What is Galois Theory?
- symmetry of roots of polynomials, rings of polynomials, field extensions

Can I solve poly by extending $\mathbb{Q}$ economically?

For quadratics $x^2+px+q=0$, $-\frac{p}{2} \pm \sqrt{\frac{p^2}{4}-q}$
- cubics and quartics solved by radicals
- can't for quintics

Galois' idea: taking radicals $\leftrightsquigarrow$ extending fields

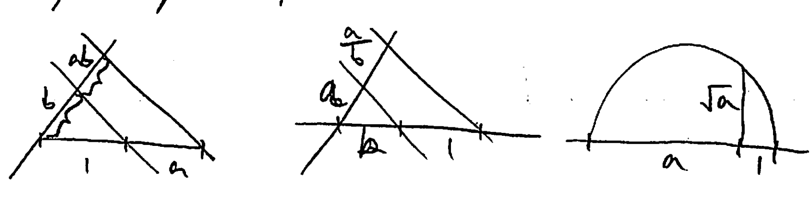
Given $f(x)$ a poly with coeff's in field K can we find larger field L s.t. f factors into linear terms?

Straightedge / compass constructions

Which regular n-gons can be constructed?

Start with 2 pts unit distance apart
(i) Can draw circle at constr. pt. w/ radius of constr. len.
(ii) Can draw line between 2 constr. pts.
(iii) Intersection of circles & lines in (i) and (ii) is constr. pt.

Given $1, a, b$ as lengths, we can construct $a+b$, $a-b$, ab, $\frac{a}{b}$, $\sqrt{a}$



Thm: length constructable $\Leftrightarrow$ expressible by rationals using arithmetic & nested square roots (related to field extensions)

Groups $(G, *)$

set G w/ $* : G \times G \to G$ s.t.
① associative
② $\exists$ identity
③ each g has g^{-1}

Usually if G is abelian; use $+$ for $*$, $-g$ for g^{-1}, 0 for id

Rings $(R, +, \times)$

set R s.t.
① $(R, +)$ is abelian group
② $\times$ is associative
③ distributive $(a+b)c = ac + bc$
*④ (commutative rings): $\times$ is commutative (sometimes w/ identity 1)

Ex: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ comm. rings w/ 1
Ex: $3\mathbb{Z}$ has no identity
Ex: $\mathbb{H}$ (quaternions) not comm.

We will assume rings are commutative with identity in this class.

Let $R[x] = \{$polynomials w/ coeff in ring $R\}$
$= \{a_n x^n + \dots + a_1 x + a_0 \mid a_i \in R\}$

Note: R embeds in $R[x]$ as a subring.

Let $R[x_1, x_2, \dots, x_n]$ = poly ring over $x_1, \dots, x_n$
$= (R[x_1, \dots, x_{n-1}])[x_n]$

Ring Homomorphism $\varphi : R \to S$
satisfies $\varphi(a+b) = \varphi(a) + \varphi(b)$
$\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in R$
(in rings w/ identity) $\varphi(1_R) = 1_S$

φ is <u>isomorphism</u> if also bijective

$\ker \varphi = \varphi^{-1}(0)$ is an <u>ideal</u> (but not necessarily a subring if it is in a ring w/ 1)

$J \subset R$ is ideal of R if nonempty and
(i) $r, s \in J \Rightarrow r+s \in J$
(ii) $r \in R, s \in J \Rightarrow rs \in J$

$R/J = \{$ cosets of J in $(R,+)\}$

First Isomorphism Theorem for Rings
If $\varphi : R \to S$ homomorphism w/ $\ker \varphi = J$ then $R/J \cong \varphi(R)$
(ideals correspond to kernels of homomorphisms)

Def: Call $r \in R$ a <u>unit</u> if r has a multiplicative inverse r^{-1}.

A <u>field</u> is a commutative ring w/ 1 where every nonzero element is a unit.

$R[x]$ has the same units as R if R is an <u>integral domain</u>.

Def: R comm w/ 1. R is <u>integral domain</u> if $\forall r, s \in R$, $rs = 0$ $\Rightarrow r = 0$ or $s = 0$. (R has no <u>zero-divisors</u>)

Integral Domains are like integers:

(i) cancellation law: If $a \neq 0$, then $ab = ac \Rightarrow b = c$

(ii) can construct <u>field of fractions</u>, just like $\mathbb{Q}$ formed from $\mathbb{Z}$

Field of Fractions

If R is ID, let $R^* = R - \{0\}$.

Define relation on $R \times R^*$: $(r_1, d_1) \sim (r_2, d_2)$ if $r_1 d_2 = r_2 d_1$

We can check $\sim$ is an <u>equivalence relation</u> (transitive, symmetric, reflexive); and define $+, \times$, and check it is a field.

Given an ID, we have a way to get a larger field

Ex: ID	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{Z}/3\mathbb{Z}$	$R[x]$
field of fractions	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Z}/3\mathbb{Z}$	rational functions

A finite integral domain must be a field

Given a ring R, we can also get a field by "collapsing" it (mod by ideal)

An ideal J is <u>proper</u> if $J \neq R$. A proper ideal is <u>maximal</u> if J and R are the only ideals containing J.

field $\subseteq$ ED $\subseteq$ PID $\subseteq$ UFD $\subseteq$ ID

Def: Ideal J <u>prime</u> iff $J \neq R$ & $\forall ab \in J \Rightarrow a \in J$ or $b \in J$

Ex: in $\mathbb{Z}[x]$, $J = (x)$ is <u>prime</u> ideal

Thm: P <u>prime ideal</u> in $R \Leftrightarrow R/P$ is an ID

<u>Thm</u>: M maximal ideal in $R \Leftrightarrow R/M$ is a field

Proof: ($\Rightarrow$) Try to show $a+M$ has inverse, where $a \notin M$.
Consider ideal J gen by M and a. So, $J = R$, so
$1 \in J$ and $1 = ab + m$, for some $m \in M$, $b \in R$. We
claim $(a+M)(b+M) = 1+M$. We see that
$(a+M)(b+M) = ab + M = 1 - m + M = 1 + M$.
($\Leftarrow$) take $a \notin M$, wts ideal J gen by $(a, M) = R$
and $1 \in J$.

Col: maximal ideals are prime ideals

Thm: R field $\Leftrightarrow$ only ideals of R are (0) & R

Proof: $\{0\}$ is a maximal ideal by previous thm

Ideal structure tells us how far from a field R is

Ex: $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ where (x^2+1) is maximal and
$\mathbb{C}$ is a field

Isomorphism $\mathbb{R}[x]/(x^2+1) \to \mathbb{C}$ by $1 \mapsto 1$ $x \mapsto i$
Homomorphism (then 1st iso thm) $\mathbb{R}[x] \to \mathbb{C}$ by $1 \mapsto 1$ $x \mapsto i$

$(A) :=$ ideal gen by set A
if A finite, (A) is <u>finitely generated</u>
if A is 1 element, (A) is <u>principal</u>

in $\mathbb{Z}$, every ideal is principal

Def: A <u>principal ideal domain</u> is ID where every ideal
is principal

In PID, every non-zero prime ideal is maximal

In PID (more generally UFDs), nonzero element p, (p) is prime $\Leftrightarrow$ p is <u>irreducible</u> (can't be factored into smaller non-units)

field $\subseteq$ ED $\subseteq$ PID $\subseteq$ UFD $\subseteq$ ID $\subseteq$ ring

$\mathbb{C}$ $\quad$ $\mathbb{Z}$ $\quad$ $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ $\quad$ $\mathbb{Z}[x]$ $\quad$ $\mathbb{Z}[i\sqrt{5}]$ $\quad$ max $\Rightarrow$ prime

nonzero prime ideals $\Rightarrow$ maximal $\quad$ gcd $\quad$ finite $\Rightarrow$ field

prime $\Leftrightarrow$ irreducible $\quad$ prime $\Rightarrow$ irred.

R field $\Leftrightarrow$ $R[x]$ PID , R UFD $\Rightarrow$ $R[x]$ UFD

In $\mathbb{Z}$, ideals: $(6) \subset (3)$ (number theoretic properties reflected in ring structure, containment $\longleftrightarrow$ divisors)

In PID, prime $\Leftrightarrow$ maximal

Proof: Suppose P is prime ideal $(p) \subseteq R$. Say $(p) \subset (m)$ some ideal so $p = bm$ for some $b \in R$. Since $p \in (p)$, $b \in (p)$ or $m \in (p)$. If $m \in (p)$ then $(m) \subset (p)$ so $(m) = (p)$. If $b \in (p)$, then $b = ap$ for some $a \in R$ so $p = apm$ and $am = 1$ so m is a unit and $(m) = R$.

Def: A commutative ring is Noetherian if there is no ∞ ascending chain of ideals in R (i.e. if $I_1 \subseteq I_2 \subseteq \dots$ then $\exists n$ st $I_k = I_n$ $\forall k \geq n$)

Def: Artinian $\Leftrightarrow$ descending chain condition

Thm: PID $\Rightarrow$ Noetherian.

Proof: Given chain I_n, $I = \bigcup_{n=1}^{\infty} I_n$ is an ideal, so $I = (a)$ then $a \in I_n$ for some n so $I = (a) \subseteq I_k$, $k \geq n$

In a Noetherian ring, all ideals are finitely generated

Every element in a UFD can be factored into irreducibles, unique up to associates.

a, b associates $\Leftrightarrow$ $a = ub$ for some unit u

Thm. R is ID, $p(x), q(x) \in R[x]$ and nonzero, then
a) $\deg pq = \deg p + \deg q$ (look at leading terms)
b) $R[x]$ is ID
c) $R[x]$ units are just units of R

R PID $\not\Rightarrow$ $R[x]$ PID

Thm: F field $\Rightarrow$ $F[x]$ is ED
Proof idea: polynomial division, Given $a(x), b(x) \in F[x]$, $\exists$ unique $q(x), r(x)$ st $a(x) = q(x)b(x) + r(x)$ where $r(x) = 0$ or $\deg r < \deg b$. Field property used when scaling $b(x)$ to cancel leading $a(x)$ term.
Uniqueness follows: $a = qb + r = q'b + r' \Rightarrow r(x) - r'(x) = b(x)[q'(x) - q(x)]$ but $\deg (r - r') < \deg b + \deg (q' - q)$ so both sides are 0.

Thm: ED $\Rightarrow$ PID
Idea: Ideal gen by its norm-minimal element d.
Euclidean alg produces gcd

When can polynomials be factored?

$x^2 + 1$ not reducible in $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$
but is reducible in $\mathbb{C}[x]$ $(x-i)(x+i)$ and $\mathbb{Z}/2\mathbb{Z}[x]$ $(x+1)^2$

$R[x]$ PID $\Rightarrow$ R field
Proof: $R \subset R[x]$ is an int dom b/c $R[x]$ is PID. (x) is prime b/c $R[x]/(x) \cong R$ is ID so (x) is max'l so $R[x]/(x) \cong R$ is field.

Thm: In a UFD, nonzero prime $\Leftrightarrow$ irreducible
Proof: ($\Rightarrow$) true in any integral domain. Say p prime. If $p=ab$ then $p|a$ or $p|b$. WLOG $p|a$, then $a=pc$ and $p=pcb$ so $1=cb$ and b is a unit.
($\Leftarrow$) Suppose irred. p divides ab. Then $ab=pc$ for some c. Since we are in a UFD, $ab=(pu)\cdot p_2 \cdots p_k$ where u unit. Note that a,b also factor uniquely, so p must associate to some factor of a or b. If a then $p|a$.

Ex: x^2-5x+6 in $\mathbb{Z}[x]$ reducible? Yes. $(x-3)(x-2)$
It should also be reducible mod 4 $\quad (x+1)(x+2)$
Note: Exists natural projection $\varphi: \mathbb{Z}[x] \to \mathbb{Z}/4\mathbb{Z}[x]$, $a(x) \mapsto \overline{a(x)}$

Thm: I ideal in R. Let (I) = ideal gen by I in $R[x] = I[x]$
Then $R[x]/(I) \cong R/I[x]$. Also if I prime in R, then (I) is prime in $R[x]$

Proof: Use homomorphism $\varphi: R[x] \to \frac{R}{I}[x]$. Notice $\ker\varphi = (I)$. This shows the first part. I prime in $R \Rightarrow R/I$ is ID $\Rightarrow \frac{R}{I}[x]$ is ID $\Rightarrow R[x]/(I)$ is ID $\Rightarrow (I)$ is prime.

