Dawn of a New Day

622

• Some review

– R commutative ring w/ 1.

Recall "divisibility", $a, b \in R$, $b \neq 0$, b divides a if $\exists$ $q \in R$, $bq = a$ denoted "$b \mid a$".

"G.C.D.s" – d is a gcd of a & b if $d \mid a$ & $d \mid b$, & $c \mid a$ & $c \mid b$, then $c \mid d$.

↳ algorithm: $a = bq_0 + r_0$, $|b| > r_0 \geq 0$ (division alg.)

Fact: $b = r_0 q_1 + r_1$, $|r_0| > r_1 \geq 0$

$r_0 = r_1 q_2 + r_2$, $|r_1| > r_2 \geq 0$

$\vdots$ $\quad\quad$ $\vdots$

$r_{n-2} = r_{n-1} q_n + r_n$, $r_n = 0$ b/c well-ordering.

Observe: $d \mid a$ & $d \mid b \Leftrightarrow d \mid b$ & $d \mid r_0$

$d \mid b$ & $d \mid r_0 \Leftrightarrow d \mid r_0$ & $d \mid r_1$

$\vdots$

$\Leftrightarrow d \mid r_{n-1}$ & $d \mid r_n$ but $r_n = 0$, so we're good.

– Def: R is a Euclidean Domain if R is an int. domain & there's a "norm" $N: R \to \mathbb{N} \cup \{0\}$ $\ni \forall a, b \in R$ with $b \neq 0$, $\exists$ $q, r \in R$ $\ni$

$a = bq + r$, $r = 0$ or $N(b) > N(r)$

Ex $\mathbb{Z}$,

$N(\mathbb{Z}) = |\mathbb{Z}|$ makes $\mathbb{Z}$ into a Euclidean domain.

Ex $\mathbb{R}[x]$

$N(f(x)) = \deg f(x)$. Using Polynomial long division, we see that N is a Euclidean norm.

Ex Example of indep. interest & importance:

Recall $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a subring of $\mathbb{R}$. $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 + -2b^2 \in \mathbb{Q}$.

cont.

$\frac{(a+b\sqrt{2})(a-b\sqrt{2})}{a^2-2b^2} = 1$ ... notice that $a^2-2b^2=0$ iff $a=0=b$. It also follows $a+b\sqrt{2} = c+d\sqrt{2}$ iff $a=c, b=d$.

So let's call it a function:

$N_0: \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}$. Restrict N_0 to $\mathbb{Z}[\sqrt{2}]$.

↳ Not a field

Say $|N_0| = N$. More general... take $D \in \mathbb{Z}$, D is square free.

$\mathbb{Z}[\sqrt{D}] \subseteq \mathbb{Q}[\sqrt{D}]$

So $\mathbb{Q}[\sqrt{D}]$ is a field if $a+b\sqrt{D} \neq 0$,

$(a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - b^2 D \in \mathbb{Q}$

↳ $\neq 0$ since $\sqrt{D} \notin \mathbb{Q}$

& so we can construct an inverse of $a+b\sqrt{D}$ in $\mathbb{Q}[\sqrt{D}]$.

$N: \mathbb{Z}[\sqrt{D}] \to \mathbb{N} \cup \{0\}$, $N(a+b\sqrt{D}) = |a^2 - Db^2|$.

Fact: D is square free, so $N(a+b\sqrt{D}) = |a^2 - Db^2|$ is "multiplicative", meaning N is compatible w/ multiplication, ie.

$N((a+b\sqrt{D})(c+d\sqrt{D})) = N(a+b\sqrt{D})\,N(c+d\sqrt{D})$. You check this ☆.

