Tue Aug 27, 2013

Welcome to MTH 661/662 (Grad Algebra)

HW 1 is a review of 561/562.
It is verbatim the Prelim Exam
I gave in Summer 2012.

Course notes from 561/562 are on
my webpage.

Begin.

Math is Hard.
Algebra is Hard.
My goal in 661/662 is to try
to make some sense of it.

The Plan:

1. Fall 661.
   Noncommutative Algebra
   Groups & Representations
   Intro to "Lie Theory"

(2) Spring 662
Commutative Algebra
Rings & Fields
Intro to "Algebraic Geometry".
(and "Number Theory")

Some Philosophy:

Let X be a "space" that we want to study using algebra.
There are **two** competing approaches.

(1) Felix Klein

Find a group G that acts transitively on X. That is ...

Let $Aut(X)$ = "symmetries" of X
= group of structure-preserving bijections $X \to X$.

Let $\varphi : G \to Aut(X)$ be a group hom. written as

$$\varphi(g)(x) = \text{"}g(x)\text{"} \quad \forall\, g \in G,\ x \in X.$$

And suppose that $\forall x, y \in X$ $\exists g \in G$ such that $g(x) = y$ (Transitive)

"All the points of X look the same".

Given $x \in X$ consider the stabilizer

$$\mathrm{Stab}(x) = \{ g \in G : g(x) = x \} \leq G$$

Then we have a bijection

$$\begin{aligned} X &\longrightarrow G/\mathrm{Stab}(x) \\ g(x) &\longmapsto g\,\mathrm{Stab}(x) \end{aligned}$$

<u>Proof</u>:

$$\begin{aligned} g(x) = h(x) &\iff x = g^{-1}(h(x)) = g^{-1}h(x) \\ &\iff g^{-1}h \in \mathrm{Stab}(x) \\ &\iff g\,\mathrm{Stab}(x) = h\,\mathrm{Stab}(x) \end{aligned}$$

$\Longrightarrow$ well-defined

$\Longleftarrow$ injective

(surjective by definition) $\blacksquare$

Also note that $\mathrm{Stab}(x) \approx \mathrm{Stab}(y)$ $\forall x, y \in X$.

<u>Proof</u>: By transitivity, $\exists\, g(x) = y$. Then

$$\mathrm{Stab}(x) = g^{-1}\,\mathrm{Stab}(y)\,g$$

because $h(y) = y \iff h(g(x)) = g(x)$.
$\iff hg(x) = g(x)$.
$\iff g^{-1}hg(x) = x$.

So we might as well just say $\mathrm{Stab}(x) = H$.
Finally note that the bijection $X \leftrightarrow G/H$ preserves structure.

$$\boxed{X \approx G/H}$$

Klein's Erlangen Program (1872) says we should replace the study of X with the study of the

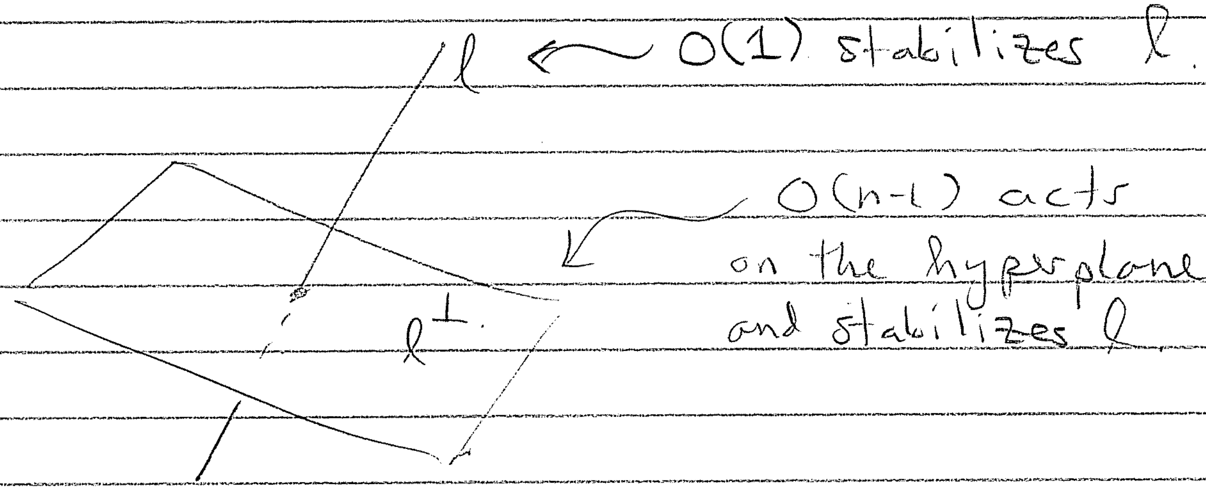
"coset space" G/H

Example: Projective Space

Let $X = \{ \text{lines through } \vec{0} \text{ in } \mathbb{R}^n \}$.