Given $p(x) \in R[x]$, how does reducibility in $R[x]$ relate to reducibility in $F[x]$ where F = field of fractions of R

Gauss' Lemma
R is a UFD with field of fractions F. Say $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$

In fact, $p(x) = A(x)B(x)$ where $A(x), B(x) \in F[x]$ are nonconst polys $\Rightarrow$ $p(x) = a(x)b(x)$ in $R[x]$ where $rA(x) = a(x)$, $sB(x) = b(x)$ for some $r,s \neq 0$ in F.

Note: converse not true $3x = 3 \cdot x$ reducible in $\mathbb{Z}[x]$ but not in $\mathbb{Q}[x]$

Proof: Given $p(x) = A(x)B(x)$ where coeffs are fractions (quotients of elements in R) Then, $d \cdot p(x) = a'(x)b'(x)$ where d is the common denominator and coeffs are in R. If d is unit, set $a(x) = \frac{1}{d}a'(x)$ and $b(x) = b'(x)$. If d is not a unit, it can be factored b/c UFD so $d = p_1 \cdots p_n$ product of irreducibles. If p_1 irred $\Rightarrow p_1$ prime $\Rightarrow (p_1)$ prime in $R[x]$ $\Rightarrow R[x]/(p_1) \cong R/p_1R[x]$ is ID. We reduce $d \cdot p(x) = a'(x)b'(x)$ mod p_1 to get $0 = \overline{a'(x)}\,\overline{b'(x)}$. Since we are in ID, WLOG, $\overline{a'(x)} = 0 \Rightarrow$ all coeffs of $a'(x)$ are divisible by $p_1 \Rightarrow \frac{1}{p_1}a'(x)$ has coeffs in R. Do the same for each p_k, can associate to either $a'(x)$ or $b'(x)$.

Corollary: If gcd of coeffs of $p(x)$ is 1, $p(x)$ irred in $F[x] \Leftrightarrow p(x)$ irred. in $R[x]$. In particular if $p(x)$ is monic, or the leading coeff is 1, this condition is satisfied).

Proof: ($\Leftarrow$) by Gauss' lemma

($\Rightarrow$) $p(x)$ red. in $R[x] \Rightarrow p(x) = a(x)b(x)$. gcd condition means neither are nonconstant polynomials so reducible in $F[x]$

Thm: R UFD $\Leftrightarrow$ $R[x]$ UFD

Proof: ($\Leftarrow$) easy

($\Rightarrow$) Say $p(x) \in R[x]$. Let d = gcd of coeff of $p(x)$. Then, $p(x) = d \cdot p'(x)$. Since d can be uniquely factored, enough to show $p'(x)$ factors uniquely. $p(x)$ factors in $R[x] \subseteq F[x]$. Say $p(x) = A(x)B(x)$. Gauss' lemma pf $\Rightarrow \exists$ factorization of $p(x)$ in $R[x]$ whose factors are F-multiples of $A(x)$, $B(x)$. Since gcd of coeffs of $p(x)=1$, then gcd coeffs of $a(x), b(x)$ are too. By previous cor., each must be irred. in $R[x]$ so $p(x)$ factors. Now we prove uniqueness. Say $p(x) = q_1(x) \dots q_r(x) = q_1'(x) \dots q_s'(x)$ in $R[x]$. gcd cond on p. By cor. each $q_i(x), q_i'(x)$ is irred in $F[x]$. UFD in $F[x] \Rightarrow q_i(x)$ associates to $q_i'(x)$ in $F[x]$. Suppose $q_i(x) = \frac{a}{b} q_i'(x) \Rightarrow b\, q_i(x) = a\, q_i'(x)$ so $a = ub$ for some unit u, so $q_i(x) = a q_i'(x)$ are associates.

How to test for irreducibility of a polynomial?
- Look for linear factors

Thm: $p(x) \in F[x]$. $p(x)$ has <u>factor</u> of deg $1 \Leftrightarrow p(x)$ has <u>root</u> in F

Proof: ($\Rightarrow$) If $p(x) = q(x)(ax+b)$, then $p(-\frac{b}{a}) = 0$ and $-\frac{b}{a}$ is a root

($\Leftarrow$) If $p(\alpha) = 0$, then consider $p(x) = q(x)(x-\alpha) + r$ by division algorithm where $\deg r < 1$, ie constant. See for $x = \alpha$, $p(\alpha) = 0 + r = 0$ so $r = 0$.

Cor: A deg 2 or 3 poly over F is reducible $\Leftrightarrow$ it has a root in F

Proof: If low deg, has linear factor.

Root Possibility

Thm: Say $p(x) = a_n x^n + \dots + a_0$ in $R[x]$ UFD. If $\frac{r}{s}$ is a root of $p(x)$ in F and in lowest terms, then $r | a_0$ and $s | a_n$.

Cor: If $p(x)$ is <u>monic</u> ($a_n = 1$) and $\forall$ divisors d of a_0, $p(d) \neq 0$, then $p(x)$ has no roots

Proof: $s^n \cdot p(\frac{r}{s}) = a_n r^n + a_{n-1} r^{n-1} s + \dots + a_0 s^n$ so $s | a_n r^n$. But $s \nmid r$ because it is in lowest terms so $s | a_n$. Similarly, $r | a_0 s^n$ which implies $r | a_0$

Ex: x^3-5x+7 irred in $\mathbb{Z}[x]$? $\overset{\text{gcd coeff } 1}{\Longleftrightarrow}$ irred in $\mathbb{Q}[x]$
If red, must have linear factor, so must have root in $\mathbb{Q}$. Possibilities: $\pm 1, \pm 7$. Check:
$7^3+35+7 \neq 0$ $(-7)^3-35+7 \neq 0$ $1^3-5+7 \neq 0$ $(-1)^3+5+7 \neq 0$
x^3-5x+7 irred

Ex: x^3+x+1 in $\mathbb{Z}_2[x]$ is irred. b/c low degree, check 0, 1.
See that $p(0)=1$, $p(1)=1^3+1+1=1$

Ex: x^4+x^2+1 in $\mathbb{Z}_2[x]$ $p(0)=1$, $p(1)=1$ but $p(x)=(x^2+x+1)^2$

Reduction Mod I
Thm: I proper ideal in ID R. $p(x)$ nonconstant monic in $R[x]$. Let $\varphi: R[x] \to R/I[x]$ the reduction homomorphism mod I. If $\varphi(p(x))$ cannot be factored in $R/I[x]$, then $p(x)$ is irred in $R[x]$.

Proof idea: If $p(x)=a(x)b(x)$ in $R[x]$ then $\overline{p(x)}=\overline{a(x)}\,\overline{b(x)}$ in $R/I[x]$. $a(x), b(x)$ leading coeffs are units so can take to be monic.

Ex. x^3+x+1 irred in $\mathbb{Z}[x]$ b/c irred in $\mathbb{Z}_2[x]$

Ex. x^3-x^2+x+1 irred in $\mathbb{Z}[x]$? Consider $\mathbb{Z}_3[x]$. In $\mathbb{Z}_3[x]$, $p(0)=1$, $p(1)=2$, $p(2)=1$, so $p(x)$ irred in $\mathbb{Z}_3[x]$ and $\mathbb{Z}[x]$

Ex. $x^4-72x+4$ irred in $\mathbb{Z}[x]$ but red mod every integer

Cor: (Eisenstein Criterion) P prime ideal in R. $f(x)=x^n+a_{n-1}x^{n-1}+\dots+a_0$ poly in $R[x]$, $n \geq 1$. Then if $a_0, \dots, a_{n-1} \in P$ but $a_0 \notin P^2$ then $f(x)$ irred in $R[x]$

Cor: If p prime in $\mathbb{Z}$, $p \mid a_i$, $p^2 \nmid a_0$, then $f(x)$ irred in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Ex: $f(x) = x^5 - 3x^3 + 15x - 21$ is irred (use $p=3$)

Ex: $f(x) = x^n - a$, where a prime, then irred (use $p=a$)

Ex: $f(x) = x^4+1$, look at $g(x) = f(x+1) = (x+1)^4 + 1 = x^4+4x^3+6x^2+4x+2$ (use $p=2$) so irred

Proof: If $f(x)$ reducible, $f(x) = a(x)b(x)$, $a(x), b(x)$ are monic. See mod P, $\overline{f(x)} = \overline{a(x)}\,\overline{b(x)} = x^n$ in $R/P[x]$ and $\overline{a(x)} = x^r + a_{r-1}x^{r-1} + \dots + a_0$, $\overline{b(x)} = x^s + \dots + a_0$. We claim all $a_i, b_i = 0$. Let i be smallest index st $a_i \neq 0$ in R/P and j smallest index st $a_j \neq 0$. Then, product has nonzero coeffs for x^{i+j} but $i+j \neq n$. So product $\neq x^n$

Let $f(x) = x^2+x+1 \in \mathbb{Z}/2\mathbb{Z}[x]$. Since $f(0) = f(1) = 0$, $f(x)$ is irreducible. Let $F = \mathbb{Z}/2\mathbb{Z}[x]/(x^2+x+1)$ be a field. The elements are $\{0, 1, x, x+1\}$. This field extends $\mathbb{Z}/2\mathbb{Z}$. This

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$f(x)$ has no root in $\mathbb{Z}/2\mathbb{Z}$, but it does in the extension, namely x and $x+1$.

Say F is a field. Recall $\mathrm{char}(F)$ = smallest n st $1+1+1+\dots+1 = 0$ where 1 is added to itself n times. It equals 0 if no such n exists. Note that $\mathrm{char}(F)$ is always prime or zero or it would have zero divisors. The prime subfield of F is generated by 1_F, and is either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$.

If field K contains F, call K an extension (field) of F. We say "K over F" and write K/F or $\frac{K}{F}$. F is called the base field of the extension.

Notice: K is a vector space over F, e.g. $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$

Ex: $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \,;\, a, b \in \mathbb{Q}\}$ has dimension 2 as a vector space over $\mathbb{Q}$.

Ex: $\mathbb{Q}(5^{1/3}) = \{a + b \cdot 5^{1/3} + c \cdot 5^{2/3} \mid a, b, c \in \mathbb{Q}\}$ (3 dimensions)

Def: The <u>degree</u> or <u>index</u> of K/F is the <u>dimension</u> of K as a vector space over F. We write $[K:F]$. If $[K:F]$ finite, we say <u>extension is finite</u> (otherwise infinite)

Ex: $[\mathbb{C}:\mathbb{R}] = 2$, $[\mathbb{Q}(5^{1/3}):\mathbb{Q}] = 3$

Suppose $p(x) \in F[x]$ doesn't have root in F. Does it have a root in some extension? Yes!

Thm [Kronecker, 1887]: Say F field, $p(x)$ irred in $F[x]$. Exists extension K of F in which $p(x)$ has a root.

Proof: $K = F[x]/(p(x))$ is a field. Let $\pi: F[x] \to F[x]/(p(x))$ be the map to the quotient. Notice $\pi|_F : F \to K$ not 0 b/c $\pi(1_F) = 1_K$. So it must be 1-to-1 bc $\ker(\pi)|_F$ is ideal & fields have only trivial ideals. Identify F with $\pi(F)$, then F is a subfield of K. Let $\bar{x} = \pi(x)$. Then $p(\bar{x}) = p(\pi(x)) = \pi(p(x))$ bc π is homomorphism $= \overline{p(x)} = 0$.

Modding out by irred is a great way to construct field extensions.

Ex: $\mathbb{Q}[x]/(x-3) \cong \mathbb{Q}$

Ex: $p(x) \in F[x]$ deg n & irred. If $K = F[x]/(p(x))$ then $[K:F] = n$, and <u>basis</u> for K/F is $\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}$, and $K \cong \{a_{n-1}x^{n-1} + \ldots + a_0 \mid a_i \in F\}$. The field structure depends on $p(x)$.

Def: K/F extension, $\alpha \in K$. Then $F(\alpha)$ = <u>unique minimal subfield</u> of K containing F and α. (exists bc $\cap$ fields is field). $F(\alpha, \beta, \ldots)$ is similiar defined but containing $F, \alpha, \beta, \ldots$ It can be thought of as field gen by $\alpha, \beta, \ldots$ If it's generated by one element $F(\alpha)$, it is a <u>simple</u> extension and α is the <u>primitive</u> element

Thm: F field, $p(x)$ irred in $F[x]$. If K/F contains a root α of $p(x)$. Let $F(\alpha)$ = subfield gen by α. Then $F(\alpha) \cong F[x]/(p(x))$.

