ 4)$

Proof of Proposition

Let x be a generator for G.
We always have a homomorphism $\phi: \mathbb{Z} \to G,\ \phi(n) = x^n,\ n \in \mathbb{Z}$

$$\phi(n+m) = x^{n+m} = \phi(n)\phi(m)$$

Case 1

x has infinite order. Then ϕ is onto $\because G$ is cyclic and if x has infinite order
$\dots, x^{-1}, 1, x, x^2, \dots$ are all distinct $\Rightarrow \phi$ is 1-1

Case 2

x has order $n \geq 1$
Now we make a map $\psi: \mathbb{Z}_n \to G$

$$\psi([i]) = x^i$$

$$\psi([i]+[j]) = x^{i+j \pmod n} = x^i x^j = \psi([i])\psi([j])$$

Onto: x has order n
1-1: $1, x, \dots, x^{n-1}$ are distinct

Proof of Theorem

Let x generate $G, G = \langle x \rangle$

If $H = \{1\}$ then there is nothing to prove. So assume $H \neq \{1\}$
Then consider $S = \{n \geq 1 : x^n \in H\}$. Then $S \neq \emptyset \because$ if $x^{-i} \in H \Rightarrow \left(x^{-i}\right)^{-1} \in H \Rightarrow x^i \in H$

Let $m =$ smallest element of S.
Then $x^m \in H$. Claim: $H = \langle x^m \rangle$

Proof of Claim

Suppose $\exists n$ such that $x^n \in H$ and n is not a multiple of m.
WLOG we may assume that $n > 0 \because x^n \in H \Leftrightarrow x^{-n} \in H$

By division algorithm: $n = qm + r,\ 0 < r < m$
Then $x^r = x^{n-qm} = x^n \cdot (x^m)^{-q} \in H \Rightarrow r \in S$
But this contradicts minimality of m.
∎

Groups of Small Order

September-24-13 10:02 AM

Proposition

Let G be a finite group and let $x \in G$.
Then $o(x)$ divides $|G|$.

Theorem

Let G be a finite group with the property that every element of G has order 1 or 2. Then $\exists n \geq 1$ such that
$G \cong \mathbb{Z}_2^n = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$
$= \{(\epsilon_1, \dots, \epsilon_n) : \epsilon_1, \dots, \epsilon_n \in \{[0],[1]\} = \mathbb{Z}_2\}$
Group under $+$
$(0, \dots, 0)$ is identity

Proof of Proposition

Let $H = \langle x \rangle \leq G$
Then $H \leq G$ and $|H| = o(x)$
By Lagrange's Theorem, $|H|$ divides $|G| \Rightarrow o(x) \mid |G|$
■

Proof of Theorem

We've shown that G is abelian. We will let '+' denote the operation on G and let 0 denote the identity.

We say that a subset $\{x_1, \dots, x_d\}$ of G is **linearly independent** if $\nexists (\epsilon_1, \dots, \epsilon_d) \in \{0,1\}^d$, not all zero such that $\epsilon_1 x_1 + \epsilon_2 x_2 + \cdots + \epsilon_d x_d = 0$.
Let $\{y_1, \dots, y_n\}$ be a maximally linearly independent subset of G

Claim

1) $X = \{\epsilon_1 y_1 + \cdots + \epsilon_n y_n : \epsilon_1, \dots, \epsilon_n \in \{0,1\}\}$ has size 2^n
2) $G = X$

Proof

1) Suppose that $\epsilon_1 y_1 + \cdots + \epsilon_n y_n = \epsilon_1' y_1 + \cdots + \epsilon_n' y_n,\ \epsilon_1, \dots, \epsilon_n, \epsilon_1', \dots, \epsilon_n' \in \{0,1\}$
$\Rightarrow \sum_{i=1}^{n} (\epsilon_i - \epsilon_i') y_i = 0$
$\Rightarrow \epsilon_i = \epsilon_i'\ \ \forall i \because \{y_1, \dots, y_n\}$ is linearly independent.
$\Rightarrow X$ has 2^n distinct elements.
2) Suppose that $X \neq G$. i.e. $X \subsetneq G$
Pick $z \in G \setminus X$
Show $\{y_1, \dots, y_n, z\}$ is linearly independent.
Proof:
If $\epsilon_1 y_1 + \cdots + \epsilon_n y_n + \epsilon z = 0,\ \epsilon_1, \dots, \epsilon_n, \epsilon \in \{0,1\}$ not all 0.
If $\epsilon = 0$, we get a contradiction $\because y_1, \dots, y_n$ are linearly independent.
If $\epsilon = 1$, $\epsilon_1 y_1 + \cdots + \epsilon_n y_n + z = 0 \Rightarrow \epsilon_1 y_1 + \cdots + \epsilon_n y_n = z$
Contradiction since $z \notin X$

So $\{y_1, \dots, y_n, z\}$ is linearly independent if $z \in G \setminus X$
But $\{y_1, \dots, y_n\}$ is a maximal linearly independent set. Contradiction.
Conclusion: $G = X$

Now we construct an isomorphism
$\phi: G \to \mathbb{Z}_2^n$
$\phi(\epsilon_1 y_1 + \cdots + \epsilon_n y_n) = (\epsilon_1, \dots, \epsilon_n)$
This is a homomorphism and 1-1 and onto.
$G \cong \mathbb{Z}_n^2$

Groups of Small Order

Order	Groups Up to Isomorphism
1	$\{1\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6, S_3$
7	$\mathbb{Z}_7$

Order 4

Case I: G has an element x of order 4

Then $G = \{1, x, x^2, x^3\} = \mathbb{Z}_4$ is cyclic

Case II: All elements of G have order < 4

Then all elements have order 1 or 2
$\Rightarrow G \cong \mathbb{Z}_2^m$ for some m
$|G| = 4 \Rightarrow m = 2 \Rightarrow G = \mathbb{Z}_2 \times \mathbb{Z}_2$

Order 6

Since $|G| = 6$ we know that $\exists x \in G$ of order 2
(by homework assignment, $|G|$ even $\Rightarrow G$ has element of order 2)
Let $H = \{1, x\} \leq G$
Let $X =$ set of left cosets of H. So $|X| = 3 = \frac{|G|}{|H|}$
$X = \{H, yH, zH\}$ for some $y, z \in G$
G acts on X by left multiplication:
$g \cdot yH = (gy)H \in \{H, yH, zH\}$
Recall that the action $G \hookrightarrow X$ gives a homomorphism
$\phi: G \to S_X \cong S_3$
If ϕ is 1-1 $\Rightarrow G \cong S_3$
If ϕ is not 1-1 $\Rightarrow \exists g \neq 1$ in G such that $gH = H, gyH = yH, gzH = zH$
What does $gH = H$ mean?
$\Rightarrow gH = H$
$\Rightarrow g \cdot H \in H$
$\Rightarrow g \in H = \{1, x\}$
So $g = x \because g \neq 1$
So $gyH = yH \Rightarrow xyH = yH \Rightarrow y^{-1}xyH = H$
$\Rightarrow y^{-1}xy \in H = \{1, x\} \Rightarrow y^{-1}xy = x$
(Otherwise $y^{-1}xy = 1 \Rightarrow x = y^{-1}y = 1$ Contradiction)

Notice that $G = \langle x, y \rangle \supsetneq \langle x \rangle$. Define $L = \langle x, y \rangle$

So $|L| > 2$ and $|L| \mid 6$ (Lagrange)

So $|L| \in \{3,6\}$

But $x \in L$ has order 2 so $2 \mid |L| \Rightarrow |L| = 6 \Rightarrow L = G$

Gut $xy = yx$ so G is abelian.

Now we have $G \cong S_3$ or G is abelian.

If G is abelian, we know $\exists x \in G$ of order 2. All elements of G have order in $\{1, 2, 3, 6\}$. If all elements have order 1 or 2

$\Rightarrow G \cong \mathbb{Z}_2^m$ for some m

Contradiction since $|G| = 6$

So $\exists y \in G$ of order 3 or 6. If $o(y) = 6 \Rightarrow G = \langle y \rangle \cong \mathbb{Z}_6$

If $o(y) = 3$, let $z = xy$. Then $o(z) \in \{1, 2, 3, 6\}$

But $z \neq 1 \because x^{-1} = x$ and $y \neq x$ so $o(z) \in \{2,3,6\}$

$z^2 = (xy)^2 = x^2y^2 = y^2 \neq 1 \Rightarrow o(z) \neq 2$

$z^3 = (xy)^3 = x^3y^3 = x^3 = x \neq 1 \Rightarrow o(z) \neq 3$

$\Rightarrow o(z) = 6 \Rightarrow G = \langle z \rangle \cong \mathbb{Z}_6$

Centralizers

September-24-13 10:53 AM

Centralizers

Given a subset $A \subseteq G$, G a group, we define **the centralizer of A in G**

$$C_G(A) := \{g \in G : ga = ag \ \forall a \in A\}$$

Notation

If $A = \{a\}$, we write $C_G(a)$ for $C_G(\{a\})$

If $A = G$, we write

$Z(G)$ for $C_G(A)$ and we call $C_G(G)$ the **centre** of G

So $Z(G) = \{g \in G : ga = ag \ \forall a \in G\}$

Proposition 1

If $A \subseteq G$, then $C_G(A)$ is a subgroup of G.

Normalizers

$A \subseteq G$

We define the **normalizer of A in G**

$$N_G(A) := \{g \in G: gag^{-1} \in A \ \ \forall a \in A\}$$

Then $C_G(A) \subseteq N_G(A)$

Proposition 2

$N_G(A)$ is a group

Example Centralizer

Let $G = S_3$

Let $A = \{\text{id}, (123)\}$

What is $C_G(A)$?

g	$g(123)$	$(123)g$
id	(123)	(123)
(12)	$(1)(23)$	$(13)(2)$
(13)	$(12)(3)$	$(1)(23)$
(23)	$(13)(2)$	$(12)(3)$
(123)	(132)	(132)
(132)	$(1)(2)(3)$	$(1)(2)(3)$

$C_G(A) = \{\text{id}, (123), (132)\}$

Example

$G = \text{GL}_2(\mathbb{R})$

$A = \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : ab \neq 0\right\}$

What is $C_G(A)$? $C_G(A) = A$

$\begin{pmatrix} u & v \\ w & x \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} ua & vb \\ wa & xb \end{pmatrix}$

$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} u & v \\ w & x \end{pmatrix} = \begin{pmatrix} au & av \\ bw & bx \end{pmatrix}$

Need $vb = av \ \forall a, b \in \mathbb{R} \Rightarrow v = 0$

$wa = bw \ \ \forall a, b \in \mathbb{R} \Rightarrow w = 0$

so $\begin{pmatrix} u & 0 \\ 0 & x \end{pmatrix} \in C_G(A) \Rightarrow C_G(A) = A$

Example

If $G = \text{GL}_2(\mathbb{R})$ what is $Z(G)$?

$Z(G) = \left\{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \neq 0\right\}$ (Exercise)

Proof of Proposition 1

1) $1 \in C_G(A) \because 1 \cdot a = a \cdot 1 = a \ \ \forall a \in A$
2) If $x, y \in C_G(A) \Rightarrow xa = ax \ \& \ ya = ay \ \forall a \in A$

   $\Rightarrow (xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy) \ \ \forall a \in A$

   $\Rightarrow xy \in A$
3) Similarly, if $x \in C_G(A) \Rightarrow xa = ax \ \forall a \in A \Rightarrow a = x^{-1}ax \Rightarrow ax^{-1} = x^{-1}a \ \ \forall a \in A$

   $\Rightarrow x^{-1} \in C_G(A)$

$\Rightarrow C_G(A)$ is a subgroup.

Proof of Proposition 2

1) $1 \in N_G(A)$
2) $x, y \in N_G(A)$ and $a \in A$, $(xy)a(xy)^{-1} = x(yay^{-1})x^{-1} = xbx^{-1}$ for some $b \in A$

   $xbx^{-1} \in A \Rightarrow xy \in N_G(A)$
3) $x \in N_G(A), \qquad a \in A$

   $\Rightarrow xax^{-1} = a'$ for some $a' \in A$

   $\Rightarrow a = x^{-1}a'x$

   But notice $\{xax^{-1} : a \in A\} = A$

   Why? $xa_1x^{-1} = xa_2x^{-1} \Rightarrow a_1 = a_2$

   Exercise: finish the proof

   So $\forall a' \in A = \{xax^{-1}: a \in A\}$, $\exists a \in A \ s.t. \ xax^{-1} = a'$

   $\Rightarrow x^{-1}a'x = a \in A \Rightarrow x^{-1} \in N_G(A)$

Example

Let $G = \{$all 1-1 and onto maps from $\mathbb{Z}$ to itself$\}$

G is a group under composition

Let.

$$f_i(n) = \begin{cases} n+1 & if\ n = 2i \\ n-1 & if\ n = 2i+1 \\ n & if\ n \notin \{2i, 2i+1\} \end{cases}$$

Let $h: \mathbb{Z} \to \mathbb{Z}$ $h(n) = n + 2$

$h \circ f_i \circ h^{-1}(2i+2) = h \circ f_i(2i) = h(2i+1) = 2i+3$

$h \circ f_i \circ h^{-1}\,(2i+3) = h \circ f_i(2i+1) = h(2i) = 2i+2$

If $n \notin \{2i+2, 2i+3\}$

$h \circ f_i \circ h^{-1}(n) = n$

So $h \circ f_i \circ h^{-1} = f_{i+1}$

So if $A = \{f_0, f_1, \ldots\}$

Then $h \circ f \circ h^{-1} \in A \ \ \forall f \in A$

But $h \circ A \circ h^{-1} \subsetneq A$

Example

$G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

$ij = k, \qquad ji = -k$
$i^2 = j^2 = k^2 = -1$
$(-1)i = i(-1) = -i$
$(-1)j = j(-1) = -j$
$(-1)k = k(-1) = -k$

Let $A = \{\pm i\}$

What is $N_G(A)$? Answer? $G = Q_8$

g	gAg^{-1}
1	$1\{\pm i\}1^{-1} = A$
-1	$-1\{\pm i\}(-1)^{-1} = A$
i	$i\{\pm i\}i^{-1} = A$
$-i$	$-i\{\pm i\}(-i)^{-1} = A$
j	$j\{\pm i\}j^{-1} = -\{\pm jk\} = \{\mp i\} = A$
$-j$	$-j\{\pm i\}(-1)^{-1} = A$
k	$k\{\pm i\}k^{-1} = -\{\pm jk\} = \{\mp i\} = A$
$-k$	$-k\{\pm i\}(-k)^{-1} = A$

Stabilizers & Conjugacy Classes

September-26-13 10:16 AM

Stabilizers

$G \hookrightarrow X, gx \to x'$

If $x \in X$, we define $G_x = \{g \in G : gx = x\}$

Remark 1

$G_x \leq G$ (G_x is a subgroup of G)

Orbit-Stabilizer Theorem

Let G be a group acting on a set X.

If $x \in X$ then $|O_x| = [G: G_x]$

$O_x = \{g \cdot x: g \in G\}$

$[G: G_x] =$ number of left/right G_x cosets in G

Corollary

If G is a finite group acting on a set X and $x \in X$ then $|O_x|$ divides $|G|$

Cauchy's Theorem

Let p be a prime number and let G be a finite group.

If $p \mid |G|$ then G has an element of order p.

Conjugacy Classes

Let G be a group and let $G \hookrightarrow G$ by conjugation

$g \cdot x = gxg^{-1}$

If $x \in G$, we call $O_x = \{gxg^{-1}: g \in G\}$ the conjugacy class of x and denote it by $\mathcal{C}_x$

Remarks

1) If $x \in G$ and $|G| < \infty \Rightarrow |\mathcal{C}_x| \mid |G|$
2) G is a disjoint union of conjugacy classes.

Proposition

If $g \in G$ then $|\mathcal{C}_g| = 1 \Leftrightarrow g \in Z(G)$

Normal Group

Let G be a be a group.

We say that a subgroup $N \leq G$ is **normal** if

$gNg^{-1} = N \ \forall g \in G$

The following are equivalent

1) $N \leq G$ is normal
2) $gN = Ng \ \ \forall g \in G$
3) $N_g(N) = G$ (N_g is normalizer)

$(1) \Leftrightarrow gNg^{-1} = N \ \ \forall g \in G$

$\Leftrightarrow N_G(N) = G \Leftrightarrow (3)$

$(1) \Leftrightarrow gNg^{-1} = N \ \forall g \in G$

$\Leftrightarrow gN = Ng \ \ \forall g \in G$

$\Leftrightarrow (2)$

Theorem

Let G be a group and let $H \leq G$ with $[G: H] = 2$

Then H **is normal in** G. Denote $H \trianglelefteq G$

Remark

1) If xH and yH are two left cosets, either $xH = yH$ or $xH \cap yH = \emptyset$

Idea

If $\exists h \in H \ s.t. \ xh \in yH, \Rightarrow x \in yHh^{-1} = yH$

$\Rightarrow xH \subseteq yHH = yH$

Similarly,

$xH \cap yH \neq \emptyset \Rightarrow yH \subseteq XH \Rightarrow xH = yH$

Normal Subgroup

$N \trianglelefteq G$: N is a normal subgroup of G if any of the following hold

1) $xNx^{-1} = N \ \ \forall x \in G$
2) $xN = Nx \ \ \forall x \in G$
3) $N_G(N) = G$

Proof of Remark 1

Since $1 \cdot x = 1 \Rightarrow 1 \in G_x$

If $g, h \in G_x \Rightarrow (gh) \cdot x = g(hx) = g \cdot x = x \Rightarrow gh \in G_x$

If $g \in G_x \Rightarrow gx = x \Rightarrow g^{-1}(gx) = g^{-1} \cdot x \Rightarrow 1 \cdot x = g^{-1} \cdot x \Rightarrow g^{-1}x = x$

So $G_x \leq G$. In particular, if $|G| < \infty$, $|G_x|$ divides $|G|$.

Example

Let $G = S_4$. Let $X = \{1,2,3,4\}$

$\sigma \cdot i = \sigma(i)$

What is G_2? $G_2 = \{\sigma \in S_4: \sigma(2) = 2\}$

How big is $|G_2|$? $|G_2| = 6$

What is O_2? $O_2 = \{1,2,3,4\}$

$|O_2| = 4$

$|G| = 24$

$|G_2| = 6$

$$|O_2| = \frac{|G|}{|G_2|} = \frac{24}{6} = 4$$

Proof of Orbit-Stabilizer Theorem (Finite)

Let $m = [G: G_x]$ and let $g_1G_x \cup g_2G_x \cup \cdots \cup g_mG_x$ be a set of left coset representations

Claim

$O_x = \{g_1x, g_2x, \dots, g_mx\}$

This will then give $|O_x| = m = [G: G_x]$

Proof of Claim

Let $y \in O_x$. Then $y = gx$ for some $g \in G$

So $\exists i$ s.t. $g \in g_iG_x$, i.e. $g = g_ih, \ h \in G_x$

So $gx = (g_i \cdot h) \cdot x = g_i(hx) = g_i \cdot x$

So $y \in \{g_1x, \dots, g_mx\}$

To finish, we must show that if $i \neq j$ then $g_ix \neq g_jx$

We do this by contradiction. Suppose that $g_ix = g_jx$

$\Rightarrow g_j^{-1}g_ix = x$

$\Rightarrow g_j^{-1}g_i \in G_x \Rightarrow g_i \in g_jG_x$. Contradiction.

$\therefore g_iG_x \cap g_jG_x = \emptyset$

So $g_ix, \dots, g_mx$ are all distinct $\Rightarrow |O_x| = m$

Proof of Corollary

$|O_x| = [G: G_x]$

But $|G| = |G_x| \cdot [G: G_x] \Rightarrow |O_x||G|$

Proof of Cauchy's Theorem

Let $X = \{(g_1, g_2, \dots, g_p) : g_1g_2 \dots g_p = 1, \ g_1, \dots, g_p \in G\}$

Then $|X| = |G|^{p-1}$

Why? $(g_1, g_2, \dots, g_{p-1}, g_p) \in X \Leftrightarrow g_p = (g_1g_2, \dots, g_{p-1})^{-1}, \ g_1, \dots, g_p \in G$

In particular, $p \mid |X|$ since $p \mid |G|$

Let $\mathbb{Z}_p$ act on X via cyclic permutation

i.e. $[i] \cdot (g_1, g_2, \dots, g_p) = (g_{1+i}, g_{2+i}, \dots, g_{p+i})$ where subscripts are taken (mod p)

Notice if $(g_1, \dots, g_p) \in X \Rightarrow g_2g_3 \cdots g_pp_1 = (g_1^{-1}g_1)(g_2 \cdots g_p)g_1 = g_1^{-1}(g_1g_2 \cdots g)g_1 = g_1^{-1}g_1 = 1$

$\Rightarrow (g_2, \dots, g_p, g_1) \in X$

So $H = \mathbb{Z}_p$ acts on X.

If $x \in X$ what can we say about $|O_x|$?

$|O_x| \mid |H| \Rightarrow |O_x|| \, p \Rightarrow |O_x| \in \{1, p\}$

Recall that X is partitioned into orbits. Also $|X| = |G|^{p-1} \equiv 0 \pmod p$

So the number of orbits of size 1 must be a multiple of p since orbits have size 1 or p

When does $x = (g_1, \dots, g_p) \in X$ have an orbit of size 1? When $x = (g, g, \dots, g)$ for some $g \in G$

Notice, we must have $g^p = 1$ by definition of X.

Notice $(1,1, \dots, 1) \in X$ so there is at least 1 orbit of size 1

Since $p \geq 2$ and the number of orbits of size 1 is a multiple of p

$\exists g \neq 1$ s.t. $(g, g, \dots, g) \in X \Rightarrow g^p = 1 \,\&\, g \neq 1$ ■

Proof of Proposition

$|\mathcal{C}_g| = 1 \Leftrightarrow \{hgh^{-1}: h \in G\} = g \Leftrightarrow hgh^{-1} = g \ \ \forall h \in G \Leftrightarrow hg = gh \, \forall h \in G \Leftrightarrow h \in Z(G)$

Example Conjugacy Class

Let $G = S_3$. Find the conjugacy classes of G

$S_3 = \{\text{id}, (12), (23), (13), (123), (132)\}$

$\mathcal{C}_{\text{id}} = \{\text{id}\}$

In general, $\mathcal{C}_1 = \{1\} \because \mathcal{C}_1 = \{g \cdot 1 \cdot g^{-1}: \ g \in G\} = \{1\}$

$\mathcal{C}_{12}$

$(12) \in \mathcal{C}_{12}$

$(123)(12)(123)^{-1} = (1)(23) \in \mathcal{C}_{12}$

$(132)(12)(132)^{-1} = (13) \in \mathcal{C}_{12}$

So $\mathcal{C}_{12} = \{(12), (13), (23)\}$

$C_{123} = \{(123), (132)\}$

Example 1
$G = Q_8$
$N = \{\pm 1, \pm i\}$ is normal
Why? $N_G(N) = G$

Example 2
$G = S_3$, $N = \{\text{id}, (123), (132)\}$ is normal
$\Rightarrow \sigma N \sigma^{-1} = N \ \forall \sigma \in S_3$

Proof of Theorem
Let $x \in G$
Case 1: $x \in H$
Then $xHx^{-1} = Hx^{-1} = H$
Case 2 $x \notin H$
Then $G = H \cup xH = H \cup Hx \Rightarrow xH = Hx \Rightarrow xHx^{-1} = H$
So in either case, $xHx^{-1} = H \Rightarrow H \trianglelefteq G$

Normal Subgroups Facts
1) If G is abelian & $N \leq G \Rightarrow N \trianglelefteq G$
   Why?
   $xNx^{-1} = Nxx^{-1} = N$ so abelian
   $\{xyx^{-1}: n \in N\} = \{nxx^{-1}: n \in N\} = \{n: n \in N\} = N$
2) If $N \leq G$ and $[G:N] = 2 \Rightarrow N \trianglelefteq G$
   Why? If $x \notin N$, $G = N \cup xN = N \cup Nx \Rightarrow Nx = xN$

Groups of Order 6 Revisited
Let $|G| = 6$
By Cauchy's theorem, $\exists x, y \in G.\ o(x) = 2, o(y) = 3$
Let $N = \{1, y, y^2\}$ Then $|N| = 3$, $[G:N] = \frac{|G|}{|N|} = \frac{6}{3} = 2$
So $N \trianglelefteq G$. Look at $xyx^{-1} = xyx \in N$. So $xyx \in \{y, y^2\}$
Remark: $G = \langle x, y \rangle$ Why? $o(y) = 3$ & $o(x) = 2 \Rightarrow 6 \mid |\langle x, y \rangle| \Rightarrow \langle x, y \rangle = G$

2 Cases
Case 1: $xyx = y \Rightarrow xy = yx$
  $\Rightarrow G$ is abelian; check xy has order 6
Case 2: $xyx = y^{-1}$
  So $G = \langle x, y \mid x^2 = y^2 = 1, xyx = y^{-1} \rangle \cong D_3 \cong S_3$

Kernel & Quotient Groups

October-01-13 10:18 AM

Kernel

Let G, H be groups and let $\phi: G \to H$ be a homomorphism. We defined the **kernel** of ϕ to be
$\ker(\phi) := \{g \in G \mid \phi(g) = 1_H\}$

Theorem

Let $\phi: G \to H$ be a homomorphism. Then ϕ is 1-1 if and only if $\ker(\phi) = \{1_G\}$

Proposition

The kernel of a homomorphism is a normal subgroup.
i.e. if $\phi: G \to H$ is a homomorphism, $\ker(\phi) \trianglelefteq G$

Quotient Groups

Let G be a group and let $N \trianglelefteq G$
N must be normal for this construction to work.

