8/25/15

Welcome to Grad Algebra I (MTH 761)

Drew Armstrong
Ungar 437
armstrong@math.miami.edu

There is no required textbook. All lecture notes will be posted on my webpage:

www.math.miami.edu/~armstrong.

Your grade in the course will be based on homework assignments (probably 5), one midterm exam and the final exam.

Lecture notes from a previous incarnation of this class (Fall 2013 – Spring 2014) along with HW and exam solutions are available on my webpage under "Old Courses".

In 2013-2014 I organized the course as follows:

Fall 2013 : Noncommutative Algebra
Groups & Representations
Intro to "Lie Theory".

Spring 2014 : Commutative Algebra
Rings & Fields
Intro to "Algebraic Geometry".

This year Profs Kalman, De Oliveira, and Griffiths will teach courses on the commutative side of things.

Therefore I will lean more toward the noncommutative side in 761/762. I will spend less time on the theory of commutative rings and more time on the theory of modules, which is a subject that connects noncommutative and commutative algebra. As time permits I will also work in some language from category theory.

BEGIN.

Prior to 1830, "algebra" was dedicated to solving polynomial equations. For example, if

$$ax^2 + bx + c = 0$$

then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Over time this subject became too hard and progress stopped. (This often happens in mathematics.) In order to move forward, Évariste Galois (1830) found a completely new way to look at the subject. It took a while for everyone else to catch up. By 1930, Galois' ideas had completely transformed the subject of "algebra" (solving polynomial equations) into "abstract algebra" (The study of groups, rings, fields, modules, etc.).

//

I will describe Galois' ideas in modern language.

Let $f(x) \in K[x]$ be a polynomial in one variable with coefficients in a field K. We will see later that there exists a field extension $K \subseteq E$ such that

- $f(x)$ "splits" over E, i.e., there exist $a_1, a_2, \cdots, a_n \in E$ such that

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_n).$$

- E is "generated over K" by the roots $a_1, \cdots, a_k$, i.e., the smallest subfield of E containing

$$K \cup \{a_1, a_2, \cdots, a_n\}$$

is E itself.

This E is unique up to isomorphism and we call it the splitting field of the polynomial $f(x)$.

Now the problem of algebra pre-1830 can be stated as follows:

To "solve" the equation $f(x) = 0$ we should find a chain of field extensions

$$K = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_d = E$$

such that each F_i is obtained from F_{i-1} by adjoining an element $\alpha \in F_i$ such that $\alpha \notin F_{i-1}$ but $\alpha^r \in F_{i-1}$ for some power r. We say

$$F_i = F_{i-1}(\alpha)$$

Basically, to get from F_{i-1} to F_i we allow ourselves to take "the rth root" of α^r. Since this doesn't exist in F_{i-1}, F_{i-1}, we end up with a bigger field F_i.

Now by induction each element of E including the roots $a_1, \ldots, a_n$ can be expressed via elements of the base field K using only field operations $+, -, \times, \div$ and pure radicals $\sqrt{\ }, \sqrt[3]{\ }, \sqrt[4]{\ }$, etc.

In other words, we have "solved the equation $f(x) = 0$ by radicals".

OK, but this is just language. The real problem is to find the field extensions $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_d = E$, or to prove that no such fields exist.

Usually they won't exist. Abel and Ruffini had recently proved that a general polynomial equation of degree ≥ 5 is not solvable by radicals.

But Abel's proof was incredibly complicated and hard to read. Galois' contribution was to significantly clean up the language so we can see why the theorem is true.

To do this, Galois come up with a revolutionary idea: He considered the collection of invertible functions

$$\varphi : E \to E$$

satisfying the properties

- $\varphi(a+b) = \varphi(a) + \varphi(b)$ $\quad \forall\, a, b \in E$
- $\varphi(ab) = \varphi(a)\varphi(b)$ $\quad \forall\, a, b \in E$
- $\varphi(a) = a$ $\quad \forall\, a \in K$.

We will call these "automorphisms" of the field extension E/K and denote the collection by

$$\mathrm{Aut}(E/K).$$

The important thing about automorphisms is that they can be composed: given $\varphi, \mu \in \mathrm{Aut}(E/K)$ we have $\varphi \circ \mu \in \mathrm{Aut}(E/K)$.

Galois used the word "group" for this kind of structure and he showed that the group operation on $\mathrm{Aut}(E/K)$ encodes everything we want to know about the structure of the field extension $K \subseteq E$.