Proof: Let $\varphi: F[x] \to F(\alpha) \subseteq K$ st $x \mapsto \alpha$ (the evaluation map) Since $\varphi(p(x)) = 0$, there's induced homomorphism $\varphi_*: F[x]/(p(x)) \to F(\alpha)$ that sends $a(x)p(x) + r(x) \mapsto r(\alpha)$. Note φ_* is a field homomorphism, nonzero, so injective. But φ_* is surjective bc $im(\varphi_*)$ is subfield of K containing F & α so φ_* is the desired isomorphism.

Ex: Roots of $x^3 - 2$ in $\mathbb{Q}[x]$: ω_1 (real), ω_2, ω_3 (complex)
$\mathbb{Q}(\omega_1) \cong \mathbb{Q}(\omega_2) \cong \mathbb{Q}(\omega_3)$ where $\mathbb{Q}(\omega_1)$ subfield of $\mathbb{R}$ and $\mathbb{Q}(\omega_2)$ and $\mathbb{Q}(\omega_3)$ subfields of $\mathbb{C}$

Recall: F field, $p(x)$ irred poly in $F[x]$, if K/F contains root α of $p(x)$, then $F(\alpha) \cong F[x]/(p(x))$

Ex: $p(x) = x^2 - 5$ $F = \mathbb{Q}$, $K = \mathbb{R} \Rightarrow \mathbb{Q}(-\sqrt{5}) \cong \mathbb{Q}(\sqrt{5}) \cong \mathbb{Q}[x]/(x^2-5)$
$\varphi = \mathbb{Q}(-\sqrt{5}) \to \mathbb{Q}(\sqrt{5})$, $a - b\sqrt{5} \mapsto a + b\sqrt{5}$

Ex: $p(x) = x^3 - 1$ (not irred in $\mathbb{Q}[x]$) roots $1, \omega_2, \omega_3$
$\mathbb{Q}(1) \cong \mathbb{Q}$ $\quad \mathbb{Q}(\omega_2) \cong \mathbb{Q}(\omega_3)$ $\quad x^3 - 1 = (x-1)(x^2+x+1)$

Thm: Say $\varphi : F \xrightarrow{\sim} F'$ isomorphism of fields. $\exists$ ring homo. $\varphi : F[x] \to F'[x]$, if irred $p(x) \in F[x]$, let $p'(x) = \varphi(p(x))$ where we replace F coeffs by F' coeffs, then $\exists$ isom. $\sigma : F(\alpha) \xrightarrow{\sim} F'(\beta)$ that maps $\alpha \mapsto \beta$ and extends φ, where α root $p(x)$ in ext. of F and β root $p'(x)$ in ext. of F'

Proof: $(p(x))$ max'l in $F[x] \xrightarrow{\varphi} (p'(x))$ max'l in $F'[x]$ (Ideal structure preserved by isom). $F(\alpha) \cong F[x]/(p(x)) \cong F'[x]/(p'(x)) \cong F'(\beta)$

Def: α is <u>algebraic</u> over F if α is the root of some nonzero polynomial $f(x) \in F[x]$.

Def: An extension K/F is <u>algebraic</u> if every element of K is algebraic over F

Ex: $\sqrt{6}$ is algebraic over $\mathbb{Q}$ (root of x^2-6)

Thm: If α is alg/F and L/F, then α alg/L
pf: $f(x) \in F[x] \subseteq L[x]$

Ex: $\sqrt{6}$ alg/$\mathbb{Q}$ $\Rightarrow$ $\sqrt{6}$ alg/$\mathbb{Q}(\sqrt{2})$

If $\alpha \in K/F$ & α alg/F, then consider $\varphi_\alpha : F[x] \to K$, $f(x) \mapsto f(\alpha)$ (evaluation map) [Note: φ_α not 1-1 $\Leftrightarrow$ α is alg/F] So α alg/F $\Rightarrow$ $\ker \varphi_\alpha$ is nonzero ideal in $F[x]$ so $\ker \varphi_\alpha = (m_{\alpha,F})$, where $m_{\alpha,F}$ called <u>minimal polynomial</u>. $m_{\alpha,F}$ unique up to units, so if you require $m_{\alpha,F}$ monic, it is unique. Also $m_{\alpha,F}$ is irred in $F[x]$ else $m_{\alpha,F}(x) = a(x)b(x)$. Plug α, $m_{\alpha,F}(\alpha) = 0 = a(\alpha)b(\alpha)$. WLOG $a(\alpha) = 0$ so a has root α so $a(x) = c(x)\cdot m_{\alpha,F}(x) \Rightarrow b(x)c(x) = 1$ so b is unit, a contradiction.

This shows thm: α alg/F, $\exists$ unique monic irred poly $m_{\alpha,F}(x) \in F[x]$ with α as root. Therefore, any $f(x) \in F[x]$ has α as root $\Leftrightarrow m_{\alpha,F}(x) \mid f(x)$ in $F[x]$

Ex: x^3-1 has roots $1, \omega_2, \omega_3$, min poly $(x-1)$ and (x^2+x+1)

Def: The <u>degree</u> of α is degree of min poly

Ex: $\sqrt{6}$ alg/$\mathbb{Q} \Rightarrow m_{\alpha,\mathbb{Q}}(x) = x^2-6 \Rightarrow \deg \alpha = 2$

Cor: If L/F and α alg/F then $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$ in $L[x]$

Ex: $\sqrt{6}$ alg/$\mathbb{Q} \Rightarrow \sqrt{6}$ alg/$\mathbb{Q}(\sqrt{6})$, $m_{\sqrt{6},\mathbb{Q}} = x^2-6$, $m_{\sqrt{6},\mathbb{Q}(\sqrt{6})} = x-\sqrt{6}$, $m_{\sqrt{6},\mathbb{Q}(\sqrt{6})} \mid m_{\sqrt{6},\mathbb{Q}}$

Prop: α alg/F, then $F(\alpha) \cong F[x]/(m_\alpha(x))$ and $\deg \alpha = [F(\alpha):F]$
Proof: m_α irred & has α as root. Use previous thms.

Prop: α alg/F $\Leftrightarrow F(\alpha)/F$ is <u>finite extension</u>. In fact, α satisfies poly deg $n \Rightarrow [F(\alpha):F] \le n$ and $\alpha \in K/F$, $[K:F] = n \Rightarrow \deg \alpha \le n$

Proof: $(\Rightarrow)$ α alg/F $\Rightarrow [F(\alpha):F] = \deg \alpha = \deg m_\alpha \le n$ because m_α divides poly that made α algebraic.
$(\Leftarrow)$ Say $[K:F] = n \Rightarrow 1, \alpha, \alpha^2, \ldots, \alpha^n$ must be linearly independent $\Rightarrow \exists$ coeffs b_i not all 0 st $b_0 + b_1\alpha + \ldots + b_n\alpha^n = 0 \Rightarrow$ α root of poly

Cor: K/F is finite $\Rightarrow K/F$ is algebraic

Pf: $\forall \alpha \in K$, $F(\alpha)$ subfield of $K \Rightarrow [F(\alpha):F] \le [K:F]$ so $[F(\alpha):F]$ finite $\Rightarrow \alpha$ algebraic

Note: converse is not true: $\overline{\mathbb{Q}} = \{$all elts of $\mathbb{C}$ alg/$\mathbb{Q}\}$ (the algebraic #s) has elts of all degrees: $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots$

extension degrees say a lot!

Thm: (Tower Law) $F \subseteq K \subseteq L$ fields, then $[L:F] = [L:K][K:F]$ (if one side infinite, other is infinite)

Proof idea: If L/K has basis $\alpha_1, \dots, \alpha_m$ and K/F has basis $\beta_1, \dots, \beta_n$, then $\{\alpha_i \beta_j\}$ are basis of L/F, size mn.

Recall: Extension K/F, <u>degree</u> is $\dim K$ as vector space over F.
If α is algebraic, $F(\alpha)/F$ extension, has $\deg = \deg m_{\alpha,F}$ (min poly)
Also, $F(\alpha)/F$ finite ext $\Leftrightarrow$ α alg/F and K/F finite extension $\Rightarrow$ extension algebraic

Cor. of Tower Law: $F \subseteq K \subseteq L$ fields, $[K:F] \mid [L:F]$

Is $\sqrt{5}$ in $\mathbb{Q}(\sqrt[3]{5})$?
$[\mathbb{Q}(\sqrt[3]{5}):\mathbb{Q}] = 3$ because min poly is $x^3 - 5$
$[\mathbb{Q}(\sqrt{5}):\mathbb{Q}] = 2$ because min poly is $x^2 - 5$ but $2 \nmid 3$ so no.

Is $x^3 - \sqrt{2}$ irred over $\mathbb{Q}(\sqrt{2})$?
But $\sqrt[6]{2}$ is deg 6 over $\mathbb{Q}$ and $\overbrace{\underbrace{\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})}_{\deg 2} \subset \mathbb{Q}(\sqrt[6]{2})}^{\deg 6}$ so $\sqrt[6]{2}$ must have min poly deg 3, so it must be min poly.

Def: K/F is <u>finitely generated</u> if $K = F(\alpha_1, \dots, \alpha_n)$ where $n \in \mathbb{N}$.

Fact: $F(\alpha, \beta) = (F(\alpha))(\beta)$. $\supseteq$ by min prop of $(F(\alpha))(\beta)$ and $\subseteq$ by min prop of $F(\alpha, \beta)$

Thm: K/F finite $\Leftrightarrow$ $K = F(\alpha_1, \alpha_2, \dots, \alpha_k)$ and α_i alg/F. If $\alpha_1, \dots, \alpha_k$ have degs $n_1, \dots, n_k$ then $F(\alpha_1, \dots, \alpha_k)/F$ has degree $\le n_1 n_2 \cdots n_k$

Proof: ($\Rightarrow$) K/F finite $\Rightarrow$ let $\alpha_1, \ldots, \alpha_n$ be vector space basis for K/F. Then $[F(\alpha_i) : F] \leq [K:F]$ so its finite, hence α_i algebraic.
So $K = F(\alpha_1, \ldots, \alpha_n)$ [Ex: $1, 2^{1/3}, 2^{2/3}$ basis for $\mathbb{Q}(2^{1/3})$] ($\alpha_1, \ldots, \alpha_n$ may be more than needed)
($\Leftarrow$) Assume $K = F(\alpha_1, \ldots, \alpha_n)$. Let $F_i = (\alpha_1, \ldots, \alpha_i)$ so
$F \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_{n-1} \subseteq K$ and $[K:F] = [K:F_{n-1}][F_{n-1}:F_{n-2}] \ldots [F_1 : F]$
$\leq n_k \; n_{k-1} \; n_1$
because F_i/F_{i-1} has deg at most n_i b/c α_i alg/$F \Rightarrow$ alg/F_{i-1}
and $m_{\alpha_i, F} \mid m_{\alpha_i, F_{i-1}}$.

Ex: $[\mathbb{Q}(\underset{\deg 2}{\uparrow i}, \underset{\deg 2}{\uparrow 2i}) : \mathbb{Q}] \leq 4$ (but it's really 2)
x^2+1 $\quad$ x^2+4

Ex: $[\mathbb{Q}(\underset{\deg 2}{\uparrow \sqrt{3}}, \underset{\deg 2}{\uparrow \sqrt{5}}) : \mathbb{Q}] \leq 4$
x^2-3 $\quad$ x^2-5

Cor: α, β alg/$F \Rightarrow \alpha \pm \beta$, $\alpha\beta$, α/β alg/F (for $\beta \neq 0$ in α/β)
Proof: all are elements of $F(\alpha, \beta)$, which is finite ext so $F(\alpha,\beta)$ alg ext of F_i since α, β algebraic.

Cor: All alg elements of L/F form subfield of L.

Ex: $\overline{\mathbb{Q}} = \{$alg elts of $\mathbb{R}/\mathbb{Q}\}$ is algebraic extension but not finite. $\overline{\mathbb{Q}}$ countable, $\mathbb{R}$ not so $\exists$ transcendentals

Def: K_1, K_2 subfield of K. Let K_1K_2 be the <u>composite field</u>, the smallest field containing both.

Prop: For finite extensions $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$ (= when basis for one is indep over the other)
Proof: α_i, b_j bases for $K_1, K_2 \Rightarrow \alpha_i b_j$ span K_1K_2/F

So
$$\begin{tikzcd} & K_1K_2 \arrow[dl, dash, "\le m"'] \arrow[dr, dash, "\le n"] & \\ K_1 \arrow[dr, dash, "n"'] & & K_2 \arrow[dl, dash, "m"] \\ & F & \end{tikzcd}$$
Note: If m, n rel prime then must have equality.