We can form a quotient group $G_{/N}$ as follows

- If G is finite, we'll see $|G_{/N}| = \frac{|G|}{|N|}$

$G_{/N}$ as a set $= \{xN : x \in G\} = \{Nx : x \in G\}$
So $|G_{/N}| = [G : N]$

How do we multiply?
$(xN) \cdot (yN) = x(Ny)N = x(yN)N = xyNN = xyN$

Notice that $G_{/N}$ is a group.
The coset $N = 1 \cdot N$ is the identity
and $(aN)(a^{-1}) = aa^{-1}N = N$ so $(aN)^{-1} = a^{-1}N$

Proof of Theorem

Suppose that $\ker(\phi) \neq \{1_G\} \Rightarrow \ker(\phi) \not\supseteq \{1_G\}$
So $\exists x \neq 1_G$ in G such that $\phi(x) = 1_H$
$\Rightarrow \phi(x) = \phi(1_G) \Rightarrow \phi$ is not 1-1

Suppose that ϕ is not 1-1. $\Rightarrow \exists g, h \in G, g \neq h$ s.t. $\phi(g) = \phi(h)$
$\Rightarrow \phi(gh^{-1}) = \phi(g)\phi(h^{-1}) = \phi(g)\phi(h^{-1}) = I_H$
$\Rightarrow gh^{-1} \neq 1_G$ is in $\ker(\phi)$ so $\ker(\phi) \supsetneq \{1_G\}$
■

Note

Recall that if $G \hookrightarrow H$
$\phi: G \to S_x, \quad g \mapsto \phi_g : X \to X, \quad \phi_g(x) = gx$
$\ker(\phi) = \{g \in G : gx = x\ \forall x \in X\} = \bigcap_{x \in X} G_x =$ Intersection of all stabilizers of G

Proof of Proposition

Let $x \in G$ and let $n \in \ker(\phi)$
$\Rightarrow \phi(xnx^{-1}) = \phi(x)\phi(n)\phi(x^{-1}) = \phi(x)1_H\phi(x^{-1}) = \phi(xx^{-1}) = \phi(1_G) = 1_H$
$\Rightarrow xnx^{-1} \in \ker(\phi)$
So if $N = \ker(\phi) \Rightarrow xNx^{-1} \subseteq N \Rightarrow N \subseteq x^{-1}Nx = x^{-1}N(x^{-1})^{-1} \subseteq N \Rightarrow N \subseteq xNx^{-1}$
So $xNx^{-1} = N\ \ \forall x \in G$
$\Rightarrow N \trianglelefteq G$

Quotient Group Example 1

$G = \mathbb{Z}, +$
$N = n\mathbb{Z}, +, \quad n > 1$
$G_{/N} = \mathbb{Z}_{/n\mathbb{Z}} \cong \mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}, \quad [i] = \{j \in \mathbb{Z} : j \equiv i \pmod n\}$
In this case, our cosets are
$i + N = i + n\mathbb{Z} = \{\dots, i-n, i, i+n, i+2n, \dots\} = \{j \in \mathbb{Z} : j \equiv i \pmod n\}$
We have n cosets $\{0 + N, \dots, n-1+N\}$

Quotient Group Example 2

$G = \mathrm{GL}_2(\mathbb{R})$
$N = \mathrm{SL}_2(\mathbb{R}) = \{A \in \mathcal{M}_2(\mathbb{R}) : \det(A) = I\} \trianglelefteq G$
Why?
Let $\phi: G \to \mathbb{R}^*,\ \phi(A) = \det(A)$
$\phi(AB) = \det(AB) = \det A \det B = \phi(A)\phi(B)$
$\ker(\phi) = \{A : \phi(A) = 1\} = \mathrm{SL}_2(\mathbb{R})$
What does $G_{/N}$ look like?
Claim: A coset of N is all matrices with a given nonzero determinant.
Why?
For $A \in \mathrm{GL}_2(\mathbb{R}), B \in \mathrm{SL}_2(\mathbb{R})$
$AN \supset AB \Rightarrow \det AB = \det A \det B = \det A$
Conversely, if $\det C = \det A \Rightarrow C = A(A^{-1}C) \in An$

So there is a bijection.
Left cosets of $\mathrm{SL}_2(\mathbb{R})$ in $\mathrm{GL}_2(\mathbb{R}) \longleftrightarrow$ elements of $\mathbb{R}^*$
$A \cdot \mathrm{SL}_2(\mathbb{R}) \longleftrightarrow \det A$
$(A \cdot \mathrm{SL}_2(\mathbb{R}))(B \cdot \mathrm{SL}_2(\mathbb{R})) = AB\, \mathrm{SL}_2(\mathbb{R})$

First Isomorphism Theorem

October-01-13 10:55 AM

Image

Let $\phi: G \to H$ be a homomorphism.
Then $\text{im}(\phi) = \{\phi(g): g \in G\} \leq H$

First Isomorphism Theorem

Let $\phi: G \to H$ be a homomorphism.
Then $G_{/\ker(\phi)} \approx \text{im}(\phi)$

Proposition

Let $H, K \leq G$
Then $HK \coloneqq \{hk: h \in H, k \in K\}$ has size
$|HK| = \frac{|H||K|}{|H \cap K|}$

Image Subgroup

If $h_1, h_2 \in \text{im}(\phi) \Rightarrow \exists g_1, g_2 \in G$ s.t. $\phi(g_1) = h_1,\ \phi(g_2) = h_2$
$\Rightarrow h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1, g_2) \in \text{im}(\phi)$
$h_1^{-1} \in \phi(g_1)^{-1} = \phi(g_1^{-1}) \in \text{im}(\phi); 1_H = \phi(1_G) \in \text{im}(\phi)$

Proof of First Isomorphism

Let $N = \ker(\phi)$. So $G_{/N} = \{gN: g \in N\}$
Define $f: G_{/N} \to \text{im}(\phi)$ by $f(gN) = \phi(g)$
We have to check

1) f is well-defined
2) f is a homomorphsim
3) f is 1-1
4) f is onto

1) f is well-defined

Suppose that $g_1 N = g_2 N \Leftrightarrow g_2^{-1} g_1 N = N \Leftrightarrow g_2^{-1} g_1 \in N = \ker(\phi) \Leftrightarrow \phi(g_2^{-1} g_1) = 1_H \Leftrightarrow \phi(g_2^{-1})\phi(g_1) = 1_H \Leftrightarrow \phi(g_2)^{-1}\phi(g_1) = 1_H \Leftrightarrow \phi(g_1) = \phi(g_2)$
So $g_1 N = g_2 N \Rightarrow \phi(g_1) = \phi(g_2) \Rightarrow f$ is well-defined

2) f is a homomorphism

$f(g_1 N g_2 N) = f(g_1 g_2 N) = \phi(g_1 g_2) = \phi(g_1)\phi(g_2) = f(g_1 N) f(g_2 N)$

3) f is 1-1. What is the kernel of f?

$\ker(f) = \{gN: \phi(g) = 1_H\}$ But $\phi(g) = 1_H \Leftrightarrow g \in \ker(\phi) = N$
$= \{gN : g \in N\} = \{N\} =$ identity in $G_{/N}$

4) f is onto

If $x \in \text{im}(\phi)$
$\Rightarrow \exists y \in G$ s.t.$x = \phi(g) \Rightarrow x = f(gn) \Rightarrow f$ is onto
$G/_N$ is a group

- elements are cosets gN
- multiplication $g_1 N g_2 N = g_1 g_2 N$
- identity $1N = N$
- inverse $(gN)^{-1} = g^{-1} N$

Example

$\text{GL}_n(\mathbb{R})/_{\text{SL}_n(\mathbb{R})} \cong \mathbb{R}^*$

Example

$\mathbb{C}^*/_{\mathbb{R}_{>0}} \cong S^1 = \{e^{i\theta}: \theta \in [0, 2\pi)\}$
Why?
Define $\phi: \mathbb{C}^* \to S^1$ by $\phi(z) = \frac{z}{|z|}$ homomorphism
$\ker(\phi) = \left\{z : \frac{z}{|z|} = 1\right\} = \mathbb{R}_{>0}$

Example

$\phi: \mathbb{Z} \to \mathbb{Z}_n, \qquad i \mapsto [i]$
$\ker(\phi) = n\mathbb{Z}$
So $\mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}_n$

Example

$\phi: A \times B \to B, \qquad (a, b) \to b$
$\ker(\pi)\{(a, 1_b) : a \in A\} = A \times \{1_B\}$
So $(A \times B)_{/A \times \{1_B\}} \cong B$

Example

$G = S_3, N = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}$
$G_{/N} \cong \mathbb{Z}_2$

Proof of Proposition

$HK = \bigcup_{h \in H} hK$
When is $h_1 K = k_2 K$?
$h_1 K = h_2 K \Leftrightarrow h_2^{-1} h_1 K = K \Leftrightarrow h_2^{-1} h_1 \in K \Leftrightarrow h_2^{-1} h_1 \in K \cap H\ \because h_1, h_2 \in H$
Notice that $K \cap H \leq H$
Let $h_1(K \cap H), \ldots, h_d(K \cap H)$ be the set of left $K \cap H$ cosets in H. What is d?
$d = [H: K \cap H] = \frac{|H|}{|K \cap H|}$

Claim:
$HK = h_1 K \cup h_2 K \cup \cdots \cup h_d K$
Once we have the claim, we see
$|HK| = d|K| = \frac{|H|}{|H \cap K|}|K|, \qquad$ so we will be done

1) If $i \neq j$ then $h_i K \neq h_j K$ since otherwise
$h_i^{-1} h_j \in K \cap H \Rightarrow h_i \in h_j(K \cap H) \Rightarrow h_i(K \cap H) = h_j(K \cap H)$. Contradiction
2) Now we'll show that $HK = \cup_{i=1}^{d} h_i K$
It is enough to show that $HK \leq \cup_{i=1}^{d} h_i K \therefore h_i K \subseteq HK\ \ \forall i$
Let $hk \in HK$. Consider $h(H \cap K) = h_i(H \cap K)$ for some i

$$\Rightarrow h_i^{-1}h \in H \cap K \Rightarrow h_iK = hK \Rightarrow hk \in hK = h_iK \subseteq \bigcup_{i=1}^{d} h_iK$$

2nd & 3rd Isomorphism Theorems

October-03-13 10:21 AM

Proposition

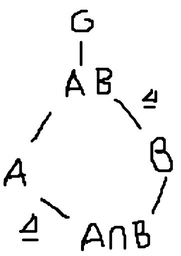
Let G be a group and let H, K be subgroups of G
Then HK is a subgroup of $G \Leftrightarrow HK = KH$

Corollary

If $H, K \leq G$ and $H \subseteq N_G(K) = \{g \in G: gKg^{-1} = K\}$
$\Rightarrow HK$ is a subgroup of G.

2nd Isomorphism Theorem

Let G be a group and let $A, B \leq G$ and suppose that $A \subseteq N_G(B)$
Then $B \trianglelefteq AB$ and $A \cap B \trianglelefteq A$ and $AB_{/B} \cong A_{/(A\cap B)}$



3rd Isomorphism Theorem

Suppose that $H \subseteq K \subseteq G, \quad H, K \trianglelefteq G$
Then $H \trianglelefteq K$ and $K_{/H} \trianglelefteq G_{/H}$ and $\left(G_{/H}\right)_{/(K_{/H})} \cong G_{/K}$

Correspondence Theorem

If G is a group, the collection of subgroups of G can be partially ordered w.r.t. inclusion.

Proof of Proposition

Suppose HK is a subgroup.
? Then $H, K \subseteq HK \Rightarrow KH \subseteq HK \therefore HK$ is a group and $K, H \subseteq HK$

If G is finite then $|KH| = \frac{|K||H|}{|K\cap H|} = |HK| \Rightarrow KH = HK$
What if G is infinite? Still OK.
Have a bijection $HK \to KH$ where $x \mapsto x^{-1}$

Suppose that $HK = KH$
1) $1 = 1 \cdot 1 \in HK$, so $HK \neq \emptyset$
2) If $h_1k_1 \& h_2k_2 \in HK$ then $(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2$
   $\therefore k_1h_2 \in KH = HK \Rightarrow \exists h_3 \in H, k_3 \in K$ s.t. $h_3k_3 = k_1h_2$
   $= (h_1h_3)(k_3k_2) \in HK$
3) If $hk \in HK \Rightarrow (hk)^{-1} = k^{-1}h^{-1} \in KH = HK$

So HK is a subgroup.

Proof of Corollary

Let $kh \in KH$. $kh = h(h^{-1}kh) \in HK$ since $h^{-1}kh \in K \Rightarrow HK \subseteq HK$
If $hk \in HK$. Then $hk = hkh^{-1}h \in KH \Rightarrow KH \subseteq HK \Rightarrow HK = KH \Rightarrow HK$ is a group
In particular $K \trianglelefteq G \Rightarrow HK$ is a subgroup.

Proof of 2nd Isomorphism Theorem

To see that $B \trianglelefteq AB$, let $ab \in AB$
Then $(ab)B(ab)^{-1} = (ab)Bb^{-1}a^{-1} = aBa^{-1} = B \because a \in A \subseteq N_G(B)$
$\Rightarrow ab \in N_{AB}(B) \forall ab \in AB \Rightarrow B \trianglelefteq AB$

Since $B \trianglelefteq AB$, we can form the quotient group $AB_{/B}$
Let $\phi: A \to AB_{/B}$ be defined by $\phi(a) = aB$
Claim: ϕ is a sujective homomorphism.
Homomorphism: $\phi(a_1a_2) = a_1a_2B = a_1Ba_2B = \phi(a_1)\phi(a_2)$
Onto: If $x \in AB_{/B} \Rightarrow x = abB$ for some $a \in A, b \in B$
$= aB = \phi(a)$ so ϕ is onto.

The identity in $AB_{/B}$ is B
$\ker\phi = \{a \in A: \phi(a) = a\} = \{a \in A: aB = B\} = \{a \in A: a \in B\} = A \cap B$
So by the 1st isomorphism theorem, $A_{/\ker\phi} \cong \operatorname{im}\phi \Rightarrow AB_{/B} \cong A_{/(A\cap B)}$

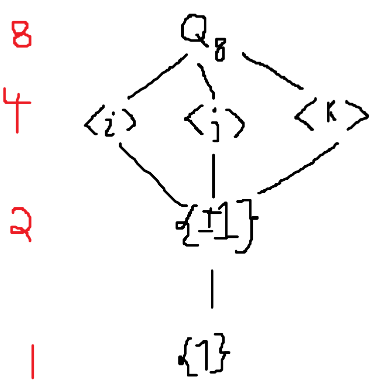
Proof of 3rd Isomorphism Theorem

To see that $H \trianglelefteq K$ notice that $N_G(H) = G, \because H \trianglelefteq G$
$\Rightarrow K \subseteq N_G(H) \Rightarrow K = N_K(H) = N_G(H) \cap K \Rightarrow H \trianglelefteq K$
Now let's check that $K_{/H} \trianglelefteq G_{/H}$
Consider
$(gH)\left(K_{/H}\right)(gH)^{-1} = (gH)\left(K_{/H}\right)g^{-1}H = \{gkg^{-1}H: k \in K\} = \{kH: k \in K\} \because g \in N_G(K)$
$= K_{/H}$
So $(gH)\left(K_{/H}\right)(gH)^{-1} = K_{/H} \quad \forall gH \in G_{/H} \Rightarrow K_{/H} \trianglelefteq G_{/H}$

Define $\phi: G_{/H} \to G_{/K}$ by $\phi(gH) = gK$
Check that this is a homomorphism
1) Well-defined
   If $g_1H = g_2H \Leftrightarrow g_2^{-1}g_1 \in H \Rightarrow g_2^{-1}g_1 \in K \because H \subseteq K \Rightarrow g_1K = g_2K \Rightarrow \phi(g_1H) = \phi(g_2H)$
2) Homomorphism
   $\phi(g_1Hg_2H) = \phi(g_1g_2H) = g_1g_2K = g_1Kg_2K = \phi(g_1)\phi(g_2)$

Notice if $gK \in G_{/K} \Rightarrow gK = \phi(gH)$ so $\operatorname{im}(\phi) = G_{/K}$
What is $\ker(\phi)$? K is the identity in $G_{/K}$ so
$\ker(\phi) = \{gH: \phi(gH) = K\} = \{gH: gK = K\} = \{gH: g \in K\} = \{kK: k \in K\} = K_{/H}$
So by the 1st isomorphism theorem,
$(G/_H)_{/\ker(\phi)} \cong \operatorname{im}(\phi) \Rightarrow \left(G_{/H}\right)_{/(K_{/H})} \cong G_{/K}$

Example Correspondence Q_8



$N = \{\pm 1\} \trianglelefteq Q_2$
$Q_{8/N} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
$(\pm iN)^2 = (\pm jN)^2 = (\pm kN)^2 = -N = N$

Conjugacy Class Equation

October-08-13 10:03 AM

Simple Groups

G is simple if its only normal subgroups are $\{1\}$ and G

Theorem

Let G be a finite group and let $x \in G$, then

$|\mathcal{C}_x| = [G: C_G(x)] = \frac{|G|}{|C_G(x)|}$

What does this mean?

If G is finite, G is the disjoint union of conjugacy classes, say

$G = \mathcal{C}_{g_1} \cup \mathcal{C}_{g_2} \cup \cdots \cup \mathcal{C}_{g_m}$

$|G| = |\mathcal{C}_{g_1}| + |\mathcal{C}_{g_2}| + \cdots + |\mathcal{C}_{g_m}| = \frac{|G|}{|C_G(g_1)|} + \cdots + \frac{|G|}{|C_G(g_m)|}$

Theorem

If G is a finite group and $\{g_1, \dots, g_m\}$ is a complete set of conjugacy class representatives, ie.e

$$G = \bigcup_{1 \le i \le m}^{*} \mathcal{C}_{g_i}$$

$\Rightarrow |G| = \sum_{i=1}^{m} \frac{|G|}{|C_G(g_i)|}$

When is $|\mathcal{C}_x| = 1$?

$\mathcal{C}_x = \{gxg^{-1} : g \in G\}$

If $|\mathcal{C}_x| = 1 \Leftrightarrow \mathcal{C}_x = \{x\} \Leftrightarrow gxg^{-1} = x \forall g \in G \Leftrightarrow gx = xg \forall g \in G \Leftrightarrow x \in Z(G)$

Let $g_1, \dots, g_m$ be a complete set of conjugacy class representatives for G and let $g_{k+1}, \dots, g_m$ be the elements with $|\mathcal{C}_{g_i}| = 1$

Then $|G| = |\mathcal{C}_{g_1}| + \cdots + |\mathcal{C}_{g_k}| + |\mathcal{C}_{g_{k+1}}| + \cdots + |\mathcal{C}_{g_m}|$

This gives

Class Equation

$|G| = \frac{|G|}{|C_G(g_1)|} + \cdots + \frac{|G|}{|C_G(g_k)|} + |Z(G)|$

where $g_1, \dots, g_k$ are a set of conjugacy class representatives for the conjugacy classes of size > 1

Theorem 3

Let p be a prime and let G be a group of size p^m for some $m \ge 1$

(G is called a **p-group**)

Then G has a non-trivial centre; i.e. $|Z(G)| = p^l$ for some $l \in \{1, 2, \dots, m\}$

Corollary

Let p be prime and let G be a group of size p^2. Then G is abelian.

Note, does not apply for higher powers.

$\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}$

is a non-abelian group of order p^3

Theorem 4

Let G be a finite group and suppose that p is the smallest prime dividing $|G|$. If $H \le G$ has index p (i.e. $\frac{|G|}{|H|} = p$) then $H \trianglelefteq G$.

Theorem 5

Let p, q be primes with $q < p$ and suppose that $p \not\equiv 1 \pmod{q}$.

Then if $|G| = pq \Rightarrow G$ is cyclic.

Lattice of Subgroups

IF G is a group, the set of subgroups of G has a **partial order** given by $\subseteq$.

So this gives us a picture of the subgroups of G, where we put bigger subgroups higher and we draw a line to two groups when one contains the other.

Example

$G = \mathbb{Z}_p$ is simple

Why? If $N \trianglelefteq G$ then $|N| \mid |G|$ (Lagrange)

$\Rightarrow |N| = \{1, p\}$

- $|N| = 1 \Rightarrow N = \{1\}$
- $|N| = p \Rightarrow N = G$

Conjugacy classes

G acts on itself via conjugation

$X = G$

$g \cdot x = gxg^{-1}$

$g(x) = gxg^{-1}$

$G \hookrightarrow X$

$g: X \to X, \quad g(x) = gx$

$1: X \to X$

$(hg)(x) = h \circ g(x) = h(g(x))$

$\mathcal{O}_x = \{g \cdot x \mid g \in G\} = \{gxg^{-1} \mid g \in G\} = \mathcal{C}_x =$ conjugacy class of x

orbit-stabilizer theorem

$|\mathcal{C}_x| = |\mathcal{O}_x| = [G: G_x] = \frac{|G|}{|G_x|}$ if G is finite

$G_x = \{g \in G : g \cdot x = x\} = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$
$= C_G(x)$

Proof of Theorem 3

By the class equation,

$|G| = \frac{|G|}{|C_G(g_1)|} + \cdots + \frac{|G|}{|C_G(g_k)|} + |Z(G)|$

where each of $\frac{|G|}{|C_G(g_i)|} > 1$ for $i = 1, \dots, k$

For $i = 1, \dots, k$

$\frac{|G|}{|C_G(g_i)|} \,\Big|\, |G| = p^m$

and since it is > 1 we have

$\frac{|G|}{|C_G(p_i)|} \equiv 0 \pmod{p}$ for $i = 1, \dots, k, \qquad$ and $|G| \equiv 0 \pmod{p}$

So $|Z(G)| \equiv 0 \pmod{p}$. Since $1 \in Z(G)$, $|Z(G)| \ge 1$

So in fact $|Z(G)| \ge p$. This result follows by Lagrance's theorem.

Proof of Corollary

We just showed that $|Z(G)| \in \{p, p^2\}$

If $|Z(G)| = p^2$ then $G = Z(G) \Rightarrow G$ is abelian.

$If\, |Z(G)| = p \Rightarrow \exists x \in G$ such that $\langle x \rangle = Z(G)$

Pick $y \in G \setminus Z(G)$

Claim, $G = \langle x, y \rangle$

Let $H = \langle x, y \rangle$, then $H \supsetneq Z(G)$

So $|H| > |Z(G)| = p$

But $|H| \,\big|\, |G|$ by Lagrange's theorem

$\Rightarrow |H| = p^2 \Rightarrow H = G$

Now $xy = yx \because x \in Z(G)$ so $\langle x, y \rangle = G$ is abelian.

Proof of Theorem 4

Let $X = \{x_1 H, \dots, x_p H\} =$ set of left cosets

Let $G \hookrightarrow X$ via $g \cdot xH \to gxH$

So this gives a homomorphism $\phi: G \to S_X = S_p$

By Q1 of assignment 4,

$\ker \phi = \bigcap_{g \in G} gHg^{-1} \subseteq H$

So $\ker \phi \subseteq H$ and also $\ker \phi \trianglelefteq G \because$ it is a kernel

So by 1st isomorphism theorem,

$G/_{\ker \phi} \cong \operatorname{im} \phi \le S_p$

So

$|G/_{\ker \phi}| \,\big|\, |S_p| = p! = p \times (p-1) \times \cdots \times 1$

$|G/_{\ker \phi}| \,\big|\, |G|, \qquad$ all prime factors of G are $\ge p$

So $|G/_{\ker \phi}| \,\big|\, p \Rightarrow |G/_{\ker \phi}| \in \{1, p\}$

But if $|G/_{\ker \phi}| = 1$ then $\ker \phi = G$. Contradiction $\because \ker \phi \subseteq H \subsetneq G$

So $|G/_{\ker \phi}| = p$

$\Rightarrow \ker \phi = H$

Why?

$p = [G: H] \le [G: \ker \phi] = p \because \ker \phi \subseteq H$

This means we have equality so $H = \ker \phi$

So $H \trianglelefteq G \because$ it is a kernel

Proof of Theorem 5

By Cauchy's theorem, $\exists x \in G$ of order p.