To state Galois' theorem we need a bit of notation:

- For any subgroup $H \leq \mathrm{Aut}(E/K)$, define the set

$$E^H := \{ a \in E : \varphi(a) = a \ \ \forall \varphi \in H \}.$$

Note that this is a subfield of E containing K.

- For any intermediate field $K \subseteq F \subseteq E$, define the set

$$\mathrm{Aut}(E/F) := \{ \varphi \in \mathrm{Aut}(E/K) : \varphi(a) = a \ \ \forall a \in F \}.$$

Note that this is a subgroup of $\mathrm{Aut}(E/K)$.

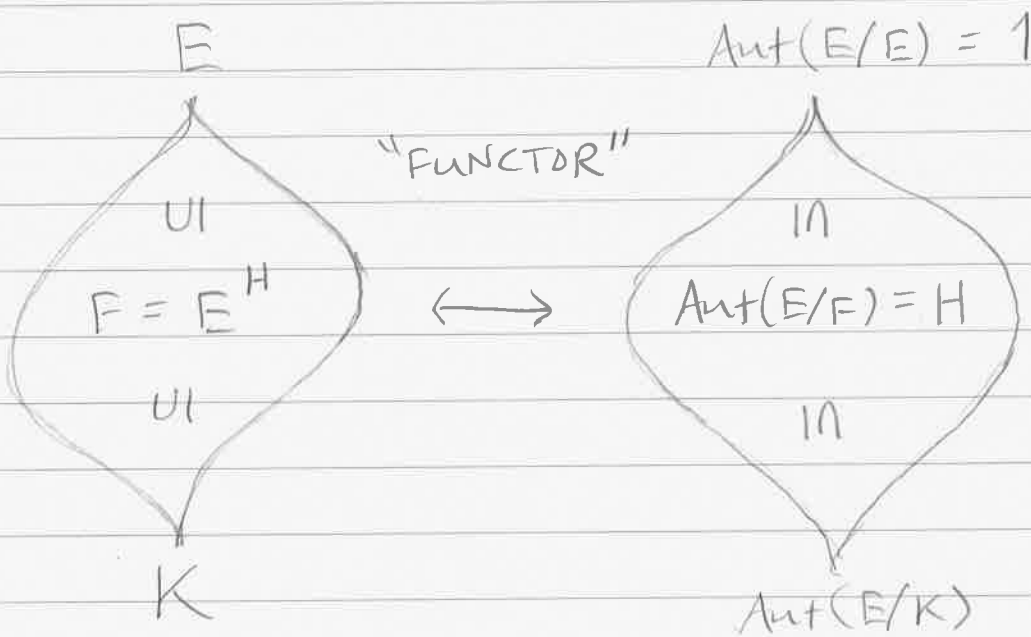
✡ Fundamental Theorem of Galois Theory:

Let $f(x) \in K[x]$ have splitting field E. Under mild conditions on $f(x)$ [its irreducible factors must be "separable"; never mind what that means], the maps

$$H \longmapsto E^H \qquad \& \qquad F \mapsto \mathrm{Aut}(E/F)$$

set up an order-reversing bijection between subgroups of $\mathrm{Aut}(E/K)$ and intermediate fields $K \subseteq F \subseteq E$.

Picture:



In particular, a chain of subfields

$$K = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_d = E$$

in which $F_i = F_{i-1}(\alpha)$ for some α such that $\alpha \notin F_{i-1}$ and $\alpha^r \in F_{i-1}$ corresponds to a chain of subgroups

$$\mathrm{Aut}(E/K) = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_d = 1$$

in which each quotient G_{i-1}/G_i is abelian.

[By analogy, we will say that any such group is "solvable".]

Finally, if $f(x) \in K[x]$ is a generic polynomial of degree n with splitting field E, then its "Galois group"

$$\mathrm{Aut}(E/K)$$

is isomorphic to the symmetric group S_n of all permutations of n things.

We will prove later that the group S_n is not solvable when $n \geq 5$, from which the Abel-Ruffini theorem follows. In particular, we will show that the alternating subgroup $A_n < S_n$ is simple for all $n \geq 5$.

Special Case: The group A_5 is isomorphic to the group of rotational symmetries of the regular icosahedron.