Def: Elts of $\mathbb{R}$ are <u>constructable</u> if length possible with straightedge and compass. (call it K_{con})

We saw $a, b \in K \Rightarrow a+b, ab, a/b \in K$ so K field. K contains $\mathbb{Q}$ since $1 \in K$, but also more. $x, y \in K \Rightarrow (x,y)$ is constructable in $\mathbb{R}^2$.

Operations: ① intersect lines
② intersect line + circle
③ intersect circles

Let $F_0 = \mathbb{Q}$ and F_k = constructable #'s using ①, ②, ③ in sequence of k operations on (x,y), $x, y \in F_0$ so $K_{con} = \bigcup_{k=0}^{\infty} F_k$ and $F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots$

① $\cap$ (lines): solve $ax+by+c=0$, $dx+ey+f=0$, $a, \ldots, f \in F_k \Rightarrow x, y \in F_k$
② line $\cap$ circle: solve $ax+by+c=0$, $(x-d)^2+(y-e)^2=f^2$, $a, \ldots, f \in F_k \Rightarrow x, y$ at worst in <u>quadratic extension</u> (adjoining with deg 2 elt) of F_k
③ $\cap$ (circles): similar to ②

Notice $[F_k : F_{k-1}] = 1$ or 2 so deg $[F_k : F_0]$ = power of $2 \Rightarrow$ any $\alpha \in K_{con}$ is in some F_k so deg $\alpha \mid [F_k : F]$ so deg α = power of 2

Ⓘ doubling cube (volume) $\longleftrightarrow$ construct $\sqrt[3]{2}$ (deg 3) so impossible
Ⓘⓘ trisecting angle $\longleftrightarrow$ given $\cos\theta$ construct $\cos\frac{\theta}{3}$ (Note: $\cos\theta$ constr $\longleftrightarrow$ angle θ constructable) But $\cos\theta = 4\cos^3(\frac{\theta}{3}) - 3\cos(\frac{\theta}{3})$. If $\theta = 60^\circ$, $\alpha = \cos 20^\circ$ satisfies $\frac{1}{2} = 4\alpha^3 - 3\alpha$ or $8\alpha^3 - 6\alpha - 1 = 0$. If $\gamma = 2\alpha$, $\gamma^3 - 3\gamma - 1 = 0$ (irred) then $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 3$ (Note: with ruler & compass, possible!)

(III) squaring the circle (given ○, make □ same area) $\leftrightarrow$ π constr.
FACT: $[\mathbb{Q}(\pi):\mathbb{Q}] = \infty$, not algebraic!

Splitting Fields
If $f(x) \in F[x]$, we've seen $\exists$ field K/F in which f has a root.
Question: Is there field in which all roots live?
Ex: $x^3 - 5 \in \mathbb{Q}[x]$ has root $\sqrt[3]{5} \in \mathbb{Q}(\sqrt[3]{5})$ but this does not contain other complex roots.

Def: K/F is splitting field for $f(x) \in F[x]$ if $f(x)$ factors ("splits") into linear factors in $K[x]$ & does not split in any subfield of K containing F ("smallest extension over which f splits, K has all roots of F")

Ex: Splitting field of $x^3 - 5$ over $\mathbb{Q}$?
other roots $\sqrt[3]{5}\left(\frac{-1 \pm i\sqrt{3}}{2}\right)$. $\mathbb{Q}(\sqrt[3]{5}, \sqrt{3}i)$ (degree/$\mathbb{Q}$ is $6 = 3!$)

Ex: $f(x) = x^6 - 1$ in $\mathbb{Q}[x]$. Find splitting field.
$f(x) = (x-1)(x^2+x+1)(x+1)(x^2-x+1)$. If ω is root of x^2+x+1 then $f(x) = (x-1)(x-\omega)(x-\omega^2)(x+1)(x+\omega)(x+\omega^2)$ so $\mathbb{Q}(\omega)$ is splitting field/$\mathbb{Q}$. $[\mathbb{Q}(\omega):\mathbb{Q}] = 2$

Ex: $f(x) = x^6 + 1$ in $\mathbb{Q}[x]$.
roots in $\mathbb{C}$, $i, i\omega, i\omega^2, -i, -i\omega, -i\omega^2$ so $\mathbb{Q}(i, \omega)$ is splitting field/$\mathbb{Q}$ for f. $[\mathbb{Q}(i,\omega):\mathbb{Q}] = 4$

Thm: Any $f(x) \in F[x]$ has splitting field K/F for f with $[K:F] \leq (\deg f)!$

Proof: Induction on $n = \deg f$. Base case $n = 0$ or 1, take $K = F$. If $n > 1$: if f splits in F, let $K = F$. Else, say $p(x)$ is irred factor, $\deg p \geq 2$. Recall $\exists$ extension L in which $p(x)$ has root. Over this L, $f(x) = (x-\alpha)h(x)$ (h has deg $n-1$). By IHOP, $\exists\, M/L$ splitting field for h, $\deg \leq (n-1)!$ Take $K = M$, See $[M:F] = [M:L][L:F] \leq n!$

Are splitting fields unique?

Thm: Given $\varphi : F \xrightarrow{\sim} F'$ field isomorphism. Say $f(x) \in F[x]$. Let $f'(x) \in F'[x]$ be corr. poly $\varphi_*(f(x))$. If E is splitting field for f over F & E' splitting field for f' over F', then φ extends to isom $\hat{\varphi} : E \xrightarrow{\sim} E'$.

Proof idea: Recall if α root of irred f, α' root of corr. f', then $\varphi : F \xrightarrow{\sim} F'$ extends to $\hat{\varphi} : F(\alpha) \to F'(\alpha')$. We induct on deg f & use this. Factor f, f' into irreds, say α, α' roots of corr irred factors of f, f'. Write $f(x) = (x-\alpha) f_1(x)$ in $F(\alpha)$, $f'(x) = (x-\alpha') f_1'(x)$ in $F'(\alpha')$. E is a splitting field for f_1 over $F(\alpha)$ and E' split. field for f_1' over $F'(\alpha')$ because f_1 splits in E, but if it split in smaller field, so would f. By ind. hyp, $E \cong E'$ via some $\hat{\varphi}$.

Cor: Using $\varphi = id$, any 2 splitting fields for $f(x) \in F[x]$ are isomorphic.

Is there an extension of F over which any poly splits? Some sort of maximal algebraic extension.

Def: Let F be field. $\overline{F}$ is an <u>algebraic closure</u> of F if
1. $\overline{F}$ is alg/F
2. every $f(x) \in F[x]$ splits completely in $\overline{F}$

($\overline{F}$ contains all alg elts of F)

Ex: $\mathbb{C}$ is ~~not~~ an alg closure for $\mathbb{Q}$ (doesn't satisfy 1)

Def: K is <u>algebraically closed</u> if every poly $f(x) \in K[x]$ has a root in K

K alg closed $\Leftrightarrow \overline{K} = K$

why? b/c all alg elts/K live in K

Thm: $\overline{F}$ is alg closure of $F \Rightarrow \overline{F}$ is alg closed

Proof: Say $f \in \overline{F}[x]$ has root α. Wts $\alpha \in \overline{F}$. Then $\overline{F}(\alpha)$ is alg ext / $\overline{F}$. But $\overline{F}$ alg/F so $\overline{F}(\alpha)$ alg/$F \Rightarrow \alpha$ alg/F $\Rightarrow \alpha \in \overline{F}$. So $\overline{F}$ alg closed.

Thm: For any field F, $\exists K$ alg closed & $K \supseteq F$.

Proof: $\forall$ non-constant monic poly $f \in F[x]$, let x_f be an indeterminate. Consider $F[\ldots, x_f, \ldots]$, a union of poly rings in finite # vars, gen by x_f vars. Let I = ideal gen by polys: $f(x_f)$. Say $\alpha(x) = \pi x^2 - 2x$, $\alpha(x_\alpha) = \pi x_\alpha^2 - 2x_\alpha$. Claim, I is proper. Pf claim: If not, $\exists$ relation in $F[\ldots, x_f, \ldots]$: $g_1 f_1(x_{f_1}) + \ldots + g_n f_n(x_{f_n}) = 1$, $g_i \in F[\ldots, x_f, \ldots]$ and g_i involve only finitely many vars. $\exists$ finite extension F'/F st each f_i has root α_i in F'/F. Then set $x_{f_i} = \alpha_i$ and all other indets $= 0$, get $0 = 1$ contradiction. Claim: $I \subseteq$ some M max'l ideal (Zorn's lemma). Let $K_1 = F[\ldots, x_f, \ldots]/M$ all polys f in $F[x]$ have root in K_1. Let K_2 = same construction using K_1 so all polys in $K_1[x]$ have root in K_2. $F \subseteq K_1 \subseteq K_2 \subseteq \ldots$. Take $K = \bigcup_{j=1}^{\infty} K_j$ is field, any poly in $K[x]$ is in some $K_i[x]$, has root in $K_{i+1}[x] \subseteq K[x]$ so K is algebraically closed.

Thm: K alg closed, $F \subseteq K \Rightarrow \exists$ collection $\overline{F}$ of alg elts/F & this alg closure of F

Separable Extensions

Recall: Given any field F, $\exists K$ alg closed & $K \supseteq F$.

Thm: If K alg closed, $F \subseteq K$ then $\overline{F}$, the collection of algebraic elts$/F$ is an algebraic closure of F.

Pf: $\overline{F}$ is alg$/F$ by def'n & any poly $f(x)$ in $F[x]$ splits completely in K, into factors like $(x-\alpha)$. But each root α is alg$/F$ so $\alpha \in \overline{F}$.

Fact: Alg closures are unique up to isomorphism.
Pf idea: Follows from uniqueness of splitting fields

Ex: $\mathbb{Q} \subseteq \mathbb{C}$ alg closed $\Rightarrow \overline{\mathbb{Q}}$ is alg closure of $\mathbb{Q}$

Def: $f(x) \in F[x]$ is <u>separable</u> if all its roots are distinct in its splitting field (else <u>inseparable</u>)

Ex: in $\mathbb{Q}[x]$: x^2-5 is sep'ble (roots in $\mathbb{Q}(\sqrt{5})$)
x^2+1 sep'ble (roots in $\mathbb{Q}(i)$)
x^2-2x+1 insep'ble $(x-1)^2$
in $\mathbb{F}_2[x]$: x^2+1 insep'ble $(x+1)^2$

Given $f(x) \in F[x]$, define $D_x f(x) \in F[x]$ to be "usual derivative wrt x": if $f(x) = a_n x^n + \dots + a_0$ define $D_x f(x) = n a_n x^{n-1} + \dots + a_1$. (verify sum, product rules hold)

Ex: $f(x) = x^2+1 \Rightarrow D_x f(x) = 2x$

Thm: $f(x)$ has a repeated root α (in its splitting field) $\Leftrightarrow$ α is a root of f and $D_x f$.
Proof idea: product rule

This means $f, D_x f$ divisible by $m_{\alpha,F}$

Ex: f has root i in $\mathbb{Q}(i)$, but $D_x f(i) \neq 0$ where $f = x^2+1$
f has root 1 in $\mathbb{F}_2$ and $D_x f(1) = 2 \cdot 1 = 0$ in $\mathbb{F}_2$

Cor: Every irred poly over characteristic 0 field F is separable. Any poly/F is separable $\Leftrightarrow$ it's product of distinct irreducibles

Pf: If $p(x)$ irred in $F[x]$, deg n. Then $D_x p(x)$ has lower degree $n-1$ (bc char 0). Any root α of $p(x)$ has min poly $p(x)$, since $p(x)$ smallest poly w/ α root. But $p(x) \nmid D_x p(x)$ of deg $n-1$. Second claim: note distinct irreducibles can't have common roots (if both had root α, then $m_{\alpha,F} \mid$ both ireds)

What about polys over field of char p?
Above: $p(x)$ could divide $D_x p$ if $D_x p(x) = 0$. But then $p(x)$ has terms of form $(x^p)^k$, i.e, $p(x) = q(x^p)$ a poly in x^p

Fact: If $\text{char}(F) = p$, then $\forall a, b \in F$, $(a+b)^p = a^p + b^p$ (freshman's dream) and $(ab)^p = a^p + b^p$. Then $\varphi(a) = a^p$ is an injective field homomorphism $\varphi : F \to F$ (the Frobenius endomorphism of F) If F finite then φ is isomorphism

Cor: If finite field, char p, then every elt of F is a p-th power, called a perfect field.