Let $H = \langle x \rangle \le G$. (so $|H| = p$)

Notice $[G: H] = \frac{|G|}{|H|} = \frac{pq}{p} = q$, the smallest prime dividing $|G|$

So $H \trianglelefteq G$

By Cauchy's theorem,
$\exists y \in G$ of order q
notice that $G = \langle x, y \rangle$
Why? Let $K = \langle x, y \rangle$

$$\text{Then } \left.\begin{array}{l} \langle x \rangle \le K \Rightarrow p \mid |K| \\ \langle y \rangle \le K \Rightarrow q \mid |K| \end{array}\right\} \Rightarrow pq \mid |K| \Rightarrow |K| = pq \Rightarrow K = G$$

Since $\langle x \rangle \trianglelefteq G$,
$yxy^{-1} = x^i$ for some $i \in \{1, 2, \dots, p-1\}$
$\Rightarrow y^2xy^{-2} = y(yxy^{-1})y^{-1} = yx^iy^{-1} = (yxy^{-1})^i = (x^i)^i = x^{i^2}$
$y^3xy^{-3} = x^\wedge i^3$
Then $\boxed{y^q xy^{-q} = x^{i^q}}$ but $y^q = 1$
Thus $x = y^q xy^{-q} = x^{i^q}$
$\Rightarrow i^q \equiv 1 \pmod p$
By FLT $i^{p-1} \equiv 1 (\text{mod } p)$

Consider $\mathbb{Z}_p^*$ group under $\cdot$
Look at $[i] \in \mathbb{Z}_p^*$
$[i]^q = [i^q] = [1] \Rightarrow [i]$ has order dividing q
$[i]^{p-1} = [i^{p-1}] = 1 \Rightarrow [i]$ has order dividing $p-1$
$\Rightarrow o([i]) \mid \gcd(q, p-1)$
$[i] = [1] \Leftrightarrow i \equiv 1 \pmod p$
$yxy^{-1} = x \Rightarrow xy = yx$

So G is abelian $\because G = \langle x, y \rangle$ and $xy = yx$

Let $z = xy$
$\Rightarrow z^{pq} = x^{pq}y^{pq} = 1 \cdot 1 = 1$
$z^p = x^py^p = 1 \cdot y^p = y^p \neq 1 \because o(y) = q$
$z^q = x^qy^q = x^q \cdot 1 = x^1 \neq 1 \because o(x) = p$
So $o(z) = pq \Rightarrow G = \langle z \rangle \cong \mathbb{Z}_{pq}$
■

Groups of small order up to isomorphism

1	$\{1\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, S_3
7	$\mathbb{Z}_7$
8	TDB
9	abelian TDB
10	$\mathbb{Z}_{10}$, D_5
11	$\mathbb{Z}_{11}$
12	TBD
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}$, D_7

Correspondence Theorem

October-10-13 10:20 AM

Correspondence Theorem

Let G be a group and let $N \trianglelefteq G$.
Then there is a surjective homomorphism

$\pi: G \to G_{/N}, \quad \pi(g) = gN$

which gives a bijective correspondence between the subgroup of $G_{/N}$ and the subgroups of G that contain N.

1) Bijection
   $N \le K \le G \to \pi(K) \le G_{/N}$
   $N \le \pi^{-1}(L) \le G \leftarrow L \le G_{/N}$
2) If $N \le A \le B \le G \Rightarrow \pi(A) \le \pi(B)$
   and if $1 \le K \le L \le G_{/N} \Rightarrow \pi^{-1}(K) \le \pi^{-1}(L)$
3) If $N \le A \le B \le G \Rightarrow [B:A] = [\pi(B):\pi(A)]$
4) If $N \le A \le G$ then $A \trianglelefteq G \Leftrightarrow \pi(A) \trianglelefteq G_{/N}$

Canonical Surjective

The map $\pi: G \to G_{/N},\ g \mapsto gN$ is called a **canonical surjective**.
$\pi(gh) = ghN = gHhH = \pi(g)\pi(h)$

Problem

Let G be a group and let $N \trianglelefteq G$. Show that if $G_{/N}$ is abelian, then all subgroups that contain N are normal in G.

Cayley's Theorem

Let G be a finite group. Then G is isomorphic to some subgroup of S_n for some $n \ge 1$. In fact, we can take $n = |G|$

Correspondence Theorem Example

$D_6 = \langle \sigma, \rho \mid \sigma^6 = \rho^2 = \mathrm{id}, \quad \sigma\rho = \rho\sigma^{-1} \rangle$
Subgroups:

Order 12 $\quad D_6$

Order 6 $\quad \langle \sigma, \sigma^3 \rangle = \langle \sigma \rangle \cong \mathbb{Z}_6, \quad \langle \sigma^2, \rho \rangle = \langle \sigma, \rho \rangle \cong \mathbb{Z}_6$

Order 4 $\quad \langle \rho, \sigma^3 \rangle,\ \langle \rho\sigma, \sigma^3 \rangle,\ \langle \rho^2, \sigma^3 \rangle$

Order 3 $\quad \langle \sigma^2 \rangle$

Order 2 $\quad N = \langle \sigma^3 \rho \rangle\ \langle \rho\sigma \rangle\ \langle \rho\sigma^2 \rangle\ \langle \rho\sigma^3 \rangle\ \langle \rho\sigma^4 \rangle\ \langle \rho\sigma^5 \rangle$

Order 1 $\quad \{1\}$

D_6 has order 12: $1, \sigma, \sigma^2, \sigma^3, \sigma^5, \sigma^6, \rho, \sigma\rho, \sigma^2\rho, \sigma$^

Proof of Correspondence Theorem

1) If $N \le K \le G \Rightarrow \pi(K) \le G_{/N}$
   $\pi\big|_K : K \to G_{/N}, \quad \pi(K) = \mathrm{im}\left(\pi\big|_k\right) \le G_{/N}$ subgroup
   If $L \le G_{/N}$ then $\pi^{-1}(L) \le G$ and $\pi^{-1}(L) \supseteq N$
   Since $\pi^{-1}(\{1\}) = \ker \pi = N$
   Notice $a, b \in \pi^{-1}(L) \Leftrightarrow \pi(a), \pi(b) \in L \Rightarrow \pi(ab) = \pi(a) + \pi(b) \in L \Rightarrow ab \in \pi^{-1}(L)$
   and $\pi(a) \in L \Rightarrow \pi(a)^{-1} \in L \Rightarrow \pi(a^{-1}) \in L \Rightarrow a^{-1} \in \pi^{-1}(L)$
   So $L \le G$ and $N \subseteq L$

   If $N \le K \le G$ then what is $\pi^{-1}(\pi(K))$?
   Ans: $\pi^{-1}(\pi(K)) = K$
   We have $\pi^{-1}(\pi(K)) \supseteq K \because \pi(K) \subseteq \pi(K)$
   We want to show that $K \supseteq \pi^{-1}(\pi(K))$
   If $\pi^{-1}(\pi(K)) \supsetneq K$ then we have $N \le K \lneqq G$
   Pick $x \in L \backslash K$. Then $xH \nsubseteq KN = K$
   So $\pi(x) = xN \ne kN = \pi(k)$ for any $k \in K$
   $\Rightarrow \pi(L) \supsetneq \pi(K)$ but $\pi(L) = \pi(\pi^{-1}(\pi(K)) = \pi(K)$
   Contradiction
      Why? $\pi: S \to T$ onto
      Claim: $\pi\left(\pi^{-1}(\pi(U))\right) = \pi(U)$
      If $x \in \pi(U) \Rightarrow x = \pi(u)$ for some $u \in U$
      ....
   So $\pi^{-1}(\pi(K)) = K$

   ### Exercise
   If $\{1\} \le K \le G_{/N} \Rightarrow \pi(\pi^{-1}(K)) = K$

   So this shows that π and π^{-1} induce bijections between subgroups of G that contain N and subgroups of $G_{/N}$

2) If $N \le A \le B \le G \Rightarrow \pi(A) \le \pi(B)$
   If $\{1\} \le K \le L \le G_{/N} \Rightarrow \pi^{-1}(K) \le \pi^{-1}(L)$

3) If $N \le A \le B \le G$ and $[B:A] = m \Rightarrow [\pi(B):\pi(A)] = m$
   ### Proof
   If $[B:A] = m \Rightarrow B = b_1A \sqcup b_2A \sqcup \cdots \sqcup b_mA$, disjoint
   $\Rightarrow \pi(B) = \pi(b_1)\pi(A) \cup \pi(b_2)\pi(A) \cup \cdots \cup \pi(b_m)\pi(A)$
   So $[\pi(B):\pi(A)] \le m$

   ### Claim
   If $i \ne j \Rightarrow \pi(b_i)\pi(A) \ne \pi(b_j)\pi(A)$
   $\pi(b_i)\pi(A) = \pi(b_j)\pi(A) \Leftrightarrow \pi(b_j)^{-1}\pi(b_i) = \pi(A) \Leftrightarrow \pi(b_j^{-1}b_i) \in \pi(A) \Leftrightarrow b_j^{-1}b_i \in AN \Leftrightarrow b_i \in b_jA \Leftrightarrow b_iA = b_j$

$G \to G_{/N}$
$|\qquad \le$
$A \to \pi(A)$
$|$
$N \leftrightarrow \pi(N) = \{N\} \in$ identity of $G_{/N}$

4) $N \le A \trianglelefteq G \Rightarrow \pi(A) = A_{/N} \trianglelefteq G_{/N}$
   Criterion for normality. Let $H \le G$ then $N \trianglelefteq G \Leftrightarrow gHg^{-1} \subseteq H\ \forall g \in G$
   Proof: If $H \trianglelefteq G \Rightarrow$ every $g \in G$ is in normalizer of H
      $\Rightarrow gHg^{-1} = H \Rightarrow gHg^{-1} \subseteq H$
      Conversely, if $gHg^{-1} \subseteq H\ \forall g \in G$
      $\Rightarrow (g^{-1})H(g^{-1})^{-1} \subseteq H \Rightarrow g^{-1}Hg \subseteq H \Rightarrow H \subseteq gHg^{-1}$
      $\Rightarrow gHg^{-1} = H\ \forall g \in G \Rightarrow N_G(H) = G \Rightarrow H \trianglelefteq G$

   Let $gN \in G_{/N}$
   Then $(gH)\pi(A)(gN)^{-1} = \pi(g)\pi(A)\pi(g^{-1}) = \pi(gAg^{-1}) = \pi(A)$
   So $gH \in N_{G_{/N}}(\pi(A))\ \forall g \in G \Rightarrow \pi(A) \trianglelefteq G$
   A similar argument shows that if $K \trianglelefteq G_{/N} \Rightarrow \pi^{-1}(K) \trianglelefteq G$

Answer to Problem

$G \rightsquigarrow G_{/N}$

|

$K \rightsquigarrow \pi(K) \trianglelefteq G_{\backslash \mathrm{N}} \because G_{/N}$ abelian $\Rightarrow K \trianglelefteq G$

|

N

Proof of Cayley's Theorem

Let $X = G$ and let G act on X by left multiplication

$g \cdot G = g \cdot \{g_1, \dots, g_n\} = \{gg_1, gg_2, \dots, gg_n\}$

This gives a homomorphism

$\Phi: G \to S_x \cong S_n$

What is $\ker \phi$? $\ker \phi = \{g \in G : gg_i = g_i \text{ for } i = 1, \dots, n\} = \{1\}$

So Φ is 1-1

So Φ gives an embedding of G and $G \cong \mathrm{im}(\Phi) \leq S_n$

Important part Φ is a **faithful action**.

ie.e $\{g: gx = x \forall x\} = \{x\}$

This action is also **transitive** - this means that there is exactly one orbit

Equivalently, $\forall x, y \in X \Rightarrow \exists g \in G \;\; g \cdot x = y$

Symmetric Groups Revisited

October-15-13 10:08 AM

Theorem

Let $n \geq 1$ and let $\sigma \in S$. Then $\mathcal{C}_\sigma$ consists of all $\tau \in S_n$ whose disjoint cycle structructure is the same as σ's
i.e. if σ has m_i i-cycles for $1 \leq i \leq n$ (disjoint)
$\Rightarrow \tau$ has m_i i-cycles for $1 \leq i \leq m$

Theorem (Centre of S_n)

If $n > 2$, then $Z(S_n) = \{\text{id}\}$

Theorem

If $n \neq 2,6$
Then $\text{Aut}(S_n) = \text{Inn}(S_n) \cong S_n$

Remark 1

If $f: G \to G$ is an automorphism
Then $f(\mathcal{C}_g) = \{f(x): x \in \mathcal{C}_g\} = \{f(ygy^{-1}) : y \in G\} = \{f(y)f(g)f(y)^{-1} : y \in G\} = \{xf(g)x^{-1} : x \in G\} = \mathcal{C}_{f(g)}$

Remark 2:

If g has order $d \Rightarrow f(g)$ has order d.
Why?

$f(g)^d = f(g^d) = f(1) = 1$
So $o(f(g)) | o(g)$
Bu this holds for any automorphism
$o\left(f^{-1}(f(g))\right) \Big| \, o(f(g)) \Rightarrow o(g) \mid o(f(g))$
$\Rightarrow o(g) = o(f(g))$

Corollary

Suppose $f: S_n \to S_n$ is an automorphism.
Then $f(\mathcal{C}_{(1\,2)}) = \mathcal{C}_{(1\,2)(3\,4)\cdots(2j-1\,2j)}$ for some $j \geq 1$

What is $|\mathcal{C}_{(1\,2)(3\,4)\cdots(2j-1\,2j)}|$?

$j = 1$: $|\mathcal{C}_{(1\,2)}| = \binom{n}{2}$

$j = 2$: $|\mathcal{C}_{(1\,2)(3\,4)}| = \dfrac{\binom{n}{2}\binom{n-2}{2}}{2}$

$j = 3$: $|\mathcal{C}_{(1\,2)(3\,4)(5\,6)}| = \dfrac{\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}}{3!} = \dfrac{n!}{(n-6)!\,3!\,2^3}$

$|\mathcal{C}_{(1\,2)(3\,4)\cdots(2j-1\,2j)}| = \dfrac{n!}{(n-2j)!\,j!\,2^j}$

Remark 3

If $f: S_n \to S_n$ is an automorphism and $f(\mathcal{C}_{(1\,2)}) = \mathcal{C}_{(1\,2)(2\,3)\cdots(2j-1\,2j)}$ for some $j \geq 1$ then
$|\mathcal{C}_{(1\,2)}| = |\mathcal{C}_{(1\,2)(3\,4)\cdots(2j-1\,2j)}| \Rightarrow \dfrac{n!}{(n-2)!\,2} = \dfrac{n!}{(n-2j)!\,j!\,2^j}$

In particular
$(*)$ $j!\,2^{j-1} = (n-2)(n-3)\cdots(n-2j+1)$
Notice $n \geq 2j$ so
$(n-2)(n-3)\cdots(n-2j+1) \geq (2j-2)!$
$(n-2) \geq (2j-2)$
So equation (*) gives $(2j-2)! \leq j!\,2^{j-1} \Rightarrow$
$(2j-2)(2j-3)\cdots(j+1) \leq 2^{j-1}$
There are $j-2$ terms on LHS
If $j \geq 4 \Rightarrow (2j-3)\cdots(j+1) \leq 2^{j-1} \Rightarrow 4^{j-2} \leq 2^{j-1} \Rightarrow 2(j-2) \leq j-1 \Rightarrow j \leq 3$ Contradiction.
So conclude that if
$|\mathcal{C}_{(1\,2)}| = |\mathcal{C}_{(1\,2)(3\,4)\cdots(2j-1\,2j)}| \Rightarrow j \in \{1,2,3\}$

$j = 2$

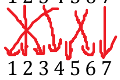
If $|\mathcal{C}_{(1\,2)}| = |\mathcal{C}_{(1\,2)(3\,4)}| \Rightarrow \binom{n}{2} = \dfrac{\binom{n}{2}\binom{n-2}{2}}{2}$
$\Rightarrow 2 = \dfrac{(n-2)(n-3)}{2}$
$\Rightarrow 4 = (n-2)(n-3)$. No solutions

$j = 3$

If $|\mathcal{C}_{(1\,2)}| = |\mathcal{C}_{(1\,2)(3\,4)(5\,6)}| \Rightarrow \binom{n}{2} = \dfrac{\binom{n}{2}\binom{n-2}{2}\binom{n-6}{2}}{6}$
$\Rightarrow 24 = (n-2)(n-3)(n-4)(n-5)$
has a solution only when $n = 6$

$n \geq 1$, $S_n = \{\sigma: \{1, \dots, n\} \to \{1, \dots, n\} \mid \sigma \text{ is 1-1}\}$, $|S_n| = n!$

Disjoint cycle notation

e.g. $n = 7$
1 2 3 4 5 6 7

1 2 3 4 5 6 7

$(1\,3\,4)(2)(5\,6)(7) = (2)(7)(5\,6)(1\,3\,4) = (5\,6)(1\,3\,4)$

Conjugacy Classes

What is the conjugacy class of a permutation $\sigma \in S_n$?
Let's first consider the case of a single cycle $(a_1 a_2 a_3 \cdots a_k)$
What is $\tau(a_1 a_2 \cdots a_k)\tau^{-1}$
Let $\sigma = \tau(a_1 a_2 \cdots a_k)\tau^{-1}$
What does σ do to $\tau(a_1)$?
$\tau(a_1 \cdots a_k)\tau^{-1}(\tau(a_1)) = \tau(a_1 a_2 \cdots a_k)(a_1) = \tau(a_2)$
In general,
$\tau(a_1, \dots, a_k)\tau^{-1}$ sends $\tau(a_i) = \tau(a_{i+1})$ for $i = 1, \dots, k$ where we take $a_{k+1} = a_1$

If $m \notin \{\tau(a_1), \dots, \tau(a_k)\}$ what is $\tau(a_1, \dots, a_k)\tau^{-1}(m)$?
Answer: it is m
So $\tau(a_1, \dots, a_k)\tau^{-1} = (\tau(a_1), \tau(a_2), \dots, \tau(a_k))$

Proof of Theorem

Suppose σ has s disjoint cycles of lengths $k_1, k_2, \dots, k_s$; $k_1 + k_2 + \cdots + k_s = n$
Write $\sigma = (a_1 a_2 \cdots a_{k_1})(a_{k+1} \cdots a_{k_1+k_2}) \cdots (a_{k_1+\cdots+k_{s-1}+1} \cdots a_{k_1+\cdots+k_{s-1}+k_s})$
Let $\tau \in S_n$
Then, as we just showed,
$\tau\sigma\tau^{-1} = [\tau(a_1 \cdots a_k)\tau^{-1}][\tau(a_{k_1+1} \cdots a_{k_1+k_2})\tau^{-1}] \cdots [\tau(a_{k_1+\cdots+k_{s-1}+1} \cdots a_{k_1+\cdots+k_{s-1}+k_s})\tau^{-1}]$
$= (\tau(a_1) \cdots \tau(a_2))\left(\tau(a_{k_1+1}) \cdots \tau(a_{k_1+k_2})\right) \cdots \left(\tau(a_{k_1+\cdots+k_{s-1}+1}) \dots \tau(a_{k_1+\cdots+k_{s-1}+k_s})\right)$

Thus $\mathcal{C}_\sigma \subseteq \{$all permutations with same disjoint cycle structure$\}$
To finish, suppose that $\mu = (b_1 \cdots b_{k_1}) \cdots (b_{k_1+\cdots+k_{s-1}+1} \cdots b_{k_1+\cdots+k_s})$ has the same cycle structure as σ.
Thus, $\mu = \tau\sigma\tau^{-1}$, where τ sends $a_i \mapsto b_i$ for $1 \leq i \leq n$ so $\mu \in \mathcal{C}_\sigma$. Thus the result follows. ∎

Example

S_4

Conjugacy class	size
id	1
(1 2)	$\binom{4}{2} = 6$
(1 3 2) & (1 2 3)	$\binom{4}{3} \times 2 = 8$
(1 2)(3 4)	3
(1 2 3 4)	6

Find all normal subgroups of S_4
Remember,
$N \trianglelefteq G \Rightarrow n \in N$ then $gng^{-1} \in N \ \ \forall g \in G$; i.e. $\mathcal{C}_n \leq N$

Assignment Q: N is a union of conjugacy classes
Answer:
$N \in \left\{\{1\}, \{1\} \cup \mathcal{C}_{(1\,2)(3\,4)}, \{1\} \cup \mathcal{C}_{(1\,2)(3\,4)} \cup \mathcal{C}_{(1\,2)}, S_4\right\}$
$\{\text{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \in$ Klein 4 subgroup of S_4

Proof of Theorem (Centre of S_n)

Let $n > 2$. Let $\sigma \in Z(S_n)$ and suppose that $\sigma \neq \text{id}$.
Then σ has at least one k-cycle for some $k > 1$. Then for any μ with the same cycle structure $\exists \tau$ such that $\tau\sigma\tau^{-1} = \mu$.
But note that there is some $\mu \neq \sigma$ with the same cycle structure
Why?

$\sigma = (a_1 \cdots a_k)(\dots)\cdots(\dots)$
We know $k > 1$
Case 1: $k \geq 3$
$\mu = (a_1 a_2 \cdots a_{k-2} a_k a_{k-1})(\dots)\cdots(\dots)$
Case 2: $k = 2, n > 2$
$\sigma = (a_1 a_2) \dots (a_i) \dots \exists a_i \neq a_1, a_2$
$\mu = (a_1 a_i) \dots (a_2)$

So $\tau\sigma\tau^{-1} = \mu \neq \sigma$ and so $\tau\sigma \neq \sigma\tau \Rightarrow \sigma \notin Z(S_n) \Rightarrow Z(S_n) = \{id\}$

Automorphisms of S_n

Recall that if G is a group we have a homomomorphism
$\Phi: G \to \text{Aut}(G)$, $g \to \Phi_g: G \to G$, $\Phi_G(x) = gxg^{-1}$
$\ker(\Phi) = \{g: \Phi_G = \text{id}\} = \{g: gxg^{-1} = x \ \ \forall x \in G\} = \{g \in G : gx = xg \ \forall x \in G\} = Z(G)$
So by 1st isomorphism theorem,

$G_{/Z(G)} \cong \text{Im}(\Phi) =: \text{Inn}(G)$ The inner automorphism group of G

If $|\mathcal{C}_{(1\ 2)}| = |\mathcal{C}_{(1\ 2)(3\ 4)(5\ 6)}| \Rightarrow \binom{n}{2} = \dfrac{\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}}{6}$
$\Rightarrow 24 = (n-2)(n-3)(n-4)(n-5)$
has a solution only when $n = 6$

Combining all of this, we see that if $n \neq 6$ and $f\colon S_n \to S_n$ then $f(\mathcal{C}_{(1\ 2)}) = \mathcal{C}_{(1\ 2)}$

Fact

$\exists$ an automorpthism of S_n that sends (1 2) to (1 2)(3 4)(5 6)
Next time, we'll show that if $f\colon S_n \to S_n$ sends $\mathcal{C}_{(1\ 2)}$ to $\mathcal{C}_{(1\ 2)}$ then f is given by conjugation. This will prove the result.

$\ker(\Phi) = \{g\colon \Phi_G = \mathrm{id}\} = \{g\colon gxg^{-1} = x\ \ \forall x \in G\} = \{g \in G : gx = xg\ \forall x \in G\} = Z(G)$
So by 1st isomorphism theorem,
$G_{/Z(G)} \cong \mathrm{Im}(\Phi) =: \mathrm{Inn}(G)$ The inner automorphism group of G

Symmetric Groups Cont.

October-22-13 10:03 AM

Last Time

We showed that if $f: S_n \to S_n$ and $n \neq 6$ then $f(C_{(1\,2)}) = C_{(1\,2)}$, i.e. f takes transpositions to transpositions

Goal

To show that if $n \neq 6 \Rightarrow f$ is **inner** (i.e. $\exists$ a permutation $\tau \in S_n$ such that $f(\sigma) = \tau\sigma\tau^{-1}\ \forall \sigma \in S_n$)

Remaining Steps

Step 1

Show that if G is a group and $S \subseteq G$ generates G and $f, g \in \mathrm{Aut}(G)$ such that $f(s) = g(s) \forall s \in S \Rightarrow f \equiv g$

Step 2

Show $S = \{(i\ i+1) : i = 1, \dots, n-1\}$ generates S_n

Step 3

Show that if $f \in \mathrm{Aut}(S_n)$ takes transpositions to transpositions then $\exists \tau \in S_n$ such that
$f((i\ i+1)) = \tau(i\ i+1)\tau^{-1}$ for $i = 1, 2, \dots, n-1$

Proof of Step 1

Let $x \in G$. We want to show $f(x) = g(x)$
Since S generates G, we can write $x = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k}$, where $s_1, \dots, s_k \in S$, $\epsilon_1, \dots, \epsilon_k \in \{\pm 1\}$
Then $f(x) = f(s_1^{\epsilon_1} \cdots s_k^{\epsilon_k}) = f(s_1^{\epsilon_1}) \cdots f(s_k^{\epsilon_k}) = f(s_1)^{\epsilon_1} \cdots f(s_k)^{\epsilon_k} = g(s_1)^{\epsilon_1} \cdots g(s_k)^{\epsilon_k} = g(s_1^{\epsilon_1} \cdots s_k^{\epsilon_k}) = g(x)$

Proof of Step 2

Lemma

1) The set of all transpositions generates S_n

   Since each $\sigma \in S_n$ is a product of disjoint cycles, it is enough to show we can write any cycle as a product of transpositions.