That's quite a revolution. :)

8/27/15

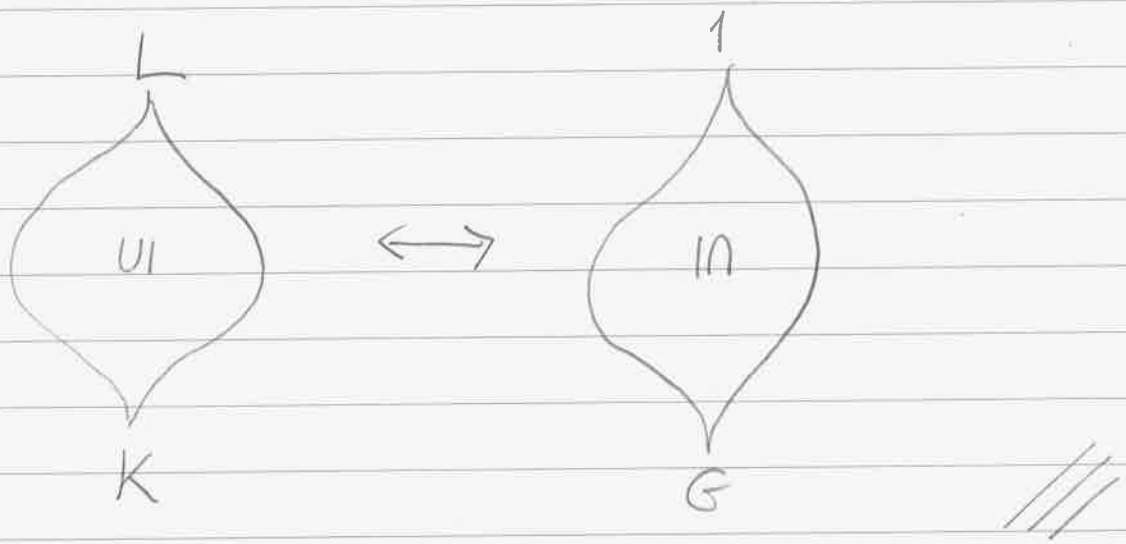
Last time we discussed the first theorem of abstract algebra.

✡ F.T.G.T. (~1830):

Let $f(x) \in K[x]$ be a polynomial whose irreducible factors are "separable" (never mind what that means; it's automatically true when $\operatorname{char} K = 0$). Let L be the splitting field of $f(x)$ and consider the group

$$G = \operatorname{Aut}(L/K).$$

Then the maps $H \mapsto L^H$, $F \mapsto \operatorname{Aut}(L/F)$ set up an order-reversing bijection between subgroups of G and intermediate fields $K \subseteq F \subseteq L$. Picture:



The full proof of this theorem is quite involved, but it's worth noting that certain aspects of the proof are "trivial", i.e., have nothing whatsoever to do with groups and fields.

The concept of an "abstract Galois connection" will recur throughout the course, so let's discuss it now.

Here I will follow George Bergman's book "Invitation to General Algebra and Universal Constructions", Chap. 6.5.

Let S and T be sets and let $R \subseteq S \times T$ be an arbitrary relation. We will write

$$\text{"}aRb\text{"} \iff (a,b) \in R.$$

Given any subset $A \subseteq S$ we will define

$$A^* := \{ t \in T : aRt \ \forall\, a \in A \} \subseteq T.$$

and similarly for all $B \subseteq T$ we define

$$B^* := \{ s \in S : sRb \ \forall \ b \in B \} \subseteq S.$$

This gives us a pair of maps between the power sets

$$* : 2^S \to 2^T$$
$$* : 2^T \to 2^S.$$

This is called an abstract Galois connection. Let's explore the basic properties.

(1) $*$ is order-reversing. That is, for all $A_1, A_2 \subseteq S$ we have

$$A_1 \subseteq A_2 \implies A_2^* \subseteq A_1^*.$$

and for all $B_1, B_2 \subseteq T$ we have

$$B_1 \subseteq B_2 \implies B_2^* \subseteq B_1^*.$$

[Since the statements are dual, we only need to prove the first.]

Proof: Assume that $A_1 \subseteq A_2 \subseteq S$ and consider any $t \in A_2^* \subseteq T$. By definition this means that

$$aRt \quad \forall \quad a \in A_2.$$

But since $A_1 \subseteq A_2$ this implies that

$$aRt \quad \forall \quad a \in A_1,$$

and hence $t \in A_1^*$. ///

Now we consider the compositions

$$** : 2^S \to 2^S$$
$$** : 2^T \to 2^T.$$

[Sorry for the abuse of notation.]

