# Modern Algebra

Fall 2015
UH Manoa

Professor: Rob Harron
Book: Dummit and Foote

## August 25, 2015

### Solving Polynomials By Radicals

Given a quadratic equation $ax^2+bx+c=0$, we can find the solutions using the quadratic formula to get roots: $\frac{-b\pm\sqrt{\Delta}}{2a}$ where $\Delta$ is the discriminant ($\Delta=b^2-4ac$)

There is a symmetry in the roots. If you know one root then you know the other

Example: If $1+\sqrt{2}$ is one root, then $1-\sqrt{2}$ is the other root of the quadratic

There is "Galois Study" i.e. the study of the Galois group

Definition: The Galois group is a permutation group of the roots of a polynomial

Similarly, we can consider cubic equations $ax^3+bx^2+cx+d=0$ (involving square and cubic roots) and degree four polynomials (square and quartic roots)

$\sqrt{\sqrt{\ }} = \sqrt[4]{\ }$

For a cubic equation:
Start with $\mathbb{Q}$, add $\sqrt[3]{1}$ and adjoin roots

$$\begin{tikzcd}
& & & & K_3(\sqrt{\ }) \\
\mathbb{Q} \arrow[r, dash] & K_1=\mathbb{Q}(\sqrt[3]{1}) \arrow[r, dash] & K_2=K_1(\sqrt{\ }) \arrow[r, dash] & K_2(\sqrt[3]{\ }) \arrow[ur, dash] &
\end{tikzcd}$$

can express root as an element of the upper field

Generalize:

$$\begin{tikzcd}
& & & \mathbb{Q}(i)(\sqrt[3]{\ })(\sqrt{\ }) \\
& & \mathbb{Q}(i)(\sqrt[3]{\ }) \arrow[ur, dash, "C_2"] & \\
& \mathbb{Q}(i)(\sqrt{\ }) \arrow[ur, dash, "C_3"] & & \\
\mathbb{Q}(i) \arrow[ur, dash, "C_2"] \arrow[dr, dash, "C_2"'] & & & \\
& \mathbb{Q} & &
\end{tikzcd}$$

adding $\sqrt[3]{\ }$ is a cyclic group of order 3 (i.e. $C_3$). Adding $\sqrt{\ }$ is a cyclic group of order 2

If you can solve (i.e. write down roots/radicals) then there is a field made from steps that the roots lie in:
↳ $S_5$ or $A_5$ are not built up out of cyclic groups (i.e. not solvable)
  ↳ $A_5$ is a simple group: it is not built up by anything but itself

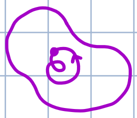
### Fundamental Group (Topology)

If $X$ is a "nice" topological space (ex: $S^1$, the unit circle). Attached to $X$ is the fundamental group $\pi_1(X)$

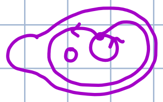
Definition: The fundamental group measures the loops in $X$

Examples:

1) Take a point and look at all of the loops that start and end at that point



you can take all the loops and contract them down to that point so the fundamental group is the trivial group

2) 

cannot contract to the point if the loop goes around the hole since you will get stuck in the hole

↳ Direction matters. Also, going around the same loop twice is different than going around it once

If $X \xrightarrow{f} Y$ is a continuous function then there is a map of the fundamental groups $f_*: \pi_1(X) \to \pi_1(Y)$

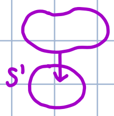
↳ note: the group operation works by equating two loops and the loop formed by both

The structure of the topological space is reflected in the structure of the groups (covariant functor)

Definition: Homotopic maps can be deformed to each other

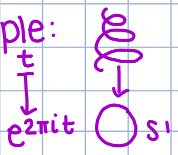
There are covering maps

Example: $Y = S^1$



Definition: The universal cover covers all other covers

Example:



The universal cover for the circle is a copy of $\mathbb{R}$

## Groups and Group Actions

Definition: A group is a set $G$ and a binary operation $\cdot: G \times G \to G$ and an element $e \in G$ satisfying:

i) $\cdot$ is associative

ii) $e$ is an identity

↳ $e \cdot a = a = a \cdot e \quad \forall a \in G$

iii) existence of inverses

↳ $\forall a \in G, \exists b \in G$ s.t. $a \cdot b = e = b \cdot a$

Definition: A group $G$ is abelian if $\cdot$ is commutative

↳ $a \cdot b = b \cdot a \quad \forall a, b \in G$

Definition: A group $G$ is finite if $\#G < \infty$ where $\#$ is the cardinality or order (i.e. the number of elements)

Examples:

1) $(\mathbb{Z},+,0)$

↳ inverses denoted $-a$ for $a\in\mathbb{Z}$

2) $(\mathbb{R},+,0)$

3) $(\mathbb{Z}/n\mathbb{Z},+,0)$

↳ cyclic group of order $n$ (i.e. $C_n$) since you can take 1 and add it to itself $n$ times to get all elements

4) $(\mathbb{R}^\times,\cdot,1)$ where $\mathbb{R}^\times=\mathbb{R}\setminus\{0\}$

5) $(\mathbb{Z}^\times,\cdot,1)$ where $\mathbb{Z}^\times=\{\pm1\}$

6) $(\mathbb{Z}/n\mathbb{Z}^\times,\cdot,1)$

There are also symmetry groups

Examples:

1) $S_n=\{f:\{1,\dots,n\}\to\{1,\dots,n\}: f \text{ is a bijection}\}$ is a group (the symmetric group of degree $n$) with the operation of function composition and the identity function which sends everything to itself

2) More generally, if $X$ is any set $S_X=\{f:X\to X: f \text{ is a bijection}\}$ is a group with function composition

3) The Group $D_3$ (book uses $D_6$) studies the rotational and reflective symmetries ($\rho$= rotation, $r$= reflection) of the equilateral triangle: $D_3=\{1,\rho,\rho^2,r,r\rho,r\rho^2\}$

4) More generally, $D_n$ (or $D_{2n}$ according to the book) looks at the rotational symmetries of the regular n-gon and has size $2n$ ($n$ rotations, $n$ reflections}

↳ $D_n$ is called the Dihedral group of degree $n$ (or order $2n$)

5) $GL_2(\mathbb{R})=\{2\text{x}2 \text{ real matrices}: \det M\neq0\}$

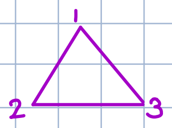
6) $GL_2(\mathbb{Z})=\{2\text{x}2 \text{ integer matrices}: \det M\in\mathbb{Z}^\times=\{\pm1\}\}$

↳ can generalize to nxn matrices

## Homomorphisms

We can study an object by studying how everything interacts with it

Example: $D_3$



We get a map $\varphi: D_3\to S_3$ that is such that $\varphi(a\cdot b)=\varphi(a)\varphi(b)$

↳ claim: $\varphi$ is injective

↳ Proof: If $\varphi(f)$ is the trivial permutation (i.e. $\varphi(f)=1$), then $f(v_1)=v_1$, $f(v_2)=v_2$, $f(v_3)=v_3$ where $v_1,v_2$, and $v_3$ are position vectors

$v_1$ and $v_2$ are a basis of $\mathbb{R}^2$ and $f$ is a linear transformation. Thus $f(v_i)=v_i$ and so $f=\text{id}$ in $D_3$ ▨

We know $\#D_3\geq6$ and $\#S_3=3!=6$. Thus since $\varphi$ is injective $\Rightarrow \#D_3=6$

Definition: Given two groups $G$ and $G'$, a group homomorphism is a function $\varphi:G\to G'$ s.t. $\varphi(ab)=\varphi(a)\varphi(b)$ $\forall a,b\in G$. A homomorphism is an isomorphism if $\exists\psi:G'\to G$ s.t. $\psi\circ\varphi=\text{id}_G$ and $\varphi\circ\psi=\text{id}_{G'}$ (equivalently $\varphi$ is a bijection

# August 27, 2015

Examples:

1) $\forall G, G', \exists \varphi: G \to G'$
$g \mapsto e$

↳ $\varphi$ is the trivial homomorphism

2) $\varphi: D_3 \to S_3$ is an isomorphism

3) $\varphi: D_n \to S_n$ for $n \geq 4$ is not surjective so it is not an isomorphism

4) $\varphi: D_3 \to GL_2(\mathbb{R})$

$$\varphi(\rho) = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix} \quad \varphi(r) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

5) There is no nontrivial homomorphism $\varphi: S_3 \to C_3$

6) $\varphi: \mathbb{R}$ (over addition) $\longrightarrow \mathbb{R}^{>0}$ (over multiplication)
$x \longmapsto e^x$

is an isomorphism since $x+y \longmapsto e^{x+y} = e^x e^y$ and $\psi: \mathbb{R}^{>0} \longrightarrow \mathbb{R}$, $x \longmapsto \log x$ is an inverse homomorphism

$\log(xy) = \log(x) + \log(y)$

7) $\det: GL_n(\mathbb{R}) \to \mathbb{R}^{\times} = \mathbb{R} \setminus 0$ is a homomorphism since $\det(AB) = \det(A)\det(B)$

8) $f: G \to G$, $g \mapsto g^2$ is a homomorphism <=> $G$ is abelian

Proposition: If $\varphi: G \to G'$, $\psi: G' \to G''$ are homomorphisms, then $\psi \circ \varphi: G \to G''$ is also a homomorphism

Definition: A homomorphism $\varphi: G \to G$ is called an endomorphism. If $\varphi$ is also an isomorphism, call it an automorphism

Use automorphisms in studying the structure of a group. You can have groups of the same size that have different automorphisms

Example: If $G$ is abelian, squaring is an endomorphism

Proposition: The set of automorphisms of a group $G$, denoted $\mathrm{Aut}(G)$ forms a group under function composition

↳ Proof: $\mathrm{Aut}(G)$ contains isomorphisms (bijections) from $G$ to itself. The composition of two homomorphisms is a homomorphism. Similarly, the composition of two automorphisms is an automorphism. Since an isomorphism is bijective, the inverse of an automorphism is an automorphism ▨

Definition: The bijections from a set to itself form a group, denoted $S_G$

Example: Let $g \in G$ and define $C_g: G \longrightarrow G$, $a \longmapsto gag^{-1}$ (called conjugation by g)

↳ Claim: $C_g$ is an automorphism

↳ Proof: $gag^{-1} = gbg^{-1} \Rightarrow ga = gb \Rightarrow a = b$ thus $C_g$ is injective
let $b \in G$, then $C_g(g^{-1}bg) = b$ so $C_g$ is surjective. Thus $C_g$ is bijective.
$C_g(ab) = gabg^{-1}$, $C_g(a)C_g(b) = gag^{-1}gbg^{-1} = gabg^{-1}$. Thus $C_g$ is a homomorphism and hence an automorphism ▨

Definition: An automorphism of the form $\varphi(g)=h^{-1}gh$, where $h\in G$ is fixed, is called an inner automorphism

Example: $C_g$ is an inner automorphism

Example: $G=S_3$, $h=(12)$, $h^{-1}=(12)$
$h(1)h^{-1}=1 \ \forall h$
$(12)(12)(12)=(12)$ $(12)(23)(12)=(13)$ $(12)(132)(12)=(123)$
$(12)(13)(12)=(23)$ $(12)(123)(12)=(132)$

The inner automorphisms of an abelian group map an element to itself

Definition: A subset $H\subseteq G$, where $G$ is a group, is a subgroup, denoted $H\leq G$, if $(H, \bullet|_{H\times H}, e)$ is itself a group

↳ i.e. it is a subset that is itself a group with respect to the same binary operation and identity as $G$

The Subgroup Test: $H\subseteq G$ is a subgroup if and only if
i) $H\neq\emptyset$
ii) $\forall a,b\in H$, $a\cdot b\in H$
iii) $\forall a\in H$, $a^{-1}\in H$
$\Big\}$ i.e. $\forall a,b\in H$ $a\cdot b^{-1}\in H$

↳ If $G$ is finite, you only need the first two

Example: $\forall G$, $\{1\}\leq G$ is a subgroup denoted $1$ (or $0$ if $G$ is additive).
↳ $1$ is called the trivial subgroup
Similarly, $G\leq G$
↳ These are the only two subsets that are subgroups $\forall G$. Further, there are groups in which these are the only subgroups

Definition: If $H\leq G$ and $H\subsetneq G$ (i.e. $H$ is a proper subset of $G$) then $H$ is a proper subgroup
↳ Typically you would ask for any non-trivial proper subgroups