   Aside
   $(i\ j\ k) = (i\ j)(j\ k)$
   Similarly
   $(i_1\ i_2 \dots i_n) = (i_1\ i_2)(i_2\ i_3) \cdots (i_{n-1}\ i_n)$

   So every cycle is a product of transpositions. This proves (1)

2) $\{(i\ i+1) : i = 1, \dots, n-1\}$ generates S_n

   For (2), it suffices by (1) to show each transposition is a product of transpositions of the form $(i\ i+1)$
   $(i\ i+2) = (i\ i+1)(i+1\ i+2)(i\ i+1)$
   $(i\ i+3) = (i+2\ i+3)(i\ i+2)(i+2\ i+3)$
   In general, if $i < j, j - i \geq 2 \Rightarrow (i\ j) = (j-1\ \ j)(i\ j-1)(j-1\ \ j)$
   So by induction on $j - i$ we can write each trasposition as a product of elements from $\{(k\ k+1), k = 1, \dots, n-1\}$

Proof of Step 3

Proposition

Let $f: S_n \to S_n$ be an automorphism that takes transpositions to transpositions.
Then $\exists \tau \in S_n$ such that $f((i\ i+1)) = \tau(i+1)\tau^{-1}$ for $i = 1, \dots, n-1$
Before we begin, note that $\tau(i\ i+1)\tau^{-1} = (\tau(i), \tau(i+1))$

Proof of Proposition

Since f takes transpositions to transpositions,
$f((1\ 2)) = (a_1\ a_2)$ for some $a_1, a_2 \in \{1, \dots, n\}$ and
$f((2\ 3)) = (a_3\ b)$ for some $a_3, b \in \{1, \dots, n\}$
$(1\ 2)(2\ 3) \neq (2\ 3)(1\ 2)$ so $f((1\ 2)(2\ 3)) \neq f((2\ 3)(1\ 2))$ since f is 1-1
$\Rightarrow f((1\ 2))f((2\ 3)) \neq f((2\ 3))f((1\ 2)) \Rightarrow (a_1\ a_2)(a_2\ b) \neq (a_3\ b)(a_1\ a_2)$ so $\{a_1, a_2\} \cap \{a_3, b\} \neq \emptyset$
WLOG $a_2 = b$ so $f((1\ 2)) = (a_1\ a_2)$, $f((2\ 3)) = (a_2\ a_3)$, a_1, a_2, a_3 pairwise distrinct $\because f$ is 1-1
Similarly, $f((3\ 4)) = (a_3\ a_4)$ for some a_4 with a_1, a_2, a_3, a_4 pairwise distinct.
Continuing in this manner we see that $\exists a_1, \dots, a_n$ pairwise distinct such that
$f((i\ i+1)) = (a_i\ \ a_{i+1})$ for $i = 1, 2, \dots, n-1$

Let $\tau: \{1, \dots, n\} \to \{1, \dots, n\}$ be given by $\tau(i) = a_i\ \forall i$
So τ is a permutation of $\{1, \dots, n\}$ and $\tau(i\ i+1)\tau^{-1} = (\tau(i)\ \tau(i+1)) = (a_i\ a_{i+1}) = f((i\ i+1))$
■

Theorem

If $n \neq 6$ and $f: S_n \to S_n$ is an automorphsim then $\exists \tau \in S_n$ such that $f(\sigma) = \tau\sigma\tau^{-1}\ \forall \sigma \in S_n$, $i.e. f$ is inner

Proof of Theorem

We showed last time that $f(C_{(1\,2)}) = C_{(1\,2)}$. By step 3, $\exists \tau \in S_n$ such that
$f((i\ i+1)) = \tau(i\ i+1)\tau^{-1}$ for $i = 1, \dots, n-1$

By step 2,
$S = \{(i\ i+1) : i = 1, \dots n-1\}$ generates S_n
Define $g(\sigma) = \tau\sigma\tau^{-1}$ then $f(s) = g(s)\ \forall s \in S$ and so by step 1, $f \equiv g$, i.e. $f(\sigma) = g(\sigma) = \tau\sigma\tau^{-1}\ \forall \sigma \in S_n$
So f is inner. ■

Corollary

If $n \neq 2{,}6$ then $\mathrm{Aut}(S_n) \cong \mathrm{Inn}(S_n) \cong S_n$

Proof of Corollary

If $n \neq 6$, we have shown $\text{Aut}(S_n) = \text{Inn}(S_n)$
We showed that for a group G, $\text{Inn}(G) \cong G_{/Z(G)}$ (we showed for $n \neq 2$, $Z(S_n) = \{\text{id}\}$
So if $n \neq 2$, $\text{Inn}(S_n) \cong S_{n/\{id\}} \cong S_n$

Structure Theorem

October-22-13 10:58 AM

Finitely Generated

Saying that A is finitely generated means $\exists k \geq 1$ and $x_1, \dots, x_k \in A$ such that every $a \in A$ can be written as $a = m_1x_1 + \cdots + m_kx_k,\ m_1, \dots, m_k \in \mathbb{Z}$

Structure Theorem for Finitely Generated Abelian Groups

1) Let A be a finitely generated abelian group.
   Then $\exists$ a nonnegative integer r and a finite abelian group T such that
   $A = \mathbb{Z}^r \times T$
2) Let $|T| = n = p_1^{i_1}p_2^{i_2}\cdots p_k^{i_k},\quad p_1, \dots, p_k$ prime
   Then $T \cong T_1 \times T_2 \times \cdots \times T_k$ were T_j is an abelian group of size $p_j^{a_j}$
3) If p is prime and B is an abelian group of order p^m then
   $B \cong \mathbb{Z}_{p^{l_1}} \times \mathbb{Z}_{p^{l_2}} \times \cdots \times \mathbb{Z}_{p^{l_s}}$ for some $s \geq 1$ with $l_1 \leq l_2 \leq \cdots \leq l_s$
   and $l_1 + l_2 + \cdots + l_s = m$
   Moreover, s and $l_1 \leq l_2 \leq \cdots \leq l_s$ are unique.

Corollary to STFFGAG

If G is a group of size p^2 then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$

Lemma

Let $(A, +)$ be an abelian group of order mn with $\gcd(m,n) = 1$
Then $A \cong B \times C$ with B, C abelian and $|B| = m$ and $|C| = n$.

Note

Recall that any cyclic group C has the property that either
$C \cong \mathbb{Z}$ or $\exists n \geq 1$ such that $C \cong \mathbb{Z}_n$

Weak Structure Theorem for Finitely Generated Abelian Groups

Let A be an abelian group. Then A isi isomorphic to a finite product of cyclic groups.
More specifically, $\exists r, s \geq 0$ and $n_1, \dots, n_s \geq 1$ not necessarily distinct such that
$A \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$
Moreover, if $A \cong \mathbb{Z}^{r'} \times \mathbb{Z}_{n_1'} \times \mathbb{Z}_{n_2'} \times \cdots \times \mathbb{Z}_{n_s'}$
then $r = r'$. We call r the **rank** of A.

Strong Version of Structure Theorem

Let A be a finitely generated abelian group.
Then $\exists r \geq 0, s \geq 0, p_1^{n_1}, \dots, p_s^{n_s}$, prime powers, such that
$A \cong \mathbb{Z}^r \times \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_s^{n_s}}$

Chinese Remainder Theorem

If $m_1, \dots, m_k$ are pairwise relatively prime, i.e. $i \backslash en\ j \Rightarrow \gcd(m_i, m_j) = 1$ and
$a_1, \dots, a_k \in \mathbb{Z}$
Then $\exists x \in \mathbb{Z}$ such that
$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$\vdots$
$x \equiv a_k \pmod{m_k}$

Example

What are the abelian groups of order 72?
$72 = 2^3 \cdot 3^2$
If T is abelian of order 72 then by (2), $T \cong T_1 \times T_2, |T_1| = 2^3, |T_2| = 3^2$
by (3), $T_1 \cong \mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
$T_2 \cong \mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$

So $T \cong$ one of $\mathbb{Z}_8 \times \mathbb{Z}_9,\ \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3,\ \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9, \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

How may (up to isomorphism) abelian group of order p^5 are there?
Answer: 7
$\mathbb{Z}_{p^5},\quad \mathbb{Z}_p \times \mathbb{Z}_{p^4},\quad \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^3},\quad \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2},$
$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p,\quad \mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2},\quad \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^3}$

Proof of Lemma

Let $B = \{a \in A : ma = 0\}$ and $C = \{a \in A : na = 0\}$
Claim:
$B \cap C = \{0\}$. Why? If $a \in B \cap C,\ a \in B \Rightarrow ma = 0,\ a \in C \Rightarrow na = 0$
$a \in B \cap C \Rightarrow \gcd(m,n)\, a = 0 \Rightarrow a = 0$
Next we have $A = B + C$
Why? Since $\gcd(m,n) = 1\ \exists c, d$ such that $cm + dn = 1$
So if $a \in A \Rightarrow a = (dn + cn)a = dna + cma \in B + C$
So $A = B + C\ \because B \cap C = \{0\} \Rightarrow A = B \bigoplus C \cong B + C$

Proof of Weak Structure Theorem

Let $x_1, \dots, x_m$ be a generating set for A. We prove this by induction on m.

Base Case: $m = 1$

$A = \langle x_1 \rangle$ is cyclic. We showed before that cyclic groups are either $\mathbb{Z}$ or $\mathbb{Z}_n, n \geq 1$

Induction

Assume the results holds whenever $m < k$ and suppose that $A = \langle x_1, \dots, x_, \rangle$
Let $\mathcal{G} = \{\{y_1, \dots, y_k\} \subseteq A.\ A = \langle y_1, \dots, y_k \rangle\}$

Case 1

$x_1, \dots, x_k$ are $\mathbb{Z}$-linearly independent
that is, if $n_1x_1 + \cdots + n_kx_k = 0, n_1, \dots, n_k \in \mathbb{Z}$ then $n_1 = n_2 = \cdots = n_k = 0$
In this case we claim that $A \cong \mathbb{Z}^k$

Proof of Claim

Define $\phi: \mathbb{Z}^k \to A$ by $\phi\big((n_1, \dots, n_k)\big) = n_1x_1 + \cdots + n_kx_k \in A$
Notice that ϕ iis a homomorphism.
$\phi\big((n_1, \dots, n_k) + (m_1, \dots, m_k)\big) = \phi(n_1 + m_1, \dots, n_k + m_k)$
$= (n_1 + m_1)x_1 + \cdots + (n_k + m_k)x_k$
$= (n_1x_1 + \cdots + n_kx_k) + (m_1x_1 + \cdots + m_kx_k)$
$= \phi(n_1, \dots, n_k) + \phi(m_1, \dots, m_k)$
Note: $x_1, \dots, x_k$ generates A. If $a \in A \Rightarrow \exists n_1, \dots, n_k \in \mathbb{Z}$ such that
$a = \phi(n_1, \dots, n_k) = n_1x_1, \dots, n_kx_k$
Notice that $(n_1, \dots, n_k) \in \ker\phi \Leftrightarrow \phi\big((n_1, \dots, n_k)\big) = 0 \Leftrightarrow n_1x_1 + \cdots + n_kx_k = 0$
$\Leftrightarrow n_1, \dots, n_k = 0$
So $\ker\phi = \{(0, \dots, 0)\} \Rightarrow \phi$ is 1-1
So ϕ is a bijection hence isomorphism $\Rightarrow A \cong \mathbb{Z}^k$

Case 2

$x_1, \dots, x_k$ are $\mathbb{Z}$-linearly dependent. i.e. $\exists c_1, \dots, c_k \in \mathbb{Z}$ not all 0 such that
$c_1x_1 + \cdots + c_kx_k = 0$
Define $c(x_1, \dots, x_k) + 0$ to be the smallest positive $c_i \neq 0$ that appears in some relation among $x_1, \dots, x_k$
$c(x_1, \dots, x_k) =$ smallest positive integer C such that $\exists c_1, \dots, c_k \in \mathbb{Z}$ and
$c_1x_1 + \cdots + c_kx_k = 0$ and $c_i = C$ for some i

Example

Suppose $\mathbb{Z}^3, x_1 = (2,4,6), x_2 = (3,6,9), x_3 = (5,10,15)$
$x_3 - x_2 - x_1 = 0 \Rightarrow c(x_1, x_2, x_3) = 1$

Let $N = \min\{c(y_1, \dots, y_k) : \{y_1, \dots, y_,\} \in \mathcal{G}\}$
Then $\exists (y_1, \dots, y_k) \in \mathcal{G}$ and $c_1, \dots, c_k \in \mathbb{Z}$ with $c_1 = N$ such that
$c_1y_1 + c_2y_2 + \cdots + c_ky_k = 0$

Claim

$N | c_1, \dots, N | c_k$

Proof of Claim

By the division algorithm, we can write
$c_i = Nq + c_i',\ 0 \leq c_i' < N$ for $i = 1, \dots, k$
So $c_1y_1 + c_2y_2 + \cdots + c_ky_k = 0$
$\Rightarrow Ny_1 + (Nq_2 + c_2')y_2 + \cdots + (Nq_k + c_k')y_k = 0$
$\Rightarrow N(y_1 + q_2y_2 + \cdots + q_ky_k) + c_2'y_2 + \cdots + c_k'y_k = 0$
Let $z_1 = (y_1 + q_2y_2 + \cdots + q_ky_k)$
$z_2 = y_2$
$z_3 = y_3$
...
$z_k = y_k$
$\Rightarrow Nz_1 + c_2'z_2 + \cdots + c_k'z_k = 0$

If one of $c_2', \ldots, c_k'$ is nonzero then $c(z_1, \ldots, z_k) < N$ which contradictcts minimality of N. We we have that $c_2' = \cdots = c_k' = 0 \Rightarrow Nz_1 = 0$

Have $A = \langle z_1, z_2, \ldots, z_k \rangle$ and $Nz_1 = 0$
We claim that
$A \cong \langle z_1 \rangle \times \langle z_2, \ldots, z_k \rangle, \qquad \langle z_1 \rangle \cong \mathbb{Z}_N$
Once we have this we are done since by the induction hypothesis, $\langle z_2, \ldots, z_k \rangle$, which is generated by a set of size $k - 1 < k$ is a product of cyclic groups and $\langle z_1 \rangle$ is cyclic $\Rightarrow A$ is isomorphic to a product of cyclic groups.

Let $B = \langle z_1 \rangle \subseteq A$
Let $C = \langle z_2, \ldots, z_k \rangle$
Then $B + C = \langle z_1, z_2, \ldots, z_k \rangle = A$
Notice that $B \cap C = (0)$. To see this, if $a \in B \cap C, a \neq 0$
$a \in B \Rightarrow a = rz_1, \qquad r \in \{1, 2, \ldots, N-1\}$
$\because a \neq 0, r \neq 0$ and $r < N \because Nz_1 = 0$
$a \in C \Rightarrow \exists d_2, \ldots, d_k \in \mathbb{Z}$ such that $d_2 z_2 + \cdots + d_k z_k = a$
$\Rightarrow rz_1 = d_2 z_2 + \cdots + d_k z_k \Rightarrow rz_1 - d_2 z_2 - \cdots - d_k z_k = 0$ but $0 < r < N$
This contradicts minimality of N. So $B \cap C = (0)$

Now we have an isomorphism
$\Psi: B \times C \to A, \qquad \Psi\big((b, c)\big) = b + c$

- Homomorphism
  $\Psi\big((b_1, c_1) + (b_2, c_2)\big) = \Psi\big((b_1 + b_2, c_1 + c_2)\big) = (b_1 + b_2) + (c_1 + c_2)$
  $= (b_1 + c_1) + (b_2 + c_2) = \Psi\big((b_1, c_1)\big) + \Psi\big((b_2, c_2)\big)$
- Onto $A = B + C \because B + C = \langle z_1, \ldots, z_k \rangle = A$
- 1-1 If $\Psi\big((b, c)\big) = 0 \Leftrightarrow b + c = 0 \Leftrightarrow b = -c \Leftrightarrow b_1 - c \in B \cap C = (0) \Leftrightarrow b = c = 0$
  So $\ker \Psi = \big((0, 0)\big) \Rightarrow \Psi$ is 1-1

So $A \cong B \times C \cong \langle z_1 \rangle \times \langle z_2, \ldots, z_k \rangle$
■

to finish, we need to show that rank is an invariant. .e. if
$A \cong \mathbb{Z}^{r_1} \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s} = \mathbb{Z}^{r_2} \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$
Then $\boxed{r_1 = r_2}\ \big(= \operatorname{rank}(A)\big)$

Proof

Suppose WLOG $r_1 > r_2$
Let $\phi: \mathbb{Z}^{r_1} \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s} \to \mathbb{Z}^{r_2} \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$
be an isomorphism.
Let $e_1 = (1, 0, 0, \ldots, 0) \times (0, \ldots, 0)$
$e_2 = (0, 1, \ldots, 0) \times (0, \ldots, 0)$
$e_{r_1} = (0, 0, \ldots, 0, 1) \times (0, \ldots, 0)$
Notice that $e_1, \ldots, e_r$ are $\mathbb{Z}$-linearly independent.
$\phi(e_1) = (\vec{v}_1, t_1), \qquad \vec{v}_1 \in \mathbb{Z}^{r_2}, \qquad t_1 \in T = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$
...
$\phi(e_k) = \big(\vec{v}_{r_1}, t_{r_1}\big), \qquad \vec{v}_{r_1} \in \mathbb{Z}^{r_2}, \qquad t_{r_1} \in T$
$\mathbb{Z}^{r_2} \subseteq \mathbb{Q}^{r_2}$
Then $r_1 > r_2$ so $\vec{v}_1, \ldots, \vec{v}_{r_1}$ are linearly dependent.
So $\exists c_1, \ldots, c_{r_1} \in \mathbb{Q}$ not all 0 such that
$c_1 \vec{v}_1 + \cdots + c_{r_1} \vec{v}_{r_1} = 0$. Let $D =$ common denominator for $c_1, \ldots, c_{r_1}$
$\Rightarrow (Dc_1)\vec{v}_1 + \cdots + \big(Dc_{r_1}\big)\vec{v}_{r_1} = 0$
Let $0 \neq x = (Dc_1)e_1 + \cdots + \big(Dc_{r_1}\big)e_{r_1}$
$\phi(x) = Dc_1 \phi(x_1) + \cdots + Dc_{r_1} \phi\big(e_{r_1}\big) = Dc_1(\vec{v}_1, t) + \cdots + Dc_{r_1}\big(\vec{v}_{r_1}, t_{r_1}\big) =$
$\big(Dc_1 \vec{v}_1 + \cdots + Dc_{r_1} \vec{v}_{r_1}, Dc_1 t_1 + \cdots + Dc_{r_1} t_{r_1}\big) = \big(\vec{0}, t\big)$ for some $t \in T$
Since T is a finite group, t has finite order so $\exists M \geq 1$ such that $Mt = 0$.
So $\phi(Mx) = M\phi(x) = M\big(\vec{0}, t\big) = \big(\vec{0}, 0\big)$
But $Mx = (MDc_1)e_1 + \cdots + \big(MDc_{r_1}\big)e_k \neq 0$ and ϕ is 1-1, a contradiction.
So $r_1 = r_2$

Proof of Strong Structure Theorem

We already have that
$A \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t}$
So it is enough to show that if $n > 1$ then $\mathbb{Z}_n$ is the product of cyclic groups of prime power order.
Write $n = p_1^{t_1} \cdots p_s^{t_s}$
Claim $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{t_1}} \times \cdots \times \mathbb{Z}_{p_s^{t_s}}$
We make a map
$\phi: \mathbb{Z}_n \to \mathbb{Z}_{p_1^{t_1}} \times \cdots \times \mathbb{Z}_{p_s^{t_s}}, \qquad \phi([x]) = \Big([x]_{p_1^{t_1}}, \ldots, [x]_{p_s^{t_s}}\Big)$
Notice that ϕ is well-defined.
If $[x]_n = [y_n] \Leftrightarrow x \equiv y \pmod{n}$ But $n = p_1^{t_1} \ldots p_s^{t_s}$
$\Leftrightarrow n\big|(x - y) \Rightarrow p_i^{t_i}\big|(x - y) \Rightarrow x \equiv y \left(\bmod p_i^{t_i}\right) \Rightarrow [x]_{p_i^{t_i}} = [y]_{p_i^{t_i}}$

Next Class

Key tool: Chinese Remainder Theorem
Says if $m_1, \ldots, m_t$ are pairwise relatively prime and if $a_1, \ldots, a_t \in \mathbb{Z} \Rightarrow \exists x \in \mathbb{Z}$ such that $x \equiv a_i (\bmod m_i)$ for $i = 1, \ldots, t$
Last time , we constructed a map $\phi: \mathbb{Z}_n \to \mathbb{Z}_{p_1^{i_1}} \times \cdots \times \mathbb{Z}_{p_t^{i_t}}$
$[x]_n \mapsto ([x]_{p_1^{i_1}}, \ldots, [x]_{p_t^{i_t}}$

where $[x]_m$ is the equivalence class of x in $\mathbb{Z}_m$; i.e. $[x]_m = \{i : i \equiv x \pmod{m}\}$
Last time we showed this map is well-defined.
Notice that ϕ is a homomorphism
$\phi([x]_n + [y]_n) = \phi([x+y]_n) + \left([x+y]_{p_1^{i_1}}, \dots, [x+y]_{p_t^{i_t}}\right)$
$= \left([x]_{p_1^{i_1}} + [y]_{p_1^{i_1}}, \dots, [x]_{p_t^{i_t}} + [y]_{p_t^{i_t}}\right) = \left([x]_{p_1^{i_1}}, \dots, [x]_{p_t^{i_t}}\right) + \left([y]_{p_1^{i_1}}, \dots, [y]_{p_t^{i_t}}\right)$
$= \phi([x]_n) + \phi([y]_n)$

Notice that given $\left([a_1]_{p_1^{t_1}}, \dots, [a_t]_{p_t^{i_t}}\right) \in \mathbb{Z}_{p_1^{i_1}} \times \cdots \times \mathbb{Z}_{p_t^{i_t}}$
by CRT $\exists x \in \mathbb{Z}$ such that $x \equiv a_j \bmod (p_j^{i_j})$ for $j = 1, \dots, t$
So $\phi([x]_n) = \left([x]_{p_1^{i_1}}, \dots, [x]_{p_t^{i_t}}\right) = \left([a_1]_{p_1^{t_1}}, \dots, [a_t]_{p_t^{i_t}}\right)$
So ϕ is onto. Since $|\mathbb{Z}_n| = n = p_1^{i_1} \cdots p_t^{i_t} = \left|\mathbb{Z}_{p_1^{t_1}} \times \cdots \times \mathbb{Z}_{p_t^{i_t}}\right|$
we see ϕ must be 1-1 also and have it is an isomorphism. ■

Rings

October-29-13 10:15 AM

Ring

A ring R is a set equipped with two binary operations $+, \times : R \times R \to R$
Denote $\times(r_1, r_2) = r$ as $r_1 \times r_2 = r$
Such that the following hold:

1. $(R, +)$ is an abelian group under addition, we let $0 \in R$ denote the (additive) identity and $-r$ denote the inverse in R
2. x is associative; i.e. $(rx)t = r(st) = rst \;\; \forall r, s, t \in R$
   This allows us to unambiguously write the product $r_1, \ldots, r_n$

   We will assume that our rings have identity 1_R
   i.e. $\exists 1 = 1_R \in R \; s.t. \, 1r = r1 = r \;\; \forall r \in R$
3. Distributivity
   $r(a + b) = ra + rb, \qquad (a + b)r = ar + br$

Commutativity

A ring is commutative if $ab = ba \; \forall a, b \in R$

Division Ring

More generally, we call a ring D a division ring if $D^* = D \backslash \{0\}$ is a group under multiplication.

Proposition

Let R be a ring. Then we have

1) $0a = a0 = 0 \; \forall a \in \mathbb{R}$
2) $(-a)b = a(-b) = -ab \;\; \forall a, b \in R$
3) $(-a)(-b) = ab$
4) The multiplicative identity is unique

Zero divisor

Let R be a ring.
We say that r is a zero divisor if $\exists 0 \neq s \in R$ such that either $rs = 0$ or $sr = 0$ (or both)

Units

Let R be a ring. We say that $r \in R$ is a unit if $\exists s \in R$ such that $sr = rs = 1$.
We denote the set of units in R by R^*. Notice that R^* is a group under multiplication.