(2) $**$ is monotone increasing. That is, for all $A \subseteq S$ and $B \subseteq T$ we have

$$A \subseteq A^{**} \quad \text{and} \quad B \subseteq B^{**}.$$

Proof: Given $a \in A$ we want to show that $a \in A^{**}$. Recall that

$$A^{**} = (A^*)^* = \{ s \in S : sRt \ \forall \ t \in A^* \}.$$

Hence we want to show that

$$aRt \quad \forall \quad t \in A^*.$$

So consider any $t \in A^*$. By definition this means that $sRt \ \forall \ s \in A$, and in particular we have aRt. Since $t \in A^*$ was arbitrary we obtain

$$aRt \quad \forall \quad t \in A^*$$

as desired. ///

(3) For all $A \subseteq S$ and $B \subseteq T$ we have

$$A^{***} = A^* \text{ and } B^{***} = B^*.$$

Proof: Consider any $A \subseteq S$. By (2) we have $A \subseteq A^{**}$. Then by (1) we have

$$(A^{**})^* \subseteq A^*$$
$$A^{***} \subseteq A^*.$$

Conversely, applying (2) to the set $A^* \subseteq T$ gives

$$A^* \subseteq (A^*)^{**}$$
$$A^* \subseteq A^{***}.$$

///

The function $**$ is often called a "closure operator". Let's define this.

Def: Given a set U we say that

$$cl : 2^U \to 2^U$$

is a closure operator if for all subsets $X, Y \subseteq U$ we have

i) $X \subseteq cl(X)$
ii) $X \subseteq Y \implies cl(X) \subseteq cl(Y)$
iii) $cl(cl(X)) = cl(X)$.

we say that the set $X \subseteq U$ is closed if

$$cl(X) = X.$$

///

(4) $**: 2^S \to 2^S$ and $**: 2^T \to 2^T$ are closure operators.

Proof: i) Given $A \subseteq S$, part (2) says that $A \subseteq A^{**}$. ✓

ii) Given $A_1, A_2 \subseteq S$ we apply part (1) twice to get

$$A_1 \subseteq A_2 \Longrightarrow A_2^* \subseteq A_1^* \Longrightarrow A_1^{**} \subseteq A_2^{**} \checkmark$$

iii) Given $A \subseteq S$ we apply (3) to get

$$(A^{**})^{**} = (A^{***})^* = (A^*)^* = A^{**} \checkmark$$

///

Great, now what?

Note that the sets

$$S, S^*, T, T^*$$

are all $**$-closed. Indeed since $S^{**} \subseteq S$ (by definition) and $S \subseteq S^{**}$ (by part (2)) we must have

$$S^{**} = S,$$

so S is $**$-closed. And by part (3) we have

$$(S^*)^{**} = S^{***} = S^*,$$

so S^* is $**$-closed. ///

Furthermore, note that S^* and T^* are minimal among $**$-closed sets.