Examples:
1) $\mathrm{Aut}(G)\leq S_G$
2) The inner automorphisms of a group is denoted $\mathrm{Inn}(G)$
↳ Claim: $\mathrm{Inn}(G)\leq \mathrm{Aut}(G)$
Proof:
i) $\forall g\in G$, $C_g\in \mathrm{Inn}(G)$
ii) let $C_g, C_h\in \mathrm{Inn}(G)$, then $C_g\circ C_h=C_{gh}$ since $g(hah^{-1})g^{-1}=(gh)a(gh)^{-1}$
iii) if $C_g\in \mathrm{Inn}(G)$ then $C_g^{-1}=C_{g^{-1}}\in \mathrm{Inn}(G)$ ▨
3) $\mathbb{Z}\leq\mathbb{R}$ as additive groups
4) $SL_n(\mathbb{R})\leq GL_n(\mathbb{R})$
↳ Definition: $SL_n(\mathbb{R})=\{\text{real } n\times n \text{ matrices } m : \det(m)=1\}$
Proof:
i) $\det(I)=1 \in SL_n(\mathbb{R})$
ii) let $A,B\in SL_n(\mathbb{R})$, then $\det(AB)=\det(A)\det(B)=1$
iii) let $A\in SL_n(\mathbb{R})$ then $\det(A^{-1})=(\det A)^{-1}=1$ ▨

We can also get subgroups from homomorphisms. There are two important subgroups: the image of a homomorphism and the kernel of a homomorphism

Definition: If $\varphi: G \to G'$ is a group homomorphism, the image of $\varphi$ denoted $\text{im}(\varphi) := \{\varphi(g) : g \in G\}$
↳ $\text{im}(\varphi) \leq G'$

Motivation for the kernel: Given a homomorphism $\varphi: G \to G'$, you get an equivalence relation on the domain, $G$. For $a, b \in G$, define $a \sim b$ if $\varphi(a) = \varphi(b)$. Denote the set of equivalence classes by $G/\sim = \{[a] : a \in G\}$ where $[a] = \{b \in G : b \sim a\}$. Then $\varphi$ induces a bijection

$$\begin{aligned} \bar{\varphi}: G/\sim &\xrightarrow{\sim} \text{im}(\varphi) \\ [a] &\longmapsto \varphi(a) \end{aligned}$$

(bijective from the definition of equivalence classes). The right hand side, $\text{im}(\varphi)$, is a group so the bijection induces a group structure on the left hand side, $G/\sim$.

Another description of $\sim$:
claim: $\exists$ a subgroup $K \leq G$ such that $a \sim b$ if and only if $aK = bK$ (where $aK = \{ak : k \in K\}$) if and only if $a^{-1}b \in K$. In particular, $[a] = aK$. $aK = bK \Rightarrow \forall k \in K, ak = bk'$ for $k' \in K \Rightarrow kk'^{-1} = a^{-1}b$

Definition: The kernel of $\varphi$, denoted $\ker(\varphi)$, is the above $K$. i.e. $[1] = 1K = K = \varphi^{-1}(1)$

Proposition: $\ker(\varphi) \leq G$
↳ $\ker(\varphi) = \varphi^{-1}(\{e\})$

More generally, if $H' \leq G'$ then $\varphi^{-1}(H') \leq G$ (the converse is not true)

Definition: $[a] = aK$ is called a (left) coset of $K$ and $G/\sim$ is denoted $G/K$

More generally, if $H \leq G$, define $a \sim b$ if and only if $a^{-1}b \in H$ if and only if $aH = bH$.
↳ The equivalence classes are called left cosets and the set of them is denoted $G/H$

Question: For which $H \leq G$ does $(aH) \cdot (bH) = (a \cdot b)H$ and $e = 1H$ make $G/H$ into a group?
Abstract answer: $G/H$ is a group if and only if $H$ is the kernel of some homomorphism $\varphi$
↳ proof:
($\Leftarrow$) done previously
($\Rightarrow$) if $G/H$ is a group, define $\begin{aligned} \varphi: G &\longrightarrow G/H \\ a &\longmapsto aH \end{aligned}$. This is by definition a homomorphism. $\ker(\varphi) = H$ ▨

concrete answer: when $H$ is normal

Definition: $H \leq G$ is called a normal subgroup, denoted, $H \trianglelefteq G$, if $\forall g \in H$ $gHg^{-1} \subseteq H$ (equivalently $gHg^{-1} = H$) where $gHg^{-1} = \{ghg^{-1} : h \in H\}$

Theorem: $H$ is a kernel if and only if $H \trianglelefteq G$
↳ proof: (exercise)
↳ you have to show that the multiplication is well-defined i.e. consider whether $aH = a'H$ and $bH = b'H$ means $abH = a'b'H$ making $aH \cdot bH = abH$ is well-defined

Definition: The index of $H$ in $G$ is $[G:H] = \# G/H$ i.e. the number of left cosets of $H$

Example: $G = S_3$, $H = \{1, (13)\}$. Is $H \trianglelefteq G$?
$(12)(13)(12)^{-1} = (23) \notin H \Rightarrow H$ is not normal. Similarly any $H = \{1, (ij)\}$ is not normal. There is only one non-trivial proper subgroup of $S_3$. That is, $N = \{1, (123), (132)\}$

The first isomorphism theorem: If $\varphi: G \to G'$ is a homomorphism then $\varphi$ induces an isomorphism $\bar{\varphi}: G/\ker(\varphi) \xrightarrow{\sim} \text{im}(\varphi)$

Example: what is $GL_n(\mathbb{R})/SL_n(\mathbb{R})$?

Define $\varphi: GL_n(\mathbb{R}) \longrightarrow G'$ such that $\ker(\varphi) = SL_n(\mathbb{R})$, then you can identify the quotient with the $\operatorname{im}(\varphi)$.

Use det: $GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ (i.e. the determinant) then $\ker\varphi = SL_n(\mathbb{R})$ so $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \operatorname{im}(\det) = \mathbb{R}^\times$

since if $r \in \mathbb{R}^\times$ then $\det\left(\begin{pmatrix} r & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}\right) = r$

Example: Is there a non-trivial homomorphism from $S_3 \longrightarrow C_3$?

since the only non-trivial proper normal subgroup of $S_3$ is $N = \{1, (123), (132)\}$, we need $\ker(\varphi) = N$

what is $G/N$? is it $C_3$?

$C_3$ has no proper non-trivial subgroups but $G/N$ only has two elements so it cannot be $C_3$.

## September 1, 2017

### Group Actions

Definition: Let $G$ be a group and $X$ be a set. A (left) action of $G$ on $X$ is a function
$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \bullet x \end{aligned}$$

where $g \bullet x$ is "g acting on x" satisfying:

i) $1 \bullet x = x \quad \forall x \in X$

ii) $\forall g_1, g_2 \in G$ and $\forall x \in X$, $g_1 \bullet (g_2 \bullet x) = (g_1 \cdot g_2) \bullet x$

The set $X$ is called a G-set. We say $G$ acts on $X$, denoted $G \circlearrowright X$

Examples:

1) $G = S_n$, $X = \{1, 2, \ldots, n\}$, then $\sigma \bullet x = \sigma(x)$

2) $G = D_n$, $X =$ regular n-gon

Remark: For $g \in G \circlearrowright X$, the map $\sigma_g : \begin{aligned} X &\to X \\ x &\mapsto g \bullet x \end{aligned}$ is in $S_X$ (the group of bijections from $X$ to itself)

↳ Proof:

Claim: $(\sigma_g)^{-1} = \sigma_{g^{-1}}$

↳ Proof: $(\sigma_g \circ \sigma_{g^{-1}})(x) = g \bullet (g^{-1} \bullet x) = (g \cdot g^{-1}) \bullet x = 1 \bullet x = x$. Similarly, $(\sigma_{g^{-1}} \circ \sigma_g)(x) = x$ ▨

The data of a group action $G \times X \longrightarrow X$ is the same as giving a homomorphism $\varphi: \begin{aligned} G &\longrightarrow S_X \\ g &\longmapsto \sigma_g \end{aligned}$

Definition: If $G$ is a group and $X$ is a set, a homomorphism $G \longrightarrow S_X$ is called a permutation representation of $G$

↳ It gives a concrete representation of $G$

Example: $D_n \longrightarrow S_n$ by labelling the vertices

Cayley's Theorem: Every group is a permutation group

↳ Proof: $G \circlearrowright G$ by left multiplication with $g \cdot h = gh$. This gives a map $G \longrightarrow S_G$ and multiplication by $G$ is a bijection ▨

Definition: An action $G \circlearrowright X$ is called faithful if $G \longrightarrow S_X$ is injective. We say that the map $G \longrightarrow S_X$ is a faithful representation of $G$. The kernel of the action is $\ker(G \circlearrowright X) = \ker(G \rightarrow S_X)$

↳ Since the kernel of a homomorphism is trivial if and only if the map is injective, the action $G \circlearrowright X$ is faithful if the kernel is trivial

Examples:

1) Cayley's Theorem gives us that $G \circlearrowright G$ by left multiplication is faithful

2) $D_n \to S_n$, $n \geq 3$ is faithful where $D_n$ is acting on the $n$ vertices of the regular $n$-gon.

↳ on assignment we saw this is not true for $n=2$

3) $G=S_3$, $X=\{1,2,3\}$. If $g=(12) \in G$, $(12)\cdot 3 = 3$ but $(12)\cdot 1 = 2 \neq 1$ so $G \circlearrowright X$ is faithful

Definition: $g \in G$ acts trivially on $x \in X$ if $g \cdot x = x$. Similarly $G$ acts trivially on $X$ if $g \cdot x = x$ $\forall g \in G$ $\forall x \in X$

Example: $G=S_3$, $X=\{1,2,3\}$. $(12)$ acts trivially on $3$

Faithful means the only element that acts trivially on every $x \in X$ is $1 \in G$

Definition: If $G \circlearrowright X$, $x \in X$. The stabilizer of $x$ (in $G$) is $\text{Stab}_G(x)=\{g \in G : g\cdot x = x\}$ i.e. the $g \in G$ that acts trivially on $x$ (also denoted $G_x$). The orbit of $x$ (under $G$) is $Gx = \{g \cdot x : g \in G\}$ (also denoted $\text{Orb}_G(x)$)

Example: $G = S_3 \circlearrowright \{1,2,3\}$

| | |
|---|---|
| $\text{Stab}_{S_3}(3)=\{1,(12)\}$ | $\text{Orb}_{S_3}(3)=\{1,2,3\}=X$ |
| $\text{Stab}_{S_3}(2)=\{1,(13)\}$ | $\text{Orb}_{S_3}(2)=X$ |
| $\text{Stab}_{S_3}(1)=\{1,(23)\}$ | $\text{Orb}_{S_3}(1)=X$ |

↳ This shows that elements can have stabilizers but still have the action be faithful

Proposition: $\text{Ker}(G \circlearrowright X) = \bigcap_{x \in X} \text{Stab}_G(x)$

Proposition:

i) $\forall x \in X$, $\text{Stab}_G(x) \leq G$ (and $\text{Orb}_G(x)$ is a $G$-set)

↳ In fact, $\text{Orb}_G(x)$ is the smallest set containing $x$ on which $G$ acts

ii) The orbits of the action partition $X$

↳ Thus any two orbits that share an element are equal

iii) If $Gx = Gx'$ then $\text{Stab}_G(x)$ and $\text{Stab}_G(x')$ are conjugate (i.e. $\exists g \in G$ such that $g\,\text{Stab}_G(x)\,g^{-1} = \text{Stab}_G(x')$)

↳ Since conjugation is a bijection, this means they're isomorphic

↳ Proof:

i) $\forall x$, $1 \in \text{Stab}_G(x)$ so $\text{Stab}_G(x) \neq \emptyset$. If $g, g' \in \text{Stab}_G(x) \Rightarrow (gg')\cdot x = g\cdot(g'\cdot x) = g \cdot x = x \Rightarrow gg' \in \text{Stab}_G(x)$ so $\text{Stab}_G(x)$ is closed under multiplication. If $g \in \text{Stab}_G(x)$, then $g \cdot x = x$ and $g^{-1}(g\cdot x) = g^{-1}x \Rightarrow$ $(g^{-1}g)\cdot x = g^{-1}\cdot x \Rightarrow x = g^{-1}\cdot x$ so $g^{-1} \in \text{Stab}_G(x)$

ii) To show the equivalence classes are an equivalence relation. Define $x \sim x'$ if $\exists g \in G$ such that $x' = g\cdot x$. Our claim is that this is an equivalence relation and the equivalence classes are the orbits. Since the equivalence classes of any equivalence relation partition the set.

reflexive: $x = 1\cdot x$ so $x \sim x$

Symmetric: If $x' = g\cdot x$ then $g^{-1}\cdot x' = x$ so $x' \sim x$ if and only if $x \sim x'$

transitive: If $x' = g\cdot x$ and $x'' = h \cdot x'$ then $x'' = hg\cdot x$ so $x \sim x'$, $x' \sim x'' \Rightarrow x \sim x''$ and $[x] = \{x' \in X : x' \sim x\} = \{g\cdot x : g \in G\} = Gx$

iii) If $x' = g\cdot x$ and $h \in \text{Stab}_G(x)$ then $h \cdot x = x$ so $x = g^{-1}\cdot x$ and $hg^{-1}\cdot x' = g^{-1}\cdot x' \Rightarrow ghg^{-1}\cdot x' = x'$ so $h \in \text{Stab}_G(x)$ if and only if $ghg^{-1} \in \text{Stab}_G(x')$ ▨