Thm: Every irred poly over perfect field is separable. Any poly is separable $\Leftrightarrow$ product of distinct ireds

Pf: Say $q(x)$ irred in $F[x]$. If q not sep'ble, then $D_x q = 0$ so
$$\begin{aligned} p(x) &= a_m x^{pm} + a_{m-1} x^{p(m-1)} + \dots + a_1 x^p + a_0 \\ &= b_m^p x^{pm} + b_{m-1}^p x^{p(m-1)} + \dots + b_1^p x^p + b_0^p \\ &= (b_m x^m)^p + \dots + (b_1 x)^p + b_0^p \\ &= (b_m x^m + \dots + b_1 x + b_0)^p \end{aligned}$$
contradicts irred of q

Ex: Let $K = \mathbb{F}_p(\alpha)$. Can show $x^p - \alpha$ irred & α is not p-th power. Let γ be root of $x^p - \alpha$ in its split field then $(x-\gamma)^p = x^p - \gamma^p = x^p - \alpha$

Def: An extension K/F is <u>separable</u> (over F) if any elt of K is a root of a separable poly in $F[x]$ (else inseparable)

Thus, separable $\Rightarrow$ algebraic

Cor: Any finite extension of perfect field is seperable

Pf: Finite ext are alg, min poly are irred over a perfect field hence separable

Existence & Uniqueness of Finite Fields

A finite field of order p^k exists:

Consider $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$. If α is a root in a splitting field, then $\alpha^{p^n} = \alpha$. If α, β roots, then $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$ so $\alpha + \beta$ also root. Also, $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$ so $\alpha\beta$ is root. Also, $(\alpha^{-1})^{p^n} = \alpha^{-1}$. So, $\mathbb{F} = \{\text{roots of } x^{p^n} - x \text{ over } \mathbb{F}_p\}$ is a field, and must be a subfield of the splitting field of $f(x)$, so it must be the splitting field of $f(x)$. And $[\mathbb{F} : \mathbb{F}_p] = n$ so has p^n elements.

Uniqueness of finite field of order p^n:
If K is field of char p, $[K:\mathbb{F}_p]=n$, we will show $K \cong \mathbb{F}$.
Let $K^\times = \{$nonzero elts of $K\}$, group under $\times$. So $\forall \alpha \in K$, $\alpha \neq 0$
$\alpha^{p^n-1}=1$ or $\forall \alpha \in K, \alpha^{p^n}=\alpha$. So all $\alpha \in K$ are roots of $f(x)$. Thus, $K \subseteq \mathbb{F}$ means $K=\mathbb{F}$, as desired.

Call this field $\mathbb{F}_{p^n}$

Galois Theory: Given poly $f(x) \in F[x]$, roots live in a splitting field K/F, K has automorphisms that fix F (automorphisms form a group G), G permutes the roots of $f(x)$

Ex: $f(x)=x^2+1$ in $\mathbb{Q}(i)$ and conjugation is one such auto'

field structure of $K/F \longleftrightarrow$ group structure of G

Galois motivation: solvability by radicals $\leftrightarrow$ solvability of G

Def: K field, Any isom. $\sigma: K \to K$ is an <u>automorphism</u>. We say $a \mapsto \sigma a$. Let <u>$\mathrm{Aut}(K)$</u> $=\{$all aut's of $K\}$. Say σ <u>fixes</u> a if $\sigma a = a$. Say σ <u>fixes</u> subset F if $\sigma a = a$ for $\forall a \in F$.

Ex: $K=\mathbb{C}$ $\sigma: \mathbb{C} \to \mathbb{C}$ conjugation: $a+bi \mapsto a-bi$. σ fixes $\mathbb{R}$

Prop: The set fixed by σ must be a field. The set fixed by a subset of $\mathrm{Aut}(K)$, called H, must be a field. Called the <u>fixed field</u> of H in K.

Note: Any $\sigma \in \mathrm{Aut}(K)$ must fix the <u>prime subfield</u> of K

Def: $\mathrm{Aut}(K/F)$ = autom. of K that fix F

So $\mathrm{Aut}(K) = \mathrm{Aut}(K/\text{prime subfield})$

Prop: $\mathrm{Aut}(K)$ is a group, $\mathrm{Aut}(K/F)$ a subgroup

So we can associate

$$\text{subfield } F \text{ of } K \xrightarrow{\Gamma} \text{subgroup } \mathrm{Aut}(K/F) \text{ of } \mathrm{Aut}(K)$$
$$\text{the \underline{fixed field} of } H\text{, a subfield of } K \xleftarrow{\Phi} \text{subgroup } H \text{ of } \mathrm{Aut}(K)$$

Q: How do Γ, Φ relate? Are they inverses?

Thm: $\sigma \in \mathrm{Aut}(K/F) \Rightarrow$ any poly that has α as root has $\sigma\alpha$ as root

See $\sigma \in \mathrm{Aut}(K/F)$ permutes the roots of irred polys. We use this idea to find $\mathrm{Aut}(K/F)$

Ex: $\mathrm{Aut}(\mathbb{Q}(i)) = ?$
Any autom. fixes $\mathbb{Q}$, the prime subfield. What does it do to i? Note x^2+1 is min poly of i so autom. is determined since roots of x^2+1 are permuted. Only other root of x^2+1 is $-i$ so for any $\tau \in \mathrm{Aut}(\mathbb{Q}(i))$ either $\tau(i) = i$ or $\tau(i) = -i$. So $\mathrm{Aut}(\mathbb{Q}(i)) = \mathbb{Z}/2\mathbb{Z}$.

$\mathrm{Aut}(K)$ always fixes prime subfield of K b/c $1 \mapsto 1$

Ex: $K = \mathbb{Q}(\sqrt[3]{2})$. $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = ?$
Given $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, τ must permute roots of x^3-2. But roots of x^3-2 are $\sqrt[3]{2}$ and two complex roots, so $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ and not the complex roots (b/c not in $\mathbb{Q}(\sqrt[3]{2})$). Thus, $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ = trivial group. Here, we couldn't get all possible automs we expected.

$H \subseteq \Gamma\Phi(H)$ b/c field fixed by H could be fixed by more automorphisms.

$F \subseteq \Phi\Gamma(F)$ b/c automorphisms fixing F could fix a bigger field

Ex: $K = \mathbb{Q}(\sqrt[3]{2})$ $\quad \mathbb{Q} \xrightarrow{\Gamma} \underset{\text{trivial group}}{\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}))} \xrightarrow{\Phi} \mathbb{Q}(\sqrt[3]{2})$

Not enough autom to make the image of Φ smaller

Ex: $K = \mathbb{Q}(i)$ $\quad \mathbb{Q} \xrightarrow{\Gamma} \underset{\mathbb{Z}/2\mathbb{Z}}{\mathrm{Aut}(\mathbb{Q}(i))} \xrightarrow{\Phi} \mathbb{Q}$

Prop: E split field of $f(x) \in F[x]$. Then $|\mathrm{Aut}(E/F)| \leq [E:F]$. Equality occurs when $f(x)$ is seperable over F

Proof:
$$\begin{array}{rcl} \sigma: E & \xrightarrow{\sim} & E' \\ \tau: F(\alpha) & \longrightarrow & F'(\alpha') \\ \varphi: F & \xrightarrow{\sim} & F' \end{array}$$
Given $\varphi: F \xrightarrow{\sim} F'$, $\varphi(f(x)) = f'(x)$. We know $\exists \sigma$ (earlier thm). How many ways can σ occur? We induct on $[E:F]$. Base case $[E:F]=1$, then $\sigma = \varphi$. If $[E:F]>1$, then $f(x)$ has irred factor $p(x)$ w/ deg >1. Similarly for $f'(x)$ and $p'(x)$. Say α is a root of $p(x)$. Define $\tau: F(\alpha) \to F'(\alpha')$ by restricting σ. We know τ sends roots of $p(x)$ to roots of $p'(x)$. Since $\tau(\alpha)$ determines τ, the # of such τ is at most $\deg p'(x) = [F(\alpha):F]$ and equality if all roots distinct. # ways to extend τ to σ is by inductive hypothesis at most $[E:F(\alpha)]$ with equality if roots of $f(x)$ distinct. So # ways to extend φ to σ is $\leq [E:F]$ with equality if roots of $f(x)$ distinct. Take $F=F'$, $\varphi = id$ for result. (more general version needed for inductive step)

Def: K/F finite ext, call K <u>Galois</u> over F or "K/F is a <u>Galois extension</u>" if $|\mathrm{Aut}(K/F)| = [K:F]$. If so, call $\mathrm{Aut}(K/F)$ the <u>Galois group</u> of K/F. We write $\mathrm{Gal}(K/F)$

Cor: If K is a splitting field of sep poly $f(x) \in F[x]$, then K/F is Galois. (In fact, converse is true)

Def: If $f(x)$ sep over F, then Galois group of its splitting field is called the Galois group of the poly $f(x)$

Ex: $\mathbb{Q}(i)/\mathbb{Q}$ is Galois. b/c $|\mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q})| = [\mathbb{Q}(i):\mathbb{Q}] = 2$

Ex: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois b/c $1 \neq 3$

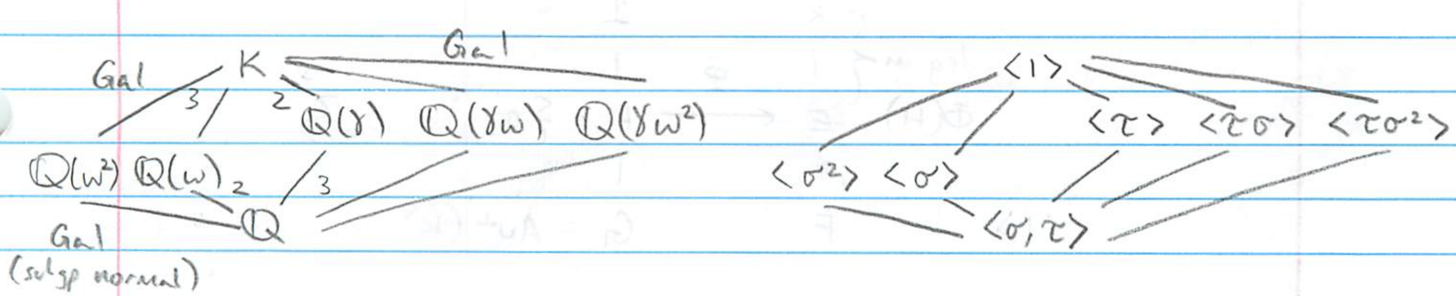
Ex: split field of x^3-2 is $\mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = \frac{1}{2} + \frac{\sqrt{3}}{2} i$, and is Galois ext. In fact, Galois group permutes roots of x^3-2 and is isom to S_3

Fundamental Theorem of Galois Theory
If K/F is Galois and $G = \mathrm{Gal}(K/F)$, then

$$\begin{array}{cccc} & K & & 1 \\ & | & & | \\ \text{subfield} & E & \underset{\Phi}{\overset{\Gamma}{\rightleftarrows}} & H \ \text{subgroup} \\ & | & & | \\ & F & & G \end{array}$$

⓪ Γ, Φ are inverses
① both are inclusion-reversing
② deg of exts = index of subgps
③ K/E Galois w/ $\mathrm{Gal}(K/E) = H$
④ E/F Galois $\Leftrightarrow$ $H \trianglelefteq G$, if so $\mathrm{Gal}(E/F) = G/H$
if not, $\mathrm{Aut}(E/F)$ is H corr. w/ cosets of H in G
⑤ If $E_1 \leftrightarrow H_1$, $E_2 \leftrightarrow H_2$, then $E_1 \cap E_2 \leftrightarrow \langle H_1, H_2 \rangle$ and $E_1E_2 \leftrightarrow H_1 \cap H_2$

Ex: $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$. K is Galois and $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$, generated by σ, τ where $\sigma = \begin{cases} \gamma \mapsto \gamma\omega \\ \omega \mapsto \omega \end{cases}$ $\tau = \begin{cases} \gamma \mapsto \gamma \\ \omega \mapsto \omega^2 \end{cases}$ $(\gamma = \sqrt[3]{2})$
σ has order 3, τ has order 2
See $\sigma(\gamma\omega) = \gamma\omega^2$ $\tau(\gamma\omega) = \gamma\omega^2$



If $\sigma : K \to L$ is non-trivial field homomorphism, we know σ is injective. So $\exists \sigma : K^\times \to L^\times$ (nonzero elts). This is a group homomorphism (mult. as gp op)

Def: L field. A <u>character</u> χ of gp G is a homom: $\chi : G \to L^\times$. Thus, $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$, $\forall g_1, g_2 \in G$

Ex: $G = \mathbb{Z}/5\mathbb{Z}$ $\quad L = \mathbb{C}$ $\quad \chi_1(j) = e^{2\pi i j/5}$ $\quad \chi_m(j) = e^{2\pi i m j/5}$. These are functions on G, can talk about linear dependence.