Cartesian Product

If R, S are rings, we can make a new ring $R \times S$
$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$
$(r_1, s_2) \times (r_2, s_2) = (r_1 r_2, s_1 s_2)$
$1_{R \times S} = (1_R, 1_S)$
$0_{R \times S} = (0_R, 0_S)$

Proposition

$(R \times S)^* = R^* \times S^*$

Nilpotent

An element r of a ring R is called nilpotent if $\exists n \geq 1$ such that $r^n = 0$

Example Rings

$R = \mathbb{Z}$ is a ring
A field F is a ring, where $F^* = F \backslash \{0\}$ is an abelian group under $\times$
$H = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$
$\quad (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$
So $(a + bi + cj + dk)^{-1}$

$$= \frac{a}{a^2 + b^2 + c^2 + d^2} - \frac{b}{a^2 + b^2 + c^2 + d^2} i - \frac{c}{a^2 + b^2 + c^2 + d^2} j - \frac{d}{a^2 + b^2 + c^2 + d^2} k$$

$\mathbb{R}[t]$ all polynomials with real coefficients
$C(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} : f \text{ is continuous}\}$
$\quad (f \cdot g)(x) = f(x)g(x)$
$\quad (f + g)(x) = f(x) + g(x)$
$R = M_2(\mathbb{R})$ is a non-commutative ring
$\quad$ But it is "close" to being commutative
$\quad$ Recall that R is commutative if $xy - yx = 0 \forall x, y \in R$
$\quad$ Similarly, $M_2(\mathbb{R})$, while not commutative, satisfies the identity
$\qquad$ (Wagner's Identity) $z(xy - yx)^2 - (xy - yx)^2 z = 0 \; \forall x, y, z$

Proof of Proposition

1) $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \Rightarrow 0 = 0 \cdot a$
   Similarly, $a \cdot 0 = 0$
2) $0 = (a - a) \cdot b = ab + (-a)b$ So $(-a)b = -ab$
   Similarly, for the other size
3) $(-a)(-b) = -1 \cdot a(-b) = (-1)(-ab) = (-1)(-1)ab = ab$
   Since $0 = (1 - 1)(-1) = 1 \cdot (-1) + (-1)(-1) = -1 + (-1)(-1) \Rightarrow 1 = (-1)(-1)$
4) Suppose that x is another multiplicative identity. Then $xa = a \forall a \in R$
   $x = x \cdot 1 = 1 \Rightarrow x = 1$

Example Zero Divisor

$R = \mathbb{Z}_n, \qquad [a] + [b] = [a + b], \qquad [a] \cdot [b] = [ab]$

$\mathbb{Z}_6 : [2][3] = [6]$
So $[2], [3]$ are 0-divisors

$M_2(\mathbb{R}) : r = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, s = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \qquad rs = sr = 0$
$\quad r = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}, \qquad s = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \qquad rs = 0, \qquad sr = \begin{pmatrix} 3 & 3 \\ -3 & -3 \end{pmatrix} \neq 0$
$\qquad$ So s only works on one side. s is still a 0-divisor

Let V = real vector space with basis $e_1, e_2, e_3, \ldots$ such that each element is a linear combination of finitely many basis vectors.
Let $\mathcal{T}(V)$ = all linearly transformations $T : V \to V$
Then $\mathcal{T}(V)$ is a ring
$\quad (T + S)(\vec{v}) = T\vec{v} + S\vec{v}, \qquad TS(\vec{v}) = T(S(\vec{v}))$
Let $T : V \to V$ be the forward shift $Te_1 = e_2, Te_2 = e_3, Te_3 = e_4, \ldots$
$\quad S : V \to V$ back shift: $Se_1 = 0, Se_2 = e_1, Se_3 = e_2, \ldots,$
$\quad Ue_1 = s_1, \qquad Ue_2 = 0, Ue_3 = 0$
$UTe_i = U(e_{i+1}) = 0$
$STe_i = S(e_{i+1}) = e_i \; \forall i \Rightarrow ST = I_V$ identity
T has a left inverse but cannot have a right inverse. Why? Suppose $TM = I_V$
$\quad U(TM) = UI_V = U$ but $(UT)M = 0M = 0$ contradiction
$\quad UT = 0$ and $U \neq 0$ so T is a zero divisor but $\nexists M \in \mathcal{T}(V), M \neq 0$ such that $TM = 0$
$\quad$ Why? If $TM = 0 \Rightarrow (ST)M = S0 = 0 \Rightarrow I_V M = 0 \Rightarrow M = 0^{-1}$

R^* a group

Notice if r_1, r_2 are units $\Rightarrow \exists s_1, s_2$ such that $s_1 r_1 = r_1 s_1 = r_2 s_2 = s_2 r_2$
So $(r_1 r_2)(s_2 s_1) = r_1 (r_2 s_2) s_1 = r_1 s_1 = 1$
And similarly, $(s_2 s_1)(r_1 r_2) = 1$ so $r_1, r_2 \in \mathbb{R}^* \Rightarrow r_1, r_2 \in \mathbb{R}^*$
$(R^*, \times)$ is associative. R is associative under $\times$.
Obviously $1 \in R^* \; 1 \cdot 1 = 1 \cdot 1 = 1$

If $r \in R^* \Rightarrow \exists s \in R$uch that $rs = sr = 1$ so $s = r^{-1}$ and $r = s^{-1}$ so $s \in R^*$

Example Sets of Units

$\mathbb{Z}^* = \{\pm 1\} \cong \mathbb{Z}_2$
$\quad$ Why? If $n \in \mathbb{Z}$ and $\exists m \in \mathbb{Z}$ such that $nm = mn = 1$ then $n, m = \pm 1$
$\mathbb{Z}[i]^* = (a + bi)(a - bi) = a^2 + b^2$

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \Rightarrow (a, b) \in \{(0,1), (1,0), (0,-1), (-1,0)\}$$

$\quad \mathbb{Z}[i]^* = \{1, -1, i, -i\} \cong \mathbb{Z}_4$
$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$
$\quad \mathbb{Z}_5^* = \{[1], [2], [3], [4]\} = \langle [2] \rangle \cong \mathbb{Z}_4$

$R = M_2(\mathbb{Z}_2) \Rightarrow R^* = \mathrm{GL}_2(\mathbb{Z}_2) \cong S_3$

Proof of Proposition

$(r_1, s_1) \in (R \times S)^* \Leftrightarrow \exists (r_2, s_2) \in R \times S$ such that
$\quad (r_2, s_2)(r_1, s_1) = (r_1, s_1)(r_2, s_2) = (1_R, 1_S)$
$\quad \Leftrightarrow \; (r_2 r_1, s_2 s_1) = (r_1 r_2, s_1 s_2) = (1_R, 1_S)$
$\quad \Leftrightarrow r_2 r_1 = r_1 r_2 = 1_R \; \& \; s_2 s_1 = s_1 s_2 = 1_S$

$\Leftrightarrow r_1 \in R^*, \qquad s_1 \in S^*$

So $(r, s) \in (R \times S)^* \Leftrightarrow r \in R^*$ & $s \in S^* \Leftrightarrow (r, s) \in R^* \times S^*$

Example

$(\mathbb{Z} \times \mathbb{Z})^* \cong \mathbb{Z}^* \times \mathbb{Z}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Example Nilpotent Elements

$R \in \mathbb{Z}_4, r = [2]$ is nilpotent since $[2]^2 = [4] = [0]$

Ring Properties & Defs.

October-31-13 10:00 AM

Idempotent
Let R be a ring. We say that $e \in R$ is idempotent if $e^2 = e$

Theorem (Jacobson)
We won't prove this

Let R be a ring and suppose that for each $r \in R$, $\exists n = n(r) \geq 2$ such that $r^n = r$. Then R is commutative.

Integral Domain
A commutative ring R is called an integral domain if the only zero divisor in R is 0.
That is, if $r, s \in R, r \neq 0, s \neq 0 \Rightarrow rs \neq 0$

Assignment
Prove that if R is a finite integral domain then R is a field.

Remark
If R is an integral domain $\Rightarrow$ 0 and 1 are the only idempotents in R.

Characteristic
Let R be a ring.
We say that R has characteristic $n \geq 2$ if
$1 + 1 + 1 + \cdots + 1 = n \cdot 1 = 0$
(n 1's)
and if $0 < d < n$, $1 + 1 + \cdots + 1 = d \cdot n \neq 0$
(d 1's)
In other words, $o(1) = n$ in the group $(R, +)$
If $\nexists n \geq 2$ s.t. $1 + \cdots + 1 = n \cdot 1 = 0$ then we say R has characteristic 0.

Proposition 1
Let R be an integral domain. Then either R has characteric 0 or characteristic p, p prime

Proposition 2
Let R be a finite integral domain (from assignment $\Rightarrow$ field)
Then $\exists$ prime p such that $\mathrm{char}(R) = p$ and $|R| = p^d$

Subrings
Let R be a ring and let $S \subseteq R$
Then S is a subring of R if
1) $(S, +)$ is a subgroup of $(R, +)$
2) S is closed under multiplication i.e. if $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$
3) $1_R \in S$ is the identity of S

So S is a subset that is also a ring with $+,\times$ and $1_S = 1_R$

Centre of a Ring
Let R be a ring.
We define the centre of R
$$Z(R) = \{z \in R : zr = rz \ \forall r \in R\}$$
1) Notice $Z(R)$ is a subring of R
2) $Z(R)$ is a commutative ring.
3) If D is a division ring then $Z(D)$ is a field
   why? $zr = rz \Leftrightarrow rz^{-1} = z^{-1}r$

Ideals
Let R be a ring.
We say that $I \subseteq R$ is a **left ideal** of R if
1) $(I, +)$ is a subgroup of $(R, +)$ under $+$
2) If $r \in R$ and $\lambda \in I$ then $r\lambda \in I$

Similarly if
1) Same
2) If $r \in R$ and $\lambda \in I$ then $\lambda r \in I$

we say I is a **right ideal.**
An **ideal** (2-sided ideal) I is a subset that is both a left and a right ideal.
Write $I \trianglelefteq R$

Simple Ring
A R is called **simple** if (0) and R are the only **ideals** of R.

Theorem 1
Let R be a simple commutative ring.
Then R is a field. Conversely, a field is simple and commutative.

Theorem 2
Let D be a division ring.
Then $M_n(D)$ is simple.

Example Idempotent Elements
$0^2 = 0$ and $1^2 = 1$ so 0 and 1 are idempotent
$\mathbb{Z}_2 \times \mathbb{Z}_2$, $(0,1)$ is idempotent
$R = M_2(R)$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is idempotent

Proof of Remark
Suppose $e^2 = e$. Then $e^2 - e = e(e-1) = 0 \Rightarrow e = 0$ or $e = 1$

Example
$\mathbb{Z}_n$ is an integral domain iff n is prime.
Why? If n is composite, $n = ab$, $1 < a, b < n$ then $[a][b] = [n] = [0]$
$[a], [b] \neq [0]$

If n is prime p and $[a],[b] \in \mathbb{Z}_p$, $[a] \neq 0, [b] \neq 0 \Rightarrow ab \not\equiv 0 \pmod{p} \Rightarrow [a][b] = [ab] \neq [0]$

Example Characteristic
$R = \mathbb{Z}_n$ has characteristic n
$[1] + \cdots + [1] = n \cdot [1] = [n] = [0]$
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$ have characteristic 0

Proof of Proposition 1
Suppose $\mathrm{char}(R) = n \geq 2$
If n is not prime, $n = ab$, $1 < a, b < n$
Then $0 = \underbrace{(1 + \cdots + 1)}_{\text{n times}} = \underbrace{(1 + \cdots + 1)}_{\text{a times}}\underbrace{(1 + \cdots + 1)}_{\text{b times}}$
So if R is an integral domain, either $\underbrace{1 + \cdots + 1}_{\text{a times}} = 0$ or $\underbrace{1 + \cdots + 1}_{\text{b times}} = 0$
But this contradicts the fact that $\mathrm{char}(R) = n$

Proof of Proposition 2
Let $|R| = m$
then $1, 1+1, 1+1+1, \ldots, \underbrace{1 + \cdots + 1}_{\text{m times}}$ cannot all be different
So $\exists i < j$ such that $\underbrace{1 + \cdots + 1}_{\text{i times}} = \underbrace{1 + \cdots + 1}_{\text{j times}} \Rightarrow \underbrace{1 + \cdots + 1}_{j-i \text{ times}} = 0 \Rightarrow \mathrm{char}(R)$ is finite
So $\exists p$ prime such that $\mathrm{char}(R) = p$
Now we can regard R as a $\mathbb{Z}_p$-vector space.
If $r, s \in R$ and $a, b \in \mathbb{Z}_p$ then
$$ar + bs = \underbrace{r + \cdots + r}_{\text{a times}} + \underbrace{s + \cdots + s}_{\text{b times}} = ar + bs$$
$$pr = 0, ps = 0$$
We say a subset $r_1, \ldots, r_k$ is linearly independent if
$$c_1 r_1 + \cdots + c_k r_k = 0, \quad c_1, \ldots, c_k \in \mathbb{Z}_p \Rightarrow c_1 = \cdots = c_k = 0$$
As with vector spaces, we can pick a maximal linearly independent set and it will be a basis for R.
Let $\beta = \{r_1, \ldots, r_d\}$ be a basis for R ($d < \infty$ since $|R| < \infty$)
Then $R = \{c_1 r_1 + \cdots + c_d r_d, \ c_1, \ldots, c_d \in \mathbb{Z}_p\}$
So $|R| = \underbrace{p \cdot p \cdot \cdots \cdot p}_{d \text{ times}} = p^d$

Example Subrings
$R = \mathbb{R}$, $S = \mathbb{Q}$

$R = M_n(\mathbb{C})$, $S = M_n(\mathbb{R})$
$R = M_n(\mathbb{R})$, $S =$ upper triangle real matrices
$R = \mathbb{R}[t]$, $S = \mathbb{R}$

Example Ideals
Example 1
$R = \mathbb{Z}$
$I = n\mathbb{Z}$
Then I is an ideal of $\mathbb{Z}$. Why?
If $na, nb \in I \Rightarrow na \pm nb = n(a \pm b) \in I$
If $na \in I$, and $m \in \mathbb{Z} \Rightarrow m(na) = n(ma) \in I$

Example 2
$R = M_2(\mathbb{R})$
$I = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R}\right\}$
I is a right ideal but not a left ideal
$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ w & z \end{pmatrix} = \begin{pmatrix} ax + bw & ay + bz \\ 0 & 0 \end{pmatrix} \in I$
$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin I$

Proof of Theorem 1
Let R be a simple commutative ring and let $x \in R \backslash \{0\}$
Let $I = \{rx : r \in R\}$
Notice that I is an ideal.
Why? $r_1 x, r_2 x \in I$, $r_1 x \pm r_2 = (r_1 \pm r_2)x \in I$ so $(I, +)$ is a subgroup
If $a \in R$ and $rx \in I \Rightarrow arx = (ar)x \in I$, $rxa = (ar)x \in I$
Also, $1 \cdot x \in I, 1 \cdot x \neq 0$ so $I \supsetneq (0)$
Since R is simple, $I = R$

Theorem 2

Let D be a division ring.
Then $M_n(D)$ is simple.

Remark

1) If R is a ring and $a \in R$ then
   $Ra = I = \{ra : r \in R\}$ is a left ideal
   $aR = J = \{ar : r \in R\}$ is a right ideal
   $RaR = \{$all finite sums of the form $ras,\ r, s \in R\}$ is a 2-sided ideal.

Proposition

Let R be a ring and let $a \in R$. Then

$$RaR = \left\{\sum_{j=1}^{m} r_j a s_j : m \geq 1\ r_1, \ldots, r_m, s_1, \ldots, s_m \in R\right\}$$

is an ideal and is the smallest ideal that contains a.

Remark

If I, J are left ideals of R
$\Rightarrow I + J = \{x + y : x \in I, y \in J\}$ is a left ideal of R
Similarly for right ideals and ideals.
Why? Check that $I + J$ is a group and if $x \in I, y \in J$ and $r \in R$ then
$r(x + y) = rx + ry \in I + J$

Why? $r_1x, r_2x \in I,\ r_1x \pm r_2 = (r_1 \pm r_2)x \in I$ so $(I, +)$ is a subgroup
If $a \in R$ and $rx \in I \Rightarrow arx = (ar)x \in I,\ rxa = (ar)x \in I$
Also, $1 \cdot x \in I, 1 \cdot x \neq 0$ so $I \supsetneq (0)$
Since R is simple, $I = R$
So $1 \in I \Rightarrow \exists r \in R\ s.t.\ 1 = rx = xr$ so $x^{-1} = r$
So R is a field.
Conversely, if R is a field and if I is a nonzero ideal of R
$\exists r \neq 0$ in I. So $r^{-1} \cdot r \in I \Rightarrow 1 \in I \Rightarrow r \cdot 1 \in I\ \forall r \in R \Rightarrow I = R \Rightarrow R$ is simple.

Proof of Theorem 2

Let E_{ij} = matrix with zeros everywhere except 1 at i-th row and j-th column.

$$E_{ij}E_{kl} = \delta_{j,k}E_{il} = \begin{cases} E_{il} \text{ if } j = k \\ 0 \text{ otherwise} \end{cases}$$

Suppose that $I \trianglelefteq M_n(D)$ (is an ideal of) and that $I \neq (0)$

Since $I \neq (0), \exists \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in I,\ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \neq 0$

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} = \sum_{1 \leq i,j \leq n} a_{ij}E_{ij}$$

Since

$$A = \sum_{1 \leq i,j \leq n} a_{ij}E_{ij} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \neq 0, \qquad \exists i_0, j_0\ s.t.\ a_{i_0j_0} \neq 0$$

$$E_{ki_0}AE_{j_0l} = E_{ki_0}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}E_{ij}\right)E_{j_0l} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}E_{ki_0}E_{ij}E_{j_0l} = \sum_{j=1}^{n} a_{i_0j}E_{kj}E_{j_0l} = a_{i_0j_0}E_{kl}$$

Since I is an ideal,
$a_{i_0j_0}E_{kl} = E_{ki_0}AE_{j_0l} \in I\ \forall k, l$

$$\begin{pmatrix} a_{i_0j_0}^{-1} & & \\ & \ddots & \\ & & a_{i_0j_0}^{-1} \end{pmatrix} a_{i_0j_0}E_{kl} = E_{kl} \in I\ \ \forall k, l$$

$\Rightarrow E_{1,1} + E_{2,2} + \cdots + E_{n,n} =$ identity $\in I$ So $1_{M_n(D)} \in I \Rightarrow I = M_n(D)$

Proof of Proposition

1) RaR is a subgroup under $+$:
   $$\sum_{j=1}^{m} r_j a s_j\ ,\qquad \sum_{l=1}^{n} r_l' a s_l' \in RaR \Rightarrow \text{sum } r_1as_1 + \cdots + r_mas_m + r_1'as_1' + \cdots + r_n'as_n'$$
   If $\sum_{j=1}^{n} r_j a s_j \in I$ and $x \in R$
   $$x\left(\sum_{j=1}^{n} r_j a s_j\right) = \sum_{j=1}^{n} (xr_j) a s_j \in RaR$$
   $$\left(\sum_{j=1}^{n} r_j a s_j\right)x = \sum_{j=1}^{n} r_j a (s_j x) \in RaR$$
2) Proof that RaR is minimal: exercise

Ideals of $\mathbb{Z}$

What are the ideals of $\mathbb{Z}$? Answer: $I \trianglelefteq \mathbb{Z} \Leftrightarrow I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Proof

If $I = (0) \Rightarrow I = 0\mathbb{Z}$
If $I \neq (0)$ $\exists n \neq 0$ in I and since $n, -n \in I$, we have a positive integer in I.
Let d be the smallest integer in I.
Claim: $I = d\mathbb{Z}$.
Why?
$I \supseteq d\mathbb{Z}$ and if $\exists k \in I \setminus d\mathbb{Z}$ then write $k = dq + r,\ \ 0 < r < d$
Then $r = k + d(-q) \in I$ but this contradicts the minimality of d.
So $I = d\mathbb{Z}$.

Quotient Rings

November-05-13 10:04 AM

Let R be a ring and let $I \trianglelefteq R$ (ideal)
$I \trianglelefteq R$ means $(I,+)$ is a subgroup of $(R,+)$ and if $x \in I$ & $r \in R \Rightarrow rx, xr \in I$
I is an ideal $\Leftrightarrow$ if $x, y \in I \Rightarrow x + y \in I$ & $x \in I, r \in R \Rightarrow xr, rx \in I$

Quotient Ring

Let $I \trianglelefteq R$ be a proper ideal of R
We can form a quotient ring, R/I as follows:
We say $r_1 \sim r_2 \Leftrightarrow r_1 - r_2 \in I$. Then $\sim$ is an equivalence relation.

Transitivity

$r_1 \sim r_2, \quad r_2 \sim r_3$
$r_1 - r_2 \in I, r_2 - r_3 \in I \Rightarrow (r_1 - r_2) + (r_2 - r_3) = r_1 - r_3 \in I \Rightarrow r_1 \sim r_3$

Equivalence Classes

Given $r \in R$, we let $[r] = \{s \in R : r \sim s\} = r + I$
This is the **equivalence class** of R.
As a set, $R/I = \{[r] : r \in R\}$
Addition and multiplication are defined as one would expect. Namely,
$[r_1] + [r_2] = [r_1 + r_2]$
$[r_1] \cdot [r_2] = [r_1 r_2]$
$1_{R/S} = [1]$

Well-Defined

Suppose that $r_1 \sim s_1$ and $r_2 \sim s_2$
Want to show $[r_1 + r_2] = [s_1 + s_2]$
Notice $(r_1 + r_2) - (s_1 + s_2) = (r_1 - s_1) + (r_2 - s_2) \in I$
$\Rightarrow r_1 + r_2 \sim s_1 + s_2$
$\Rightarrow [r_1 + r_2] = [s_1 + s_2]$

Want to show $[r_1 r_2] = [s_1 s_2]$
$[r_1 r_2] = [s_1 s_2] \Leftrightarrow r_1 r_2 - s_1 s_2 \in I \Leftrightarrow r_1 r_2 - r_1 s_2 + r_1 s_2 - s_1 s_2 \in I$
$\Leftrightarrow r_1(r_2 - s_2) + (r_1 - s_1)s_2 \in I$
Last holds since $r_1, (r_2 - s_2), (r_1 - s_2), s_2 \in I$

Finally, $[1] \cdot [r] = [r] \cdot [1] = [r]$
So $[1]$ is an identity. Associativity and distributive rules com from R.
$[r]([s] \cdot [t]) = [r][st] = [(rs)t] = [rs][t] = ([r][s])[t]$

Quotient Rings

Example

$R = \mathbb{Z}, \quad I = n\mathbb{Z}, \quad n \geq 2$
$R/I = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$
$[a] = \{b \in \mathbb{Z} : a \equiv b \ (\mathrm{mod}\ n)\} = \{b \in \mathbb{Z} : a - b \in n\mathbb{Z}\}$

Example

$R = \mathbb{R}[x]$ = all polynomials with real coefficients
$I = \{p(x)(x^2+1) : p(x) = \mathbb{R}[x]\} = R(x^2+1)$ is an ideal
What is R/I? We'll show that R/I "looks like" $\mathbb{C}$
Why?

Remark 1

If $p(x) \in \mathbb{R}[x] \Rightarrow \exists a, b \in \mathbb{R}$ such that
$[p(x)] = [ax + b]$
Why?
$p(x) = (x^2+1)q(x) + r(x)$, where $\deg(r) < 2$
Polynomial division algorithm
$\Rightarrow p(x) - r(x) = q(x)(x^2+1) \in I$
$\Rightarrow [p(x)] = [r(x)] = [ax + b]$

$+$ and $\times$
$[a + bx] + [c + dx] = [(a + c) + (b + d)x]$
$[a + bx][c + dx] = [ac + (ad + bc)x + bdx^2]$
$= [ac + (ad + bc)x + bd(x^2 + 1) - bd] = [(ac - bd) + (ad + bc)x]$
"Looks like" $\mathbb{C}$. $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$
$(a + bi) + (c + di) = (a + c) + (b + d)i$

Homomorphism

November-05-13 10:29 AM

Homomorphism

Let R, S be rings.
Se say that a map $f: R \to S$ is a (ring) homomorphism if

$f(x+y) = f(x) + f(y)\ \forall x, y \in R$
$f(xy) = f(x)f(y)\ \forall x, y \in R$
$f(1_R) = 1_S$

Note:
The last condition does not follow automatically from the first two.
For example $f(x) = 0\ \forall x \in R$

Remark 1

$f(0_R) = 0_S$

Remark 2

$\ker(f) = \{r \in R : f(r) = 0\}$
$\ker(f)$ is an ideal of R.
Why? If $x, y \in \ker(f) \Rightarrow f(x+y) = f(x) + f(y) = 0_S + 0_S = 0_S \Rightarrow x + y \in \ker(f)$
If $x \in \ker(f), r \in R \Rightarrow f(rx) = f(r)f(x) = f(r)0_S \Rightarrow rx \in \ker(f)$
$\Rightarrow f(xr) = f(x)f(r) = 0_S f(r) = 0_S \Rightarrow xr \in \ker(f)$

Remark 3

f is 1-1 $\Leftrightarrow \ker(f) = \{0\}$
Why? Look at f has a group homomorphism of $(R, +)$ to $(S, +)$
Then f is 1-1 $, \Rightarrow \ker(f) = (0_S)$

Proposition

If $f: R \to S$ is a homomorphism, then $\operatorname{im}(f) = \{f(r) : r \in R\} \subseteq S$ is a subring of S.