Example: We saw for $S_3 \circlearrowright \{1,2,3\}$ there is one orbit so the stabilizers are all conjugate (i.e. isomorphic)

Orbit-Stabilizer Theorem: If $G \circlearrowright X$ and $x \in X$, then $\#G = \#\mathrm{Stab}_G(x) \cdot \#Gx$

↳ Proof 1 (Pictoral Proof): Start with an orbit of $x$ and $\gamma_i \in \mathrm{Stab}_G(x)$

$$\begin{array}{llll} x = 1\cdot x \longrightarrow \bullet & g_1\cdot x \longrightarrow \bullet & g_2\cdot x \rightarrow \bullet & \cdots \\ x = \gamma_1\cdot x \longrightarrow \bullet & g_1\gamma_1 g_1^{-1} \longrightarrow \bullet & \bullet & \\ x = \gamma_2\cdot x \longrightarrow \bullet & g_1\gamma_2 g_1^{-1} \longrightarrow \bullet & \bullet & \\ x = \gamma_3\cdot x \longrightarrow \bullet & g_1\gamma_3 g_1^{-1} \longrightarrow \bullet & \bullet & \cdots \end{array}$$

Since the stabilizers of each point are conjugate to the stabilizers of $x$

this rectangle has all the elements of $G$. The number of row elements is the size of the orbit and the column is the size of the stabilizer

↳ Proof 2: let $x' \in Gx$ and $G_{x,x'} = \{g \in G : g\cdot x = x'\}$ (so $G_{x,x} = G_x$) then $G = \bigsqcup_{x' \in Gx} G_{x,x'}$

(Every element in $G$ brings $x$ to some element in the orbit and this is the only element so they are disjoint) $\Rightarrow \#G = \sum_{x' \in Gx} \#G_{x,x'}$ so if we show $\forall x'$, $\#G_{x,x'} = \#\mathrm{Stab}_G(x)$ then we're done.

Claim: Given $g' \in G_{x,x'}$, the other elements are $g'\gamma$ as $\gamma$ runs over $\mathrm{Stab}_G(x)$

↳ Proof: (to show there is a bijection

Define $f: \mathrm{Stab}_G(x) \longrightarrow G_{x,x'}$ where $g'$ is fixed
$\gamma \longmapsto g'\gamma$

The function $G_{x,x'} \longrightarrow \mathrm{Stab}_G(x)$ is an inverse of $f$ ▨
$h' \longmapsto (g')^{-1}h'$

Application: Lagrange's Theorem: If $H \leq G$ then $\#G = \#H \cdot [G:H]$ i.e. the size of a subgroup divides the size of the group

↳ Proof: let $H \leq G$, $X = G/H$ then $G \circlearrowright X$ by $g\cdot(g'H) = (gg')H$.
$\mathrm{Stab}_G(1\cdot H) = \{g \in G : gH = H\} = H$ and $\mathrm{Orb}_G(1\cdot H) = G/H$ Since $gH = g\cdot(1\cdot H)$ $\forall g \Rightarrow \#G = \#H \, \# G/H$ ▨

**September 3, 2015**

Theorem: If $G \circlearrowright X$ then $\forall x \in X$ there is a natural bijection $f: G/\mathrm{Stab}_G(x) \longrightarrow \mathrm{Orb}_G(x)$ (For instance if $G$ is finite then $\#\mathrm{Orb}_G(x) = \#G/\#\mathrm{Stab}_G(x)$ i.e. the Orbit-Stabilizer Theorem)

↳ Proof: let $H = \mathrm{Stab}_G(x)$ and define $f(gH) = g\cdot x$

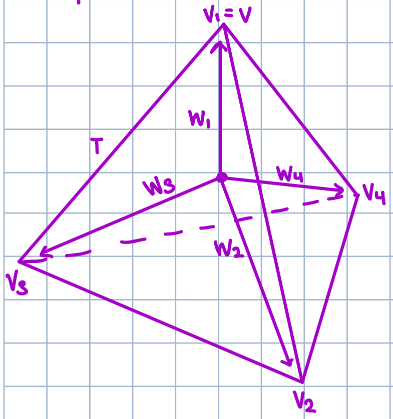
well-defined: If $gH = g'H$ then $gh = g'h'$ for some $h, h' \in H$
$\Rightarrow gh(h')^{-1} = g'$ i.e. If $gH = g'H$, then $g' = gh''$ for $h'' \in H$. Check that $f(g'H) = f(gH)$
$f(g'H) = g'\cdot x = gh''\cdot x = g\cdot x$ since $h \in \mathrm{Stab}_G(x) \Rightarrow f(g'H) = f(gH)$

Surjective: $\forall x' \in \mathrm{Orb}_G(x)$, $\exists g \in G$ such that $x' = g\cdot x$ by definition so $f(gH) = x'$

injective: If $f(gH) = f(g'H)$ wts $gH = g'H$
$g\cdot x = g'\cdot x \Rightarrow x = g^{-1}g'\cdot x \Rightarrow g^{-1}g' \in \mathrm{Stab}_G(x) = H \Rightarrow g^{-1}g' = h$ for some $h \in H \Rightarrow g' = gh \Rightarrow g'H = gH$ ▨

Remark: This bijection has an extra property. Note that $G \circlearrowright G/H$ (Lagrange) and here $G \circlearrowright X$. Looking at how the map is defined, $\forall \gamma \in G$ and $\forall gH \in G/H$, $\gamma \cdot f(gH) = f(\gamma \cdot gH)$ since $\gamma\cdot(g\cdot x) = (\gamma \cdot g)\cdot x$. Since the bijection is compatible with the action. $G/H$ and $X$ are the same as $G$-sets.

Example: Tetrahedron (4 equilateral triangles)



Let $\mathbb{T}$ (The Tetrahedral Group) be the group of rotational symmetries of the tetrahedron i.e. $\mathbb{T} = \{g \in SO_3(\mathbb{R}) : g(T) = T\}$ where $SO_3(\mathbb{R})$ is the Special orthogonal group of $3 \times 3$ matrices i.e. $gg^T = I$ and $\det(g) = 1$ i.e. the rotations fixing the origin, 0, in $\mathbb{R}^3$

Question: What is $\mathbb{T}$?

Let $G = \mathbb{T}$, $X = \{\text{vertices}\}$. Let $v$ be the top vertex. $Stab_{\mathbb{T}}(v) = \{1, \rho, \rho^2, \ldots\}$ where $\rho$ is rotation clockwise by $120°$ so $\#Stab_{\mathbb{T}}(v) \geq 3$.

$Orb_{\mathbb{T}}(v) = X \Rightarrow \#Orb_{\mathbb{T}}(v) = 4$. Thus by the orbit-stabilizer theorem, $\#\mathbb{T} \geq 3 \cdot 4 = 12$

Since we labelled the vertices we have a map $\varphi : \mathbb{T} \to S_4$ (the action map)

Question: Is the action faithful i.e. is $\varphi$ injective?

let $g \in \mathbb{T}$ such that $g \cdot v_i = v_i$ i.e. $g \in Ker(\varphi)$. Is $g = I$?

Think of the vertices as position vectors instead of points. Let the position vector of $v_i$ be $w_i$ then $g \cdot v_i = v_i \Rightarrow g \cdot w_i = w_i$. Any three of these vectors form a basis of $\mathbb{R}^3$ i.e. $w_1, w_2, w_3$ form a basis $\Rightarrow g = I$ since if you have a linear map that does nothing to a basis, it must be the identity

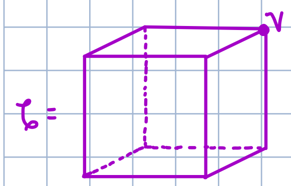
$\Rightarrow \mathbb{T} \hookrightarrow S_4$, $\#S_4 = 4! = 24$, and $\#\mathbb{T} \geq 12$. By Lagrange's Theorem, $\#\mathbb{T} = 12$ or $24$

Question: Does there exist an element in $S_4$ not in $\mathbb{T}$?

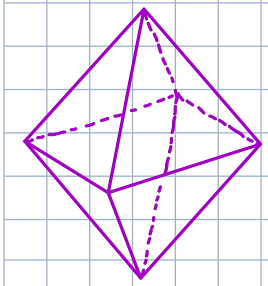
Yes $(12) \notin \mathbb{T}$ (first day). You would have to flip $(34) \Rightarrow \#\mathbb{T} = 12$. Since $A_n$ is the only index two subgroup of $S_n \Rightarrow \mathbb{T} \cong A_4$

Note: If you can take a group and map it into $S_n$, you can know a lot about it

Example: cube



The symmetry group of the cube is denoted $\mathbb{O}$ and is called the octahedral group since the octahedron is dual to the cube. The notion of duality comes from the idea that an object comes from three sets of objects: vertices (0 dimensional), edges (1 dimensional), and faces (2 dimensional). If you switch the roles of the vertices and faces of the cube, you get an octahedron (The dual of a tetrahedron is itself)



$\mathbb{O} = \{g \in SO_3(\mathbb{R}) : g(\mathcal{C}) = \mathcal{C}\}$

$Stab_{\mathbb{O}}(v) = \{1, \rho, \rho^2, \ldots\}$, $\rho =$ rotation by $120°$

$\mathbb{O} \circlearrowright$ vertices: $Orb_{\mathbb{O}}(v) = V = \{\text{vertices}\} \Rightarrow \#\mathbb{O} \geq 3 \cdot 8 = 24$

Theres nothing special about vertices. You could also use the faces (easier way to see the stabilizer) to get $4 \cdot 6 = 24$, or edges to get $2 \cdot 12 = 24$

eight vertices $\Rightarrow V : \mathbb{O} \to S_8$

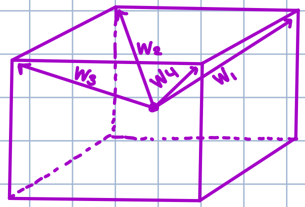
six faces $\Rightarrow F : \mathbb{O} \to S_6$

twelve edges $\Rightarrow E : \mathbb{O} \to S_{12}$

would be easier to study faces since there are less of them but there's an even smaller set to study

You could act on the pairs of opposite faces (3 of them) but this would give a map to $S_3$ and $\#\mathbb{O} \geq 24$, $\#S_3 = 6$ which wouldn't help much.

Instead, consider $X = \{\text{pairs of opposite vertices}\}$, $\#X = 4$ so $\varphi : \mathbb{O} \to S_4$ thus if $\varphi$ is injective, then $\mathbb{O} \cong S_4$.



Then $X=\{\{w_i,-w_i\}\}$

If $g\cdot\{w_i,-w_i\}=\{w_j,-w_i\}$ $\forall i=1,2,3,4$ then is $g=I$?
consider $w_1,w_2,w_3$. If $\exists\, i=1,2,3$ s.t. $g\cdot w_i=w_i$ then WLOG $g\cdot w_2=-w_2$ so

$$g=\begin{pmatrix}\pm1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & \pm1\end{pmatrix}$$

By definition $\det g=1 \Rightarrow$ WLOG $g\cdot w_1=w_1$, $g\cdot w_3=-w_3$
Now look at $w_1,w_3,w_4$ to get $\det g=1\Rightarrow g\cdot w_4=-w_4$ but looking at $w_2,w_3,w_4$, $\det g=-1\neq1 \rightarrow\leftarrow$
so $g\cdot w_i=w_i$ $\forall i \Rightarrow g=I \Rightarrow \theta\cong S_4$

## Class Equations

Let $G$ be a group and $X=G$, then $G\curvearrowright G$ by $g\cdot a=gag^{-1}$ (left action)

Definition: A right action of $G$ on $X$, denoted $X\curvearrowleft G$ is a function $X\times G\longrightarrow X$, $(x,g)\longmapsto x^g$ satisfying:

i) $x^1=x$ $\forall x\in X$
ii) $(x^g)^h=x^{gh}$ $\forall x\in X$, $\forall g,h\in G$

Thus $G\curvearrowleft G$ by $a^g:=g^{-1}ag$ since $(a)^{gh}=(gh)^{-1}a(gh)=h^{-1}g^{-1}agh=(g^{-1}ag)^h=(a^g)^h$
↳ note: If you have a group and you see this exponent notation, it means conjugation

Definition: An orbit of the above action is called conjugacy class i.e. the conjugacy class of $a$ is $\{g^{-1}ag : g\in G\}$
↳ conjugacy class of 1 is 1
↳ the conjugacy class of $z\in Z(G)$ is $\{z\}$
↳ note: the conjugacy class of $a$ contains $1^{-1}a1=\{a\}$
↳ can never contain everything (1 is in its own class)

Definition: The stabilizer of the action, $\mathrm{Stab}_G(a)=\{g\in G: g^{-1}ag=a\}=\{g\in G: ag=ga\}$ is the centralizer.
The kernel is $\{g\in G: g^{-1}ag=a\ \forall a\in G\}=\{g\in G: ag=ga\ \forall a\in G\}=Z(G)\leftarrow$ the center (notation used previously)

If $X=G=\bigsqcup$ orbits, note: $\#\mathrm{orb}_G(g)=1$ iff $g\in Z(G)$

Theorem (Class Equation): If $G$ is a finite group and $g_1,\dots,g_r\in G$ be a set of representatives of the conjugacy classes that arent in $Z(G)$, then $\#G=\#Z(G)+\sum_{i=1}^{r}[G:C_G(g_i)]$

↳ note: $\#Z(G)$ and $[G:C_G(g_i)]$ divide $\#G$
↳ Proof: $\#G=\sum\#$orbits. If $\#\mathrm{orb}_G(g)=1 \Rightarrow g\in Z(G)$ so collect the orbits of size one. Otherwise, $\#\mathrm{orb}_G(g)=\dfrac{\#G}{\#\mathrm{Stab}_G(g_i)}$ but $\mathrm{Stab}_G(g_i)=C_G(g_i)$ and $\dfrac{\#G}{\#H}=[G:H]$ by definition so $[G:C_G(g_i)]=\#\mathrm{Orb}_G(g_i)$ ▨

# September 8, 2015

Example: Symmetries of the icosahedron

let $I$=icosahedron group=rotational symmetries in $\mathbb{R}^3$ of the icosahedron= rotational symmetries of the dodecahedron= rotational symmetries of the dodecahedron (since they are dual)

The dodecahedron consists of 12 faces that are regular 5-gons, 30 edges, and 20 vertices.