Ex) $D=-1$, & $D=-5$

For $D=-1$: $N(a+bi) = a^2+b^2$. What are the units of $\mathbb{Z}[i]$? These are the Gaussian integers. Using that N is multiplicative, if $a+bi$ is a unit, $\exists\ c+di \in \mathbb{Z}[i] \Rightarrow (a+bi)(c+di) = 1$ & so $1 = N(1) = N((a+bi)(c+di)) = N(a+bi)\,N(c+di)$ & must be that $N(a+bi) = 1$ ie. $a^2+b^2 = 1$ Hence $a+bi \in \{1, -1, i, -i\}$

For $D=-5$: Units of $\mathbb{Z}[-5]$?

My work: $N(a+bi\sqrt{5}) = (a+bi\sqrt{5})(a-bi\sqrt{5})$

$= a^2 + 5b^2$

$a+b\sqrt{-5}$ unit $\Rightarrow N(a+b\sqrt{5}) = 1$ so $a^2+5b^2 = 1$

So $b=0$, $a = \{\pm 1\}$.

1) Euclidean Dom. $\Rightarrow$ PID's
2) $\mathbb{Z}[\sqrt{-5}]$ not a PID
3) Healed into UFD's
4) Integral domain prime $\Rightarrow$ irreducible
   PID irreducible $\Rightarrow$ prime
5) $\forall$ PID is a UFD

$\forall$ discussion today R is an integral Domain.

~~Prime Ideal Domain $\Rightarrow$ PID~~

- Def: An elt, $p \in R$, is prime if (p) is a prime ideal.
  Recall an ideal I is prime if whenever $y, z \in R$ & $yz \in I$, then $y \in I$ or $z \in I$.
  - An elt q is irreducible if whenever $q = yz$ then y or z is a unit.

- Lemma: R is an int. dom. $y \in R$. y is prime $\Rightarrow$ y is irred.

  Proof:
  Suppose $y = ab$ & y is prime. Since y is prime, (y) is prime.
  So a or $b \in (y)$. WLOG, suppose $a \in (y)$, i.e. $\exists$ $s \in R \ni ys = a$
  Thus $y = (ys)b = ysb$, So $y(1 - sb) = 0$ & $y \neq 0$,
  thus b is a unit. QED

- Lemma: R is a PID & y is irreducible $\Rightarrow$ y is prime.

  Proof:
  Consider (y) & suppose $\exists$ $a, b \in R \ni ab \in (y)$. So
  $\exists$ $s \in R \ni ab = ys$ To be continued

- Thm: R PID $\Rightarrow$ R UFD

- Def: Integral Domain R is a UFD (Unique Factorization Domain)
  if every non-zero, non-unit elt $b \in R$ has a factorization
  $b = q_1 \cdots q_s$ into irreducibles,
  & if $b = p_1 \cdots p_t$ into irreducible, then $s = t$, & up to reordering,
  q_i & p_i are associates for $i = 1, \ldots, s$.

Proof of Thm:

We show b can be factored into a product of irreducibles. (and non-units)

Suppose $b = b_0 b_1$. Assume here neither b_0 or b_1 are irreducible. In which case we can factor b_1 non trivially. So we find $b = b_0 b_{1,1} b_{1,2}$ where $b_1 = b_{1,1} b_{1,2}$. Observe that (b) (principal ideal generated by b) is $\ni (b) \subseteq (b_1)$ & $(b) \subsetneq (b_1)$ (properly contained) since otherwise b & b_1 are associates & so would be a unit.

So we continue our factorization to $b = b_0 \cdots b_n$ leading to $(b) \subsetneq (b_1) \subsetneq \cdots \subsetneq (b_n)$.

Claim: If $(b) \subsetneq (b_1) \subsetneq \cdots \subsetneq (b_n) \subsetneq \cdots$ (potentially goes on forever) Then the containments terminate in a finite # of steps.

Let $I = \bigcup_{i=1,2,\ldots} (b_i)$. Observe that I is ~~an ideal~~ a nested increasing union, if $r \in R$ & $i \in I$, $\exists\ n \in \mathbb{N} \ni i \in (b_n)$ (an ideal of R) $\Rightarrow$ $ri \in (b_n) \subseteq I$. Also I is closed under subtraction b/c if $y, z \in I$ $\exists\ n \in \mathbb{N} \ni y, z \subseteq (b_n)$ which is an ideal & closed under subtraction. Thus we've shown I is an ideal.