Let $O(n) = \{ A \in GL(n, \mathbb{R}) : A^t A = I \}$
= distance-preserving linear maps $\mathbb{R}^n \to \mathbb{R}^n$
= the "orthogonal group"

Note that $O(n) \curvearrowright X$ transitively.
What is the stabilizer of a line?



Hence $X \approx \dfrac{O(n)}{O(1) \times O(n-1)} = \mathbb{RP}^{n-1}$

(real projective $n-1$ dim space)

More generally, let

$$Gr(r,n) = \{ r\text{-dim subspaces of } \mathbb{R}^n \}$$

Again $O(n) \curvearrowright Gr(r,n)$ transitively.

Stabilizer of a r-dim subspace is $\approx O(r) \times O(n-r)$.

Hence $Gr(r,n) \approx \dfrac{O(n)}{O(r) \times O(n-r)}$

the "Grassmannian".

[Does it remind you of binomial coefficients? Good.]

Today the philosophy

$$X \approx G/H$$

falls under Lie Theory and Representation Theory

② The Competing Approach 662
(Alexander Grothendieck).

Let X be a "space" we want to study, and consider a field K

Let R $(= K[X])$ be the ring of structure-preserving maps $X \to K$ pointwise addition/multiplication.

i.e. $\forall\, f, g \in R$, $x \in X$ we define

$$(f+g)(x) := f(x) + g(x)$$
$$(fg)(x) := f(x)\,g(x).$$

– Given a subset $Y \subseteq X$ define

$$\underline{I}(Y) := \{ f \in R : f(y) = 0 \ \forall\, y \in Y \} \subseteq R$$

and note that $\underline{I}(Y) \leq R$ is an ideal.

Proof: Given $f \in \underline{I}(Y)$ and any $g \in R$ we have

$$fg(y) = f(y)\,g(y) = 0 \cdot g(y) = 0 \quad \forall\, y \in Y \ \boxtimes$$

— Given a subset $S \subseteq R$ define

$$V(S) := \{ x \in X : f(x) = 0 \ \forall f \in S \} \subseteq X$$

Then the functions

$$V \circ I : 2^X \to 2^X$$
$$I \circ V : 2^R \to 2^R$$

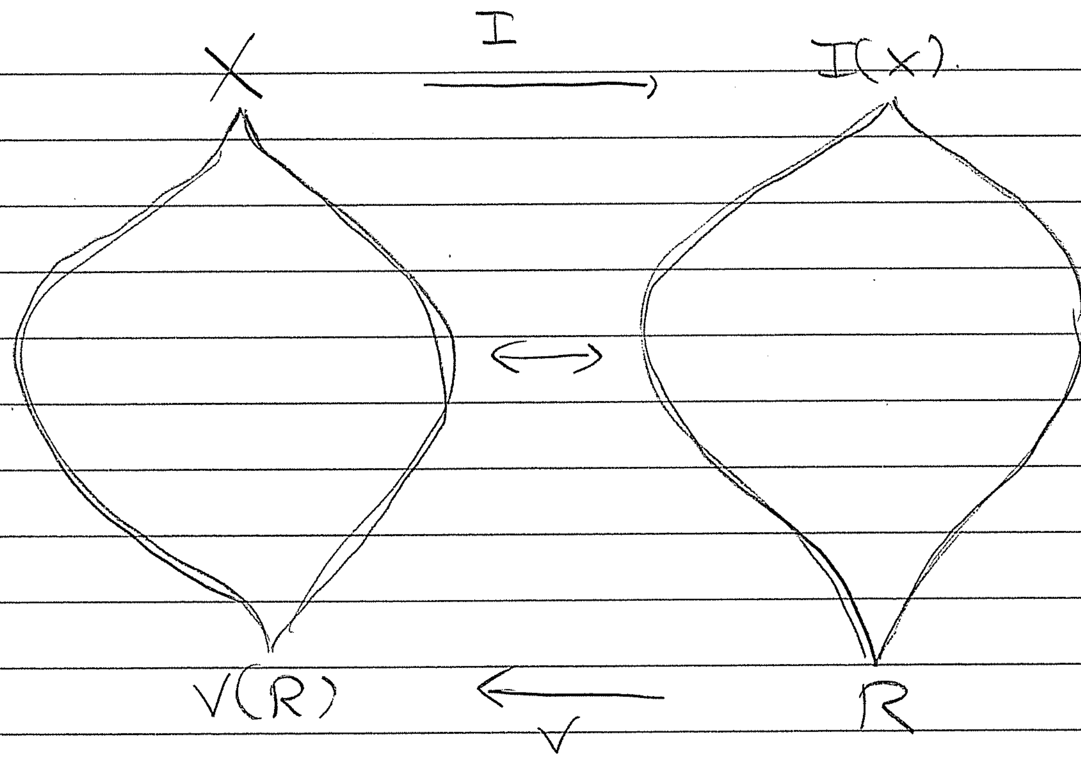
are "closure operators".

Def: Say $cl : 2^S \to 2^S$ is a <u>closure</u> if for all $A, B \subseteq S$

- $A \subseteq cl(A)$
- $A \subseteq B \Rightarrow cl(A) \subseteq cl(B)$
- $cl(cl(A)) = cl(A)$.