Indeed, if $B \subseteq T$ is $**$-closed, i.e.,

$$B^{**} = B,$$

$\Downarrow$

Then since $B^* \subseteq S$ (by definition), part (1) implies that

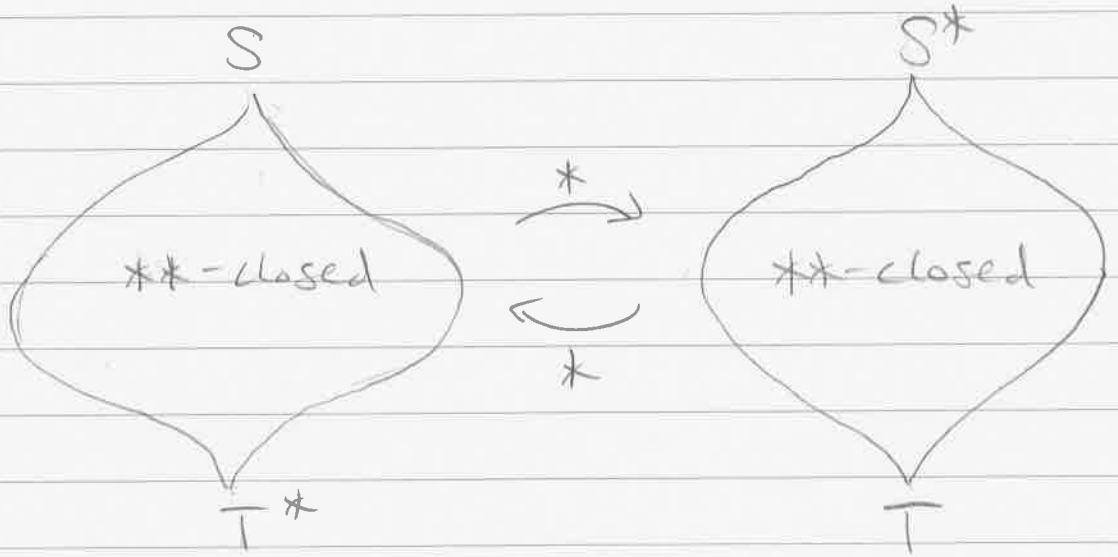
$$S^* \subseteq (B^*)^* = B^{**} = B,$$

as desired. ///

Finally, putting everything together gives the following.

Theorem (Abstract Galois Connection):

The maps $*: 2^S \to 2^T$ and $*: 2^T \to 2^S$ set up an order-reversing bijection between $**$-closed subsets of S and $**$-closed subsets of T.



///

I apologize for putting you through that extreme abstraction, but I assure you that it is worth doing once in your life (we do it once so that we never have to do it again).

Now let's apply abstract Galois theory to concrete Galois theory.

With the notation as before, let

$$S = L \qquad \& \qquad T = \mathrm{Aut}(L/K)$$

Let $R \subseteq L \times \mathrm{Aut}(L/K)$ be the relation

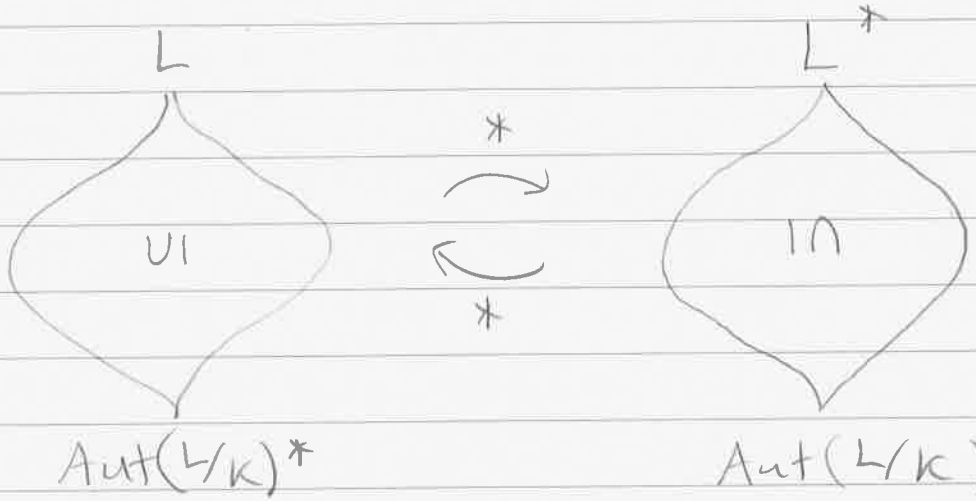
$$a R \varphi \iff \varphi(a) = a.$$

Then for all subsets $H \subseteq \mathrm{Aut}(L/K)$ and $F \subseteq L$ we have

$$H^* = \{ a \in L : \varphi(a) = a \ \forall \varphi \in H \} = L^H$$

$$F^* = \{ \varphi \in \mathrm{Aut}(L/K) : \varphi(a) = a \ \forall a \in F \} = \mathrm{Aut}(L/F).$$

We automatically obtain an order-reversing bijection between **-closed sets:



The actual content of the F.T.G.T is the following pair of statements.

- The **-closed subsets of Aut(L/K) are precisely the subgroups.
- The **-closed subsets of L are precisely the subfields containing K.

[I hope to prove these next semester as a consequence of something called "Wedderburn Theory".]

Remark: I assure you that our efforts today will be repaid later. Once you have learned the concept of "Galois connection" you will start to see them everywhere. This will also provide a natural path into the language of categories.

9/1/15

HW1 is due in two weeks (i.e., on Tues Sept 15).

Recall: Last time we discussed the notion of an "abstract Galois connection".