Isomorphism

$f: R \to S$ is an isomorphism if it is a homomorphism that is 1-1 and onto.
If $f: R \to R$ is a homomorphism, we call it an endomorphism
If it is an isomorphism, we call it an automorphism.

Proposition

1) If $f: R \to S$ is an isomorphism, $f^{-1}: S \to R$ is an isomorphism
2) If $f: R \to S$ and $g: S \to T$ are homomorphisms, $g \circ f: R \to T$ is a homomorphism.

- [ ] Proof on Assignment

First Isomorphism Theorem

Let R, S be rings and let $f: R \to S$ be a homomorphism.
Then $R/\ker(f) \cong \operatorname{im}(f) \subseteq S$

Proof of Proposition

1) $(\operatorname{im}(f), +)$ is a subgroup of $(S, +)$ because
$f: (R, +) \to (S, +)$ is a group homomorphism and $\operatorname{im}(f)$ is a subgroup.
2) If $x, y \in \operatorname{im}(f) \Rightarrow \left.\begin{matrix} x = f(r_1) \\ y = f(r_2) \end{matrix}\right\} \Rightarrow xy = f(r_1)f(r_2) = f(r_1 r_2) \in \operatorname{im}(f)$
3) $1_S = f(1_R)$

First Isomorphism Theorem

Before we prove this, consider
$R = \mathbb{R}[x], \quad S = \mathbb{C}$
$f: \mathbb{R}[x] \to \mathbb{C},\ f(p(x)) = p(i)$ homorphism
$\ker(f) = \mathbb{R}[x](x^2+1)$

Proof of First Isomorphism Theorem

Define $F: R/\ker(f) \to \operatorname{im}(f)$
$F([r]) = f(r)$
Notice that if $[r] = [s]$ then $r - s = x \in \ker(f)$
$\Rightarrow f(r-s) = f(x) = 0, \quad f(r-s) = f(r) - f(s) \Rightarrow f(r) = f(s)$
$\Rightarrow F([r]) = F([s])$
Now we'll check that F is a homomorphism
1) $F([r] + [s]) = F([r+s]) = f(r+s) = f(r) + f(s) = F([r]) + F[s])$
2) $F([r][s]) = F([rs]) = f(rs) == f(r)f(s) = F([r])F([s])$
3) $F([1_R]) = f(1_R) = 1_S$

Notice F is onto.
If $x \in \operatorname{im}(f) \Rightarrow \exists r \in R\ s.t.\ s = f(r) = F([r])$ so $x \in \operatorname{im}(F)$
To show F is 1-1
$F([r]) = 0 \Leftrightarrow f(r) = 0 \Leftrightarrow r \in \ker(f) \Leftrightarrow [r] = [0]$
So $\ker(F) = \{[0]\} \Rightarrow F$ is 1-1. The result follows.

Examples

Example 1

Let $R = \mathbb{R}[x],\ I = \mathbb{R}[x](x-7)$
What is R/I? $R/I \cong \mathbb{R}$
Why? Consider $f: \mathbb{R}[x] \to \mathbb{R},\ f(p(x)) = p(7)$
$f(p(x) + q(x)) = (p+q)(7) = p(7) + q(7) = f(p(x)) + f(q(x))$
$f(p(x)q(x) = p(7)q * 7) = f(p(x))f(q(x))$
$f(1) = 1$
f is onto, $\ker(f) = I$
So $\operatorname{im}(f) = \mathbb{R} \cong R/I$

Example 2

$R = \mathbb{Q}[x], \quad I = R(x^2-2)$
What is R/I?
$R/I \cong \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$
$f: R \to \mathbb{Q}[\sqrt{2}]$ by $f(p(x)) = p(\sqrt{2})$.
Then f is onto and $\ker(f) = I$

Example 3

$R = \mathbb{R}[x], \quad I = R(x^3 - x) = Rx(x-1)(x+1)$
Then $R/I \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R}$
Why? $f: \mathbb{R}[x] \to \mathbb{R} \times \mathbb{R} \times \mathbb{R}$
$f(p(x)) = (p(0), p(1), p(-1)),\ f$ is a homomorphism
$p(x) \in \ker(f) \Leftrightarrow p(0) = p(1) = p(-1) = 0 \Leftrightarrow x(x-1)(x+1) | p(x)$
$\Leftrightarrow p(x) \in I$
f is onto. Given $(a, b, c) \in \mathbb{R} \times \mathbb{R} \times \mathbb{R}$,
Let $p(x) = -a(x^2-1) + \frac{b}{2}x(x+1) + \frac{c}{2}x(x-1)$
$f(p(x)) = (p(0), p(1), p(-1)) = (a, b, c)$

Example 4

Let $R = \mathcal{C}([0,1]) = \{f: [0,1] \to \mathbb{R} : f \text{ is continuous}\}$
$(f+g)(x) = f(x) + g(x)$
$(fg)(x) = f(x)g(x)$
$1_R =$ constant function 1
Let $I = \left\{f \in R : f\left(\frac{1}{2}\right) = 0\right\}$
What is R/I? $R/I \cong \mathbb{R}$
Proof
Consider $\Psi: \mathcal{C}([0,1]) \to \mathbb{R},\ \Psi(f) = f\left(\frac{1}{2}\right)$
Ψ is onto because constant map $\lambda \cdot 1 \to \lambda$
$\ker \Psi = I$
So $R/I \cong \mathbb{R}$

Example 5

For each $\alpha \in [0, 1]$
Let $I_\alpha = \{f \in \mathcal{C}([0,1]) : f(\alpha) = 0\}$
If $I \trianglelefteq \mathcal{C}([0,1])$ and $I \subsetneq \mathcal{C}([0,1]) \Rightarrow \exists \alpha \in [0,1]$ such that $I \subseteq I_\alpha$

Proof

Suppose $I \trianglelefteq \mathcal{C}([0,1])$ and $\nexists \alpha$ such that $I \subseteq I_\alpha$
1) Then $\forall \alpha \in [0,1],\ \exists f_\alpha \in I$ such that $f_\alpha(\alpha) \neq 0$

2) For each α $\exists$ an $\epsilon_\alpha > 0$ such that $f_\alpha(x) \neq 0$ for $x \in (\alpha - \epsilon_\alpha, \alpha + \epsilon_\alpha)$

3) (Fact) $\bigcup_{\alpha \in [0,1]} (\alpha - \epsilon_\alpha, \alpha + \epsilon_\alpha) \supseteq [0, 1]$

So $\exists \alpha_1, \dots, \alpha_n$ such that

$$\bigcup_{i=1}^{n} (\alpha_i - \epsilon_{\alpha_i}, \alpha_i + \epsilon_{\alpha_i}) \supseteq [0, 1]$$

4) Let $g = \sum_{i=1}^{n} f_{\alpha_i}^2 \in I, \qquad g(\beta) \neq 0 \forall \beta \in [0, 1]$

5) So $h(x) \coloneqq \frac{1}{g(x)}$ is continusous on $[0, 1]$

So $h \cdot g = 1 \in I \Rightarrow I \in \mathcal{C}([0, 1])$

Correspondence Theorem

November-07-13 10:00 AM

Correspondence Theorem

Let R be a ring and let $I \lhd R$ be a proper ideal.
Then there is a bijective correspondence between the ideals of R/I and the ideals of R that conatin I, given as follows:
$f: R \to R/I, \quad f(r) = [r] = r + I$
This is a homomorphism.

$\{\text{ideals of } R \text{ that contain } I\} \leftrightarrow \{\text{ideals of } R/I\}$
$J \trianglelefteq R, J \supseteq I \mapsto f(J) \trianglelefteq R/I$
$f^{-1}(K), \quad f^{-1}(K) \supseteq I \leftarrow K \trianglelefteq R/I$

Moreover, $I \subseteq J_1 \subseteq J_2$ in $R \Leftrightarrow f(J_1) \subseteq f(J_2)$ in R/I

Remark

Let R and S be rings and let $g: R \to S$ be a homomorphism.
Then we have

1) If $K \trianglelefteq S \Rightarrow g^{-1}(K) = \{x \in R : g(x) \in K\}$ is an ideal in R
2) If g is onto and $J \trianglelefteq R \Rightarrow g(J) \trianglelefteq S$

Maximal Ideals

Let R be a ring and let $I \trianglelefteq R$ be a proper ideal of R. We say that I is a **maximal** ideal of R if whenever $J \trianglelefteq R$ with $I \subseteq J \subseteq R$, we have either $J = I$ or $J = R$.

Proposition

Let R be a ring. Then an ideal $I \trianglelefteq R$ is maximal if and only if R/I is simple.

Corollary

Let R be a commutative ring. An ideal $I \trianglelefteq R$ is maximal $\Leftrightarrow R/I$ is a field.

Posets

A poset P is a set with a partial order $\leq$ such that

a) $a \leq a$ (reflexive)
b) $a \leq b$ & $b \leq a \Rightarrow a = b$ (anti-symmetry)
c) $a \leq b$ and $b \leq c \Rightarrow a \leq c$

A **totally ordered set** is a poset P in which $\forall a, b \in P$ either $a \leq b$ or $b \leq a$

Chain

A chain in a poset P is a totally ordered subset of P. In other words, $\exists$ a totally ordered set I and a map $f: I \to P$ such that $x \leq y$ in $I \Rightarrow f(x) \leq f(y)$ in P. $\{f(x) : x \in I\}$ is a chain.

We say that a chain in P has an **upper bound** in P
if $\exists x \in P$ such that $x \geq y \ \forall y \in$ the chain

Zorn's Lemma

(Equivalent to the axiom of choice)

Let P be a poset with the property that every chain has an uppoer bound in P.
Then P has at least one **maximal element.**
i.e. $\exists x \in P$ s.t. if $y \in P$ and $y \geq x$ then $y = x$.

Applications of Zorn's Lemma

Every vector space has a basis.

Theorem

Let R be a ring. Then R has a maximal ideal.

Proof of Remarks

1) So let $K \trianglelefteq S$ and let $x, y \in g^{-1}(K) \Leftrightarrow g(x), g(y) \in K \Rightarrow g(x) + g(y) \in K \Rightarrow g(x+y) \in K \Rightarrow x + y \in g^{-1}(K)$
If $r \in R$ and $x \in g^{-1}(K) \Leftrightarrow g(x) \in K$
$\Rightarrow g(rx) = g(r)g(x) \in k \Rightarrow rx \in g^{-1}(K)$
Similarly, $g(xr) = g(x)g(r) \in K \Rightarrow xr \in g^{-1}(K)$

2) Suppose that g is onto and $J \trianglelefteq R$
We want to show that $g(J) \trianglelefteq S$.
Suppose $x, g \in g(J) \Rightarrow \exists u, v \in J$ s.t. $x = g(u), y = g(v)$
$\Rightarrow x + y = g(u) + g(v) = g(u + v) \in g(J)$
Next, suppose that $x \in g(J)$ and $s \in S$. We must show that sx and xs ar in $g(J)$
$\because$ g is onto $\exists r \in R$ s.t. $g(r) = s$ and $\because x \in g(J) \exists u \in J$ s.t. $x = g(u)$
So $sx = g(r)g(u) = g(ru) \in g(J)$
$xs = g(u)g(r) = g(ur) \in g(J)$

Proof of Correspondence Theorem

$f: \{\text{ideals of } R \text{ containing I}\} \to \{\text{ideals of } R/I\}$
$f: J \to f(J), \quad f^{-1}(K) \leftarrow K$
$f: R \to R/I, \quad r \mapsto [r] = r + I$
$\ker(f) = I = \{r : [r] = 0\} = \{r : r + I = I\}$

To show these maps are inverses we must check

1) If $J \trianglelefteq R \& J \supseteq I \Rightarrow f^{-1}(f(J)) = I$
2) If $K \trianglelefteq R/I \Rightarrow f(f^{-1}(K)) = K$

1) Notice $f^{-1}(f(J)) \supseteq J \because f^{-1}(f(J)) = \{x : f(x) \in f(J)\} \supseteq J$
Suppose that $x \in f^{-1}(f(J))$. We must show that $x \in J$
$\Rightarrow f(x) \in f(G) \Rightarrow \exists y \in J \ s.t. \ f(x) = f(y) \Rightarrow f(x) - f(y) = 0 \Rightarrow f(x - y) = 0$
$\Rightarrow x - y \in \ker(f) = I \Rightarrow x \in y + \ker(f) \subseteq J + I = J \because J \supseteq I$
So $x \in J$

2) Notice that $f(f^{-1}(K)) \subseteq K$
Why? If $x \in f^{-1}(K) \Rightarrow f(x) \in K \Rightarrow f(f^{-1}(K)) \subseteq K$
Let $x \in K$. Since f is onto $\exists y \in R$ s.t. $f(y) = x$
$\Rightarrow y \in f^{-1}(K) \Rightarrow f(y) \in f(f^{-1}(K)) \Rightarrow k \subseteq f(f^{-1}(K))$

And we are done.

Proof of Proposition

Suppose that I is maximal.
Then the only ideals of R that contain I are I and R.
Let $f: R \to R/I = s$
By the correspondence theorem, the only ideals of R/I are $f(I) = \{[0]\}$ and $f(R) = R/I$. So the only ideals of S are (0) and S so $S = R/I$ is simple.

Next, if $S = R/I$ is simple then S has only two ideals (0) and S.
So by the correspondence theorem, R has only 2 ideals containing I:
$f^{-1}(\{0\}) = \ker(f) = I$ and $f^{-1}(S) = R$
So I is maximal.

Proof of Corollary

We showed that R is a commutative simple ring $\Leftrightarrow R$ is a field.

We showed that I is maximal $\Leftrightarrow R/I$ is simple and since R is commutative, this holds $\Leftrightarrow R/I$ is a field.

Example

What are the maximal ideals of $\mathbb{Z}$?
Answer: $I \trianglelefteq \mathbb{Z}$ is maximal $\Leftrightarrow I = p\mathbb{Z}$
Ideals of $\mathbb{Z}$:
$2\mathbb{Z}$ $3\mathbb{Z}$ $5\mathbb{Z}$ $7\mathbb{Z}$ ...
| \/ \/ \/
$4\mathbb{Z}$ $6\mathbb{Z}$ $15\mathbb{Z}$ ...
|
$8\mathbb{Z}$
Notice $\mathbb{Z}/n\mathbb{Z}$ is an integral domain $\Leftrightarrow n = p$ since a field is an integral domain and a finite integral domain is a field. $\mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow n\mathbb{Z} = p\mathbb{Z}$, p prime.

Example

If R does not have a 1 (R is a **rng**). Then R need not have any maximal ideals.
$G = \{x \in \mathbb{C} : \exists m \ s.t. \ x^{2^m} = 1\} = \left\{e^{\frac{2\pi i j}{2^m}} : j \in \mathbb{Z}, m \geq 1\right\}$
G is an abelian group.
☐ Show that G has no maximal proper subgroups. If $H \subsetneq G$ $\exists K \subsetneq G$ with $H \subsetneq K$
Let $R = G$ as a set
$x \oplus y = xy$ in G, $x \otimes y = 0_R$
$I \trianglelefteq R \Leftrightarrow I \leq G$

Proof of Theorem (Maximal Ideal)

Let $P = \{\text{all proper ideals of } R\}$ ordered by inclusion. $I \leq J \Leftrightarrow I \subseteq J$
Let T be a totally ordered set and let $\{I_\alpha\}_{\alpha \in T}$ be a chain in P.
i.e. $\alpha \leq \beta$ in $T \leftrightarrow I_\alpha \subseteq I_\beta$

Let $I = \bigcup_{\alpha \in T} I_\alpha$

Claim

I is a proper ideal of R.

Proof

(ideal) if $x, y \in I \Rightarrow \exists \alpha, \beta \; s.t. \; x \in I_\alpha$ & $y \in I_\beta$.

Since this is a chain, either $I_\alpha \subseteq I_\beta$ or $I_\beta \subseteq I_\alpha$. WLOG $I_\alpha \subseteq I\beta$

so $x, y \in I_\beta \Rightarrow x + y \in I_\beta \subseteq I$

Similarly, $x \in I, r \in R \Rightarrow x \in I_\alpha \Rightarrow rx, xr \in I_\alpha \in I$

Notice if I were not proper then $1 \in I \Rightarrow 1 \in I_\alpha$ for some $\alpha \in T \Rightarrow I_\alpha \notin P$ contradiction.

So I is proper.

So by Zorn's Lemma, P has a maximal element which by definition of P, is a maximal ideal.

Ideals

November-12-13 10:04 AM

Maximal Ideals

$I \trianglelefteq R$ is maximal if
$I \subsetneq R$ and if $J \trianglelefteq R$ with $I \subsetneq J \Rightarrow J = R$

(Zorn's Lemma) $\Rightarrow$ Maximal ideals exist

Claim

In fact, we can say more.
If $J \trianglelefteq R$ is proper then $\exists$ a maximal ideal I that contains J

$M \trianglelefteq R$ is maximal $\Leftrightarrow R/M$ is simple
and if R is commutative $\Leftrightarrow R/M$ is a field

Prime Ideals

Let R be a ring and let $P \triangleleft R$ be a proper ideal of R.
We say that P is a **prime ideal** if whenever $a, b \in R$ are such that
$axb \in P\ \forall x \in R \Rightarrow a \in P$ or $b \in P$
In the case that R is commutative, the definition becomes simpler:
$axb \in P\ \forall x \in R \Leftrightarrow ab \in P$
Take $x = 1 \Rightarrow ab \in P \Rightarrow abx \in P\ \forall x \in R$
If R is commutative and $P \trianglelefteq R$ we say that P is a **prime ideal**
if $ab \in P \Rightarrow a \in P$ or $b \in P$

Comments

For now, R is commutative.

?
- Any maximal ideal is a prime ideal.
  Why? Let $M \trianglelefteq R$ be maximal and suppose M is not prime.
  Then $\exists a, b \in R \setminus M$ but $ab \in M$
  So $Ra + M = R \Rightarrow \exists x \in R$ and $m_1 \in M$ such that $xa = m_1 = 1$
  and $Rb + M = R \Rightarrow \exists y \in R$ and $m_2 \in M$ s.t. $yb + m_2 = 1$
  Multiply $(xa + m_1)(yb + m_2) = 1 \cdot 1 = 1$
  $\Rightarrow \underbrace{xyab}_{M} + \underbrace{xam_2}_{M} + \underbrace{ybm_1}_{M} + \underbrace{m_1m_2}_{M} = \underbrace{1}_{M}$
  Contradiction.

Note

No symbol for normal subgroup but not equal to. Using $\triangleleft$

Theorem

Let R be a commutative ring and let $P \triangleleft R$ be a proper ideal.
Then P is a prime ideal $\Leftrightarrow R/P$ is an integral domain.

Remark

If P is prime and $a_1 a_2 \cdots a_n \in P \Rightarrow a_i \in P$ for some i.

Remark

R commutative
If $x \in R$ and $x^n \in P \Rightarrow x \in P$
(Take $a_1 = a_2 = \cdots = a_n = x$)

Notation

If $a_1, \dots, a_k \in R$ we'll write $(a_1, \dots, a_k)$ to denote the ideal generated by $a_1, \dots, a_k$
$Ra_1R + \cdots + Ra_kR$ (if R commutative $= Ra_1 + \cdots + Ra_k$)

Proof of Claim

Consider the ring $S = R/J$
We know $\exists$ a maximal ideal $M \trianglelefteq S$
By the correspondence theorem, if $f: R \to R/J = S,\ r \to [r] = r \cdot J$

We have $I = f^{-1}(M)$ is an ideal that contains J.
$R = f^{-1}(S) \leftarrow S \trianglelefteq S$
$I = f^{-1}(M) \leftarrow M \trianglelefteq S$
By correspondence, I is a maximal ideal and it contains J

Example Ideals

$M_2(\mathbb{C}),\ P = (0)$ is a prime ideal
If $A, B \in M_2(\mathbb{C})$ and $AXB = 0\ \ \forall X \in M_2(\mathbb{C}) \Rightarrow A = 0$ or $B = 0$
$$E_{ij} = \sum_{k,l} A_{ik} X_{kl} B_{lj} = 0$$
For $X_{kl} = \delta_{kk_0}\delta_{ll_0},\ E_{ij} = A_{ik_0}B_{l_0j} \Rightarrow A_{ik_0} = 0$ or $B_{l_0j} = 0$

Example

$R = \mathbb{Z}$
What are the prime ideals?

- $p\mathbb{Z}, p$ prime
  If $a, b \in \mathbb{Z}$ and $ab \in p\mathbb{Z} \Leftrightarrow p|ab \Rightarrow p|a$ or $p|b \Rightarrow a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$
  IF $n > 2$ is not prime, write $n = ab, 1 < a, b < n$. So $ab \in n\mathbb{Z}$ but $a \notin n\mathbb{Z}, b \notin n\mathbb{Z} \Rightarrow n\mathbb{Z}$ is not prime.
- $\mathbb{Z}$ is not a prime ideal because it is not proper
- $0 \cdot \mathbb{Z} = \{0\}$ is prime. If $ab = 0 \Rightarrow a = 0$ or $b = 0$

Example

(0) is **not** a prime ideal of $\mathbb{Z} \times \mathbb{Z}$
$a = (1,0) \notin (0), \qquad b = (0,1) \notin (0)$
but $ab = (1,0)(0,1) = (0,0) = (0)$

Proof of Theorem

Suppose that P is a prime ideal and suppose that $[a], [b] \in R/P$
and $[a] \cdot [b] = 0, a, b \in R$
Then $[ab] = [0] \Rightarrow ab - 0 \in P \Rightarrow ab \in P \Rightarrow a \in P$ or $b \in P \Rightarrow [a] = [0]$ or $[b] = 0 \Rightarrow R/P$ is an integral domain.

Conversely, suppose that $P \triangleleft R$ is not prime.
Then $\exists a, b \in R$ such that $a \notin P, b \notin P$ but $ab \in P$
$[a] \neq [0]$ in R/P, $[b] \neq [0]$ in R/P
$[a][b] = [ab] = 0$ is R/P
So R/P is not ain integral domain.

Proof of Remark

Proof by induction on n.
Base case. $n = 2$: Holds.
Let $a = (a_1 \cdots a_{n-1}),\ b = a_n$ if $b \notin P \Rightarrow a \in P \Rightarrow a_1 \cdots a_{n-1} \in P \Rightarrow a_i \in P$ for some i by inductive hypothesis.

Example generating ideals

If $m, n \in \mathbb{Z} \setminus \{0\}$ then $(m, n) = (\gcd(m, n)) = \gcd(m, n)\,\mathbb{Z}$
$(12, 8) = 12\mathbb{Z} + 8\mathbb{Z} = 4\mathbb{Z}$

Polynomial, Group, Matrix Rings

November-12-13 10:44 AM

Polynomial Ring

Let R be a ring.
We write $R[x] = \{r_0 + r_1 x + \cdots + r_m x^m : m \geq 0,\ r_1, \ldots, r_m \in R\}$
Multiplication

$$(r_0 + r_1 x + \cdots + r_m x^m)(s_0 + s_1 x + \cdots + s_n x^n)$$
$$= r_0 s_0 + (r_0 s_1 + r_1 s_0)x + (r_0 s_2 + r_1 s_1 + r_2 s_0)x^2 + \cdots + r_m s_n x^{n+m}$$

Addition

$$(r_0 + \cdots + r_m x^m) + (s_0 + \cdots + s_n x^n)$$
$$= (r_0 + s_0) + \cdots + (r_{\max(n,m)} + s_{\max(n,m)})x^{\max(n,m)}$$

Where $r_i = 0\ \forall i > m,\ s_i = 0 \forall i > n$

This is called the polynomial ring over R in one variable.

So $x \in Z(R[x]) \because rx = xr\ \ (r_0)(1x) = (1 \cdot x)r_0$
In general, $S = R[x], s[y]$ we write $S[y] = R[x, y]$
More generally, $R[x_1, \ldots, x_n] = \Big(\big((R[x_1])[x_2]\big) \cdots [x_n]\Big)$

Proposition

Let $R = F$ be a field.
Then every ideal of $F[x]$ is generated by a single element.