Icosahedron is 20 equilateral triangles (note: this example is covered in section 6.2 of Artin's algebra)

Question: For which $n$ do we have a helpful map $I \longrightarrow S_n$?

Trick: There are five cubes inscribed inside a dodecahedron and $I$ permutes the cubes giving a map $\varphi: I \longrightarrow S_5$.

Question: what is $\# I$?

We can use the orbit-stabilizer theorem

Act on the 12 faces: the stabilizer of a face is 5 rotations and the orbit is all 12 faces $\Rightarrow \# I = 5 \cdot 12 = 60$.

If we show the map is injective the it's $A_5$. We do this by showing that $\{1\}$ and $I$ are the only normal subgroups of $I$, thus any map from $I$ to another group is either injective or the trivial map.

↳ (Theorem: The class equation of $I$ is $60 = 1+15+20+12+12$)

↳ Claim: There are no proper nontrivial subgroups

↳ proof: A normal subgroup is a union of conjugacy classes and contains $\{1\}$. Thus if $N \trianglelefteq I$ then $\# N = 1 + (\text{sum of numbers from } \{15, 20, 12, 12\})$ s.t. $\# N \mid 60$. This is impossible unless $\# N = 1, 60$ ▨

Therefore $\ker(\varphi) = 1, I$. However, any nontrivial rotation of a face gives a nontrivial permutation of the cubes $\Rightarrow \ker\varphi \neq I$. Thus $\ker\varphi = 1 \Rightarrow I \hookrightarrow S_5$ and $\varphi(I)$ has index $2 \Rightarrow \varphi: I \xrightarrow{\sim} A_5$

↳ In fact, $\forall A_n, n \geq 5$, there are no nontrivial proper normal subgroups

class equation: You can partition elements by their order. $\forall \sigma \in G$, $\# \sigma = \# \sigma^g$ $\forall g \in G$

Proof of Previous Theorem: Break up $I$ into elements of a given order:

order 1: $\{1\}$

order 2: Let $e$ be an edge. The stabilizer of an edge consists of the identity and the element that rotates around the center of the edge.

opposite edges have the same stabilizer so we have $30/2=15$ elements of order 2.

order 3: let $v$ be a vertex. For each vertex there are two nontrivial elements and again opposite vertices have the same stabilizer so we get $20\cdot 2/2=20$ elements of order 3

order 5: let $f$ be a face. we've said the stabilizer has order 5 and opposite faces have the same stabilizer so $12\cdot 4/2=24$ elements

Question: Are there others?

No, since $60=1+15+20+24$

Claim: All elements of order 2 are conjugate

↳ proof: The edges form an orbit so the stabilizer of any two elements, $\text{stab}(e)$ and $\text{stab}(e')$, are conjugate. Since 1 is conjugate to $1 \Rightarrow \text{stab}(e)=\{1,\rho_e\}$ and $\text{stab}(e')=\{1,\rho_{e'}\}$, then $\rho_e$ is conjugate to $\rho_{e'}$ ✓

Claim: All elements of order 3 are conjugate

↳ proof: Again, $\text{stab}(v)$ and $\text{stab}(v')$ are conjugate.
Let $\text{stab}(v)=\{1,\rho_v,\rho_{v^{-1}}\}$ and $\text{stab}(v')=\{1,\rho_{v'},\rho_{v'^{-1}}\}$ where $\rho_v$ is a clockwise rotation and so is $\rho_{v'}$. If $\bar{v}$ is the opposite vertex then $\text{stab}(\bar{v})=\text{stab}(v)$ and $\rho_{\bar{v}}=\rho_{v^{-1}}$, $\rho_v=\rho_{\bar{v}^{-1}}$. Also $\rho_v$ is conjugate to $\rho_{\bar{v}}$ by the rotation bringing $v$ to $\bar{v}$ ✓

Now for any two faces, $f$ and $f'$, $\text{stab}(f)=\text{stab}(f')$ but the elements break up into two con'v acies.

Consider two opposite faces, $f$ and $\bar{f}$, then $\rho_f=\rho_{\bar{f}^{-1}}$ and $\rho_f$ is conjugate to $\rho_{\bar{f}}$ for the same reason as with vertices. Thus $\#[\rho_f]\geq 12$ and if $\rho_f$ is conjugate to $\rho_{f^2}$ ($\rho_f\sim\rho_{f^2}$) then $\#[\rho_f]=24$ but $\#[\rho_f]\mid 60$ so $\rho_f\nsim\rho_{f^2}$, thus 24 breaks up into $24=12+12$ ▨

Definition: A group $G$ is called simple if $G\neq\{1\}$ and its only normal subgroups are $\{1\}$ and itself.

Examples:

1) If $p$ is prime, $C_p$ is simple since the only divisors are $p$ and 1. Further, if $G$ is a finite abelian simple group, then $G\cong C_p$
2) $I\cong A_5$ is the smallest non-abelian simple group
3) The next smallest has order 162. It is $GL_3(\mathbb{F}_2)=PSL_2(\mathbb{F}_7)$
4) $A_n$ for $n\geq 3$ and $n\neq 4$ is simple

Jordan-Holder Theorem: Every finite group has an "essentially unique composition series" i.e. $\forall G\ \exists$ a sequence $1=N_0\trianglelefteq N_1\trianglelefteq N_2\trianglelefteq\ldots\trianglelefteq N_k=G$ s.t. $\forall i$, $N_i/N_{i-1}$ is simple. This is called a composition series. Further for any other composition series, $1=M_0\trianglelefteq M_1\trianglelefteq M_2\trianglelefteq\ldots\trianglelefteq M_\ell=G$, $\ell=k$ and the collection $(M_i/M_{i-1})_i$ is the same up to isomorphism as $(N_i/N_{i-1})_i$. The $N_i/N_{i-1}$'s are called Jordan-Holder constituents

Examples:

1) $1 \underset{C_3}{\trianglelefteq} \langle (1\,2\,3) \rangle \underset{C_2}{\trianglelefteq} S_3$ so the constituents are $C_3$ and $C_2$.

$\langle (1\,2\,3) \rangle$ is the only normal subgroup so this is the only composition series

2) $\mathbb{Z}/6\mathbb{Z}$ has more than one option:

$0 \underset{C_3}{\trianglelefteq} \langle 2 \rangle \underset{C_2}{\trianglelefteq} C_6 = \mathbb{Z}/6\mathbb{Z}$

$0 \underset{C_2}{\trianglelefteq} \langle 3 \rangle \underset{C_3}{\trianglelefteq} C_6 = \mathbb{Z}/6\mathbb{Z}$

3) $1 \trianglelefteq A_5$ since $A_5$ is simple

4) $1 \trianglelefteq A_5 \trianglelefteq S_3$.

In fact, for $n \geq 5$ we have $1 \trianglelefteq A_n \trianglelefteq S_n$

5) $1 \underset{C_2}{\trianglelefteq} \langle r^2 \rangle \underset{C_2}{\trianglelefteq} \langle r \rangle \underset{C_2}{\trianglelefteq} D_4$

$1 \underset{C_2}{\trianglelefteq} \langle s \rangle \underset{C_2}{\trianglelefteq} \langle s, r^2 \rangle \trianglelefteq D_4$

Definition: A group is solvable if its Jordan-Holder constituents are all cyclic

Example: $D_4, S_3, C_6$ are solvable

## September 10, 2015

### Fixed Points of P Groups

Definition: Let $G$ be a group. If $G \circlearrowright X$, a fixed point is $x \in X$ such that $g \cdot x = x$ $\forall g \in G$. The set of fixed points is denoted $X^G$.

Definition: Fix a prime $p$. A finite group $G$ is called a $p$-group if $\#G = p^r$.

Example: $G = C_2$ $(p=2)$, $C_2 = \{1, \sigma\}$. Let $G \circlearrowright X$, $X$ finite.
Question: What are the possible orbit sizes?
Any orbit is $\{x, \sigma \cdot x\}$ so the orbit is either size 1 or 2.
Either $x = \sigma \cdot x \Rightarrow x \in X^G$ or $x \neq \sigma \cdot x \Rightarrow \#Gx = 2$ so $\#X = \#X^G \pmod 2$.
Therefore, if $\#X$ is odd there is necessarily a fixed point.
↳ Fixed points are elements with orbit size 1

Fixed Point Theorem: Let $p$ be prime, $G$ be a $p$-group, and $G \circlearrowright X$ where $X$ is finite. Then $\#X^G \equiv \#X \pmod p$

↳ Proof: $X$ is a disjoint union of the orbits and $\#Gx = [G : \mathrm{stab}_G(x)] \mid \#G = p^r$. Therefore

$$\#Gx = \begin{cases} 1 & , \text{ if } x \in X^G \\ \text{divisible by } p & , \text{ if } x \notin X^G \end{cases}$$

so $\#X = \underset{\substack{\downarrow \\ \text{union of singleton orbits}}}{\#X^G} + p(\ldots) \leftarrow$ nonsingleton orbits ▨

Corollary: If $G$ is a $p$-group and $G \circlearrowright X$, with $X$ finite and $p \nmid \#X$, then there is always a fixed point.

Theorem: If $G$ is a p-group, then $Z(G) \neq \{1\}$

↳ Proof: Let $X = G \setminus \{1\}$ and $X \circlearrowleft G$ by conjugation.

↳ This is valid since if $G$ acts on a set you can remove an entire orbit and $G$ will still act on the set.

$p \nmid \#X = p^r - 1$. Thus ∃ a fixed point $z \in X^G$, i.e. $\exists z \in G, z \neq 1$ s.t. $g^{-1}zg = z \ \forall g \in G \Rightarrow zg = gz$ $\Rightarrow z \in Z(G)$ and $z \neq 1$ ▨

Lagrange's Theorem: If $H \leq G$, $G$ a group, then $\#H \mid \#G$

Question: Is there a converse? i.e. If $d \mid \#G$, does $\exists H \leq G$ such that $\#H = d$?
No.

Example: $G = A_4$. $\#A_4 = 12$ but $\nexists H \leq A_4$ s.t. $\#H = 6$

Cauchy's Theorem: If $p$ is a prime and $p \mid \#G$, then $\exists g \in G$ s.t. $\#g = p$

↳ This is a partial converse to Lagrange

↳ Proof: Let $C_p \curvearrowright X$ where $X = \{(g_1, g_2, \dots, g_p) \in G^p : g_1 g_2 \cdots g_p = 1\} \setminus \{\overbrace{(1,1,\dots,1)}^{p \text{ times}}\}$ and let $C_p = \langle \sigma \rangle$ with $\sigma \bullet (g_1, \dots, g_p) = (g_p, g_1, g_2, \dots, g_{p-1})$ i.e. a right cyclic shift. To show this is an action we need to show $g_p g_1 g_2 \cdots g_{p-1} = 1$ as the group may not be abelian.
Note that $g_p g_1 g_2 \cdots g_{p-1} = g_p (g_1 g_2 \cdots g_p) g_p^{-1} = g_p (1) g_p^{-1} = 1$. Thus this is an action.
Further, $\#X = \#G^{p-1} - 1$ because we can pick $g_1, \dots, g_{p-1}$ freely from $G^{p-1}$ but then $g_p = (g_1, \dots, g_{p-1})^{-1}$.
Since $p \mid \#G$, $p \nmid \#X$ so ∃ a fixed point $x \in X^{C_p}$. Thus $x = (g_1, g_2, \dots, g_p) = \sigma \cdot x = (g_p, g_1, g_2, \dots, g_{p-1})$
Therefore $x$ is of the form $(\underbrace{g_1, g_1, \dots, g_1}_{p \text{ times}})$. Also the product is 1 so $g_1 \neq 1$, $g_1^p = 1 \Rightarrow \#g_1 = p$ ▨

Theorem: A group of order $p^2$ is isomorphic to $C_{p^2}$ or $C_p \times C_p$.