Given two sets S, T and a relation $R \subseteq S \times T$ we define maps $R: 2^S \to 2^T$ and $R: 2^T \to 2^S$ as follows:

- For all $A \subseteq S$ we set

$$A^R := \{ t \in T : aRt \ \forall a \in A \} \subseteq T$$

- For all $B \subseteq T$ we set

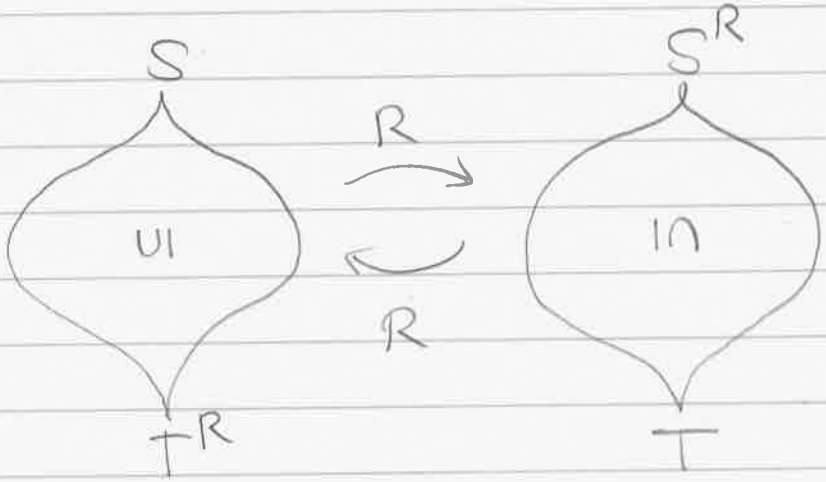
$$B^R := \{ s \in S : sRb \ \forall b \in B \} \subseteq S.$$

The pair of maps

$$R: 2^S \rightleftarrows 2^T : R$$

is called an (abstract) Galois connection.

Last time we proved that the maps $RR : 2^S \to 2^S$ and $RR : 2^T \to 2^T$ are closure operator. We saw that the Galois connection restricts to an order-reversing bijection between RR-closed sets:



But more is true: You will show on HW 1 that this bijection is actually an isomorphism of lattices.

To prepare you for HW1, today I will introduce the concepts of posets and lattices.

Definition: A poset (partially-ordered set) is a structure $(P, \leq)$ in which

- P is a set.
- $\leq$ is a relation satisfying
  - $\forall x \in P, \; x \leq x$
  - $\forall x, y \in P, \; x \leq y \;\&\; y \leq x \Rightarrow x = y.$
  - $\forall x, y, z \in P,$

    $x \leq y \;\&\; y \leq z \Rightarrow x \leq z.$

Example: If U is a set then the power set 2^U is partially ordered by inclusion $\subseteq$.

Actually the power set $(2^U, \subseteq)$ has the richer structure of a Boolean algebra. This is encoded by the three functions

- $\cup : 2^U \times 2^U \to 2^U$ (union)
- $\cap : 2^U \times 2^U \to 2^U$ (intersection)
- $c : 2^U \to 2^U$ (complement)

and the two special elements

$$\emptyset \in 2^U \quad \text{and} \quad U \in 2^U.$$ ///

More generally, we have the concept of a "Lattice".

Def: A Lattice is a structure

$$(\mathcal{L}, \leq, \vee, \wedge, 0, 1)$$

such that

- $(\mathcal{L}, \leq)$ is a poset.
- $\vee : \mathcal{L} \times \mathcal{L} \to \mathcal{L}$ is function (called the join) satisfying the following "universal property".
  - $x \leq x \vee y$ and $y \leq x \vee y$.
  - if $x \leq z$ and $y \leq z$ for some z then we must have $x \vee y \leq z$.

In other words, $x \vee y$ is the "least upper bound" of x and y.

[Note that the join is necessarily unique. Suppose we have another element s such that

— $x \leq s$ and $y \leq s$
— if $x \leq z$ and $y \leq z$ then $s \leq z$.

Since $x \leq x \vee y$ and $y \leq x \vee y$, this implies that $s \leq x \vee y$. Conversely, since $x \leq s$ and $y \leq s$, the definition of $x \vee y$ gives $x \vee y \leq s$. Hence

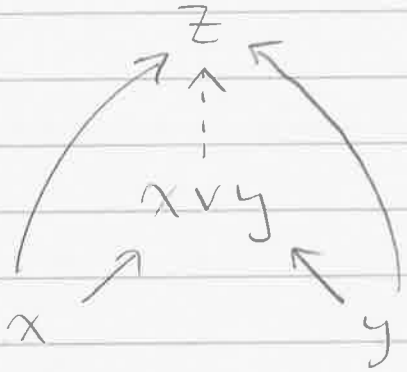
$$s = x \vee y.$$

Universal properties like this always lead to uniqueness.]