(Notice $1 \notin I$). Since R is a PID $\exists\ c \in I \ni I = (c)$.

By how we've constructed this, $\exists\ k \in \mathbb{N}$, $c \in (b_{k+1}) - (b_k)$.

Now $(c) = (b_{k+1})$. So the chain has at most $k+2$ containments.

$b_0 = b_1 \cdots b_{k+1}$. So here b_{k+1} is irreducible.

Recall Thm we didn't prove:

Let R be a PID, $p \in R$, then if p is irreducible, p is prime.

Proof:

Let's prove (p) is maximal (thus prime). Let I be an ideal $\ni (p) \subset I$. Then $\exists\ m \in R \ni I = (m)$. Thus $\exists\ s \in R \ni p = ms$. So by irreducible prop of p, m or s is a unit if m is a unit $I = R$. If s is a unit, $m = ms s^{-1} = p s^{-1} \in (p)$ thus $I = (p)$ & is maximal, thus it's prime.

QED.

Possible Quiz Problem

- We've proven before Every Euclidean Domain is a PID.

- Defi Let R be a ring. If $I_1 \subseteq I_2 \subseteq \dots \subseteq I_k \subseteq \dots$ are ideals, & $\exists\ n \in \mathbb{N} \ni I_n = I_{n+1} = \dots$, then R is said to satisfy the ascending chain condition (ACC) on ideals.

- Prop: If R is a PID, then R satisfies ACC on its ideals.

Proof:

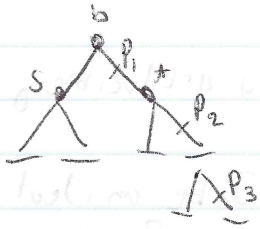
Let $I = \bigcup_{i=1}^{\infty} I_i$. If $a, b \in I$ & $r \in R$. Since $a, b \in I$, $\exists$ k in $\mathbb{N} \ni \{a, b\} \subseteq I_k$ which is an ideal, so $a - b \in I_k$. Now we look at ra, WTS it's in I_k. Well, I_k is an ideal, so $ra \in I_k$ & $I_k \subseteq I$. Since R is a PID, $I = (c)$, for some $c \in I$. But then $\exists\ \hat{i} \in \mathbb{N}$ $\ni c \in I_{\hat{i}}$. But now, since $I = (c)$, it follows that $I_{\hat{i}} = I_{\hat{i}+1} = \dots$. Thus R satisfies ACC on its ideals.

QED.

- Thm: R is a PID $\Rightarrow R$ is a UFD.

Proof:

Let $b \in R \ni b$ is nonzero & non unit. If b is irreducible, we're done. So suppose b is reducible. $\exists\ s$ & $t \in R$ then such neither is zero & a unit & $b = st$.



If we proceed down from the root along a path, the elts. down that path $b = p_1, p_2, \dots$ & we observe $(p_i) \subsetneq (p_{i+1})$ (proper).

So any tree formed in this manner is in fact finite. Ie, the procedure halts in a finite # of steps since R satisfies ACC on ideals. Now we have $b = u_1 \cdots u_k$ where $\{u_1, \dots, u_k\}$ are the irreducible leaves of our tree. This proves existance. Now we need to prove uniqueness. Suppose $b = v_1 \cdots v_r = u_1 \cdots u_k$ where u_i & v_i are irreducible $\forall\ i$, (we will use exercise 4 a p. 278 here as a lemma of sorts).

cont.

So $u_1 | v_1 \cdots v_r \Rightarrow$ WLOG $u_1 | v_1$. Since v_1 & u_1 are irreducible $u_1 \sim v_1$ (u_1 & v_1 are associates). Proceed w/ induction to finish the proof, & we find that the irreducibles are in fact unique.