Automorphisms of fields produce characters

Def: $\chi_1, \ldots, \chi_n$ of G are lin. indep over L if there's no nontriv relation $\forall g \in G$: $a_1\chi_1(g) + \ldots + a_n\chi_n(g) = 0$, not all $a_i = 0$

Thm: Distinct characters of G over L must be linearly independent over L

Proof: Suppose $\exists$ rel'n, use min'l one using smallest # chars: $a_1\chi_1(g) + \ldots + a_m\chi_m(g) = 0$ ①, $\forall g \in G$. Then, $a_1\chi_1(hg) + \ldots a_m\chi_m(hg) = 0$ ②, $\forall h \in G$. So $\chi_1(h)$① $-$ ② $= a_2[\chi_1(h) - \chi_2(h)]\chi_2(g) + \ldots + a_m[\chi_1(h) - \chi_m(h)]\chi_m(g) = 0$ is a rel'n w/ fewer chars, a contradiction. (Choose h so one of the terms $\neq 0$)

Recall: If $\sigma_1, \ldots, \sigma_n$ distinct <u>embeddings</u> (injection into another space) of $K \to L$ then they're <u>linearly independent</u> as <u>characters</u>

Thm: (Degree-Order) If $H \subset \mathrm{Aut}(K)$, then $[K : E] = |H|$

$$\begin{array}{ccccc}
 & K & & & 1 \\
\text{deg } m \left\{ \right. & | & & & | \\
\Phi(H) = & E & \xleftarrow{\ \Phi\ } & & H = \{\sigma_1, \ldots, \sigma_n\} \\
 & | & & & | \\
 & F & & & G = \mathrm{Aut}(K)
\end{array}$$

- example of nonseparable extensions
solvable groups

Proof: Say $m=[K:E]$, $H=\{\sigma_1,\dots,\sigma_n\}$, $|H|=n$. We want to show $m=n$. The idea is if $m<n$, then too many characters and contradict independence. Say $\omega_1,\dots,\omega_m$ basis K/E. Seek $x_1,\dots,x_n \in E$ st $\forall \alpha \in K$, $\sigma_1(\alpha)x_1+\dots+\sigma_n(\alpha)x_n=0$. Write $\alpha=a_1\omega_1+\dots+a_m\omega_m$ for $a_i\in E$. Note $\sigma_i(\alpha)=a_1\sigma_i(\omega_1)+\dots+a_m\sigma_i(\omega_m)$, $\forall i$. So we

① $$[a_1 \dots a_m]\begin{bmatrix}\sigma_1(\omega_1) & \cdots & \sigma_n(\omega_1)\\ \vdots & \ddots & \vdots \\ \sigma_1(\omega_m) & \cdots & \sigma_n(\omega_m)\end{bmatrix}\begin{bmatrix}x_1\\ \vdots \\ x_n\end{bmatrix}=0$$

seek $x_1,\dots,x_n$ st $\forall a_1,\dots,a_m$. But we can find nontrivial x_i b/c $m<n$. Idea is if $m>n$, then too many linearly independent elements. $\exists \alpha_1,\dots,\alpha_{n+1}$ lin indep elts of K (over E). Consider the equation, which has

② $$\begin{bmatrix}\sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_{n+1})\\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_{n+1})\end{bmatrix}\begin{bmatrix}x_1\\ \vdots \\ x_{n+1}\end{bmatrix}=\begin{bmatrix}0\\ \vdots \\ 0\end{bmatrix}$$

no nontrivial sol'n $x_1,\dots,x_{n+1}$ in K (b/c $n<m$). Note at least one $x_i \notin E$, else for $\sigma_1=id$, we would have dep rel'n on α_i's. Choose a sol'n with min'l # non-0 x_i's. Say $x_1,\dots,x_r \neq 0$. We can make $x_r=1$ by scaling by x_r^{-1}. Say $x_1\notin E$, by reordering x's. So our equation ② becomes (look above). But $x_1 \notin E$, $\exists \underline{\sigma} \in H$ st $\underline{\sigma} x_1 \neq x_1$. Then, $\underline{\sigma}$ applied to ② yields a permutation of rows & changes x_i to $\underline{\sigma} x_i$. We subtract rows: ② $-$ $\underline{\sigma}$② to get $\sigma_i(\alpha)[x_1-\underline{\sigma}x_1]+\dots+\sigma_i(\alpha_{r-1})[x_{r-1}-\underline{\sigma}x_{r-1}]$. The x_r term disappeared because $1-1=0$. So we get a smaller solution.

Say K/F is <u>Galois</u> if $|\mathrm{Aut}(K/F)|=[K:F]$

Thm: K/F finite. Then $|\mathrm{Aut}(K/F)|\leq[K:F]$ with equality iff $F=\Phi(\Gamma(F))$

Proof: We know $F\subseteq\Phi(\Gamma(F))\subseteq K$ so $[K:\Phi(\Gamma(F))][\Phi(\Gamma(F)):F]=[K:F]$ but $[K:\Phi(\Gamma(F))]=|\Gamma(F)|=|\mathrm{Aut}(K/F)|$. We know $[\Phi(\Gamma(F)):F]\geq 1$ and it equals 1 iff $F=\Phi(\Gamma(F))$

Thm: H finite subgp $\subseteq \mathrm{Aut}(K)$. Then $\Gamma(\Phi(H)) = H$.
So $K/\Phi(H)$ is <u>Galois</u>.

Proof: $[K:\Phi(H)] = |H| \leq |\Gamma(\Phi(H))| \leq [K:\Phi(H)]$ so
$[K:\Phi(H)] = |H| = |\Gamma(\Phi(H))|$ so $H = \Gamma(\Phi(H))$ and $K/\Phi(H)$ is Galois

Ex: $K = \mathbb{Q}(\sqrt[3]{2})$ $\mathrm{Aut}(K/\mathbb{Q}) = $ trivial. Think about this.

Thm: If $H_1 \neq H_2$ finite subgps of $\mathrm{Aut}(K)$, then $\Phi(H_1) \neq \Phi(H_2)$

Proof: If $\Phi(H_1) = \Phi(H_2)$ then $\Gamma(\Phi(H_1)) = \Gamma(\Phi(H_2)) \Rightarrow H_1 = H_2$ by thm

Thm: K/F Galois $\Leftrightarrow$ K is a splitting field of a separable poly over F.
If so, every poly in $F[x]$ with a root in K is separable & has all its roots in K

Proof: ($\Leftarrow$) Already. ($\Rightarrow$) If K/F Galois, say $p(x)$ irred in $F[x]$ with root $\alpha \in K$. Let $G = \mathrm{Gal}(K/F) = \{\sigma_1 = id, \sigma_2, \sigma_3, \ldots, \sigma_n\}$.
Consider distinct elts of $\{\alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha)\}$ or $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ (called <u>Galois conjugates</u> of α). Let $f(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_r)$. It is separable and fixed by G since G permutes roots, so by thm the coeffs of f must be in the fixed field of G, call it $F = \Phi(G) = \Phi(\Gamma(K/F))$. So $f(x) \in F[x]$. Moreover, $f(x) \mid p(x)$ b/c if α root $p(x)$ then so is $\sigma_i(\alpha)$. But $p(x) \mid f(x)$ b/c if f has α as root, and $p(x)$ irred is min'l poly for α. So $p(x) = f(x)$, so p is separable and all roots in K. Moreover, K/F has basis, say $\{w_i\}$, with $p_i(x)$ their min'l polys. Let $g(x) = \prod p_i(x)$ with repeated factors removed (<u>square-free</u>). The splitting field S of $g(x)$ is K, since $S \subseteq K$ b/c K contains all roots of $g(x)$ but $K \subseteq S$ b/c w_i are roots of $p_i(x)$.

Fundamental Theorem of Galois Theory

Suppose K/F Galois. Then:

① Γ, Φ inverses & inclusion-reversing

② deg ext. = index subgps. $[E:F]=|G:H|$

③ K/E Galois & $Gal(K/E)=H$

what fixes

$$\begin{array}{ccccc} K & & & & 1 \\ | & & & & | \\ \Phi(H)=E & \xrightarrow{\Gamma} & & & H=Aut(K/E) \\ & \xleftarrow[\Phi]{} & & & \\ | & & & & | \\ F & & & & G \end{array}$$

what fixed

Proof: ③ Use previous thm. $K/\Phi(H) = K/E$ is Galois, $\Gamma(\Phi(H))=H$

② Use deg-ord: $K - E$ ← deg $|H|$ $K - F$ ← deg $|G|$

so $[E:F]=\frac{[K:F]}{[K:E]}=|G:H|$

① K/F Galois $\Rightarrow$ K is split. field of some sep f over F

$\Rightarrow K$ —————— " —————— E

$\Rightarrow K/E$ Galois

By previous thms, $\Phi(\Gamma(E))=E$, $\Gamma(\Phi(H))=H$ so Φ, Γ inverses.

Fundamental Theorem of Galois Theory (cont.)

④ E/F Galois $\Leftrightarrow$ $H \trianglelefteq G$. If so, $Gal(E/F)=G/H$

⑤ If $E_1 \leftrightarrow H_1$, $E_2 \leftrightarrow H_2$ then $\left.\begin{array}{l} E_1 \cap E_2 \leftrightarrow \langle H_1, H_2\rangle \\ E_1E_2 \leftrightarrow H_1 \cap H_2 \end{array}\right\}$ "lattices dual"

Ex: $K=\mathbb{Q}(\gamma=\sqrt[3]{2}, \omega)$ $\omega^3=1$

Proof: ④ Idea: we want to count $Aut(E/F)$ or $Emb(E/F)$
$\forall \sigma \in G \Rightarrow$ embedding $\sigma(E) \subseteq K$. Note if H fixes E, then $\sigma H \sigma^{-1}$ fixes $\sigma(E)$. So $\sigma(E)=E \Leftrightarrow \sigma H \sigma^{-1}=H$ by Galois correspondence. Then if above true for all $\sigma \in G$, then see $\sigma \in Aut(E/F) \Leftrightarrow H$ normal. Claim: if $\tau: E \to \overline{F}$ is an embedding (E/F) then $\tau=\sigma|_E$ for some $\sigma \in G$. Claim proof: Note $\tau(E) \subseteq K$, b/c if α is root of $m_\alpha(x)$, then $\tau(\alpha)$ is a root; since K is Galois it will contain all roots. K is split. field of some $f(x)$ (it's Galois) but also split. field of $\tau f(x)=f(x)$ over $\tau(E)$. Earlier thm says can extend τ to $\sigma: K \to K$ & fixes F b/c τ does so every embedding τ $\tau: E \to \tau(E)$ is σ/E for some σ

Idea: know how to count upstairs

Q: How many σ are "lifts" of τ?