Let me rephrase the definition of join in a more efficient way. For all $x, y \in \mathcal{L}$ we will write

$$x \to y \iff x \leq y.$$

Then we have



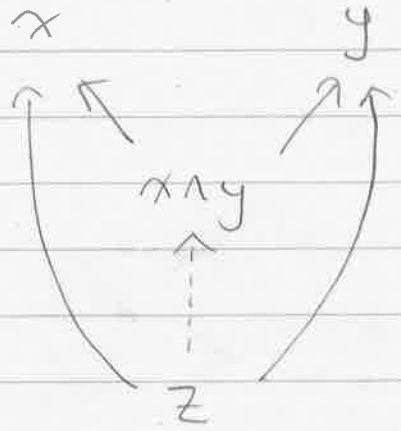
We interpret this to mean: If the solid arrows exist then the dotted arrow necessarily exists. In the language of category theory we say that $x \vee y$ is the "coproduct" of x and y. ///

- $\wedge : \mathcal{L} \times \mathcal{L} \to \mathcal{L}$ is a function (called the meet) satisfying the universal property:

  — $x \wedge y \leq x$ and $x \wedge y \leq y$.
  — if $z \leq x$ and $z \leq y$ then $z \leq x \wedge y$.

In other words, $x \wedge y$ is the "greatest lower bound" of x and y.

The corresponding "commutative diagram" is



This means that $x \wedge y$ is the "product" of x and y in the "category" $(\mathcal{L}, \leq)$. ///

- $1 \in \mathcal{L}$ is a special element satisfying

  — $x \leq 1 \quad \forall\, x \in \mathcal{L}$.

It is the "absolute maximum" or the "final object" of $(\mathcal{L}, \leq)$

[This element is unique: Suppose we have another element $m \in \mathcal{L}$ such that $x \leq m \;\forall\, x \in \mathcal{L}$. Then.

$m \leq 1$ and $1 \leq m \implies m = 1$.]

- $0 \in \mathcal{L}$ is a special element satisfying

  — $0 \leq x \quad \forall\ x \in \mathcal{L}$.

It is called the "absolute minimum" or the "initial object" of $(\mathcal{L}, \leq)$. ///

Example: Let U be a set. Then the poset $(2^U, \subseteq)$ is a lattice with

$$\vee = \cup, \quad \wedge = \cap, \quad 0 = \emptyset, \quad 1 = U.$$

Lattices of the form $(2^U, \subseteq)$ are called Boolean Lattices.

Example (Not all Lattices are Boolean):

Let n be a positive integer and consider its set of positive divisors

$$\mathrm{Div}(n) := \{ d \geq 1 : d \mid n \}.$$

{

This is a lattice under the "divisibility" partial order:

$$d_1 \leq d_2 \iff d_1 \mid d_2 .$$

The meet and join are given by

$$d_1 \vee d_2 = \operatorname{lcm}(d_1, d_2)$$
$$d_1 \wedge d_2 = \gcd(d_1, d_2) .$$

The special elements are

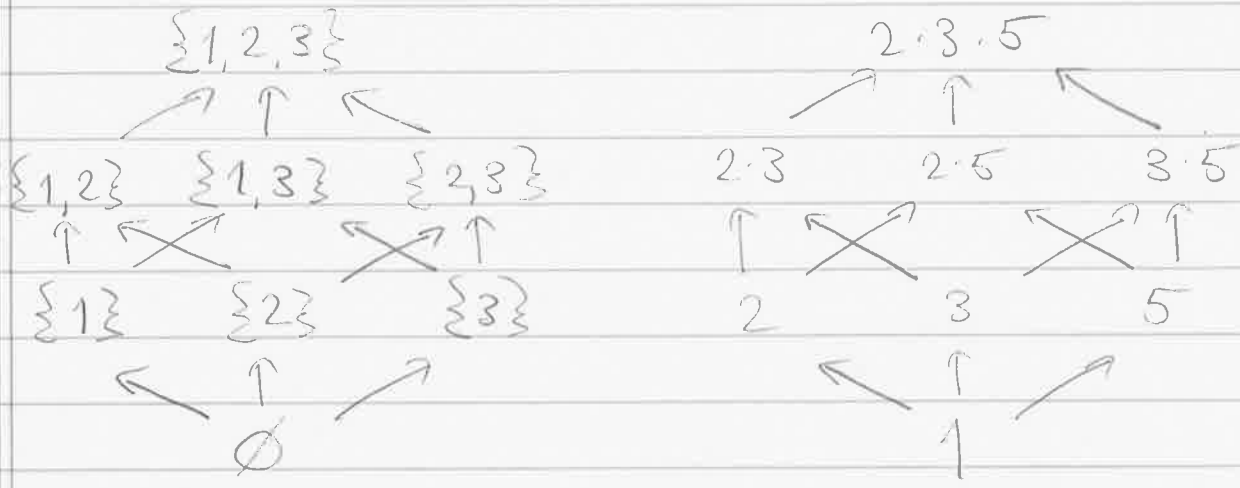
$$0 = 1 \quad \text{and} \quad 1 = n .$$