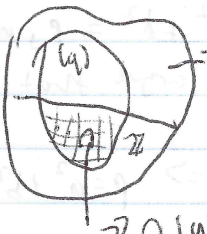
QED.

- Now we investigate $\mathbb{Z}[i]$ (Gaussian integers). We showed $\mathbb{Z}[i]$ is a Euclidean Domain. Under the Euclidean Norm, $N(a+bi) = a^2+b^2$, we showed norms of this form are multiplicative.

Note: $2 \in \mathbb{Z}[i]$, but $(1+i)(1-i)$.

We'd like to know $\mathbb{Z}[i]$ irreducibles. Recall we showed the units of $\mathbb{Z}[i]$ are $\{1, -1, i, -i\}$.

- Fact: $a+bi = \alpha$ & $N(\alpha) = a^2+b^2$ is a prime, then α is irreducible, b/c if $\alpha = \beta\gamma \Rightarrow N(\alpha) = N(\beta)N(\gamma)$ & $N(\alpha)$ prime $\Rightarrow \beta$ or γ is prime.
- Fact: If $n \in \mathbb{Z} \subseteq \mathbb{Z}[i]$ is form of $n = a^2+b^2$ where $a, b \in \mathbb{Z}$, then $n = a^2+b^2 = (a+ib)(a-ib)$ & easy to verify that neither $a+ib$ or $a-bi$ is a unit so n is reducible.
- Fact: If q is irred. in $\mathbb{Z}[i]$, then look at $(q) \cap \mathbb{Z}$.



Observe that $(q) \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$.
q irred. in $\mathbb{Z}[i] \Rightarrow q$ is prime in $\mathbb{Z}[i]$.
So $(q) \cap \mathbb{Z}$ is a prime ideal, that is $(q) \cap \mathbb{Z} = (p)$ where p is a prime number in $\mathbb{Z}$. We have this $q \to p$ relation. Note if $q \notin \mathbb{Z}$, then our p is reducible. So $p = qq'$ where $q' \in \mathbb{Z}[i]$. So $N(p) = p^2 = N(q)N(q')$, so q' can't be a unit by an easy enough argument & also $N(q) = p$.

Let $q = a+bi$, $q' = c+di$, so $ad+bc = 0$. Consider $A = \begin{bmatrix} a & c \\ -b & d \end{bmatrix}$. So $\det(A) = 0$. So $\exists\ r \in \mathbb{Q}$ s.t. $r(a,c) = (-b,d)$ i.e. $ra = -b$ & $rc = d$.

(cont. next time

*Group problems:

- The quotient of a PID by a prime ideal is a PID

Pf:

We make use of 3 important facts

1) Every field is a PID
2) Every prime ideal in a PID is maximal
3) $\frac{R}{I}$ is a field iff I is maximal in R

Let R be a PID & I a prime ideal of R. By (2), I is maximal, by (3) R/I is a field, by (1) $\frac{R}{I}$ is a PID. QED

- Back to our # theory stuff w/ the matrix.

Let our $q = a+bi$ & $q' = c+di$ $\Rightarrow ad+bc=0$

& we have $A = \begin{bmatrix} a & c \\ -b & d \end{bmatrix}$ & $\det A = 0$

Notice that both a,b & c,d are nonzero. By the above, $\exists\ r \in \mathbb{Q}$ s.t. $r\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} c \\ -d \end{pmatrix}$, but $r \in \mathbb{Z}$ but $a^2+b^2 = p$

$\Rightarrow r = \frac{m}{n} = \frac{m}{1} \in \mathbb{Z}$, Use that $c^2+d^2 = p$, a prime, & cond that $r \in \{1, -1\}$ & from here we can argue that q' is conjugate to q. $p = (a+bi)(a-bi) = a^2+b^2$.