A: Say σ, ρ both restrict to τ, so same on E
$\Leftrightarrow \sigma^{-1}\rho = id$ on E so fixes $E \Leftrightarrow \sigma^{-1}\rho \in H \Leftrightarrow \rho \in \sigma H$, a coset of H. So $|Emb(E/F)| = |G:H| = [E:F]$. H normal in $G \Leftrightarrow |Aut(E/F)| = [E:F]$

(5)
$$\begin{array}{ccc} & K & \\ E_1 & & E_2 \\ & F & \end{array} \longrightarrow \begin{array}{ccc} & 1 & \\ H_1 & & H_2 \\ & G & \end{array} \qquad \begin{array}{l} E_1E_2 \longleftrightarrow H_1 \cap H_2 \\ E_1 \cap E_2 \longleftrightarrow \langle H_1, H_2 \rangle \end{array}$$

- Quadratic eq'ns: $x^2+px+q=0$ solved by completing the square
$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$$
Note: $x_1+x_2 = -p$ and $x_1x_2 = q$

- Cubic eq'ns:
Note $(u+v)^3 = 3uv(u+v) + (u^3+v^3)$ but this is $x^3 = -px-q$ if $x = u+v$, $3uv = -p$, $u^3+v^3 = -q$. Now find u and v. But sum & product of u^3 and v^3 are known. So we solve the quadratic $w^2+qw-\frac{p^3}{27} = 0$ where u^3 and v^3 are the two solutions $-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}$. Since $x = u+v$, we have
$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}$$

Ex: $x^3+x-6=0$. See $\frac{q}{2} = -3$ and $\frac{p}{3} = \frac{1}{3}$ so
$$x = \sqrt[3]{3+\sqrt{3^2+\left(\frac{1}{3}\right)^3}} + \sqrt[3]{3-\sqrt{\frac{244}{27}}} \approx 1.634$$

Ex: $y^3-6y-6=0$. See $\frac{q}{2} = -3$ and $\frac{p}{3} = -2$ so $y = \sqrt[3]{2}+\sqrt[3]{4}$

What about x^3+ax^2+bx+d? Translate $x = y-\frac{a}{3}$ and obtain $y^3+py+q=0$ where $p = -\frac{1}{3}a^2+b$ and $q = \frac{2}{27}a^3 - \frac{1}{3}ab+c$

Ex: $x^3-3x^2-3x-1=0$ Use $x = y+1$ to obtain $y^3-6y-6=0$ so $y = \sqrt[3]{2}+\sqrt[3]{4}$ and $x = 1+\sqrt[3]{2}+\sqrt[3]{4}$

- Quartic eq'ns:

Consider $x^4+px^2+qx+r=0$ transformed into perfect squares on both sides. We add $2zx^2+z^2$ to both sides,

$x^4+2zx^2+z^2=(2z-p)x^2-qx+(z^2-r)$ and we want to choose z such that $2\sqrt{2z-p}\sqrt{z^2-r}=-q$ so the right side is also a perfect square. How? Solve $(2z-p)(z^2-r)=\frac{q^2}{4}$ for z. Hence, $z^3-(\frac{p}{2})z^2-(r)z+(\frac{pr}{2}-\frac{q^2}{8})=0$, called the cubic resolvent. Then, sol'ns to original eq'n result from $x^2+z=\pm(\sqrt{2z-p}\,x+\sqrt{z^2-r})$. Thus,

$x_{1,2}=\frac{1}{2}\sqrt{2z-p}\pm\sqrt{-\frac{1}{2}z-\frac{1}{4}p+\sqrt{z^2-r}}$ *Note cube roots might

$x_{3,4}=\frac{1}{2}\sqrt{2z-p}\pm\sqrt{-\frac{1}{2}z-\frac{1}{4}p-\sqrt{z^2-r}}$ appear here (in z)

A general $x^4+ax^3+bx^2+cx+d=0$ can be reduced to the previous case by shifting it to remove the 'a' term.

Ex: $x^4+6x^2+36=60x$

We get cubic resolvent $z^3-3z^2-36z-342=0$ which reduces using $z=y+1$ to $y^3-39y-380=0$ so

$z^3=1+\sqrt[3]{190+3\sqrt{3767}}+\sqrt[3]{190-3\sqrt{3767}}$

$F[x_1,\dots,x_n]$ = ring of poly's in $x_1,\dots,x_n$

$F(x_1,\dots,x_n)$ = field of rational functions in $x_1,\dots,x_n$

symmetric group S_n acts on $F(x_1,\dots,x_n)$ by permuting x_i's

Ex: $(1\ 2)$ acts: $x_1^2+x_2x_3\mapsto x_2^2+x_1x_3$

Each $\sigma\in S_n$ is autom. of $F(x_1,\dots,x_n)$

Q: What is the fixed field of S_n in $F(x_1,\dots,x_n)$?

Certainly includes F but includes more: all symmetric rational f'ns, a subfield S

Ex: $\frac{x_1+x_2+x_3}{x_1x_2x_3}$ in $F(x_1,x_2,x_3)$

Q: What is $[F(x_1, \dots, x_n) : S]$? $Aut(F(x_1,\dots,x_n)/S)$?

Elementary Symmetric Functions (in $x_1, \dots, x_n$)
$s_1 = \sum_{i=1}^{n} x_i$, $s_2 = \sum_{i<j} x_i x_j$, $s_3 = \sum_{i<j<k} x_i x_j x_k$, ..., $s_n = x_1 x_2 \dots x_n$

$f(x) = (x-x_1)(x-x_2)\dots(x-x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^n s_n$

Note $f(x)$ has coeff's in $F(s_1, \dots, s_n)$ but splits in $F(x_1, \dots, x_n)$ but not in a smaller field. So $F(x_1, \dots, x_n)$ is splitting field of f. Since $F(s_1, \dots, s_n) \subseteq S \subseteq F(x_1, \dots, x_n)$, $[F(x_1, \dots, x_n) : S][S : F(s_1, \dots, s_n)] = [F(x_1, \dots, x_n) : F(s_1, \dots, s_n)] \le n!$ (splitting field and tower law). But $[F(x_1, \dots, x_n) : S] = |S_n| = n!$ by the degree-order theorem so $[S : F(s_1, \dots, s_n)] = 1$ and $F(s_1, \dots, s_n) = S$.

Thm (Fund. Thm of Elem. Sym. F'ns)
Any symmetric rational f'n is a rational f'n in elem. sym. f'ns. (Also true for polys)

So: $Gal(F(x_1, \dots, x_n)/S) = S_n$

Recall the Galois group of a poly $f(x)$ is the Galois group of its splitting field K. If $\deg(f) = n$, then b/c Gal gp permutes roots, can view $Gal(K/F) \subseteq S_n$

See: The poly $x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^n s_n$ is sep'ble and has Gal gp S_n

Discriminant: $D = \prod_{i<j} (x_i - x_j)^2 \in F(x_1, \dots, x_n)$. D is symmetric so $D \in F(s_1, \dots, s_n) = S$. Also, $\sqrt{D} = \prod_{i<j} (x_i - x_j)$ not symmetric if $ch(F) \neq 2$. But $\sqrt{D}$ fixed by A_n (viewing Gal gp $G\, S_n$)

Thm: If $ch(F) \neq 2$, $\sigma \in A_n \iff \sigma$ fixes $\sqrt{D}$

$$\begin{array}{ccc} F(x_1,\dots,x_n) & \longleftrightarrow & \langle 1 \rangle \\ | & & | \\ F(s_1,\dots,s_n)(\sqrt{D}) & \longleftrightarrow & A_n \\ | & & | \\ F(s_1,\dots,s_n) & \longleftrightarrow & S_n \end{array}$$

Since $\Phi(A_n)$ is deg 2 extension and has $\sqrt{D}$ in it, so it must be $F(s_1,\dots,s_n)(\sqrt{D})$

Def'n: If $f(x)$ has roots $\alpha_1,\dots,\alpha_n$, define the discriminant of f to be $D = \prod_{i<j}(\alpha_i - \alpha_j)^2$ (lives in K = split field f). Note $D = 0 \Leftrightarrow f$ not sep'ble. D fixed by $Gal(K/F)$ so by Fund Thm, $D \in F$. $Gal(K/F)$ is subgp of $A_n \Leftrightarrow \sqrt{D} \in F$.

Ex: Poly deg 2 over $\mathbb{R}$: $f(x) = x^2 + px + q$ w/ roots α, β so $f(x) = (x-\alpha)(x-\beta)$. $D = (\alpha-\beta)^2 = s_1^2 - 4s_2 = (-p)^2 - 4q = p^2 - 4q$

Gal gp is $A_2 = \langle 1 \rangle \Leftrightarrow \sqrt{p^2-4q} \in \mathbb{Q}$

Ex: deg 3 poly: $f(x) = ax^3 + bx^2 + cx + d$ or $g(y) = y^3 + py + q$ $= (x-\alpha)(x-\beta)(x-\gamma)$. Calculate

$$D = -[27s_3^2 + 9p(s_2^2 - 2s_1s_3) + 3p^2(s_1^2 - 2s_2) + p^3] = -4p^3 - 27q^2$$
$$= a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$$

		Gal gp
$f(x)$ reducible:	3 lin factors	$\langle 1 \rangle$
	lin + quadratic	order 2
$f(x)$ irred:		A_3 or S_3
		iff $\sqrt{D} \in$ base field (A_3); $\sqrt{D} \notin$ base field (S_3)
		split field: $F(\theta)$; $F(\theta, \sqrt{D})$

Call $f(x) \in F[x]$ <u>solvable by radicals</u> over F if $\exists$ <u>tower</u> $F = K_0 \subseteq K_1 \subseteq \dots \subseteq K_s = K$ (splitting field of $f(x)$) such that $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$ (adjoin a root of $x^{n_i} - a_i$). Such an extension is a <u>simple radical extension</u> and K is a <u>root extension</u>

Def: A group G is <u>solvable</u> if $\exists$ chain:
$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_k = (e)$ where each $G_{i+1} \trianglelefteq G_i$ (normality) and G_{i+1}/G is abelian (in fact, can assume cyclic).

Let ζ satisfy $\zeta^n = 1$ but $\zeta \neq 1$, a <u>root of unity</u>. If $\sqrt[n]{a}$ is a root of $x^n - a$, then $\zeta \sqrt[n]{a}$ is, too.

Prop: Say $\mathrm{char}(F) \nmid n$ & F contains n^{th} roots of 1. Then $F(\sqrt[n]{a})/F$ is Galois with cyclic Gal gp (deg dividing n)

Proof: $F(\sqrt[n]{a})$ is Galois b/c it is split. field of $x^n - a$ (b/c F has roots of unity). Any $\sigma \in \mathrm{Gal}(K/F)$ sends $\sqrt[n]{a} \mapsto \zeta_\sigma \sqrt[n]{a}$. Check: $\sigma \mapsto \zeta_\sigma$ is an injective homom. of gps. Why? $\sigma\tau(\sqrt[n]{a}) = \sigma(\zeta_\tau \sqrt[n]{a}) = \sigma(\zeta_\tau)\sigma(\sqrt[n]{a}) = \zeta_\tau \zeta_\sigma \sqrt[n]{a}$ so $\sigma\tau \mapsto \zeta_\sigma \zeta_\tau$ and $\ker(\sigma \mapsto \zeta_\sigma) =$ all autom. fixing $\sqrt[n]{a}$, which is only the identity. But roots of unity are cyclic gps.

In fact, converse holds:
If $\mathrm{char}(F) \nmid n$ and F has roots of 1, any cyclic extension of deg n over F is of form $F(\sqrt[n]{a})$ for some $a \in F$

Thm: If $\alpha \in$ root ext K over F then $\alpha \in$ root ext that is Galois/F and each K_{i+1}/K_i cyclic.

Proof: Let L = "Galois closure" of K/F (the composite of split. fields of a basis of K/F) then since $\exists$ tower $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_k = K$, for any $\sigma \in \mathrm{Gal}(L/F)$, consider $F = \sigma K_0 \subseteq \sigma K_1 \subseteq \ldots \subseteq \sigma K_k = \sigma K$, each containment is a radical extension (gen by $\sigma \sqrt[n_i]{a_i}$, root of $x^{n_i} - \sigma(a_i)$). We do this for each σ, take composite, which is L. Note: the composite of 2 root ext $F = K_0 \subset K_1 \subset \ldots \subset K_k = K$, $F = K_0 \subset K_1' \subset \ldots \subset K_\ell' = K'$ is KK' which is also a root ext $F = K_0 \subset \ldots \subset K_k \subset K_k K_1' \subset \ldots \subset K_k K_\ell' = KK'$.

So L is Galois$/F$ and contains α. Now adjoin to F the n_i^{th} roots of 1, for all roots $\sqrt[n_i]{a_i}$ in rad. ext. of tower, get F'. Consider $F'K$ is composite of 2 Gal. ext. so its Galois $\underbrace{F \subseteq \ldots \subseteq F'}_{\text{each cyclic}} = \underbrace{F'K_0 \subset F'K_1 \subset \ldots \subset F'K_k}_{\text{each cyclic (w/ roots of 1)}}$

Thm: $f(x) \in F[x]$ is solvable by radicals $\Leftrightarrow$ Galois group of f is a solvable group.