Fact: We have an order-reversing lattice isomorphism between

$(V \circ I)$ - closed subsets of X
$(I \circ V)$ - closed subsets of R.



Note: The $V \circ I$ closure is called the Zariski Topology on X.

Philosophy (Grothendieck):
Under nice conditions we can recover the space X from the ring R

Let $\text{Spec}(R) = \{\text{prime ideals of } R\}$.

Then

$$\boxed{X \simeq \text{Spec}(R)}$$

Example:

Let X be a compact Hausdorff space.
e.g. $X = [0,1] \subseteq \mathbb{R}$

Consider the ring of continuous functions from $X \to \mathbb{R}$

$R = C^0(X)$

Then the Zariski Topology on X is just the usual topology

and the points of X are in bijection with maximal ideals of R

$$\text{points of } X \longleftrightarrow \text{maximal ideals of } R$$

This philosophy is called "Algebraic Geometry"

To be continued Spring 2014 ....

Thu Aug 29

HW 1 due next Thurs Sept 5.

MTH 661
Groups & Representations

Plan:

(A) Abstract structure theory of groups

(B) Matrix groups and representations
("Lie Theory")

First Topic: Jordan-Hölder Theorem

Definition: A (bounded) lattice is a structure $(\mathcal{L}, \leq, \wedge, \vee, 0, 1)$ in which

- $(\mathcal{L}, \leq)$ is a partially-ordered set

i.e. for all $x, y, z \in \mathcal{L}$ we have

- $x \leq x$
- $x \leq y$ and $y \leq x \Rightarrow x = y$
- $x \leq y$ and $y \leq z \Rightarrow x \leq z$.

"x meet y"

- For all $x, y \in \mathcal{L}$ $\exists$ $x \wedge y \in \mathcal{L}$ with

$(z \leq x$ and $z \leq y) \Rightarrow z \leq x \wedge y$

"greatest lower bound".

"x join y"

- for all $x, y \in \mathcal{L}$ $\exists$ $x \vee y \in \mathcal{L}$ with

$(x \leq z$ and $y \leq z) \Rightarrow x \vee y \leq z$.

"least upper bound".

- $\exists\, 0 \in \mathcal{L}$ with $0 \leq x$ $\forall\, x \in \mathcal{L}$.

- $\exists\, 1 \in \mathcal{L}$ with $x \leq 1$ $\forall\, x \in \mathcal{L}$ //

Examples:

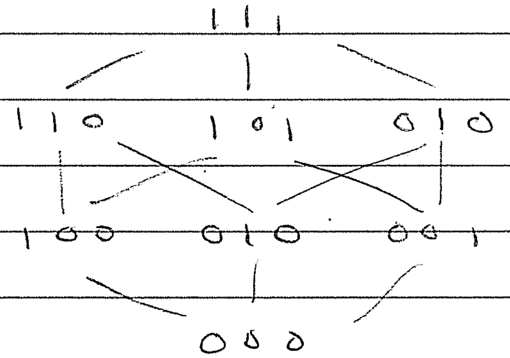
Let U be any set. Then

$2^U := \{$ subsets of $U \}$

is a lattice with $\leq = \subseteq$, $\wedge = \cap$, $\vee = \cup$, $0 = \emptyset$, $1 = U$.

Let $\mathcal{L} = B(n) = \{$ binary strings of length $n \}$

e.g. $B(3)$



Think $0 =$ False, $1 =$ True

$\wedge$	0	1
0	0	0
1	0	1

"AND"

$\vee$	0	1
0	0	1
1	1	1

"OR"

componentwise

$B(n)$ is called a Boolean Lattice/Algebra

Let $\mathcal{L} = \mathbb{N} = \{0, 1, 2, 3, \ldots\}$

with $a \leq b$ = "a divisible by b"
$= b \mid a$

Note. $a \leq 1 \quad \forall\, a \in \mathbb{N}$
$0 \leq a \quad \forall\, a \in \mathbb{N}$

Then $a \wedge b$ = least common multiple
$a \vee b$ = greatest common divisor.

Let $D(n) = \{\text{divisors of } n\}$
with again $a \leq b \equiv b \mid a$

e.g. $D(12) =$

$$\begin{tikzcd}
 & 1 \arrow[dl, dash] \arrow[dr, dash] & & \\
3 \arrow[dr, dash] & & 2 \arrow[dl, dash] \arrow[dr, dash] & \\
 & 6 \arrow[dr, dash] & & 4 \arrow[dl, dash] \\
 & & 12 &
\end{tikzcd}$$

12 plays the role of 0

I guess we could say $D(0) = \mathbb{N}$?

Let G be a group with identity $1 \in G$, and

$\mathcal{L}(G) = \{\text{subgroups of } G\}$

This is a lattice (the subgroup lattice of G) with

$0 = \{1\}$
$1 = G$
$\leq \; = \; \subseteq$

what about $\wedge$ and $\vee$?

— $\wedge$ is easy.