So a is irreducible. $(q) \cap \mathbb{Z} = (p) \Rightarrow p = a^2+b^2 \Rightarrow p \equiv 1 \bmod 4$, $p=2$.

- Last thing to consider: What if p is prime, $p \equiv 1 \bmod 4$?

Claim: $\exists\ a,b \in \mathbb{Z}$ $p = a^2+b^2 = (a+bi)(a-bi)$

look at the units of $\mathbb{Z}_p^\times$, $p \equiv 1 \bmod 4$.

$4 \mid |\mathbb{Z}_p^*| = p-1$. We claim $\mathbb{Z}_p^*$ is cyclic. Recall given G where G is a group, $\exp(G) = \min\{k \in \mathbb{N} \mid \forall g \in G,\ g^k = e\}$.

As a corollary of Lagrange's Thm, $\exp(G) \mid |G|$ & $\exp(G) = |G| \iff G$ is cyclic.

So if $\mathbb{Z}_p^\times$ is not cyclic, $\exists\ n < p-1$ s.t. for $b \in \mathbb{Z}_p^\times$ $b^n = 1$ So $p(x) = x^n - 1$ has $p-1$ roots, which is a contradiction, So $\mathbb{Z}_p^\times$ is cyclic. So $4 \mid |\mathbb{Z}_p^\times| \Rightarrow \exists\ c \in \mathbb{Z}_p^\times$ s.t. $|c| = 4$.

cont.

$\Rightarrow c^4 = 1$ so $c^2 \neq 1$ but $c^2 = -1$ or $p \mid c^2+1 = (c+i)(c-i)$. If p is irred. in $\mathbb{Z}[i]$ then $p \mid c+i$ WLOG so $\exists\ s \in \mathbb{Z}[i] \Rightarrow$
$ps = c+i$ but $p\bar{s} = c-i$ so $p \mid c-i$ where $p \nmid 2$ which is not possible from contradiction. QED.

mostly ch. 9 stuff today

Ch 9

What's a polynomial? defn. $b(x) = a_n x^n + \dots + a_0$ where $a_0, \dots, a_n$ are in R. Assumed $a_n \neq 0$. Then $\deg(b(x)) = n$. If R is an integral domain, $a(x), b(x) \in R[x]$, $\deg(a(x)\,b(x)) = \deg(a(x)) + \deg(b(x))$.
Also, if R is an integral domain, then $R[x]$ is an integral domain.

<u>def:</u> I is assumed to be an ideal of R. Then
$(I) = \{ b_n x^n + \dots + b_0 \in R[x] \mid b_0, b_1, \dots, b_n \in I \}$.

<u>Ex</u> $\mathbb{Z} = R$, $I = (2)$. Then (I) is the poly's w/ coefficients in $2\mathbb{Z}$. (Don't forget how to multiply polynomials).

<u>Lemma:</u> $\dfrac{R[x]}{(I)} \cong \dfrac{R}{I}[x]$

Side note eg. $\dfrac{\mathbb{Z}[x]}{(I)} \cong \mathbb{Z}_2[x]$

<u>Proof:</u> Instead of $a+I$ in $\frac{R}{I}$, we'll write $\bar{a}$.
Let $\phi : R[x] \to \frac{R}{I}[x]$ where $b_n x^n + \dots + b_0 \mapsto \bar{b}_n x^n + \dots + \bar{b}_0$. This map is a ring homomorphism then & it's fairly obvious that it's onto. If $\phi(b_n x^n + \dots + b_0) = 0 \iff$ then $\bar{b}_n = \bar{b}_{n-1} = \dots = \bar{b}_0 = 0 \iff b_n, b_{n-1}, \dots, b_0 \in I$
$\iff b_n x^n + \dots + b_0 \in (I)$ so by the 1st Isomorphism Thm, we're done. QED

9.2 on next page

$b_n x^n + \dots + b_0 \overline{)\, a_m x^m + \dots + a_0}$

- F is a field.