↳ Therefore it is necessarily abelian

↳ Proof: $Z(G) \neq \{1\}$ so $\#Z(G) = p$ or $p^2$.
If $\#Z(G) = p^2$ then $G = Z(G) \Rightarrow G$ is abelian.
Otherwise $Z(G) \trianglelefteq G$ and $\#G/Z(G) = \#G / \#Z(G) = p^2/p = p \Rightarrow G/Z(G)$ is cyclic $\Rightarrow G$ is abelian.
If $\exists g \in G$ s.t. $\#g = p^2$ then $G = \langle g \rangle \cong C_{p^2}$. Otherwise $\forall g \neq 1, \#g = p$.
Let $g_1 \neq 1$ and $H_1 = \langle g_1 \rangle = \langle g_1^i \rangle$ $i = 1, \dots, p-1$. Let $g_2 \in G \setminus H_1$, $H_2 = \langle g_2 \rangle = \langle g_2^j \rangle$ $j = 1, \dots, p-1$ so $g_1^i \neq g_2^j$ for $1 \leq i, j \leq p-1 \Rightarrow H_1 \cap H_2 = \{1\}$ so $H_1 H_2 = \{g_1^i g_2^j\} = G$ $0 \leq i, j \leq p-1$ with

$$\#H_1 H_2 = \frac{\#H_1 \, \#H_2}{\#H_1 \cap \# H_2} = p^2$$

The function $\varphi: G \longrightarrow H_1 \times H_2$, $g_1^i g_2^j \longmapsto (g_1^i, g_2^j)$ $(0 \leq i, j \leq p-1)$ is well-defined and a bijection.

Also $\varphi(g_1^i g_2^j g_1^{i'} g_2^{j'}) = \varphi(g_1^i g_1^{i'} g_2^j g_2^{j'}) = (g_1^{i+i'}, g_2^{j+j'}) = \varphi(g_1^i g_2^j) \varphi(g_1^{i'} g_2^{j'})$
$\Rightarrow \varphi$ is a homomorphism and $H_1 \times H_2 \cong C_p \times C_p \Rightarrow G \cong C_p \times C_p$ ▨

## Sylow Theorems

Theorem: If $p$ is prime and $p^j \mid \#G$ then $\exists H \leq G$ s.t. $\#H = p^j$

↳ This is a partial converse to Lagrange. Cayley's Theorem is $j = 1$.

↳ Proof: By induction ▨

Definition: Let $G$ be finite and $p$ be prime. A p-subgroup of $G$ is $H \leq G$ s.t. $\#H = p^j$ for $j \geq 1$.
If $p^r \| \#G$ (i.e. $\#G = p^r m$, $p \nmid m$) then a subgroup of order $p^r$ is called a Sylow p-subgroup.
The set of Sylow p-subgroups of $G$ is denoted $\mathrm{Syl}_p(G)$. Further $n_p(G) := \#\mathrm{Syl}_p(G)$ (sometimes just denoted $n_p$)

Sylow Theorems: Let $\#G = p^r m$, $p \nmid m$

(I) $n_p(G) \geq 1$. In fact $\forall j$ s.t. $0 \leq j \leq r$, $\exists H \leq G$ s.t. $\#H = p^j$

↳ Proof: To show: If $H \leq G$, $\#H = p^i$, $i<r$ then $\exists H'$, $H \leq H' \leq G$ with $[H':H]=p$ i.e. $\#H' = p^{i+1}$

Let $H \circlearrowright G/H$ by $h \bullet gH = hgH$. (Note: $h \bullet (1H) = 1H$)

$\#X = [G:H]$ and $i<r \Rightarrow p \mid [G:H]$

$x \in X^H$ means $x = gH$ s.t. $hgH = gH$ $\forall h \in H$ iff $hg \in gH$ $\forall h$ iff $g^{-1}hg \in H$ $\forall h$ iff $g^{-1}Hg = H$ iff $g \in N_G(H)$

so $X^H = N_G(H)/H \subseteq G/H$.

$\# N_G(H)/H = \# X^H \equiv \# X = [G:H] \pmod p \Rightarrow p \mid [N_G(H):H]$

Note: $H \trianglelefteq N_G(H)$ so $N_G(H)/H$ is a group with $p \mid \# N_G(H)/H$ so by Cauchy's Theorem $\exists \overline{H}' \leq N_G(H)/H$ s.t. $\#\overline{H}' = p$. Let $H'$ be the inverse image of $\overline{H'}$ in $N_G(H)$ then $[H':H]=p$ and $H' \leq G$. Induction ▨

(II) All sylow p-subgroups are conjugate. In fact $\forall P \in Syl_p(G)$ and $\forall Q \leq G$ s.t. $\#Q = p^j$, $\exists g \in G$ s.t. $Q \leq gPg^{-1}$

↳ Proof: Let $P, Q \in Syl_p(G)$, $P \neq Q$ and let $Q \circlearrowright G/P$ by $q \bullet (gP) = (qg)P$. $p \nmid \# G/P$ so $\exists$ $g \in G$ s.t. $qgP = gP$ $\forall q \in Q \Rightarrow qg \in gP$ $\forall q \in Q \Rightarrow q \in gPg^{-1}$ $\forall q \in Q \Rightarrow Q \leq gPg^{-1}$ and since conjugation is a bijection so $\#Q \mid \# gPg^{-1} \Rightarrow Q = gPg^{-1}$ ▨

(III) $n_p \equiv 1 \pmod p$. In fact, $n_p = [G:N_G(P)]$ for any $P \in Syl_p(G)$ and $n_p \mid m$.

## September 15, 2015

Proof of Sylow Theorem (III): Let $P \in Syl_p(G)$ and $Syl_p(G) \circlearrowleft P$ by conjugation. By the fixed point theorem, $n_p = \# Syl_p(G) \equiv \# Syl_p(G)^P \pmod p$

Claim: $Syl_p(G)^P = \{P\}$

↳ Proof: $Q \in Syl_p(G)^P$ iff $g^{-1}Qg = Q$ $\forall g \in P$ iff $P \leq N_G(Q)$ iff $P$ is a Sylow p-subgroup of $N_G(Q)$

Since $\# N_G(Q) \mid p^r m$, $\#Q = p^r$ and $N_G(Q) \trianglerighteq Q$ but $Q$ is also a Sylow p-subgroup of $N_G(Q)$ so $\exists g_0 \in N_G(Q)$ s.t. $g_0^{-1} Q g_0 = P \Rightarrow Q = P$ ✓

$\Rightarrow n_p \equiv 1 \pmod p$

Now consider $Syl_p(G) \circlearrowleft G$ by conjugation with one orbit. $Stab_G(S) = N_G(S)$ $\forall S \leq G$ so by the Orbit-Stabilizer Theorem $n_p = \# Syl_p(G) = \# Orb_G(P) = [G : Stab_G(P)] = [G : N_G(P)]$

$\Rightarrow n_p \mid m$ since $\#G = p^r m$ and since $P \leq N_G(P)$, $\# N_G(P) = p^r m'$ so

$$n_p = \frac{\#G}{\# N_G(P)} = \frac{m}{m'} \text{ so } m' n_p = m \text{ ▨}$$

Theorem: If $p, q$ are primes, $p<q$, $q \not\equiv 1 \pmod p$ then every group of size $p^2 q$ is abelian (so if $\#G = p^2 q$ then $G \cong C_{p^2} \times C_q \cong C_{p^2 q}$ or $G \cong C_p \times C_p \times C_q \cong C_p \times C_{pq}$)

↳ Proof: $n_p \equiv 1 \pmod p$ and $n_p \mid q \Rightarrow n_p = 1$ since $q$ is prime and $q \not\equiv 1 \pmod p$

Claim: $n_q = 1$

↳ Proof: $n_q \equiv 1 \pmod q$ and $n_q \mid p^2$ so $n_q = 1, p, p^2$. $n_q \neq p$ since $p<q$ so $p \not\equiv 1 \pmod q$. If $n_q = p^2$ then $p^2 \equiv 1 \pmod q \Rightarrow q \mid p^2 - 1 = (p-1)(p+1) \Rightarrow q \mid p-1$ or $q \mid p+1$. $q \nmid p-1$ since $q>p$ and $p-1<p$ so $q \mid p+1$ but $q>p \Rightarrow q = p+1 \Rightarrow q \equiv 1 \pmod p$ which is a contradiction ✓

By Assignment 3, if $n_p = 1$ and $n_q = 1$, $P \in Syl_p(G)$, $Q \in Syl_q(G)$ then $\forall g \in P$, $h \in Q$, $gh = hg$.

$\#P = p^2 \Rightarrow P \cong C_{p^2}$ or $C_p \times C_p$ and $\#Q = p$ so $Q \cong C_p$ and $PQ = G$ since $\#P \#Q = \#G$ and $P \cap G = 1$ ▨

# Semidirect Products

Motivating Example: Let $R$ be a field (or a commutative ring with 1) and let $V$ be an $n$-dimensional $R$-vector so $V \cong R^n$, then $GL(V) \cong GL_n(R)$ where $GL(V) = \{T : V \longrightarrow V : T \text{ is linear and invertible}\}$ (so $n \times n$ invertible matrices).

An affine linear transformation of $V$ is $f : V \longrightarrow V$ s.t. $f(v) = Av + b$ where $A \in M_{n,n}(R)$, $b \in V$.

If $f(v) = Av + b$, $g(v) = A'v + b'$, $(f \circ g)(v) = A(A'v + b') + b = (AA')v + (b + Ab')$ so $f$ is invertible iff $A$ is invertible.

$Aff_n(R)$ = the group of invertible affine linear transformations $= \{f : V \longrightarrow V : A \in GL_n(R)\}$ where the operation is function composition and $f(v) = v$ is the identity.

As a set, $Aff_n(R) = GL_n(R) \times V = \{(A,b) : A \in GL_n(R), b \in V\}$ but the group $GL_n(R) \times V$ has operation $(A,b) \cdot (A',b') = (AA', b+b') \neq (AA', b + Ab')$ so the group is not the direct product of the groups. Also $V = \{I\} \times V \subseteq Aff_n(R)$, $V \trianglelefteq Aff_n(R)$ so $(A,b^{-1})(I,b')(A,b) = (A^{-1}A, \ldots) = (I, \ldots) \subseteq V$ but $GL_n(R) = GL_n(R) \times \{0\} \subseteq Aff_n(R) \ntrianglelefteq Aff_n(R)$ since $(A,b)^{-1}(A',0)(A,b) = (A,b)^{-1}(A'A, A'b) = (A^{-1}A'A, \ldots)$ but in $H_1 \times H_2$ both $H_1, H_2 \trianglelefteq H_1 \times H_2$

↳ we use what is called a semi-direct product to generalize the direct product to get $Aff_n(R) = V \rtimes GL_n(R)$

Theorem: Let $N$ and $K$ be two groups and $K \circlearrowright N$ (i.e. we have a homomorphism $\varphi : K \longrightarrow Aut(N)$) Let $G = N \times K$ as a set and define $(n_1, k_1) \cdot (n_2, k_2) = (n_1(k_1 \cdot n_2), k_1k_2)$. This defines a group structure on $G = N \times K$ denoted $N \rtimes K$ (or $N \rtimes_\varphi K$) called the semidirect product of $N$ and $K$ with respect to $\varphi$.