Given subgroups $H, K \leq G$ we see that $H \cap K$ is also a subgroup (easy)

Claim: $H \cap K = H \wedge K$.

<u>Proof</u>: Certainly $H \cap K \leq H$
and $H \cap K \leq K$.

Now let N be any subgroup with $N \leq H$ and $N \leq K$. Then $N \subseteq H \cap K$ <u>as sets</u>, hence $N \leq H \cap K$ as <u>groups</u>

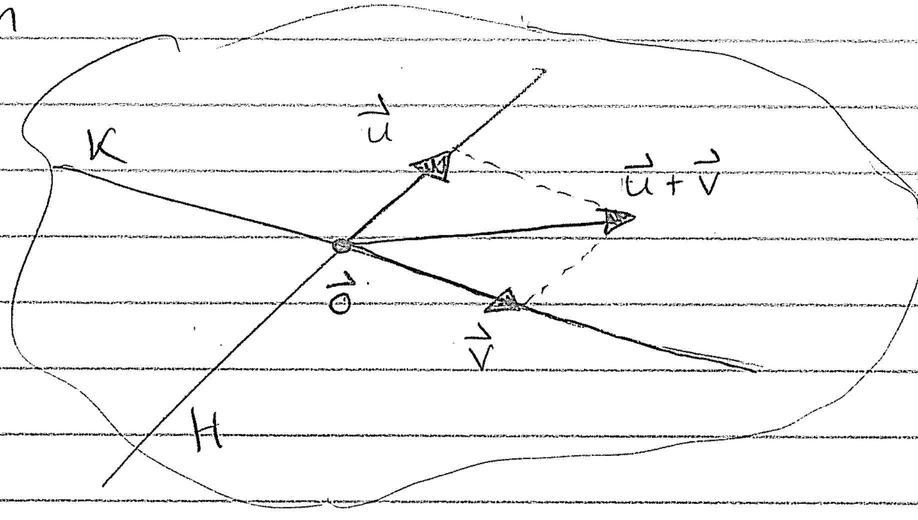
$\blacksquare$

— $\vee$ is not so easy.

Given subgroups $H, K \leq G$, note that $H \cup K$ is probably <u>NOT</u> a subgroup.

e.g. Let $G = (\mathbb{R}^n, +)$.
let H, K be 1-dim subspaces (lines).

$G = \mathbb{R}^n$



If $\vec{u} \in H$, $\vec{v} \in K$, then $\vec{u}+\vec{v} \notin H \cup K$.

In linear algebra we fix this by taking the span of H and K.

$$H \vee K := \operatorname{span}(H, K) = H + K$$

For a general group G, the best we can say is

$$\boxed{H \vee K = \bigcap_{\substack{N \leq G \\ H \cup K \subseteq N}} N}.$$

Exercise: Prove this is the smallest subgroup of G containing H and K

//.

Now we can state some structure theorems.

Given $g \in G$, we can define the cyclic sugroup generated by g:

$$\langle g \rangle := \{ \dots, g^{-2}, g^{-1}, 1, g, g^2, \dots \}$$

If $\langle g \rangle$ is finite we say $|\langle g \rangle|$ is the <u>order</u> of $g \in G$.

<u>Exercise</u>: Show $\langle g \rangle = \bigcap_{\substack{H \leq G \\ g \in H}} H$ //

<u>Def</u>: We say that G is a <u>cyclic group</u> if $\exists\ g \in G$ such that

$$G = \langle g \rangle.$$

☆ Fundamental Theorem of Cyclic Groups (Theorems 1.1.4 & 1.1.5 in Alperin). ☆

If $G = \langle g \rangle$ is cyclic then

$$\mathcal{L}(G) \approx D(n) \quad \text{for some } n \in \mathbb{N}$$

lattice isomorphism.

Specifically, the isomorphism is given by

$$\begin{aligned} D(n) &\longrightarrow \mathcal{L}(G). \\ d &\longmapsto \langle g^d \rangle \end{aligned}$$