Group Ring

Let R be a ring.
The group ring of G over R is
$R[G] = \{\sum_{g \in G} r_g \cdot g \mid r_g \in R,\ r_g = 0 \text{ for all all but finitely many } g \in G\}$
Multiplication

$$\left(\sum_{g \in G} r_g g\right)\left(\sum_{h \in G} s_h h\right) = \sum_{k \in G}\left(\sum_{g \in G} r_g s_{g^{-1}k}\right)k$$
$$(r \cdot g)(s \cdot h) = (rs)gh$$

Matrix Ring

R is a ring, $n \geq 1$

Then $M_n(R) = \left\{\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{n1} & \cdots & r_{nn}\end{pmatrix} : r_{ij} \in R\right\}$

$(r_{ij}) + (s_{ij}) = (r_{ij} + s_{ij})$

$(r_{ij}) \cdot (s_{ij}) = (t_{ij}), \qquad t_{ij} = \sum_{k=1}^{n} r_{ik} s_{kj}$

Some Rings

A few rings related to polynomial rings

1) Laurent Polynomials

$$R[x, x^{-1}] = \left\{\sum_{i=-M}^{n} r_i x^i : M, n \geq 0, r_i \in R\right\}$$

2) $R[[x]]$ formal power series

$$R[[x]] = \left\{\sum_{n=0}^{\infty} r_n x^n : r_0, r_1, \ldots \in R\right\}$$
$$(r_0 + r_1 x + r_2 x^2 + \cdots)(s_0 + s_1 x + s_2 x^2 + \cdots)$$
$$= r_0 s_0 + (r_0 s_1 + r_1 s_0)x + (r_2 s_0 + r_1 s_1 + r_0 s_2)x^2 + \cdots$$

Example

$$R = \mathbb{Z}, \qquad \mathbb{Z}[[x]], \qquad \sum_{n=0}^{\infty} n!\, x^n \in \mathbb{Z}[[x]]$$

Proof of Proposition

Let $I \trianglelefteq F[x]$. If $I = (0)$ the result holds.
If $I \neq (0), \exists p(x) \in I$ of smallest possible degree.

Claim

$I = (p(x)) = p(x)F[x]$

Proof

Suppose that $\exists q(x) \in I \setminus (p(x))$.
Then $\deg(q) \geq \deg(p)$ by inimimality of p.
$q(x) = p(x)a(x) + r(x)$ where $r(x) = 0$ or $\deg(r(x)) < \deg(p(x))$
So $r(x) \in I \because r(x) = q(x) - p(x)a(x) \in I$
If $r(x) \neq 0 \Rightarrow \deg(r(x)) < \deg(p(x))$
$\quad \therefore r(x) \in I$ this contradicts minimality of $\deg(p)$
So $r(x) = 0 \Rightarrow q(x) = p(x)a(x) \in (p(x))$. Contradiction
So $I = (p(x))$

Example Group Rings

$G = \mathbb{Z}_2 = \langle x | x^2 = 1\rangle$
$\mathbb{C}[G] = \{a \cdot 1 + b \cdot x \,|a, b \in \mathbb{C}\} \cong \mathbb{C}[x]/(x^2 - 1)$

$$(a + bx)(c + dx) = ac + adx + bcx + bdx^2 = (ac + bd) + (ad + bc)x$$

$f: \mathbb{C}[x] \to \mathbb{C}[G], \qquad x \mapsto x$

Question

If R is a ring and G and H are groups,
Is it true that if $R[G] \cong R[H]$ as rings $\Rightarrow G \cong H$ as groups?

No

$G = \mathbb{Z}_4, \qquad H = \mathbb{Z}_2 \times \mathbb{Z}_2$
Claim: $\mathbb{C}[G] \cong \mathbb{C}[H] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$

$G = \langle x \,| x^4 = 1\rangle \cong \mathbb{Z}_4$
$H = \langle u, v \,| u^2 = 1, v^2 = 1, uvv = vu\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
Let's show that $\mathbb{C}[H] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$
$\mathbb{C}[H] = \{a + bu + cv + duv \,| a, b, c, d \in \mathbb{C}\}$
Let $\pi_1: \mathbb{C}[H] \to \mathbb{C},\ \pi_2: \mathbb{C}[H] \to \mathbb{C}$
$a + bu + cv + buv \mapsto a + b + c + d, \qquad a + bu + cv + duv \mapsto a + b - c - d$
$\pi_3(a + bu + cv + duv) = a - b + c - d$
$\pi_4(a + bu + cv + duv) = a - b - c + d$
Let $\pi: \mathbb{C}[H] \to \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$

$$\pi(x) \mapsto (\pi_1(x), \pi_2(x), \pi_3(x), \pi_4(x))$$
$$\pi(1) = (1, 1, 1, 1)$$
$$\pi(u) = (1, 1, -1, -1)$$
$$\pi(v) = (1, -1, 1, -1)$$
$$\pi(uv) = (1, -1, -1, 1)$$
$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix} \neq 0$$

so π is onto and since $\dim(\mathbb{C}[H]) = \dim \mathbb{C}^4 = 4$ and π is a linear transform
$\Rightarrow \pi$ is 1-1 and onto

Field of Fractions

November-14-13 10:03 AM

Field of Fractions

Let R be a commutative integral domain. We will construct a field F ($=\text{Frac}(R)$), called the field of fractions of R.
Let $\mathcal{R} = \{(a,b): a \in R, b \in R \setminus \{0\}\}$. We put an equivalence relation $\sim$ on $\mathcal{R}$ by declaring that $(a,b)\sim(c,d) \Leftrightarrow ad = bc$

Claim

$\sim$ is an equivalence relation.

We define $F =$ field of fractions of R to be $\mathcal{R}/\sim$
$[(a,b)] = \{(c,d) \in \mathcal{R} : (a,b)\sim(c,d)\}$

$[(a,b)] + [(c,d)] \Leftrightarrow \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = [(ad+bc, bd)]$
$[(a,b)] \cdot [(c,d)] = [(ac, bd)]$
Notice $[(0,1)] = 0_F$
$[(0,1)] + [(a,b)] = [(a\cdot 1 + b \cdot 0, b \cdot 1)] = [(a,b)]$
$[(1,1)] = 1_F, \quad [(1,1)][(a,b)] = [(a,b)]$

Notice F is a field.
If $[(a,b)] \neq 0_F \Leftrightarrow a \neq 0 \Rightarrow [(b,a)] \in F$
So $[(a,b)] \cdot [(b,a)] = [(1,1)] = 1_F$
So every nonzero element has in inverse.
Now that we've done this, we write $\frac{a}{b}$ for $[(a,b)] \in F$ and we have
$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

Chinese Remainder Theorem

Integer Version

If $m_1, \dots, m_k$ are integers ≥ 1 with $\gcd(m_i, m_j) = 1$ for $i \neq j$ and $a_1, \dots, a_k \in \mathbb{Z}$
$\Rightarrow \exists x \in \mathbb{Z}$ s.t. $x \equiv a_1 (\text{mod } m_1), \dots, x \equiv a_k (\text{mod } m_k)$

General Ring Version

Let R be a ring and let $I_1, \dots, I_k$ be ideals of R and suppose that $I_1, \dots, I_k$ are pairwise **comaximal** (i.e. $I_i + I_j = R$ when $i \neq j$)

Then $R/\left(\bigcap_{i=1}^{k} I_k\right) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k$

General

R ring

- $I_1, \dots, I_k \lhd R$
- $I_i + I_j = R$ for $i \neq j$

Then $R/\left(\bigcap_{i=1}^{k} I_i\right) \cong R/I_1 \times \cdots \times R/I_k$

Remark

If $I \trianglelefteq R$, we'll write $[r]_I$ for the equivalence class fo r in R/I.
If $I \trianglelefteq J \lhd R$. Then we have a "forgetful" surjective homomorphism
$\pi: R/I \to R/J, \quad \pi([r]_I) = [r]_J$
This is well-defined
$[r]_I = [s]_I \Leftrightarrow r - s \in I \Rightarrow r - s \in J \because I \subseteq J \Rightarrow [r]_J = [s]_J$
So $\pi([r]_I) = \pi([s]_I)$

Proof of Claim

Reflexivity
$(a,b)\sim(a,b) \Leftrightarrow ab = ba$, which is true
Symmetry
$(a,b)\sim(c,d) \Leftrightarrow ad = bc \Leftrightarrow cb = da \Leftrightarrow (c,d)\sim(a,b)$
Transitivity
If $(a,b)\sim(c,d)$ and $(c,d)\sim(e,f)$
$ad = bc \Rightarrow adf = bcf = bde \Rightarrow (af - bc)d = 0$
$\because d \neq 0$ and R is an integral domain, $af = bc \Rightarrow (a,b)\sim(e,f)$

Example

$R = \mathbb{Z}, \quad \text{Frac}(R) = \mathbb{Q}$
$R = \mathbb{R}[t], \quad \text{Frac}(R) = \mathbb{R}(t) = \left\{\frac{p(t)}{q(t)} : p(t), q(t) \in \mathbb{R}[t], \quad q(t) \neq 0\right\}$
$R = \mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}$
$\text{Frac}(R) = \mathbb{Q}[i] = \{c + di : c, d \in \mathbb{Q}\}$
$a, b, e, f \in \mathbb{Z}, e, f \neq 0$
$\frac{a+ib}{e+if} = \frac{(a+ib)(e-if)}{e^2+f^2} = \frac{ae+bf}{e^2+f^2} + \frac{be-af}{e^2+f^2} i \in \mathbb{Q}[i]$

Example General CRT

$n = p_1^{i_1} \cdots p_k^{i_k}, \ p_1, \dots, p_k$ distinct primes.
$\Rightarrow \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{i_1}\mathbb{Z} \times \mathbb{Z}/p_2^{i_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{i_k}\mathbb{Z}$
or $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{i_1}} \times \cdots \times \mathbb{Z}_{p_k^{i_k}}$
$I_1 = p_1^{i_1}\mathbb{Z}, I_2 = p_2^{i_2}\mathbb{Z}, \dots, I_k = p_k^{i_k}\mathbb{Z}$
$I_1 \cap I_2 \cap \cdots \cap I_k = n\mathbb{Z}$
So $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{i_1}} \times \cdots \times \mathbb{Z}_{p_k^{i_k}}$

Example 2

Let $p(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_k) \in \mathbb{R}[x], \ \lambda_1, \dots, \lambda_k$ are distinct real numbers
Then $\mathbb{R}[x]/(p(x)) \cong \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}, \ k$ times
Why? Let $I_i = (x - \lambda_i) = (x - \lambda_i)\mathbb{R}[x]$
$\mathbb{R}[x] = I_i + I_j$. Why?
$(x - \lambda_i) + (x - \lambda_j) = \lambda_j - \lambda_i \in I_i + I_j \Rightarrow 1 \in I_i + I_j \Rightarrow I_i + I_j = \mathbb{R}[x]$
Notice that $I_1 \cap I_2 \cap \cdots \cap I_k = (p(x)) = p(x)\mathbb{R}[x]$
Why? $q(x) = I_k \Leftrightarrow (x - \lambda_k) | q(x)$
$\Rightarrow q(x) = I_1 \cap I_2 \cap \cdots \cap I_k \Leftrightarrow (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_k) | q(x) \Leftrightarrow p(x) | q(x) \Leftrightarrow q(x) \in (p(x)) = p(x)\mathbb{R}[x]$
So CRT
$\mathbb{R}[x]/(p(x)) = \mathbb{R}[x]/(I_1 \cap I_2 \cap \cdots \cap I_k) \cong \mathbb{R}[x]/(x - \lambda_1) \times \cdots \times \mathbb{R}[x]/(x - \lambda_k)$

To finish, if $\lambda \in \mathbb{R}$ we have a surjective homomorphism $\phi: \mathbb{R}[x] \to \mathbb{R}, \ \phi(q(\lambda)) = q(\lambda)$
$\ker \phi = \{q(x): q(\lambda) = 0\} = (x - \lambda)\mathbb{R}[x]$
So $\mathbb{R}[x]/(x - \lambda) \cong \mathbb{R}$

$\therefore \mathbb{R}[x]/(p(x)) \cong \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}, \quad k$ times

Proof of Chinese Remainder Theorem

Let $L = \bigcap_{i=1}^{k} I_i \trianglelefteq R$
Then $L \subseteq I_1, I_2, \dots, I_k$
So $\exists$ a surjective homomorphism $\pi_i: R/L \to R/I_i, \ [r]_L \mapsto [r]_{I_i}$
We define a homomorphism
$\phi: R/L \to R/I_1 \times R/I_2 \times \cdots \times R/I_k$
by $\phi([r]_L) = ([r]_{I_1}, [r]_{I_2}, \dots, [r]_{I_k})$
To show that ϕ is an isomorphism, must check that ϕ is 1-1 and onto.
To see that ϕ is 1-1, let's find $\ker \phi$
So $[r]_L$ is in $\ker \phi \Leftrightarrow \phi([r]_L) = ([r]_{I_1}, \dots, [r]_{I_k}) = (0, \dots, 0)$

$\Leftrightarrow [r]_i = 0 \ \forall i \in \{1, \dots, k\} \Leftrightarrow r \in I_i \ \forall i \in \{1, \dots, k\} \Leftrightarrow r \in \bigcup_{i=1}^{k} I_i = L \Leftrightarrow [r]_L = [0]_L$

So $\ker \phi = \{[0]_L\} \Rightarrow \phi$ is 1-1
We now show that ϕ is onto.

Claim:

$\exists u_1, u_2, \dots, u_k \in R$ such that $\phi([u_i]_L) = (0, 0, \dots, 0, 1, 0, 0, \dots, 0)$ 1 in position i
Once we have the claim, we are done because if
$([r_1]_{I_1}, [r_2]_{I_2}, \dots, [r_k]_{I_k}) \in R/I_1 \times R/I_2 \times \cdots \times R/I_k$
Then $\phi([r_1 u_1 + r_2 u_k + \cdots + r_k u_k]_L) = \phi([r_1 u_1]_L) + \phi([r_2 u_2]_L) + \cdots + \phi([r_k u_k]_L) = ([r_1]_{I_1}, \dots, [r_k]_{I_k})$

Notice that $\phi([r_i u_i]_L) = \phi([r_i]_L)\phi([u_i]_L) = ([r_i]_{I_1}, [r_i]_{I_2}, \dots, [r_i]_{I_k}) \cdot (0, 0, \dots, 0, 1, 0, \dots, 0) = (0, 0, \dots, 0, [r_i]_{I_i}, 0, \dots, 0)$

Proof of Claim

Let's see how to construct u_1.
Notice that $I_1 + I_2 = R \Rightarrow \exists x_2 \in I_1, y_2 \in I_2 \ s.t. \ x_2 + y_2 = 1 \Rightarrow y_2 = 1 - x_2$
$I_1 + I_3 = R \Rightarrow \exists x_3 \in I_1, y_3 \in I_3 \ s.t. \ x_3 + y_3 = 1 \Rightarrow y_3 = 1 - x_3$
$\vdots$

$$I_1 + I_k = R \Rightarrow \exists x_k \in I_1, y_k \in I_k \; s.t. x_k + y_k = 1 \Rightarrow y_k = 1 - x_k$$

Let $u_1 = y_2 y_3 \dots y_k = (1 - x_2)(1 - x_3) \dots (1 - x_k)$

Then $\phi([u_1]_L) = \left([u_1]_{I_1}, [u_1]_{I_2}, \dots, [u_1]_{I_k}\right)$

Notice $u_1 = y_2 y_3, \dots y_j \dots y_k, j \geq 2$

$\Rightarrow u_i \in I_j \forall j \geq 2 \because I_j$ is an ideal and $y_j \in I_j$

$\Rightarrow [u_i]_{I_j} = 0$ for $j = 2, \dots, k$

Also, $[u_1]_{I_1} = [(1 - x_2)(1 - x_3) \dots (1 - x_k)]_{I_1} = [(1 - x_2)]_{I_1} \cdot [(1 - x_3)]_{I_2} \cdots [(1 - x_k)]_{I_1}$

Notice $x_i \in I_1$ for $i = 2, \dots, k$

so $1 \equiv 1 - x_i \pmod{I_1} \; \forall i$

$\Rightarrow [1 - x_i]_{I_1} = [1]_{I_1}$

So $\phi([u_1]_L) = \left([1]_{I_1}, [0]_{I_2}, \dots, [0]_{I_k}\right)$

By symmetry, we can construct $u_2, \dots, u_k$.

The result follows.

PIDs and UFDs

November-19-13 10:02 AM

From Now On

R is a commutative integral domain

Principal Ideal Domain

Let R be a commutative integral domain. We say that R is a **pricipal ideal domain** (PID) if for every ideal $I \trianglelefteq R, \exists f \in I$ s.t. $I = Rf = (f)$

Irreducible & Prime

In general, if R is a communtative integral domain and $f \in R$ is nonzero and not a unit, we say that f is **irreducible** if f cannot be written as a product of $a \cdot b$ with neither a nor b a unit. We say that f is **prime** if $(f) = Rf$ is a prime ideal.

Example

If $R = \mathbb{Z}, n$ is irreducible $\Leftrightarrow n$ is a prime number or - a prime number.
If $R = \mathbb{Z}, n$ is prime $\Leftrightarrow n = \pm p, p$ prime

Remark

If f is prime then f is irreducible.

Remark 2

In a PID, we have irreducible $\Leftrightarrow$ prime.

Unique Factorization Domain

Let R be a communtative integral domain. We say that R is a unique factorization domain

1) If every nonzero, non-unit $r \in R$ can be written as a product of irreducible elements $r = f_1 \dots f_k$
2) If $r = f_1 \dots f_k = g_1 \dots g_j$ are two factorizations into irreducibles then $k = j$ and after a sutiable permutation of $g_1, \dots, g_k$ we have $f_i = u_i g_i$, u_i is a unit for $i = 1, \dots, k$

Wilson's Theorem

p prime, $p > 2 \Rightarrow (p-1)! \equiv -1 \pmod p$

Example PIDs

- $R = \mathbb{Z}$ is a PID
- If F is a field $\Rightarrow F[x]$ is a PID
- (assignment) $R = \left\{\frac{a}{2^b}, a \in \mathbb{Z}, b \geq 0\right\}$ is a PID
- A field F is a PID $\rightarrow$ only has two ideals, $(0), F = F \cdot 1$
- $R = \mathbb{Z}[i]$ is a PID

Proof that $\mathbb{Z}[i]$ is a PID

Let $I \trianglelefteq \mathbb{Z}[i]$.
If $I = (0)$, there is nothing to show, $I = 0\mathbb{Z}[i]$
So assume that $I \neq (0)$
Given $a + ib \in \mathbb{Z}[i]$, define $a^2 + b^2 = |a + ib|^2$ to the the norm of $a + ib$
Pick $a + ib$ nonzero in I with smallest possible norm.
We claim that $I = (a + ib) = (a + ib)\mathbb{Z}[i]$

Why?

Let $c + id \in I$. Then let $x + iy = \frac{c+id}{a+ib} \in \mathbb{C}$
Pick $m + in \in \mathbb{Z}[i]$ that is closest to $x + iy$.
Then $|(x + iy) - (m + in)| \leq \frac{1}{\sqrt{2}}$

$$\Rightarrow \left|\frac{c + id}{a + ib} - (m + in)\right| \leq \frac{1}{\sqrt{2}}$$

$$\Rightarrow |c + id - (m + in)(a + ib)| \leq \frac{|a + ib|}{\sqrt{2}} = \sqrt{\frac{a^2 + b^2}{2}}$$

So if $e + fi = c + id - (m_{in})(a + ib) \in I$ and $|e + fi| = \sqrt{c^2 + f^2} \leq \sqrt{\frac{a^2+b^2}{2}}$
$\Rightarrow$ norm of $e + fi = e^2 + f^2 \leq \frac{1}{2}$norm of $a + ib$
Since $a + ib \in I$ is a nonzero element with emallest norm and norm of $e + fi$ is smaller
$\Rightarrow e + if = 0 \Rightarrow c + id = (a + ib)(m + in) \Rightarrow c + id \in (a + ib) \Rightarrow I = (a + ib)$

Proof of Remark

Suppose that f is prime. Let $f = ab$ with neighter a nor b a unit. $\Rightarrow ab \in (f)$
$\therefore (f)$ is prime, $ab \in (f) \Rightarrow a \in (f)$ or $b \in (f)$
WLOG $a \in (f) \Rightarrow a = fu$
$f = ab = fub \Rightarrow f(1 - ub) = 0 \Rightarrow b$ is a unit. Contradiction.

Example

If $R = \{a_0 + a_2t^2 + a_3t^3 + \dots + a_mt^m : m \geq 2, a_0, a_2, \dots, a_m \in \mathbb{Q}\}$
t^2 and t^3 are irreducible in R
But (t^2) is not a prime ideal: $t^3 \cdot t^3 = t^6 \in (t^2), but\ t^3 \notin (t^2)$

Proof of Remark 2

Let $J \trianglelefteq R$ with $I \trianglelefteq J \trianglelefteq R$
Since R is a PID, $\exists a \in R$ s.t. $J = (a)$
So $I = (f) \subseteq (a) = J \Rightarrow f = ab$ for some $b \in R$
$\because f$ is irreducible either a or b is a unit
Case I: a is a unit
$\Rightarrow J = aR \supseteq a(a^{-1}R) = R$
Case II: b is a unit
$\Rightarrow J = I$ because $I = fR = a(bR) = aR = J$
So I is maximal $\Rightarrow J = (f)$ is a prime ideal $\Rightarrow f$ is prime

Example Unique Factorization

in $\mathbb{Z}$ UFD, $6 = 2 \cdot 3 = (-3)(-2) = (-2)(-3)$

Example

Let's look at $\mathbb{Z}[i]$. Want to show $p \equiv 1 \pmod 4 \Rightarrow p = a^2 + b^2$

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$$

$$= (1 \cdot (p-1))(2 \cdot (p-2))(3 \cdot (p-3)) \cdots \left(\left(\frac{p-1}{2}\right)\left(p - \left(\frac{p-1}{2}\right)\right)\right)$$

$$\equiv (-1)(-4)(-9) \cdots \left(-\left(\frac{p-1}{2}\right)^2\right) \equiv (-1)^{\frac{p-1}{2}}\left(\left(\frac{p-1}{2}\right)!\right)^2$$

$$\equiv -1 \pmod p$$

So if $p \equiv 1 \pmod 4$

$$\Rightarrow \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod p$$

$$\Rightarrow \left(\left(\frac{p-1}{2}\right)!\right)^2 + 1 \equiv 0 \pmod p$$

Let $N = \left(\frac{p-1}{2}\right)!$. Then $p|(N^2 + 1) \Rightarrow p|(N + i)(N - i)$ in $\mathbb{Z}[i]$
This shows that p is not prime in $\mathbb{Z}[i]$
If p were prime we would have either $N + i$ or $N - i \in (p) = p$\dz $[i]$
But this is impossible .
If $N + 1 \cdot i = p(c + di) = pc + pdi$
$\Rightarrow pd = 1$. Contradiction
Since $\mathbb{Z}[i]$ is a PID and p is not prime.
So p is not irreducible

$\Rightarrow p = (a + ib)(c + di)$
Take modulus squared
$\Rightarrow p^2 = (a^2 + b^2)(c^2 + d^2)$

Since p is a prime in $\mathbb{Z}$ (not in $\mathbb{Z}[i]$), $a^2 + b^2 \in \{1, p, p^2\}$
Case I: $a^2 + b^2 = 1 \Rightarrow a + ib \in \{\pm 1, \pm i\}$. All units, contradiction
Case II: $a^2 + b^2 = p^2 \Rightarrow c^2 + d^2 = 1 \Rightarrow c + id \in \{\pm 1, \pm i\}$ Contradiction
Case III is only one allowed
$\boxed{a^2 + b^2 = p}$

Notice if $p \equiv 3 \pmod 4$
$p \neq a^2 + b^2$ (0,1) mod 4 + (0,1) mod 4

$\boxed{2 = 1^2 + 1^2}$
So this characterizes the sum of squares

Noetherian Ring

November-21-13 10:03 AM

Ascending Chains

Let R be a commutative ring.
If $I_1, I_2, I_3, \ldots$ are ideals of R with $I_1 \subseteq I_2 \subseteq I_3 \subseteq I_4 \subseteq \cdots$
then we call $I_1, I_2, \ldots$ an **ascending chain** of ideals. We say that n ascending chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ **terminate** if $\exists n \geq 1$ s.t. $I_n = I_{n+1} = I_{n+2} = \cdots$
We say that a ring R satisfies the **ascending chain condition** (A.S.C.) on ideals if **every** chain of ideals terminates.

Noetherian Ring

A ring R is noetherian if it satisfies A.S.C on ideals

Theorem

If R is a PID then R is noetherian.