Furthermore $\#G = \#K \cdot \#N$. Identifying $K$ and $K \times 1 \subseteq G$, and $N$ and $1 \times N \subseteq G$ we have that $K, N \subseteq G$, $N \trianglelefteq G$, and $N \cap K = 1$. Lastly $k \bullet n = knk^{-1}$, $n \in N$

↳ If the action is the trivial action, then this is just the cross product

Example: Let $N$ be abelian and $K = C_2 = \langle \sigma \rangle$. Define $\varphi : K \longrightarrow Aut(N)$, $\sigma \longmapsto (n \longmapsto n^{-1})$ (if a group is abelian then inversion is an automorphism)

If $N = C_m = \langle r \rangle$ then $C_m \rtimes C_2$ has size $2m$, an element $(\sigma, 1)$ s.t. $(\sigma, 1)^2 = 1$, an element $(1, r)$ s.t. $(1,r)^m = 1$, and $\sigma r \sigma^{-1} = \sigma \cdot r = r^{-1}$ so $C_m \rtimes C_2 \cong D_m$

Definition: Let $N, K \leq G$. $G$ is the internal direct product of $N$ and $K$ if

i) $G = KN$ $(K \cap N = 1)$

ii) The map $KN \longrightarrow K \times N$ is an isomorphism

Definition: Let $N, K \leq G$. $G$ is an internal semidirect product if

i) $G = KN$ $(K \cap N = 1)$

ii) The map $KN \longrightarrow N \rtimes_\varphi K$ is an isomorphism where $\varphi(k)(n) = knk^{-1}$

Theorem: If $G$ is a group and $N, K \leq G$, then $KN \cong K \times N$ iff

i) $K, N \trianglelefteq G$

ii) $K \cap N = 1$

$G$ is the internal direct product iff we also have

iii) $\#K \#N = \#G$

Example: Let $n = 2m$, $m$ odd (i.e. $n \equiv 2 \pmod 4$) and consider $D_n$. $\#D_n = 2n = 4m$. Let $N = \langle s, r^2 \rangle$ ($s$ reflection, $r$ rotation) and $K = \langle r^m \rangle = \{1, r^m\}$. $N \trianglelefteq D_n$ since $[D_n : N] = 2$ and $K \trianglelefteq D_n$ since $K = Z(D_n)$. $N \cap K = 1$ since $m$ is odd. $N \cong D_{n/2}$ so $\#N \#K = n \cdot 2 = 2n = \#D_n$ so $D_n \cong N \times K \cong D_{n/2} \times C_2$

Theorem: If $N, K \leq G$, then $KN \cong N \rtimes K$ iff

i) $K \trianglelefteq G$

ii) $N \cap K = 1$

$G \cong N \rtimes K$ iff we also have

iii) $\#K \#N = \#G$

Example: $\text{Aff}_n(\mathbb{R}) = \mathbb{R}^n \rtimes GL_n(\mathbb{R})$

Definition: If $H \leq G$, then $K \leq G$ is called the complement of $H$ in $G$ if $G = HK$ and $H \cap K = 1$

↳ So $G$ is a nontrivial semi-direct product iff $\exists$ a proper nontrivial subgroup that has a complement

Example: $G = C_4 = \langle \gamma \rangle$. The only subgroups of $G$ are $\{1\}, \langle \gamma^2 \rangle, C_4$. $\langle \gamma^2 \rangle$ has no complement so $C_4$ is not a (nontrivial) semidirect product.

## September 17, 2015

Theorem: There are 5 groups of order 12 (up to isomorphism):

- $C_4 \times C_3 \cong C_{12}$
- $C_2 \times C_2 \times C_3 \cong C_2 \times C_6$
- $A_4$
- $D_6$
- $C_3 \rtimes C_4$ (if $\sigma \in C_4, \gamma \in C_3, \sigma \bullet \gamma = \gamma^2$)

↳ Proof: Let $K$ be a Sylow 2-subgroup and $N$ be a Sylow 3-subgroup.

$n_2 \equiv 1 \pmod 2$ and $n_2 \mid 3 \Rightarrow n_2 = 1$ or $3$; $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 4 \Rightarrow n_3 = 1$ or $4$

$\#K = 4 \Rightarrow K \cong C_4$ or $C_2 \times C_2$. $\#N = 3 \Rightarrow N \cong C_3$

Claim 1: One of $N$ or $K$ is normal

↳ If $N \not\trianglelefteq G$ then $n_3 = 4$, $N_1 = N, N_2, N_3, N_4$ since they are order 3 there are no nontrivial proper subgroups so $N_i \cap N_j = 1, i \neq j \Rightarrow \# \bigcup_{i=1}^{4} N_i = 1 + 4 \cdot 2 = 9$. There are 3 elements left. $K$ has order 4 so $K \cap N_i = 1$ so these 3 elements are $K \setminus \{1\} \Rightarrow n_2 = 1 \Rightarrow K \trianglelefteq G$ ✓

Case 1: $N, K \trianglelefteq G \Rightarrow G$ is abelian $\Rightarrow G \cong K \times N$ since $K \cap N = 1$, $\#K \#N = \#G$, $N, K \trianglelefteq G$

Case 2: $K \trianglelefteq G$, $N \not\trianglelefteq G$ so $n_3 \neq 1$ thus $n_3 = 4$. Let $\text{Syl}_3(G) \circlearrowleft G$ by conjugation. We get $\varphi: G \longrightarrow S_4$. If we show that $\varphi$ is injective we get $G \cong A_4$ since $\#G = 12$ and $G$ maps isomorphically into $S_4$.

$\ker \varphi = \bigcap_{i=1}^{4} \text{Stab}_G(N_i)$; $\#\text{Stab}_G(N_i) \#\text{Orb}_G(N_i) = \#G$; $\#G = 12, \#\text{Orb}_G(N_i) = 4 \Rightarrow \#\text{Stab}_G(N_i) = 3$

Since we are acting by conjugation, $\text{Stab}_G(N_i) = N_g(N_i) \geq N_i$. $\#N_i = 3 = \#N_g(N_i)$

$\Rightarrow \text{Stab}_G(N_i) = N_i \Rightarrow \ker \varphi = \bigcap_{i=1}^{4} N_i = \{1\} \Rightarrow \varphi$ is injective $\Rightarrow G \cong A_4$

Case 3: $N \trianglelefteq G$, $K \not\trianglelefteq G$.

Let $N \circlearrowleft K$ by conjugation i.e. $k \bullet n = knk^{-1}$. Note that $knk^{-1} \neq n$ since that would mean $kn = nk \Rightarrow G$ is abelian which is a contradiction. So the action is nontrivial.

Case a: $K \cong C_2 \times C_2$

$\text{Aut}(C_3) = \{id, \psi\}$ where $C_3 = \langle \gamma \rangle = \langle \gamma^2 \rangle$ and $\psi(\gamma) = \gamma^2 = \gamma^{-1}$.

Since the action is nontrivial, we have $\varphi: K \longrightarrow \text{Aut}(N)$ and $\exists\, k_0 \in K$ s.t. $\varphi(k_0) = \psi$ i.e. $k_0 n k_0^{-1} = n^{-1}$. Also $\exists\, k_1 \in K$ s.t. $\varphi(k_1) = 1$, $k_1 \neq 1$ (if $\varphi(k) = \psi, k \neq k_0 \Rightarrow \varphi(k k_0) = \psi^2 = id \Rightarrow k_1 = k k_0$)

(note: we could stop and say $G \cong N \rtimes K$ but we continue to show its $D_6$)

Let $x = k_1 n$, $\#x = \ell cm(\#k_1, \#n) = 6$. $k_0 x k_0^{-1} = k_0 k_1 n k_0^{-1} = k_1 k_0 n k_0^{-1} = k_1 n^{-1} = n^{-1} k_1$ (since $\varphi(k_1) = 1 \Rightarrow k_1 n k_1^{-1} = n \Rightarrow k_1 n = n k_1$ $\forall n \in N$) $= n^{-1} k_1^{-1}$ (since $k_1 = k_1^{-1}$) $= (k_1 n)^{-1}$.

Let $y = k_0$ then $x, y \in G$, $x^6 = 1$, $y^2 = 1$, $yxy^{-1} = x^{-1} \Rightarrow D_6 \twoheadrightarrow G$ and since $\#D_6 = \#G \Rightarrow D_6 \cong G$

Case b: $K\cong C_4$

Let $K=\langle x\rangle, N=\langle y\rangle$. We know $xy\neq yx$ since $G$ is not abelian
$\Rightarrow xyx^{-1}=y^{-1} \Rightarrow G=N\rtimes_{\varphi}N$, where $\varphi: x^i\mapsto \psi^i \Rightarrow G\cong C_3\rtimes C_4$, called the **dicyclic group of of order 12.**

## G-Sets

Definition: Let $X$ be a (left) G-set. A subset $Y\subseteq X$ is called **G-stable** (or **G-invariant**) if $G\cdot Y\subseteq Y$ (i.e $\forall g\in G, \forall y\in Y, g\cdot y\in Y$). A **G-subset** of $X$ is $Y\subseteq X$ that is a G-set under the same action

Theorem: A subset $Y\subseteq X$ is a G-subset if and only if $Y$ is G-stable. ("closure under action")

Definition: Let $X,Y$ be two G-sets. A function $f: X\longrightarrow Y$ is called a **morphism of G-sets** (or a **G-map** or a **G-equivariant map**) if $\forall g\in G$ $\forall x\in X$, $f(g\cdot x)=g\cdot f(x)$

Definition: The set of G-maps $X\longrightarrow Y$ is denoted **$Map_G(X,Y)$**. $f\in Map_G(X,Y)$ is called an **isomorphism of G-sets** if $\exists\,\tilde{f}\in Map_G(X,Y)$ such that $f\circ\tilde{f}=id_Y$ and $\tilde{f}\circ f=id_X$

Theorem: $f\in Map_G(X,Y)$ is an isomorphism if and only if $f$ is a bijection.

Construction: If $I$ is a set and $X_i$ is a G-set $\forall i\in I$, then $X=\bigsqcup_{i\in I}X_i$ is a G-set

↳ Note: If $f_i: X_i\longrightarrow X_i'$ is an isomorphism $\forall i\in I$ then $f: X\longrightarrow X'=\bigsqcup_{i\in I}X_i'$ is an isomorphism where

$f(x)=f_i(x_i)$ if $x=x_i\in X_i$

Proposition: Let $X$ be a G-set
i) $Y\subseteq X$ is a G-subset if and only if $Y$ is a union of orbits
ii) $\forall x\in X$, $Orb_G(x)\cong G/Stab_G(x)$ as G-sets
↳ Proof of (ii): Let $H=Stab_G(x)$ and define $f: G/H\longrightarrow Orb_G(x)$, $gH\longmapsto g\cdot x$. We showed (on 9/03) that $f$ is a well-defined bijection.
Let $g,\gamma\in G$. $f(\gamma\cdot(gH))=f(\gamma gH)=(\gamma g)\cdot x=\gamma\cdot(g\cdot x)=\gamma\cdot f(gH)$
$\Rightarrow f$ is G-equivariant. ▨

Definition: A G-set, $X$, is called **transitive** if there is only one orbit
↳ If $X$ is transitive then it is $G/H$ for some $H$

Structure Theorem for G-sets: If $X$ is a G-set then $\exists$ a set $I$ and $H_i\leq G$ $\forall i\in I$ such that $X\cong\bigsqcup_{i\in I}G/H_i$

↳ Proof: Let $I=\{Orb_G(x): x\in X\}$ and let $x_i\in i$ ($i=Orb_G(x_i)$) $\forall i\in I$, then $X=\bigsqcup_{i\in I}Orb_G(x_i)$.

Let $H_i=Stab_G(x_i)$ then $f_i: G/H_i\xrightarrow{\sim}Orb_G(x_i)$ which gives $f:\bigsqcup_{i\in I}G/H_i\xrightarrow{\sim}\bigsqcup_{i\in I}Orb_G(x_i)=X$ ▨

Construction: Let $X,Y$ be G-sets and $Map(X,Y)=\{f: X\longrightarrow Y : f \text{ is a function}\}$. Define $G\curvearrowright Map(X,Y)$ by $(g\cdot f)(x)=g\cdot(f(g^{-1}\cdot x))$ ("$g\cdot f=gfg^{-1}$"). This makes $Map(X,Y)$ a G-set!
↳ Proof: $1\cdot f=f$, $(g\cdot(h\cdot f))(x)=g\cdot(h\cdot f)(g^{-1}\cdot x)=g\cdot(h\cdot f(h^{-1}\cdot(g^{-1}\cdot x)))=gh\cdot f((gh)^{-1}\cdot x)=((gh)\cdot f)(x)$ ▨

Proposition: $Map_G(X,Y)=Map(X,Y)^G$ ← fixed points

# September 22, 2015

## Ring Theory

Definition: A ring is a set $R$ with two binary operations $+$ and $\cdot$, and elements $0,1 \in R$ (maybe $0=1$) satisfying:

i) $(R,+,0)$ is an abelian group:

a) $+$ is associative: $a+(b+c)=(a+b)+c$

b) $0$ is the identity

c) $\exists$ additive inverses

d) $+$ is commutative

ii) If $1 \neq 0$, $(R \setminus \{0\}, \cdot, 1)$ is a monoid, i.e. a group that may not have inverses:

a) $\cdot$ is associative: $a\cdot(b\cdot c)=(a\cdot b)\cdot c$

b) $1$ is an identity: $1\cdot a = a = a\cdot 1$

iii) Distributivity: $a\cdot(b+c)=a\cdot b+a\cdot c$
$(a+b)\cdot c = a\cdot c + b\cdot c$

$R$ is called commutative if $\cdot$ is commutative i.e. $a\cdot b = b\cdot a$ $\forall a,b$

Example: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}[x]$, $\mathbb{C}[x,y]$, $M_n(\mathbb{R})$, $\mathbb{H}$ (the quaternion ring/algebra) are all rings

Definition: An algebra satisfies (i) and (iii)
↳ Dummit and Foote's ring is our "associative algebra" (or a "rng" i.e. a ring without identity)

Remark: Some people require $1 \neq 0$. Allowing $1=0$ implies the existence of only one extra ring: the zero ring denoted $0=\{0\}$

Examples: The following are algebras:

- Octonions (have 1 but not associative)
- Lie algebras e.g. $M_n(\mathbb{R})$ with usual addition but the product is denoted $[A,B]=AB-BA$. Not associative and no identity 1
- Jordan algebras
- Composition algebras

Definition: A non-zero ring $R$ such that $\forall\, 0 \neq a \in R$, $a^{-1}$ exists ($a^{-1}a = 1 = aa^{-1}$) is called a division ring (or a skew fied). A commutative division ring is called a field.