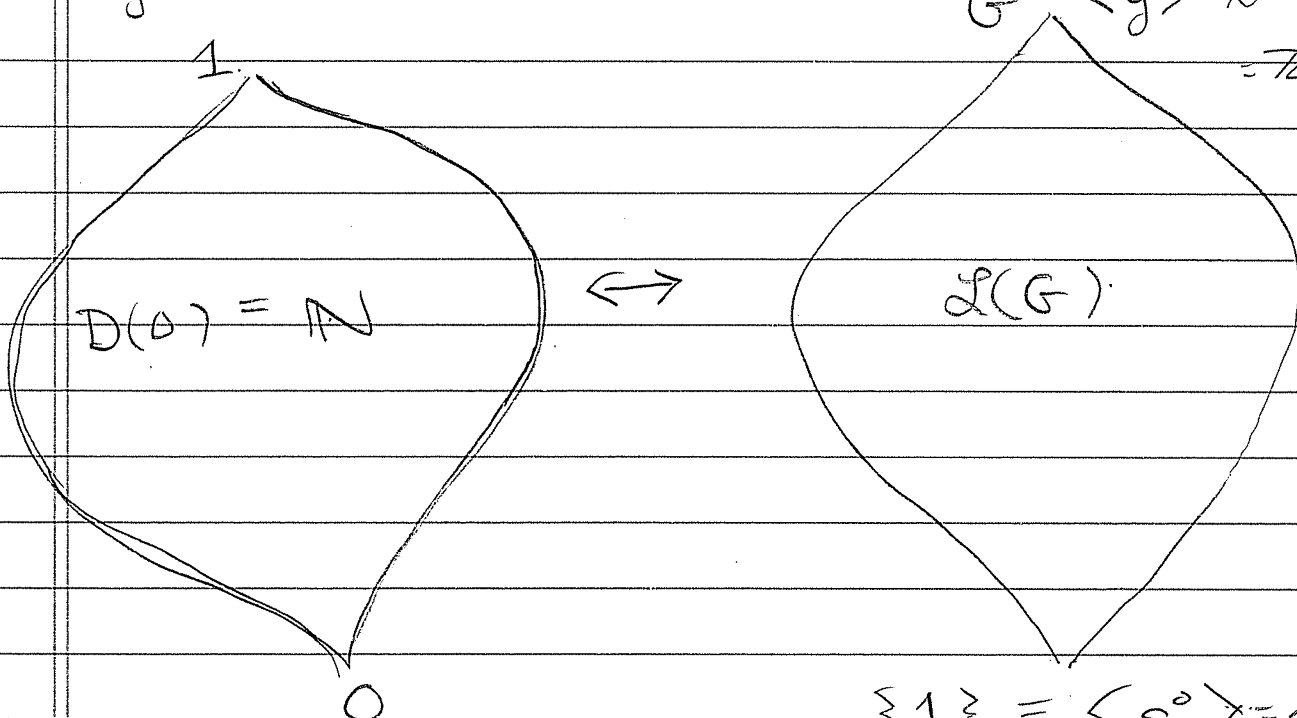
e.g. $n = 12$. $\qquad G \approx \mathbb{Z}/12\mathbb{Z}$

$$\begin{tikzcd}[column sep=small]
 & 1 \arrow[dl, dash] \arrow[dr, dash] & & & & & & \langle g \rangle \arrow[dl, dash] \arrow[dr, dash] & & \\
3 \arrow[dr, dash] & & 2 \arrow[dl, dash] \arrow[dr, dash] & \longleftrightarrow & & & \langle g^3 \rangle \arrow[dr, dash] & & \langle g^2 \rangle \arrow[dl, dash] \arrow[dr, dash] & \\
 & 6 \arrow[dr, dash] & & 4 \arrow[dl, dash] & & & & \langle g^6 \rangle \arrow[dr, dash] & & \langle g^4 \rangle \arrow[dl, dash] \\
 & & 12 & & & & & & \langle g^{12} \rangle &
\end{tikzcd}$$

$G = \langle g \rangle$

$\langle g^{12} \rangle = \{1\}$ Because $g^{12} = 1$

e.g. $n = 0$. $\qquad G = \langle g \rangle \approx \mathbb{Z} = \mathbb{Z}/0\mathbb{Z}$



$\{1\} = \langle g^0 \rangle = \langle 1 \rangle$

Q: What can we say about the structure of $\mathcal{L}(G)$ for general <u>finite</u> groups

This was actually the <u>first</u> problem of group theory, going back to Galois (1830)

Let k be a field and consider a polynomial

$$f(x) \in k[x]$$

Let $k \leq K$ be the smallest superfield in which $f(x)$ has a full set of roots ("the splitting field").

The classical problem of "algebra" was to study the structure of the lattice of intermediate fields

$$\mathcal{L}(K/k) = \{ \text{fields } L : k \leq L \leq K \}$$

Describes algebraic relationship between

$$\underset{k}{\text{coefficients}} \longleftrightarrow \underset{K}{\text{roots of } f(x)}$$

The question was: is $f(x)$ "solvable by radicals", and if so, how?