Remark: The lattice $(\mathrm{Div}(n), |)$ is isomorphic to a Boolean lattice if and only if the integer n is "squarefree" (i.e., its prime factors occur with multiplicity 1).

For example, the lattice $\mathrm{Div}(30)$ is isomorphic to the Boolean lattice

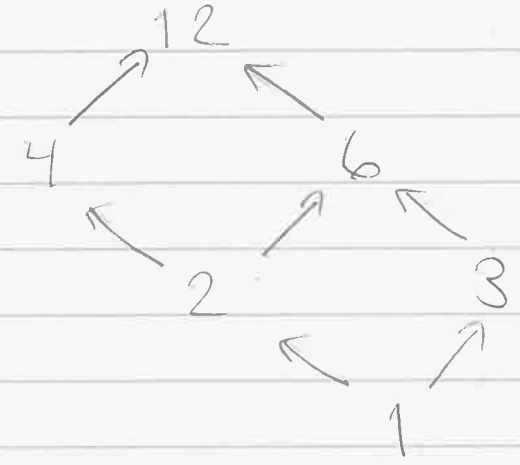
$$2^{\{1,2,3\}} .$$

Picture:



But the Lattice Div(12) is not Boolean.

Picture:



I mentioned the concept of "isomorphism" of Lattices. What does this mean?

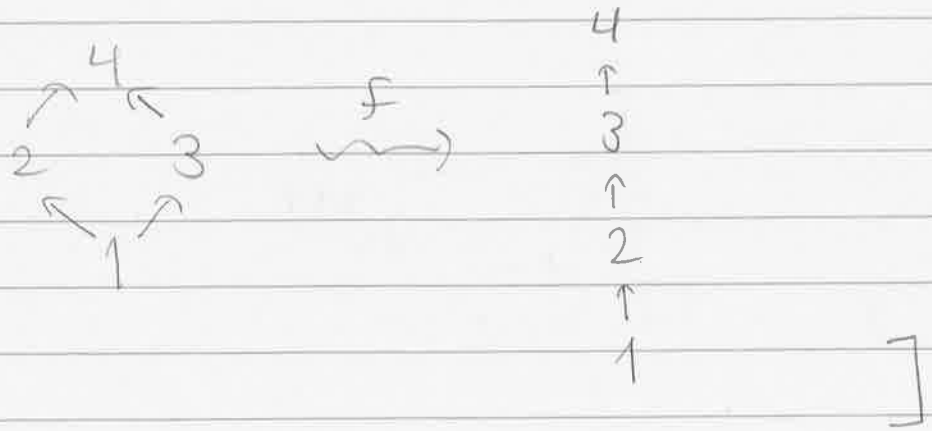
Def: Let $(P, \leq)$ and $(Q, \leq)$ be posets.

- A function $f: P \to Q$ is called a poset homomorphism if $\forall x, y \in P$,

$$x \leq y \implies f(x) \leq f(y).$$

- The function $f: P \to Q$ is a poset isomorphism if (1) it is invertible, and (2) its inverse is a poset homomorphism.

[Remark: An invertible poset hom is not necessarily an isomorphism. Consider the following.



]

- If $(P, \leq)$ and $(Q, \leq)$ are, in addition, lattices we say that $f: P \to Q$ is a lattice homomorphism if

  — f is a poset homomorphism
  — $\forall\, x, y \in P$ we have

  $$f(x \vee y) = f(x) \vee f(y) \quad \text{and}$$
  $$f(x \wedge y) = f(x) \wedge f(y).$$

- We say that a lattice hom $f: P \to Q$ is a lattice isomorphism if (1) it is invertible, and (2) its inverse is also a lattice homomorphism

[Remark: Actually, any poset isomorphism between lattices will be a lattice isomorphism. Can you see why?]