Theorem

A ring R is noetherian $\Leftrightarrow$
whenever $\mathcal{S}$ is a nonempty collection of ideals of R $\exists$ a maximal element of $\mathcal{S}$ w.r.t. $\supseteq$

Note

We will use these ideas to prove that a PID is a UFT.
$\{\text{field}\} \subseteq \{PID\} \subsetneq \{UFD\} \subsetneq \{\text{commutative integral domain}\}$

Lemma

Let R be a PID and let r be nonzero and not a unit in R.
Then $\exists s \geq 1$ and irreducible elements $f_1, \ldots, f_s \in R$ s.t. $r = f_1 f_2 \ldots f_s$

Theorem

A PID is a UFD

Example

$R = \mathbb{Z}$ is noetherian.
Why?
Suppose $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq I_4 \subsetneq \cdots$
$n_2\mathbb{Z} \subsetneq n_3\mathbb{Z} \subsetneq n_4\mathbb{Z}, \quad n_1, n_2, n_3, \ldots \geq 0$
$n\mathbb{Z} \subseteq m\mathbb{Z} \Leftrightarrow m|n$ so $n_2 > n_3 > n_4 > \cdots$
So we have an infinite sequence of decreasing positive integers. This is impossible. Contradiction

Example

$R = F$, a field is noetherian
Why?
$I \trianglelefteq R \Rightarrow I = (0)$ or $I = R$

Proof of Theorem

Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq I_4$ be a chain of ideals of R.

Let $J = \bigcup_{n=1}^{\infty} I_n \trianglelefteq R$

Since R is a PID, $\exists r \in R$ s.t. $R = (r) = Rr$

$r \in \bigcup_{n=1}^{\infty} I_n \Rightarrow \exists m \geq 1\ s.t.\ r \in I_m \Rightarrow I_m \supseteq J \Rightarrow J = I_{m+1} = I_{m+2} = \cdots$

Proof of Theorem

Suppose that R is noetherian and let $\mathcal{S}$ be a nonempty set of ideals. Let $I \in \mathcal{S}$.
If I is maximal in $\mathcal{S}$, we are done.
If not, $\exists I_2 \in \mathcal{S}$ s.t. $I_2 \supsetneq I_1$
If I_2 is maximal in $\mathcal{S}$, we're done. Otherwise $\exists I_3 \in \mathcal{S}\ s.t.\ I_3 \supsetneq I_2 \supsetneq I_1$
Continuing in this manner, we either produce a maximal element of $\mathcal{S}$ or we product a non-terminating ascneding chain: $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq I_4 \subsetneq \cdots$
$\because$ R is noetherian, the latter cannot occur.

Other direction: Suppose that every non-empty set of ideals has a maximal element and let $I_1 \subseteq I_2 \subseteq I_3 \subseteq I_4 \subseteq \cdots$ be a chain. Let $\mathcal{S} = \{I_1, I_2, I_3, \ldots\}$
By assumption, $\exists I_n \in \mathcal{S}$ s.t. I_n is maximal. So $I_n = I_{n+1} = I_{n+2} = \cdots$

Proof of Lemma

Suppose not.
Let $\mathcal{S} = \{xR : x \text{ is not a unit, } x \neq 0 \text{ and } x \text{ doesn't factor into irreducibles}\}$
Then $\mathcal{S} \neq \emptyset$. since a PID is noetherian, $\exists r \in R$ s.t. $rR \in \mathcal{S}$ is a maximal element.
So R doesn't factor into irreducibles, in particular, r is not irreducible
(otherwise $s = 1,\ f_1 = r$ is a factorization of r)
So $\exists a, b \in R\ \ a, b$ non-units such that $r = ab$ $\big((r) \subseteq (a), (b)\big)$

Claim

$(r) \subsetneq (a)$ and $(r) \subsetneq (b)$
We'll show that $(r) \subsetneq (a)$. Notice $r = ab \in (a) \Rightarrow r \subseteq (a)$
In integral domain so can cancel r in $r = rub$
So if $(r) = (a) \Rightarrow a \in (r) \Rightarrow a = ru \Rightarrow r = ab = rub \Rightarrow 1 = ub \Rightarrow b$ is a unit.
Contradiction. $\Rightarrow (r) \subsetneq (a)$
Similarly, $(r) \subsetneq (b)$
Now $(r) = rR$ is a maximal element of $\mathcal{S}$ and since $(a), (b)$ are bigger, we see they cannot be in $\mathcal{S}$. $\because aR, bR \neq \mathcal{S}$ by definition of $\mathcal{S}$, a and b factor into irreducibles,
$a = f_1 \ldots f_s, \qquad b = f_{s+1} \ldots f_t$
$\Rightarrow r = ab = f_1 f_2 \ldots f_s f_{s+1} \ldots f_s$. Contradiction. So $\mathcal{S} = \emptyset$ and everything factors into irreducibles.

Proof of Theorem

Let $r \in R$ be a nonzero, non-identity element athat does not factor uniquely.
Say $r = f_1 \ldots f_m = g_1 \ldots g_n\ \ f_i$ irreducible, g_i irreducible.
Among all elements r with non-unique factorizations as above, pick one with $\min(m, n)$ minimal.
Notice that $(f_1) = f_1 R$ is a prime ideal $\because f_1$ is irreducible and irred. $\Leftrightarrow$ prime in a PID.
Notice that $r = f_1 \ldots f_m \in (f_1)$ so $g_1 g_2 \ldots g_n \in (f_1)$
$\because (f_i)$ is prime $\Rightarrow \exists i$ s.t. $g_i \in (f_i)$
By relabeling, we may assume that $g_1 \in (f_1)$
$\Rightarrow g_1 \in f_1 R \Rightarrow \exists a \in R$ s.t. $g_1 = f_1 a$
$\because g_1$ is irreducible, a must be a unit so $g_1 = f_1 a$
So $r = f_1 f_2 \ldots f_m = (f_1 a) g_2 \ldots g_m \Rightarrow S = f_2 \ldots f_m = (a g_2) \ldots g_n$
By minimality of $\min(n, m)$, S factors uniquely so $m - 1 = n - 1$ and $f_2, \ldots, f_m$ is up to permuting and mulitiplication by units, $(a g_2), g_3, \ldots, g_n$
i.e. after relabeling g_i again we have $f_i = g_i u_i,\ \ i \geq 3$
$f_2 = (a g_2) u_2 = g_2 (a u_2)$. $a u_2$ is a unit. The result follows.

Euclidean Domains

November-21-13 10:58 AM

Euclidean domains (Norm)

A Euclidean domain (ED) is a commutative integral domain R with a function $N: R \to \{0, 1, 2, \dots\}$ called the **norm** such that

1) $N(0) = 0$;
2) $N(ab) \geq N(a)$ when $b \neq 0$
3) If $a, b \in R, b \neq 0$ then $\exists q, r \in R$ s.t. $a = qb + r$ and $N(r) < N(b)$ or $r = 0$.

Proposition

Let R be a ED then the Euclidean algorithm holds in R.

Corollary

ED $\Rightarrow$ PID

Examples

Example

$R = \mathbb{Z}, N(n) = |n|$

$R = F[x], F$ is a field, $N\big(p(x)\big) = \deg\big(p(x)\big)$

Example

$R = F$ is a field, $N(a) = 0\ \forall a \in F$

Example

$R = \mathbb{Z}[i]$ is a ED

$N(a + ib) = a^2 + b^2$

$a + ib = (c + id)(n + im) + (r + is)$

$|r + is| \leq \dfrac{|c + id|}{\sqrt{2}}$

So $N(r + is) \leq \frac{N(c+id)}{2}$

Proposition

Step 1

$a, b \in R, a = q_1 b + r_1 \Rightarrow N(r_1) < N(b)$ or $r_1 = 0$

Step 2

$b = q_2 r_1 + r_2, \qquad N(r_2) < N(r_1)$ or $r_2 = 0$

$r_1 = q_3 r_2 + r_3, \qquad N(r_3) < N(r_2)$ or $r_3 = 0$

...

$r_{n-1} = q_{n+1} r_n + r_{n+1}, \qquad r_{n+1} = 0$

So $\exists$ some largest i s.t. $r_i \neq 0, r_{i-1} = q_{i+1} r_i + 0$

This r_i is called the gcd of a and b. Notice that $r_i \in (a, b)$

Why? Induction, $r_1 = a - q_1 b \in (a, b)$

$r_2 = b - q_2 r_1 \in (a, b)$

...

Also, $r_i | a$ and $r_i | b$. Why? Induction in the reverse direction.

So $(r_i) = (a, b)$

Why? $r_i \in (a, b) \Rightarrow (r_i) \subseteq (a, b)$

$r_i | a \Rightarrow a \in (r_i), \qquad r_i | b \Rightarrow b \in (r_2) \Rightarrow (a, b) \subseteq (r_i)$

So $(r_i) = (a, b)$

Proof of Corollary

If $I \trianglelefteq R,\ I \neq (0),\ R$ is a ED

Pick $x \neq 0$ in I with $N(x)$ minimal.

Claim: $I = (x)$

If $a \in I \Rightarrow a = qx + r$

$a, x \in I \Rightarrow r \in I, \qquad$ so $N(r)\ not < N(x) \Rightarrow r = 0 \Rightarrow a \in (x)$

Irreducibility in UFDs

November-26-13 10:02 AM

Associates

Let R be a UFD. We say that $f, g \in R \setminus \{0\}$ are associates if
$\exists u \in R^* =$ units of R s.t. $f = gu$

UFD

Another way of stating the UFD property is:
If $r \in R$ is nonzero and not a unit then
1) r factors into irreducibles $f_1, \dots, f_s$
2) If $r = f_1 \cdots f_s = g_1 \cdots g_t \Rightarrow s = t$ and after relabelling the g_i we have f_i and g_i are associates.

GCDs and LCMs

If r and s are nonzero elements of R $\exists$ irreducible elements $f_1, \dots, f_m$ and units u_1 and u_2 s.t.
$r = u_1 f_1^{i_1} \cdots f_m^{i_m}$
$s = u_2 f_1^{j_1} \cdots f_m^{j_m}$
Where $i_k, j_k \geq 0$

We define a **gcd** of r and s to be: $f_1^{\min(i_1, j_1)} \cdots f_m^{\min(i_m, j_m)}$
and an **lcm** of r and s to be: $f_1^{\max(i_1, j_1)} \cdots f_m^{\max(i_m, j_m)}$
gcd is not unique, but if a and b are two gcds of r and s then $a \mid b$ and $b \mid a$ so $a = ub$, u unit.

Notes

In general, π prime $\Rightarrow \pi$ irreducible.
We showed prime $\Leftrightarrow$ irreducible in a PID. In fact, we have

Theorem

Let R be a UFD and let $r \in R$. Then r is irreducible iff r is prime.

Lemma

Let R be a UFD and let $\pi \in R$ be irreducible ($=$ prime) .
If $p(x), q(x) \in R[x]$ are such that $\pi \mid p(x)q(x)$
then either $\pi \mid p(x)$ or $\pi \mid q(x)$.

Note

Saying $\pi \in R$ divides $a(x) = a_0 + a_1 x + \cdots + a_m x^m$ in $R[x]$
means $a(x) = \pi b(x)$ for some $b(x) \in R[x]$
$\Rightarrow a(x) = \pi(b_0 + b_1 x + \cdots + b_n x^n) = (\pi b_0) + (\pi b_1)x + \cdots + (\pi b_m)x^m$

Gauß's Lemma (Gauss's Lemma)

Let R be a UFD and let F be the field of fractions of R.
If $p(x) \in R[x]$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$.

What does this mean?

$p(x)$ reducible in $F[x] \leftrightarrow p(x) = a(x)b(x), \ \ a(x), b(x) \in F[x]$ neither one is a unit
$p(x)$ reducible in $R[x] \leftrightarrow p(x) = c(x)d(x), \ \ c(x), d(x) \in R[x]$ neither one a unit.

Primitive

Let $p(x) = p_0 + p_1 x + \cdots + p_m x^m \in R[x]$ be a nonzero polynomial.
We say that $p(x)$ is primite if whenever $a \neq 0, a \mid p_0, \dots, a \mid p_m \Rightarrow a$ is a unit.

Goal

R is a UFD $\Rightarrow R[x]$ is a UFD

Corollary

R is a UFD $\Rightarrow R[x_1, \dots, x_n]$ is a UFD

Corollary

$\mathbb{Z}[x]$ is a UFD and it is not a PID
So ED $\subsetneq$ PID $\subsetneq$ UFD
Won't prove inequality part of ED $\subsetneq$ PID

Example: $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

Criterion for Irreducibility

Proposition

Let R be a UFD and let $p(x) \in R[x]$ be a non-constant polynomial.
Then $p(x)$ is irreducible in $R[x]$ **if and only if** $p(x)$ is primitive **AND** $p(x)$ is irreducible in $F[x]$.
F is the field of fractions of R.

So we're now ready to prove the ultimate theorem.

Theorem

Let R b ea UFD. Then $R[x]$ is a UFD.

Goal

If R is a UFD $\Rightarrow R[x]$ is a UFD $\Rightarrow R[x][y]$ is a UFD $\Rightarrow \dots \Rightarrow R[x_1, \dots, x_n]$ is a UFD.

Proof of Theorem

Already know prime $\Rightarrow$ irreducible.
It suffices to show that if $f \in R$ is irreducible then f is prime.
So suppose f is irreducible but $(f) \in fR$ is not a prime ideal.
$\exists a, b \in R$ neither a nor b in (f), s.t. $ab \in (f) \Rightarrow \exists s \in R$ s.t. $ab = fs$
Now we use that R is a UFD: factor $a = g_1 \cdots g_k, b = h_1 \cdots h_l$ and $s = t_1 \cdots t_m$ all irreducible. So we have two factorizations of ab
$ab = g_1 \cdots g_k h_1 \cdots h_l = f \cdot t_1 \cdots t_m$
By uniqueness, $\exists i$ s.t. f is an associate of either g_i or h_i.
WLOG, f is an associate of g_i. So $g_i = fv, v$ a unit.
$a = g_1 \cdots g_{i-1} g_i g_{i+1} \cdots g_k = g_i g_1 \cdots g_{i-1} g_{i+1} \cdots g_k = fv g_1 \cdots g_{i-1} g_{i+1} \cdots g_k \in (f)$
This is a contradiction since $a \notin (f)$
So f is prime. ∎

Now we'll prove the last theorem of the course.

Theorem

Let R be an UFD. Then $R[x]$ is a UFD.

Strategy

If R is a UFD $\Rightarrow R$ is an integral domain $\Rightarrow R$ has a field of fractions F.
$F = \left\{ \frac{r}{s} \,\middle|\, r, s \in R, s \neq 0 \right\}$
Notice we have an injective ring homomorphism $i: R \to F, \ i(r) = \frac{r}{1}$
Henceforth we identify R with its image in F and we write $R \subseteq F$.
Key idea: $R[x] \subseteq F[x]$

Remark

If S is a commutative integral domain then $S[x]^* = S^*$
Why?

$s_0 + s_1 x + \cdots + s_m x^m \in S[x]^*, s_m \neq 0$
$\Rightarrow \exists a_0 + a_1 x + \cdots + a_n x^n \in S[x], a_n \neq 0$ s.t.
$1 = (s_0 + s_1 x + \cdots + s_m x^m)(a_0 + a_1 x + \cdots + a_n x^n)$
Notice: If $m + n > 0$ the coefficient of x^{n+m} on the LHS $= 0$, on RHS $= s_m a_n \neq 0$.
Contradiction
So $m + n = 0 \Rightarrow m = n = 0 \Rightarrow s_0 a_0 = a_0 s_0 = 1 \Rightarrow s_0 \in S^*$

Conversely, if $s \in S^* \Rightarrow \exists t \in S^*$ s.t. $st = ts = 1 \Rightarrow s$ is also a unit in $S[x]$

Proof of Lemma

Write $p(x) = p_0 + p_1 x + \cdots + p_m x^m, \ q(x) = q_0 + q_1 x + \cdots + q_n x^n$
We assume that $\pi \mid p(x)q(x)$.
Suppose that $\pi \nmid p(x)$ and $\pi \nmid q(x)$.
Then $\exists$ some smallest $i_0 \geq 0$ s.t. $\pi \nmid p_{i_0}$ and $\exists$ some smallest $j_0 \geq 0$ s.t. $\pi \nmid q_{j_0}$
We have that $\pi \mid p(x)q(x) = (p_0 + p_1 x + \cdots + p_m x^m)(q_0 + q_1 x + \cdots + q_n x^n)$, so π divides every coefficient of the product.
In particular, π divides the coefficient of $x^{i_0 + j_0}$, which is:
$p_0 q_{i_0 + j_0} + p_1 q_{i_0 + j_0 - 1} + \cdots + p_{i_0 - 1} q_{j_0 + 1} + p_{i_0} q_{j_0} + p_{i_0 + 1} q_{j_0 - 1} + \cdots + p_{i_0 + j_0} q_0$
π divides $p_0, \dots, p_{i_0 - 1}$ and π divides $q_0, \dots, q_{j_0 - 1}$ so π divides every term in the sum except possibly $p_{i_0} q_{j_0}$. π divides the whole sum, so $\pi \mid p_{i_0} q_{j_0}$.
π is prime $\Rightarrow \pi \mid p_{i_0}$ or $\pi \mid q_{j_0}$. Contradiction.
The result follows.

Proof of Gauß's Lemma

Suppose that $p(x)$ is reducible in $F[x]$.
Then $p(x) = a(x)b(x), \ a(x), b(x) \in F[x]$, neither one a unit.
Write $a(x) = \frac{a_0}{s_0} + \frac{a_1}{s_1} x + \cdots + \frac{a_m}{s_m} x^m, \ a_i, s_i \in R, \ s_i \neq 0, \ m > 0$
Write $b(x) = \frac{b_0}{t_0} + \frac{b_1}{t_1} x + \cdots + \frac{b_n}{t_n} x^n, \ b_i, t_i \in R, \ t_i \neq 0, \ n > 0$
Let $A = s_0 \cdots s_m, B = t_0 \cdots t_n$
Then $Aa(x) \in R[x]$ and $Bb(x) \in R[x]$
So $ABp(x) = ABa(x)b(x) = \big(Aa(x)\big)\big(Bb(x)\big)$
Let $f(x) := Aa(x), \ g(x) := Bb(x)$
Factor AB into irreducibles: $AB = \pi_1 \cdots \pi_k, \ \pi_i$ not necessarily distinct.
Notice that $\pi_1 \mid AB \Rightarrow \pi_1 \mid ABp(x) \Rightarrow \pi_1 \mid f(x)g(x)$
By our Lemma, $\pi_1 \mid f(x)$ or $\pi_1 \mid g(x)$ (divides in $R[x]$)
Suppose $\pi_1 \mid f(x)$. Then $f(x) = \pi_1 f_1(x), \ f_1(x) \in R[x], \ g_1(x) = g(x)$
So $ABp(x) = f(x)g(x) \Rightarrow \pi_1 \pi_2 \cdots \pi_k p(x) = f(x)g(x) \Rightarrow \pi_2 \cdots \pi_k p(x) = f_1(x)g_1(x)$
Continuing in this manner, we get a factorization for
$p(x) = f_k(x)g_k(x), \qquad f_k, g_k \in R[x]$
Also, $\deg f_k = \deg f = m > 0$ and $\deg g_k = \deg g = n > 0$ so neither are units.
∎

Example of Primitive Elements

$R = \mathbb{Z}$
$4 + 12x + 6x^2$ is **not** primitive.
$3 + 2x + 11x^2$ is primitive.

Proof of Proposition

If $p(x)$ is reducible in $F[x] \Rightarrow p(x)$ is reducible in $R[x]$ (Gauß's Lemma)
In other words,
If $p(x)$ is irreducible in $R[x] \Rightarrow p(x)$ is irreducible in $F[x]$.
Also, $p(x)$ must be primitive, because if not $\exists a \in R$ not a unit, that divides $p(x)$ in $R[x]$.
i.e. $p(x) = aq(x)$. Contradiction.

So we've shown:

$p(x)$ irreducible in $R[x] \Rightarrow$ primitive and irreducible in $F[x]$.

Now we have to show the converse.
Suppose that $p(x)$ is not irreducible.
Then $p(x) = a(x)b(x)$ with neither $a(x)$ nor $b(x)$ in $R[x]^* = R^*$
If $a(x)$ and $b(x)$ both have degree ≥ 1 then $p(x)$ is reducible in $F[x]$ because $a(x), b(x) \notin F[x]^* = F^*$
So we may assume that $\deg(a)$ or $\deg(b)$ is zero, i.e. one is constant.
WLOG we may assume that $a(x) = a \in R$
So $p(x) = a \cdot b(x)$. Notice $a = a(x) \notin R[x]^* = R^*$
So a is not a unit in R^*
$p(x) = a(b_0 + b_1 x + \cdots + b_n x^n) = ab_0 + ab_1 x + ab_n x^n$. So a divides every coefficient of $p(x)$ and a is not a unit so $p(x)$ is not primitive.
So we get the converse.

Proof of Theorem

The proof has two parts:
Part 1: Show every nonzero element of $R[x]$ factors into irreducibles
Part 2: Use the fact that $F[x]$ is a UFD to show that the factorization in $R[x]$ is unique up to permuting associate factors.

Proof of Part 1

We'll do this by induction on degree. Let $p(x) \in R[x],\ p(x) \neq 0$. p has degree d.

Base Case: $d = 0$

Then $p(x) = r \neq 0$ in R
Since R is a UFD, $r = u\pi_1 \cdots \pi_k,\ u \in R^* = R[x]^*,\ \pi_1, \ldots, \pi_k$ irreducible in R.
Notice $\pi_1, \ldots, \pi_k$ are irreducible in $R[x]$ and $u \in R[x]^*$

Induction

Now suppose all nonzero elements of degree $< d$ factor into irreducibles and consider the case when $\deg p(x) = d$
Case 1: $p(x) \in R[x]$ irreducible. Then we're done: $p(x) = p(x)$
Case 2:

Write $p(x) = Cp_0(x),\ p_0(x)$ primitive.
Then $C \in R$, so it factors into irreducbles (base case)
If $p_0(x)$ is irredcible, then done.
If $p_0(x)$ is reducible then $p_0(x) = a(x)b(x)$ and $\deg a(x), b(x) > 0$
So $\deg(x), b(x) < d$
By induction hypothesis, they both factor into irreducibles .
So $p(x) = Ca(x)b(x)$ ■ (part 1)

Proof of Part 2

Let $0 \neq p(x) = p_0 + p_1 x + \cdots + p_d x^d \in R[x]$
Let $C =$ a gcd for $p_0, p_1, \ldots, p_d$
Then $p(x) = Cq(x)$, $q(x)$ is primitive.
Now suppose that we have two factorizations into irreducibles.
$p(x) = Cq(x) = \pi_1 \cdots \pi_s f_1(x) \cdots f_s(s) = \pi_1' \cdots \pi_t' g_1(x) \cdots g_u(x)$
$f_1(x) \cdots f_s(x)$ primitive and $\deg \geq 1$
$g_1(x) \cdots g_u(x)$ primitive and $\deg \geq 1$
So that means that $C = \pi_1 \cdots \pi_s = (u\pi_1') \cdots (\pi_t')$
So $s = t$ and after permuting π_i is an associate of π_i'
So it is enough to consider the factorization $f_1(x) \cdots f_s(s) = g_1(x) \cdots g_u(x)$
Since each f_i is irreducible in $R[x]$, it is irreducible in $F[x]$
Since each g_i is irreducible in $R[x]$, it is irreducible in $F[x]$
So consider $r(x) \in R[x] \subseteq F[x]$

$r(x) = f_1(x) \ldots f_s(x) = g_1(x) \cdots g_u(x)$

Since $F[x]$ is a UFD, we have $s = u$ and after permuting we have $f_i(x)$ and $g_i(x)$ are associates in $F[x]$ for $i = 1, \ldots, s$
So $\exists u_i \in F[x]^* = F^*$ s.t. $f_i(x) = u_i g_i(x)$
So $u_i \in F =$ field of fractions so $\exists\ a_i, b_i \in R,\ b_i \neq 0$ s.t. $u_i = \frac{a_i}{b_i}$
So $b_i f_i(x) = a_i g_i(x)$
Let $h_i(x) = b_i f_i(x) = a_i g_i(x)$
Both b_i and a_i are gcds of coefficients of $h_i(x)$
So $\exists v_i \in R^*$ s.t. $a_i = b_i v_i \Rightarrow u_i = \frac{a_i}{b_i} = v_i \in R^*$
So $f_i(x) = g_i(x) v_i \Rightarrow f_i$ and g_i are associates in $R[x]$
So the factorization is unique. ■

Note

If R has nonzero nilpotent elements, we do not have $R[x]^* = R^*$
e.g. $R = \mathbb{Z}_4$

$\mathbb{Z}_4[x]$: $([1] + [2]x)([1] + [2]x) = [1] + [2]x + [2]x + [4]x = [1]$

$\Rightarrow \mathbb{Z}_4[x]^* \supsetneq \mathbb{Z}_4^*$