Galois considered the group

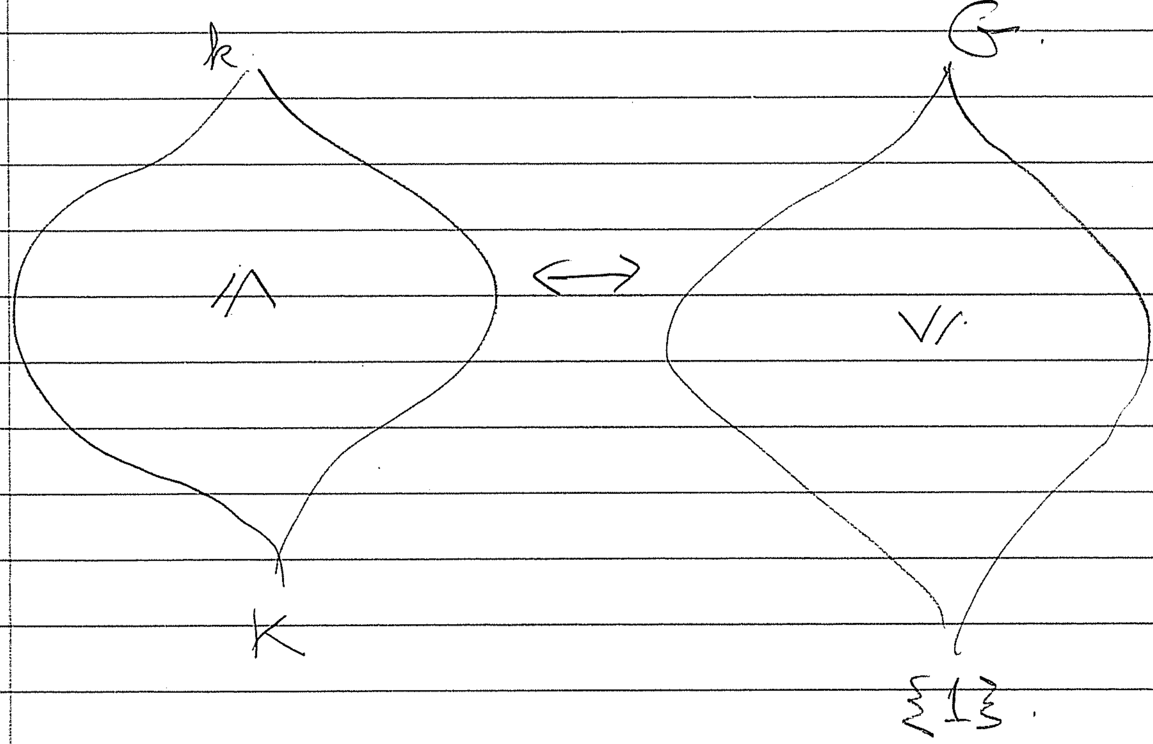
$$\mathrm{Gal}(K/k) := \{ g \in \mathrm{Aut}(K) : g(x) = x \ \forall x \in k \}.$$

Under nice conditions we have.

☆ Fundamental Theorem of Galois Theory ☆.

Let $G = \mathrm{Gal}(K/k)$. Then there is an order-reversing lattice isomorphism.

$$\mathcal{L}(K/k) \approx \mathcal{L}(G).$$



So... to "solve" the polynomial equation

$$f(x) = 0$$

we must study the structure of the subgroup lattice $\mathcal{L}(G)$.

If $f(x) = 0$ is "solvable by radicals", what does this say about $\mathcal{L}(G)$??

Tues Sept 3.

HW 1 due Thurs.

Course webpage is up.

Note: Starting Thurs we are moving to MM 205

Current Goal: Jordan-Hölder

Today: Group Homomorphism Theorems (of Dedekind-Noether).

Given a group G recall the lattice of subgroups $\mathcal{L}(G)$ with

$$H \wedge K = H \cap K$$

$$H \vee K = \langle H, K \rangle = \bigcap_{\substack{N \leq G \\ H \cup K \subseteq N}} N.$$

Q: Why can't we just say

$$H \vee K = HK := \{hk : h \in H, k \in K\}$$

A: Sometimes we can.

Let G, G' be groups and consider a group homomorphism

$$\varphi : G \longrightarrow G'$$

i.e. $\forall a, b \in G$ we have $\varphi(ab) = \varphi(a)\varphi(b)$.

Note that $\varphi(1_G) = 1_{G'}$ since

$$\cancel{\varphi(1_G)} = \varphi(1_G 1_G) = \cancel{\varphi(1_G)}\, \varphi(1_G) \qquad ///$$

and $\varphi(a^{-1}) = \varphi(a)^{-1}$ since

$$\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(1_G) = 1_{G'} \qquad ///$$

Define

$$\operatorname{im}\varphi := \{ g' \in G' : g' = \varphi(g) \text{ for some } g \in G \}$$
$$\ker\varphi := \{ g \in G : \varphi(g) = 1_{G'} \}.$$

Note that $\operatorname{im}\varphi \leq G'$ since given $\varphi(a)$ and $\varphi(b) \in \operatorname{im}\varphi$ we have

$$\varphi(a)\varphi(b) = \varphi(ab) \in \operatorname{im}\varphi$$

and $\ker \varphi \leq G$ since given $a, b \in \ker \varphi$ we have

$$\varphi(ab) = \varphi(a)\varphi(b) = 1_{G'}1_{G'} = 1_{G'}$$

$\Longrightarrow ab \in \ker \varphi$. ///

But $\ker \varphi$ is not just any subgroup.
It has a special property:

if $k \in \ker \varphi$ and $g \in G$ then
$gkg^{-1} \in \ker \varphi$.

Proof:

$$\begin{aligned}
\varphi(gkg^{-1}) &= \varphi(g)\varphi(k)\varphi(g)^{-1} \\
&= \varphi(g)\, 1_{G'}\, \varphi(g)^{-1} \\
&= \varphi(g)\varphi(g)^{-1} \\
&= 1_{G'}
\end{aligned}$$

We say $\ker \varphi$ is a normal subgroup.

$$\boxed{\ker \varphi \trianglelefteq G}$$

Conversely, any normal subgroup is the kernel of canonical homomorphism.