Proof idea: $(\Rightarrow)$ f solv. by rads. $\Rightarrow$ each root α of f lies in a root extension $F \subset \ldots \subset K_i \subset \ldots \subset K_{s_\alpha}^{\alpha}$ Galois$/F$ & K_{i+1}/K_i cyclic by prev thm. Take composite of all roots: that's another root ext. of same type: $F \subset \ldots \subset L_i \subset \ldots \subset L_\ell = L$. Since L/F Galois, by Fund. Thm, $G_0 \supset \ldots \supset G_i \supset \ldots \supset G_\ell = (e)$ and L/F_i is Galois with group G_i, $Gal(F_{i+1}/F_i) = G_i/G_{i+1}$ and is cyclic. So $G_0 = Gal(L/F)$ is solvable. But $G = Gal(K/F)$ where $K =$ split. field of $f(x)$ is a quotient group of G_0 (b/c homom. image). But quotient of solvable groups are solvable.

$(\Leftarrow)$ If G solvable, then $G = G_0 \supset G_1 \supset \ldots \supset G_s = (e)$. By Fund. Thm., fixed fields: $F = K_0 \subset K_1 \subset \ldots \subset K_s = K$ with K_{i+1}/K_i cyclic ext., deg n_i. Let F' be F adjoined all n_i^{th} roots of 1. Then $F \subset F' = F'K_0 \subset F'K_1 \subset \ldots \subset F'K_s = F'K$ each containment is a radical extension, so f is solvable by radicals.

Ex: The general polynomial $f(x)$ does not have solutions in radicals for $n \geq 5$ because the Galois group $Gal(F(x_1, x_2, \ldots, x_n)/F(s_1, \ldots, s_n)) = S_n$ and S_5 is not solvable.

Consider poly ring $K[x_1, \ldots, x_n]$; monomial $= x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ w/ exponents ≥ 0 w/ total degree $\alpha_1 + \alpha_2 + \ldots + \alpha_n$ w/ shorthand x^α where $\alpha = (\alpha_1, \ldots, \alpha_n)$. Polynomial $f = \sum_\alpha a_\alpha x^\alpha$ w/ total deg $= \max|\alpha|$

Ex: $f = x^2y^2 + xy^2 + x^2y + xy$ $\deg(f) = 4$

Polynomials are functions (by evaluation)

$f: \mathbb{A}^n \to K$ field by $(a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n)$

The coordinate ring = ring of K-valued functions

This is the idea the connects algebra (of polys) with geometry (in $\mathbb{A}^n$).

The <u>locus</u> of $g(x,y) = 4x^2 + y^2 - 4$ is an ellipse (where $g = 0$).

Careful: Say "$f=0$" could mean two things (as poly or fcn).

Thm: K infinite. Then $f = 0$ in $K[x_1, \dots, x_n] \Leftrightarrow f: \mathbb{A}^n \to K$ is zero fcn.

Cor: If K infinite, $f, g \in K[x_1, \dots, x_n]$ then $f = g$ as polys $\Leftrightarrow f, g: \mathbb{A}^n \to K$ are same fcn.

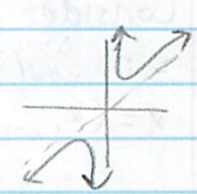
Ex: K = char 0 field, like $\mathbb{R}$ or $\mathbb{C}$

Def: Given $f_1, \dots, f_s \in K[x_1, \dots, x_n]$, let $Z(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in K^n : f_i(a_1, \dots, a_n) = 0 \ \forall 1 \le i \le s\}$ called the <u>affine algebraic set</u> (sometimes <u>variety</u> but variety usually refers to irred. alg. sets)

Ex: In $\mathbb{R}^2$, $Z(x^2+y^2-9)$ is circle of radius 3

$Z(x^2+y^2-9, x-y) = \{(3,3), (-3,-3)\}$

Ex: Graph of rational fcn $y = \frac{x^2+1}{x}$ is an alg set $Z(xy - x^2 - 1)$



Ex: In $\mathbb{R}^n$, $Z(a_{11}x_1 + \dots + a_{1n}x_n - b_1, \dots, a_{m1}x_1 + \dots + a_{mn}x_n - b_m)$ is linear alg set (sol'ns to $A\vec{x} = \vec{b}$)

Prop: If $W = Z(f_1, \dots, f_s)$, $V = Z(g_1, \dots, g_t)$ then $W \cup V$ and $W \cap V$ are also alg sets

Ideal gen by $f_1, \dots, f_s$: $\langle f_1, \dots, f_s \rangle := \{ \sum_{i=1}^{s} h_i f_i \mid h_i \in K[x_1, \dots, x_n] \}$
Note if $h \in \langle f_1, \dots, f_s \rangle$ and all $f_i(a_1, \dots, a_n) = 0$ then $h(a_1, \dots, a_n) = 0$

When we solve systems of eqn's $f_1 = 0, \dots, f_s = 0$, we are reducing this system to nicer elts in ideal

To solve a system $\qquad$ simpler

$$\begin{array}{ccc} f_1 = 0 & \xrightarrow{\text{reduce}} & g_1 = 0 \\ \vdots & & \vdots \\ f_s = 0 & & g_t = 0 \\ Z(f_1, \dots, f_s) & \xleftrightarrow[\text{same}]{\text{want}} & Z(g_1, \dots, g_t) \end{array}$$

Study ideals $\langle f_1, \dots, f_s \rangle \xrightarrow{\text{simplify?}} \langle g_1, \dots, g_t \rangle$ in $K[x_1, \dots, x_n]$

Q1) Desccription: Does ideal I have simpl(r) gen. set?
- in $K[x]$ every ideal is principal, so $I = \langle f \rangle$
  Find f using Euclidean alg. : $f = \gcd(f_1, \dots, f_s)$
- Hilbert basis thm: $I \subset K[x_1, \dots, x_n]$ is finitely generated

Q2) Membership: Is $f \in \langle f_1, \dots, f_s \rangle$?
- in $K[x]$, use Euclid. alg. $g(x) = h(x) f(x) + r(x)$ and see if $r(x) = 0$

Recall: $\langle x, y \rangle$ not principal so x, y gen $\langle x, y \rangle$ & is minimal. We say $\{x, y\}$ is a <u>basis</u> for ideal since it generates $\langle x, y \rangle$. A <u>reduced basis</u> is minimal.

Note: an ideal can have many bases =

$\langle x, y, x+y \rangle$

$\langle x, x+y \rangle \leftarrow$ reduced bases

$\langle x+x^2, x^2, y \rangle \leftarrow$

Monomial orders

In Euc. alg., we ordered terms $f = \underline{3x^2} - 4x + 2$

We had order on monomials (the degree) $x^2 > x > 1$ $\uparrow$ LT(f) leading term

How to order monomials in $K[x_1, \dots, x_n]$?

A) Lots of ways
- Lex(icographic) order
- Graded Lex order = total deg first, break ties w/ lex order
- Grevlex order = graded reverse lex order
  - $x^5yz^2 > x^4yz^3$

Def: monomial order is a rel'n $>$ on $\mathbb{Z}^n_{\geq 0}$ (exponent vector)

① $>$ total order on $\mathbb{Z}^n_{\geq 0}$

② $\alpha > \beta, \gamma \in \mathbb{Z}^n_{\geq 0} \Rightarrow \alpha + \gamma > \beta + \gamma$

③ $>$ <u>well-ordering</u> on $\mathbb{Z}^n_{\geq 0}$

Def'n: multidegree of f is $\partial(f) = \max\{\alpha : \text{coeff}(x^\alpha) \neq 0\}$

Lemma: $\partial(fg) \overset{?}{=} \partial(f) + \partial(g)$

$f+g \neq 0$ $\quad \partial(f+g) \overset{?}{\leq} \max(\partial(f), \partial(g))$

Division Algorithm in $K[x_1, \dots, x_n]$

Given f and $f_1, \dots, f_s$ we want $f = a_1 f_1 + \dots + a_s f_s + r$

Idea: Cancel LT(f) by mult f_1 by something & subtract

Q) If $r = 0$, clearly $f \in \langle f_1, \dots, f_s \rangle$ but converse false

Amazing: If $f_1, \dots, f_s$ is a <u>Groebner basis</u> for $\langle f_1, \dots, f_s \rangle$ then $r \neq 0 \Rightarrow f \notin \langle f_1, \dots, f_s \rangle$

Ex: $f = x^2y + y$ $\quad f_1 = xy + 2$, $f_2 = x + 1$ $\quad$ Use lex order

$a_1 : x$
$a_2 : -2$

$$\begin{array}{ll} f_1: & xy+2 \\ f_2: & x+1 \end{array} \quad \begin{array}{r} \overline{)x^2y + y} \\ \underline{x^2y + 2x} \\ -2x + y \\ \underline{-2x - 2} \\ y + 2 \end{array}$$

Does order of f_1, f_2 matter? Unfortunately, yes.

Def'n: $I \subset K[x_1, \dots, x_n]$ a nonzero ideal. Let $LT(I) :=$ leading terms of polys in I and $\langle LT(I) \rangle :=$ ideal gen by $LT(I)$

Ex: $I = \langle f_1 = x^2y + x, f_2 = x^3 - 1 \rangle$ $\quad LT(I)$ includes: x^3, x^2y but also x^2 (since $xf_1 - yf_2 = x^2 - y$). Note $LT(I) \neq \langle LT(f_1), LT(f_2) \rangle$ but we have inclusion $\langle LT(f_1), LT(f_2) \rangle \subseteq LT(I)$

Def'n: A <u>Groebner basis</u> of I is a subset $G = \{g_1, \dots, g_t\} \in I$ s.t. $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$

Equivalently, G is a Groebner basis of $I \Leftrightarrow \forall f \in I$, $LT(f)$ divisible by some $LT(g_i)$

Thm: G is GB for I, $f \in K[x_1, \dots, x_n]$. $\exists$ unique $r \in K[x_1, \dots, x_n]$ st. ① $\exists g \in I$ st. $f = g + r$
② no term of r divisible by any $LT(g_i)$

Proof: $f = a_1g_1 + \dots + a_tg_t + r$ satisfies ① and ② using division algorithm. Now suppose $f = g' + r_1 = g'' + r_2$. Then $r_2 - r_1 = g' - g'' \in I$ so $LT(r_2 - r_1) \in LT(I)$ hence divisible by some $LT(g_i)$. But this is impossible unless it is 0 thus $r_1 = r_2$.

Cor: $f \in I \Leftrightarrow r = 0$

Pf: ($\Leftarrow$) easy
($\Rightarrow$) $f = f + 0$ works

Cor: In div. alg. r does not depend on the order of listing $\{g_1, \dots, g_t\}$ if it's a GB. However, coeffs a_i may depend on listed order.

Thm: Fix monomial order, every nonzero ideal $I \subseteq K[x_1, \dots, x_n]$ has a Groebner basis.

Q) How to test if given G is GB?
Q) How to find a Groebner basis?

One way G can fail to be GB is if $ax^\alpha g_i - bx^\beta g_j$ cancels LT's then LT(this) is in $\langle LT(I) \rangle$ but may not be in $\langle LT(g_1), \dots, LT(g_t) \rangle$

Def'n: Given $f, g \in K[x_1, \dots, x_n]$, let $M =$ monic LCM$\{LT(f), LT(g)\}$ and let $S(f,g) = \frac{M}{LT(f)} f - \frac{M}{LT(g)} g$ be the "S-poly" of f and g"

Thm: (Buchberger's Criterion) A basis $G = \{g_1, \dots, g_t\}$ of I is a GB iff $\forall i \neq j$ the remainder of $S(g_i, g_j)$ divided by G is 0.

Buchberger's Algorithm: (Generalization of Gaussian elimination)
- Input: $G = \{g_1, \dots, g_t\}$. Set $G' = G$
- Check every pair, compute $S(g_i, g_j)$, take remainder mod G
  if remainder r nonzero, let $G = G \cup \{r\}$.
- Repeat until $G = G'$

(This algorithm terminates b/c $K[x_1, \dots, x_n]$ is Noetherian)

Lex order important for "<u>elimination ideals</u>", nice for solving poly eq'ns

GB are not unique, but a reduced GB is!

Def: A <u>reduced GB</u> G is a GB st

① polys in G are monic

② $\forall p \in G$, no monomial of p lies in $\langle LT(G - \{p\}) \rangle$

Ex: lin system

$f_1 = 3x - 6y - 2z = 0$

$f_2 = 2x - 4y + 4w = 0$

$f_3 = x - 2y - z - w = 0$

$I = \langle f_1, f_2, f_3 \rangle = \langle g_1, g_2 \rangle$ reduced

$= \langle x - 2y - z - w, z + 3w \rangle$ min'l

$= \langle x - 2y + 2w, z + 3w \rangle$ reduced

(RREF for lin. alg.)