Definition: A commutative non-zero ring satisfying the cancellation property, i.e. $\forall a,b,c \in R$, $a \neq 0$: $a\cdot b = a\cdot c \Rightarrow b=c$, is called an integral domain.

Example: $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain since $2\cdot 3 = 2\cdot 0$ but $0 \neq 3$

Examples:

1) $\mathbb{Z}$ is an integral domain but not a field ($2a \geq 2$ or $2a \leq -2$ or $2a=0$, no inverses)

2) $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are fields

3) $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring. If $n$ is composite, $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain

4) $\mathbb{Z}/p\mathbb{Z}$ is a field for $p$, prime

5) Hamilton's Quaternions, $\mathbb{H}$ is not commutative.

$\mathbb{H} = \{a+bi+cj+dk : a,b,c,d \in \mathbb{R}\}$

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

The norm is $N(q)=a^2+b^2+c^2+d^2$, $\bar{q}=a-bi-cj-dk \Rightarrow N(q)=q\bar{q}=\bar{q}q$

↳ Note: $N(q)=0$ if and only if $q=0$ so if $q \neq 0$, $q^{-1} = \bar{q}/N(q) \Rightarrow \mathbb{H}$ is a division ring

6) If $d \in \mathbb{Z}$ and $d$ is not a square, then $\mathbb{Q}(\sqrt{d})$ is a field, it is called the quadratic field.
$\mathbb{Q}(\sqrt{d}) = \{a+b\sqrt{d} : a,b \in \mathbb{Q}\}$. If $\alpha = a+b\sqrt{d}$, $\bar{\alpha} = a-b\sqrt{d}$, $N(\alpha)=\alpha\bar{\alpha}=a^2-bd$.

↳ Note: $N(\alpha)=0$ if and only if $\alpha=0$ so for $\alpha \neq 0$, $\alpha^{-1} = \bar{\alpha}/N(\alpha)$

7) Let $A$ be a ring. $R=M_n(A)$ is a ring where if $M \in R$,
$$M = \begin{pmatrix} a_{11} & a_{12} \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots\cdots & a_{nn} \end{pmatrix},\ a_{ij} \in A$$

If $M, M' \in R$, $M+M' = (a_{ij}+a'_{ij})$

$$0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix},\quad 1 = I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & \cdots & 1 \end{pmatrix}$$

$M \cdot M' = (c_{ij})$ where $c_{ij} = \sum_{k=1}^{n} a_{ik} a'_{kj}$

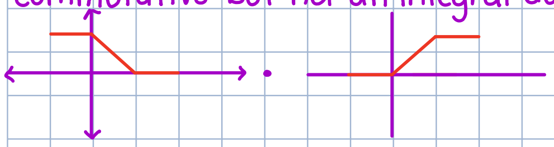
↳ This is not necessarily commutative or a division ring

8) Let $A$ be a commutative ring. Then $A[x]$, i.e. the polynomials over $A$, form a ring
$A[x] = \{P(x)=a_0+a_1x+\ldots+a_nx^n : a_i \in A, n \in \mathbb{Z}_{\geq 0}\} = \{P(x)=\sum_{i\geq 0} a_i x^i : a_i \in A, a_i \neq 0$ for all but finitely many $i\}$

If $P(x), Q(x) \in A[x]$, $P(x)+Q(x) = \sum_{i \geq 0}(a_i+b_i)x^i$ If $P(x)Q(x) = \sum_{i\geq 0} c_i x^i$ where $c_i = \sum_{k=0}^{i} a_k b_{i-k}$

9) If $X$ is any set and $A$ is any ring, $\mathrm{Map}(X,A)$ is a ring with $(f+g)(x)=f(x)+g(x)$ and $(f \cdot g)(x)=f(x)g(x)$,
$0(x)=0$, $1(x)=1$

↳ e.g. If $X=\mathbb{R}$ (or any topological space) $R=C(X,\mathbb{R})=\{f: X \to \mathbb{R} : f$ is continuous$\}$ is a ring. It is commutative but not an integral domain since for example



$= 0$ but neither is 0.

10. Let $I$ be an indexing set and $R_i$ be rings $\forall i \in I$. Then $\prod_{i\in I} R_i$ is a ring.

$(a_i)_{i\in I} + (b_i)_{i \in I} = (a_i+b_i)_{i\in I}$ $(a_i)(b_i)=(a_ib_i)$, $0=(0,\ldots,0)$, $1=(1,\ldots,1)$

If $\# I = 2$, this is not an integral domain

Definition: $a \neq 0$ is a zero divisor if $\exists\, b \neq 0$ such that $a \cdot b = 0$ or $b \cdot a = 0$

Example: 2 in $\mathbb{Z}/6\mathbb{Z}$ is a zero divisor since $2 \cdot 3 = 0$

Definition: If $R \neq 0$, $a \in R$ is a unit if $a^{-1}$ exists. The set of units is denoted $R^\times$

Proposition: $R^\times$ is a group under multiplication

Proposition: If $R \neq 0$, zero divisors can't be units

Examples:

1) $\mathbb{Z}^{\times} = \{\pm 1\}$

2) $F^{\times} = F \setminus \{0\}$ if $F$ is a field

3) For $n \geq 2$, $(\mathbb{Z}/n\mathbb{Z})^{\times} = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1\}$. The zero divisors are the nonzero, non-units i.e. $a$ such that $\gcd(a,n) > 1$

4) For $C(\mathbb{R},\mathbb{R})$, $f(x) = x$ is not a unit but also not a zero-divisor. It is not a unit since $f(0)=0$. It is not a zero-divisor since $f(x)g(x) = 0 \Rightarrow g(x) = 0$ for $x \neq 0$ but $g$ is continuous so $\lim_{x \to 0} g(x) = g(0) = 0 \Rightarrow g(x) = 0$

Proposition: If $R$ is a commutative ring, then $R$ is an integral domain if and only if $R$ has no zero-divisors.

Proposition: A finite integral domain is a field

↳ Proof: Let $a \in R$, $a \neq 0$ and $\ell_a : \begin{array}{c} R \to R \\ x \mapsto ax \end{array}$. Since $R$ is an integral domain, $\ell_a$ is injective and since $R$ is finite, $\ell_a$ is surjective

$\Rightarrow \exists x \in R$ such that $\ell_a(x) = ax = 1$ ▨

Remark (Wedderburn): A finite division ring is a field.

Definition: Let $R, R'$ be two rings. A function $\varphi : R \to R'$ is a ring homomorphism if:

i) $\varphi$ is a group homomorphism for $(R,+,0) \to (R',+,0)$ i.e. $\varphi(a+b) = \varphi(a) + \varphi(b)$

ii) $\varphi(a \cdot b) = \varphi(a)\varphi(b)$

iii) $\varphi(1) = 1$

↳ The book doesn't require (iii)

$\varphi$ is an isomorphism if $\exists \psi : R' \to R$ homomorphism such that $\varphi \circ \psi = id_{R'}$ and $\psi \circ \varphi = id_R$

## September 24, 2015

Examples:

1) $\mathbb{Z} \to \mathbb{Q}$, $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ are homomorphisms

2) Let $I$ be a set and $R_i$ be rings $\forall i \in I$. Let $R = \prod_{i \in I} R_i$. If $j \in I$ then $\pi_j : \begin{array}{c} R \to R_j \\ (a_i) \mapsto a_j \end{array}$ is a homomorphism

3) $\varphi : \mathbb{H} \hookrightarrow M_2(\mathbb{C})$ with $\varphi(a+bi+cj+dk) = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

is an injective homomorphism.

Definition: A subset $S \subseteq R$ is a subring, denoted $S \leq R$, if $(S, +, \cdot, 0, 1)$ is a ring.

↳ The identity of $S$ needs to be the identity of $R$

Proposition: $S \subseteq R$ is a subring if and only if $\forall a, b \in S$:

i) $a+b \in S$

ii) $-a \in S$

iii) $ab \in S$

iv) $1 \in S$

Examples:

1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \leq \mathbb{H}$

2) If $d \in \mathbb{Z}$ is squarefree then $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} \leq \mathbb{Q}(\sqrt{d})$

e.g. $\mathbb{Z}[i] \leq \mathbb{Q}(i)$ $(d=-1)$. $\mathbb{Z}[i]$ is called the Gaussian integers. If $d=-3$ then $\mathbb{Z}[\sqrt{-3}] \leq \mathbb{Q}(\sqrt{-3})$ but in fact $\omega = \frac{-1 \pm \sqrt{-3}}{2} \notin \mathbb{Z}[\sqrt{-3}]$ but $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\} \leq \mathbb{Q}(\sqrt{-3})$ (note: $\omega^3 = 1$, $\omega = e^{2\pi i/3}$)

$\mathbb{Z}[\omega]$ is called the Eisenstein integers.

$\mathbb{Z}\left[\frac{-1+i}{2}\right] = \left\{a + b\left(\frac{-1+i}{2}\right) : a, b \in \mathbb{Z}\right\}$ is not a subring of $\mathbb{Q}(i)$.

In general, let $\theta = \begin{cases} \sqrt{d} & , D \equiv 2,3 \pmod 4 \\ \frac{1 \pm \sqrt{d}}{2} & , D \equiv 1 \pmod 4 \end{cases}$ then $\mathbb{Z}[\theta] = \{a + b\theta : a, b \in \mathbb{Z}\} \leq \mathbb{Q}(\sqrt{d})$

↳ $\mathbb{Z}[\theta]$ is the maximal ring of this form

3) Let $p$ be prime and $\mathbb{Z}_{(p)} := \left\{\frac{a}{b} \in \mathbb{Q} : \gcd(a,b) = 1, p \nmid b\right\}$ then $\mathbb{Z}_{(p)} \leq \mathbb{Q}$ called the localization of $\mathbb{Z}$ at $p$

4) Let $R = C(\mathbb{R}, \mathbb{R})$. Fix $N > 0$ and let $S_N = \{f \in C(\mathbb{R}, \mathbb{R}) : f(x) = 0 \text{ for } |x| > N\}$. It can be shown that if $f, g \in S_N$ then $f + g \in S_N$, $fg \in S_N$, $0 \in S_N$ and if $1_N(x) = \begin{cases} 1 & , |x| \leq N \\ 0 & , |x| > N \end{cases}$ then $1_N \cdot f = f = f \cdot 1_N$ $\forall f \in S_N$

thus $S_N$ is a ring with identity $1_N$ but $1_N \neq 1 \in R$ $(1 \notin S_N)$ so $S_N$ is not a subring of $R$.

Definition: The image of a homomorphism $\varphi : R \longrightarrow R'$ is $\mathrm{im}(\varphi) = \{\varphi(r) : r \in R\}$

Proposition: $\mathrm{im}(\varphi) \leq R'$

Definition: The kernel of a homomorphism $\varphi : R \rightarrow R'$ is $\ker\varphi = \{r \in R : \varphi(r) = 0\} = \varphi^{-1}(0)$

↳ $\ker(\varphi) \trianglelefteq (R, +, 0)$ (as a subgroup)

Question: Is $\ker(\varphi) \leq R$?

Answer: No unless $R' = 0$ since $\varphi(1) = 1 \neq 0$ if $R' \neq 0$ so $1 \notin \ker(\varphi)$

Let $R/\ker\varphi$ = left cosets of $\ker\varphi = \{a + I : a \in R\}$ where $I = \ker\varphi$. This is an abelian group with $(a+I) + (b+I) = (a+b) + I$

Question: is $R/I$ a ring with $(a+I) \cdot (b+I) = (a \cdot b) + I$ ?

Answer: yes since $\bar{\varphi} : R/I \longrightarrow \mathrm{im}\varphi$, $a + I \longmapsto \varphi(a)$ is a bijection so the structure on the left is the corresponding ring structure on the right. Conversely, when is an additive subgroup $I \leq R$ such that $R/I$ is a ring with $(a+I) \cdot (b+I) = ab + I$ and $1 = 1 + I$ ?