Proof: Let $N \trianglelefteq G$ and consider the set of cosets

$$G/N = \{ aN : a \in G \}.$$

Note that the operation

$$(aN, bN) \longmapsto (ab)N$$

is well-defined. Indeed, suppose we have $aN = a'N$ and $bN = b'N$ (i.e. $\exists\, n_1, n_2 \in N$ with $a = a'n_1$ and $b = b'n_2$). Consider any $(ab)n \in (ab)N$. Then

$$\begin{aligned} abn &= a'n_1 b' n_2 n \\ &= a'b' \underbrace{[(b')^{-1} n_1 b']}_{\in N} n_2 \in (a'b')N \end{aligned}$$

Hence $(ab)N \subseteq (a'b')N$

The other direction is similar ///

Then G/N is a group with identity element $N = 1N$ and we have a canonical homomorphism

$$\begin{aligned} \varphi : G &\longrightarrow G/N \\ a &\longmapsto aN \end{aligned}$$

The kernel is

$$\ker \varphi = \{ a \in G : aN = N \} = N$$

Applying the same idea we get

☆ Fundamental Homomorphism Theorem ☆
(Dedekind-Noether, pre-1930)

Let $\varphi : G \to G'$ be a group homomorphism. Then the map

$$\begin{aligned} \operatorname{im} \varphi &\longrightarrow G/\ker \varphi \\ \varphi(g) &\longmapsto g \ker \varphi \end{aligned}$$

is a group isomorphism.

$$\boxed{\operatorname{im} \varphi \approx G/\ker \varphi}$$

This can be extended to prove the standard "isomorphism theorems" of group theory.

(I will omit tedious details)

Let $\varphi : G \to G'$ be a group hom with kernel N. Define functions

$$\overline{\varphi} : 2^{G} \to 2^{G'}$$
$$\overline{\varphi}^{-1} : 2^{G'} \to 2^{G} \qquad \text{by}$$

$\forall\, S \subseteq G,\ S' \subseteq G'$,

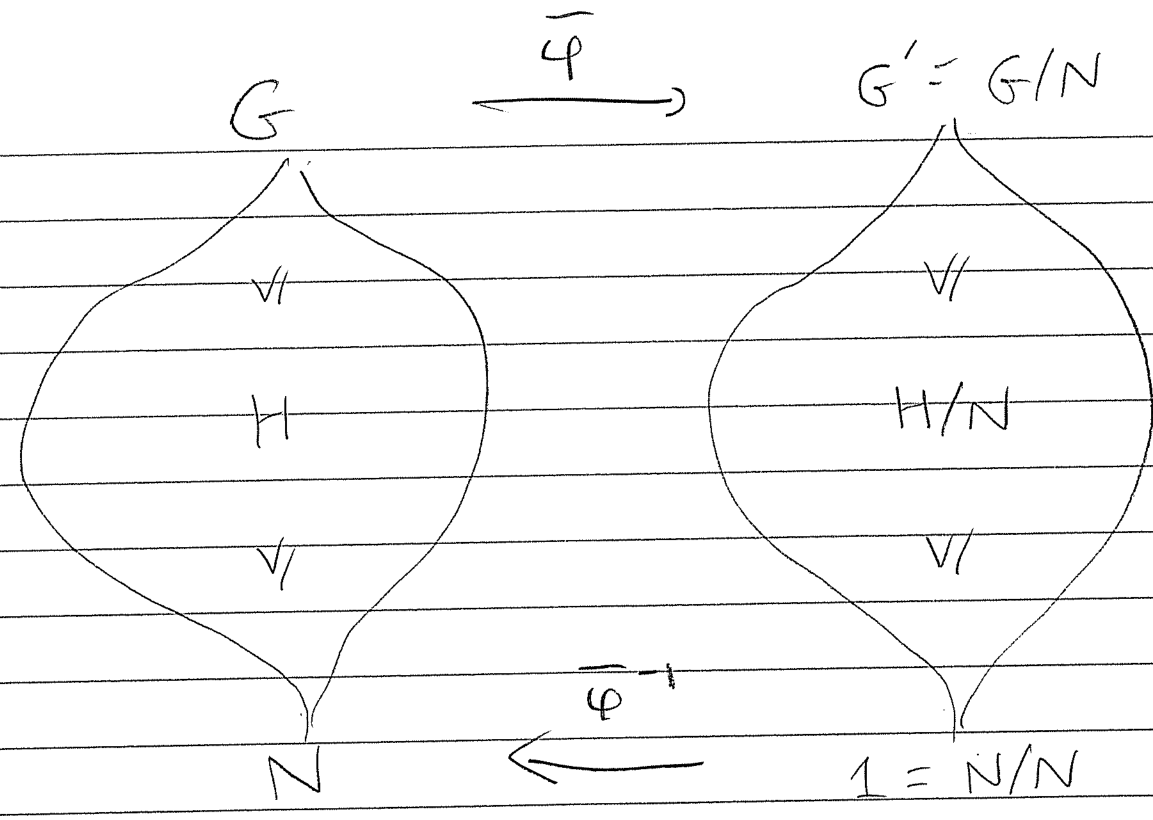
$\overline{\varphi}(S) = \{ g' \in G' : g' = \varphi(s) \text{ for some } s \in S \}$