Abstract Characterization: If and only if $I = \ker\varphi$ for some ring homomorphism $\varphi : R \longrightarrow R'$

↳ $\varphi : R \longrightarrow R/I$, $\ker\varphi = I$

Concrete Characteristic: If and only if $\forall r \in R, \forall a \in I$, $ra$ and $ar \in I$ i.e. "$I$ absorbs products"

Definition: Such an $I \leq R$ as above is called a (two-sided) ideal of $R$, denoted $I \trianglelefteq R$.

Proposition: $I \leq R$ is an ideal if and only if

i) $I \neq \emptyset$

ii) $\forall a, b \in I$, $a - b \in I$

iii) $\forall a \in I, \forall r \in R$, $ar, ra \in I$

Definition: If $I \trianglelefteq R$, then $R/I$ is called the quotient ring of $R$ by $I$

Example: For all rings $R$, $I=\{0\} \trianglelefteq R$ and $R \trianglelefteq R$. $\{0\}$ is called the trivial ideal and $I=R$ is called the unit ideal since if $I \trianglelefteq R$ then $I=R$ if and only if $\exists u \in R^{\times}$ with $u \in I$. $R/\{0\} = R$ and $R/R = 0$.

Definition: An ideal $I \trianglelefteq R$ with $I \subsetneq R$ is a proper ideal.

Examples:
1) If $R$ is commutative, $R$ is a field if and only if $I=\{0\}$ and $I=R$ are the only ideals
2) The ideals of $\mathbb{Z}$ are exactly $n\mathbb{Z}=\{an : a \in \mathbb{Z}\}$, $n \geq 0$

First Isomorphism Theorem: If $\varphi: R \to R'$ is a ring homomorphism then $\varphi$ induces an isomorphism
$$\begin{aligned} \bar{\varphi}: R/\ker\varphi &\xrightarrow{\sim} \operatorname{im}\varphi \\ a+\ker\varphi &\longmapsto \varphi(a) \end{aligned}$$

Examples:
1) Let $R=C(\mathbb{R},\mathbb{R})$ and fix $x_0 \in \mathbb{R}$. Let $I=\{f \in C(\mathbb{R},\mathbb{R}) : f(x_0)=0\}$. Show that $I \trianglelefteq R$ and determine $R/I$.
Define $\begin{aligned} ev_{x_0}: C(\mathbb{R},\mathbb{R}) &\longrightarrow \mathbb{R} \\ f &\longmapsto f(x_0) \end{aligned}$. This is a ring homorphism and $\ker(ev_{x_0}) = I$ so $I \trianglelefteq R$ and by the first isomorphism theorem, $R/I \cong \operatorname{im}(ev_{x_0}) = \mathbb{R}$ since $\forall a \in \mathbb{R}$, $f(x)=a \in C(\mathbb{R},\mathbb{R})$
2) Let $R=C(\mathbb{R},\mathbb{R})$ and $N>0$ then $S_N \trianglelefteq R$
3) $I=C_c(\mathbb{R},\mathbb{R})=\bigcup_{N>0} S_N$, where $C_c(\mathbb{R},\mathbb{R})$ is the set of continuous functions with compact support is an ideal of $R$
4) If $R$ is commutative and $a \in R$, then $(a) := aR = \{ar : r \in R\} \trianglelefteq R$ and is called the principal ideal generated by $a$
5) Let $R=\mathbb{R}[x]$ and $I=(x^2+1)$. What is $R/I$?
Look at $x+I \in R/I$, $(x+I)^2+1+I=(x^2+1)+I=0+I$ so $(x+I)^2=-1$
Define $\begin{aligned} \varphi: \mathbb{R}[x] &\longrightarrow \mathbb{C} \\ f(x) &\longmapsto f(i) \end{aligned}$ then $\ker\varphi = I$ since if $f(x)=(x^2+1)g(x) \in I \Rightarrow f(i)=(i^2+1)g(i)=0$
$\Rightarrow I \subseteq \ker\varphi$ and $\forall g(x) \in \mathbb{R}[x], \exists q(x), r(x) \in \mathbb{R}[x]$ such that $g(x)=q(x)(x^2+1)+r(x)$ where $r(x)=0$ or $\deg(r(x)) < \deg(q(x))$. If $g(i)=0$, then $r(i)=g(i)-q(i)(i^2+1)=0-0=0$.
If $r(x) \neq 0$, then $r(x)=ax+b$ and $a \cdot i+b=0$. $a,b \in \mathbb{R} \Rightarrow i=\frac{-b}{a} \Rightarrow i \in \mathbb{R}$ which is a contradiction.
$\Rightarrow \ker\varphi \subseteq I$.
$\operatorname{Im}\varphi = \mathbb{C}$ since for $a+bi \in \mathbb{C}$, $f(x)=a+bx$ gives $\varphi(f(x))=a+bi$.
Thus by the first isomorphism theorem, $R/I \cong \mathbb{C}$.
6) Let $R=\mathbb{Q}[x]$ and $d$ be a squarefree integer. Then $\mathbb{Q}[x]/(x^2-D) \cong \mathbb{Q}(\sqrt{d})$.

**September 29, 2015**

Proposition: If $\Sigma$ is a non-empty indexing set, $R$ is a ring, and $I_\sigma \trianglelefteq R$ $\forall \sigma \in \Sigma$, then $\bigcap_{\sigma \in \Sigma} I_\sigma \trianglelefteq R$

Definition: For any subset $S \subseteq R$, the ideal generated by $S$ is $(S) := \bigcap_{\substack{I \trianglelefteq R \\ S \subseteq I}} I \trianglelefteq R$.

If $S=\{a_1, a_2, \ldots\}$ then $(S)=(a_1, a_2, \ldots)$

Example: If $R$ is commutative and $S=\{a\}$, then $(S)=(a)=\{ra : r \in R\}$

Proposition: For $R$ commutative and $S \subseteq R$, $(S) = \left\{ \sum_{i=1}^{n} r_i s_i : n \in \mathbb{Z}_{\geq 0}, r_i \in R, s_i \in S \right\}$

For $R$ noncommutative $(S) = \left\{ \sum_{i=1}^{n} r_i s_i r_i' : n \in \mathbb{Z}_{\geq 0}, s_i \in S, r_i, r_i' \in R \right\}$

Examples:

1) For any ring $R$, $(0)=0$ and $(1)=R$
2) Let $R=\mathbb{Z}$, if $a_1, a_2, \dots, a_r \in \mathbb{Z}$ then $(a_1, \dots, a_r) = (\gcd(a_1, \dots, a_r))$

Bezout's Identity: Let $a, b \in \mathbb{Z}$ where $a$ and $b$ are not both zero. Then $\gcd(a,b)$ is the least positive element of the form $au+bv$, $u, v \in \mathbb{Z}$ and all other such elements are the multiples of $\gcd(a,b)$.

↳ Proof: Use the extended Euclidean Algorithm ▨

Example: $(6,8) = \{6u+8v : u,v \in \mathbb{Z}\} = (\gcd(6,8)) = (2)$

Theorem: Every ideal in $\mathbb{Z}$ is principle.

↳ Proof: If $I=0$, then $I=(0)$. Let $I \neq 0$ and let $n$ be the least positive element of $I$.

claim: $I=(n)$

↳ Proof: $n \in I \Rightarrow rn \in I \ \forall n \in \mathbb{Z} \Rightarrow (n) \subseteq I$.

$\forall a \in I, \exists q, r \in \mathbb{Z}$ such that $a = qn+r$ and $0 \leq r \leq n$.

$a \in I, n \in I \Rightarrow qn \in I \Rightarrow a - qn = r \in I$ and since $n$ is mimimal such that $n>0$ and $0 \leq r < n \Rightarrow r = 0$

$\Rightarrow a \in (n) \Rightarrow I \subseteq (n)$ ▨

Definition: An integral domain in which every ideal is principal is called a Principal Ideal Domain (PID)

Definition: An ideal $I \trianglelefteq R$ is called finitely generated if $\exists a_1, \dots, a_n \in R$ such that $I = (a_1, \dots, a_n)$

Example: If $R = \mathbb{C}[x_1, x_2, \dots]$, then $I = (x_1, x_2, \dots)$ is not finitely generated.

Definition: A ring $R$ is Noetherian if every $I \trianglelefteq R$ is finitely generated.

Hilbert Basis Theorem: If $R$ is Noetherian then so is $R[x]$.

Definition: Let $I \trianglelefteq R$, $J \trianglelefteq R$

$I + J = \{a+b : a \in I, b \in J\} = (\{a+b : a \in I, b \in J\}) = (I \cup J) \trianglelefteq R$

$IJ = (\{ab : a \in I, b \in J\}) = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_j \in J, n \in \mathbb{Z}_{\geq 0} \right\} \trianglelefteq R$

Proposition: Let $R$ be a ring. $\forall I, J \trianglelefteq R$, $IJ \subseteq I \cap J$

↳ Proof: If $a \in I$, $b \in J \Rightarrow ab \in I \cap J$ ▨

Example: Let $R=\mathbb{Z}$, $I=(n)$, $J=(m)$

$I+J=\{un+vm : u,v\in\mathbb{Z}\}=(\gcd(m,n))$

$IJ=(\{uvmn : u,v\in\mathbb{Z}\})=\left\{\sum_{i=1}^{k}u_iv_inm\right\}=\left\{nm\sum_{i=1}^{k}u_iv_i\right\}=\{nmu : u\in\mathbb{Z}\}=(mn)$

$I\cap J=\{a\in\mathbb{Z} : m|a,\ n|a\}=(\ell cm(m,n))$

↳ e.g. If $n=12$, $m=18$, $I+J=(6)$, $IJ=(216)$, $I\cap J=(36)$

$IJ=I\cap J$ if and only if $mn=\ell cm(m,n)$ if and only if $\gcd(m,n)=1$ if and only if $I+J=\mathbb{Z}$

Proposition: If $R$ is commutative, $I,J\trianglelefteq R$ and $I+J=R$, then $IJ=I\cap J$.

↳ Proof: If $I+J=R$, $\exists a\in I, b\in J$ such that $a+b=1$. Let $c\in I\cap J$, $c=c\cdot 1=c(a+b)=ca+cb=ac+bc\in IJ$ since $a\in I, c\in J, b\in I$ ⧄

Definition: If $R$ is commutative, $I,J\trianglelefteq R$ then $I$ and $J$ are called coprime if $I+J=R$.

Definition: $M\trianglelefteq R$ is a maximal ideal if its maximal within the set of proper ideals with respect to inclusion $\subseteq$. i.e. if $J\trianglelefteq R$ and $M\subseteq J\Rightarrow M=J$ or $J=R$.

Example: Let $R=\mathbb{Z}$. What are the maximal ideals?

$(0)\subseteq I$ $\forall I\trianglelefteq R$. When is $(n)\subseteq(m)$?

When every multiple of $n$ is a multiple of $m$ i.e. when $m|n$. Thus maximal ideals are $(p)$, where $p$ is prime.

Theorem: Every proper ideal is contained in a maximal ideal.

↳ Proof: Apply Zorn's Lemma. Let $X$ be a non-empty partially ordered set such that every chain $\xi\in X$ has an upper bound. Then $X$ has at least one maximal element. Let $I\trianglelefteq R$, $I\subsetneq R$ (so $R\neq 0$). Let $X=\{J\trianglelefteq R : I\subseteq J, J\subsetneq R\}$, then $X\neq 0$ since $I\in X$.

Let $\xi$ be a chain in $X$ so $\xi=\{J_i : i\in\Sigma\}$ such that $\forall i,j\in\Sigma$, $J_i\subseteq J_j$ or $J_j\subseteq J_i$.

claim: $\xi$ has an upper bound given by $J=\bigcup_{i\in\Sigma}J_i$

↳ Proof: Clearly $I\subseteq J$ and $J_i\subseteq J$

i) $0\in J_i$ $\forall i\Rightarrow 0\in J\Rightarrow J\neq\emptyset$

ii) let $a,b\in J\Rightarrow\exists i,j$ such that $a\in J_i$, $b\in J_j$. WLOG assume $J_i\subseteq J_j$.
$\Rightarrow a,b\in J_j\Rightarrow a-b\in J_j\Rightarrow a-b\in J$

iii) if $a\in J\Rightarrow a\in J_j$ for some $j$ $\Rightarrow ra\in J_j\subseteq J$ $\forall r\in R$. Thus $J\trianglelefteq R$.
If $J=R$ then $1\in J\Rightarrow 1\in J_j$ for some $j$ $\Rightarrow J_j=R$, but $J_j$ is proper so $J\neq R$.

Thus by Zorn's Lemma, $\exists M\in X$, $I\subseteq M$ with $M$ maximal. ⧄