$\overline{\varphi}^{-1}(S') = \{ g \in G : \varphi(g) = s' \text{ for some } s' \in S' \}$

☆ Theorem (Lattice Isomorphism):

The functions $\overline{\varphi}$, $\overline{\varphi}^{-1}$ are inverse isomorphisms of lattices

$$\mathcal{L}(G, N) \approx \mathcal{L}(G')$$



Given $N \trianglelefteq H, K \leq G$ one should check that

$$\frac{H \wedge K}{N} = \frac{H}{N} \wedge \frac{K}{N}$$

$$\frac{H \vee K}{N} = \frac{H}{N} \vee \frac{H}{K}$$

"Lattice structure is preserved".

But wait, there's more.

One can also show that

$$H \in \mathcal{L}(G,N) \iff H/N \in \mathcal{L}(G/N)$$

is normal ($H \trianglelefteq G$) $\quad$ is normal ($H/N \trianglelefteq G/N$).

and furthermore

$$\boxed{\frac{G/N}{H/N} \approx \frac{G}{H}}$$

"Normal structure is preserved".

Finally we will consider $H \vee K$.
Let $H, K \in \mathcal{L}(G)$.

<u>Theorem</u>: If $K \trianglelefteq G$ then

$$HK = \{hk : h \in H, k \in K\}$$

is a subgroup of G and moreover

$$H \vee K = HK$$

Proof: Given h_1k_1 and $h_2k_2 \in HK$ we have

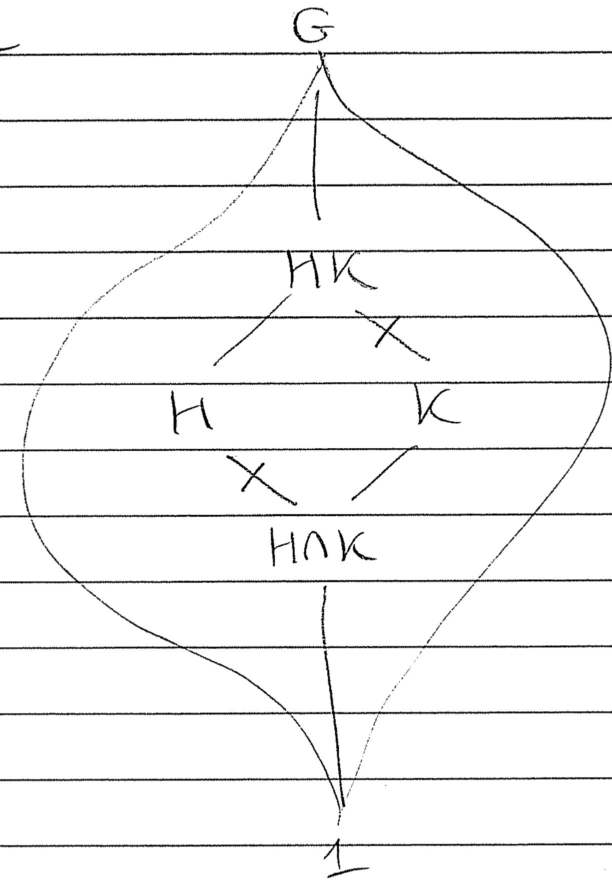
$$(h_1k_1)(h_2k_2) = h_1h_2\underbrace{(h_2^{-1}k_1h_2)}_{\in K}k_2$$

which is in HK. Hence $HK \le G$.

You will show on HW 2 that

$$HK = H \vee K.$$

Picture



Assuming $H, K \leq G$ with $K \trianglelefteq G$ we have one final isomorphism theorem

☆ Theorem (Diamond Isomorhism):

$$\boxed{\frac{H}{H \cap K} \approx \frac{HK}{K}}$$

Proof: Consider the natural map

$$\varphi : G \to G/K$$

and restrict it to H,

$$\varphi|_H : H \to G/K.$$

Note that $\text{im}\,\varphi|_H = HK/K$ since every element of HK/K looks like

$(hk)K = h(kK) = hK$ for some $h \in H$

and note that $\ker \varphi|_H = H \cap K$ since

$\forall h \in H, \quad hK = 1K \iff h \in K.$

The Fundamental Hom. Theorem gives an isomorphism.

$$\frac{H}{\ker \varphi|_H} \approx \operatorname{im} \varphi|_H$$

$$\frac{H}{H \cap K} \approx \frac{HK}{K}$$ $\boxtimes$

Corollary: If H, K are finite then

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Proof: Use Lagrange to conclude

$$\frac{|H|}{|H \cap K|} = \frac{|HK|}{|K|}$$ $\boxtimes$

Exercise: Show that the corollary still holds when neither of $H, K \leq G$ is normal