Proposition: If $a(x), b(x) \in F[x]$, $b(x) \neq 0$, $\exists$ a unique $q(x)$ & $r(x)$ $\ni$ $a(x) = b(x)\,q(x) + r(x)$ where $\deg(r(x)) < \deg(b(x))$ or $r(x) = 0$.

Corollary: With $N(b(x)) = \deg(b(x))$, N is a Euclidean norm.

~~**Proof:** By induction on $\deg(b(x))$~~

~~Base case → If $\deg(b(x)) = 0$, suppose $a_m x^m + \dots + a_0 = a(x)\, b_0^{-1} b_0 + 0$~~

~~Inductive Step → Suppose $\deg(b(x)) < n$ $\forall$ $a(x)$, $a(x) = b(x)\,q(x) + r(x)$ where $\deg(r(x)) < \deg(b(x))$ or $r(x) = 0$.~~

~~**Proof:** By induction on $\deg a(x)$. If $\deg(b(x)) = 0$, then $a(x) = a_0$, $a(x) = 0\, b(x) + a_0$~~

Proof: We'll use induction on $\deg(a(x))$. If $\deg(a(x)) = 0$,

Base case: $a(x) = a_0$, $a(x) = 0\, b(x) + a_0$ if $\deg(b(x)) > 0$.

If $\deg(b(x)) = 0$, $b(x) = b_0$ so $a_0 = a(x) = a_0 b_0^{-1} b_0 + 0$.

Inductive hyp Step: If $\deg(a(x)) < m$, then $a(x) = b(x)\,q(x) + r(x)$ where $\deg(r(x)) < \deg(b(x))$.

Let $a(x) = a_m x^m + \dots + a_0$

Case: $\deg(b(x)) > \deg(a(x))$,

$a(x) = b(x) \cdot 0 + a(x)$. Otherwise...

$a(x) - b(x)\,(b_n a_m^{-1} x^{m-n}) = A_0(x)$. By the induction hypothesis,

$A_0(x) = q_1(x) b(x) + r_1(x)$ w/ $\deg(r_1(x)) < \deg(b(x))$ or $r_1 = 0$

So now solve for $a(x)$, giving us

$a(x) = (q_1(x) + b_n^{-1} a_m x^{m-n})\, b(x) + r_1(x)$

Uniqueness is fairly easy, so we'll leave it for us, but then we're done (no induction needed for uniqueness).

QED.

- **Corollary 2:** Recall a <u>root or a zero</u> of $b(x)$ is an element $c \in R$ $\ni b(c) = 0$. Using this...
  $b(x) \in F[x]$ where F is a field is divisible by a linear polynomial iff $b(x)$ has a root in F.

  Proof: If $(a_1x + a_0) \mid b(x)$ or $(a_1x + a_0)s(x) = b(x)$ for some $b(x) \in F[x]$, then $-a_1^{-1}a_0$ is a root of $b(x)$.
  Conversely if c is a root of $b(x)$, then consider dividing $x-c$ into $b(x)$ via the division algorithm. so
  $b(x) = (x-c)q(x) + r(x)$, $\deg(r(x)) = 0$. Now $0 = b(c) = r(c)$, so $(x-c) \mid b(x)$.

- **Corollary 3:** $b(x)$ has degree n, then $b(x)$ has at most n roots.
  Proof: Fairly easy suggesting induction.

• Let $R = \mathbb{Z}$
Gauss's Lemma: $b(x) \in \mathbb{Z}[x]$ & it factors non-trivially in $\mathbb{Q}[x]$, then $b(x)$ factors non-trivially in $\mathbb{Z}[x]$.

Proof: Assume $b(x) = A_1(x) \cdots A_k(x)$ non-trivial factor in $\mathbb{Q}[x]$, $\exists\, d \in \mathbb{Z} \ni d\,b(x) = a_1(x) \cdots a_k(x)$ where $a_i(x) \in \mathbb{Z}[x]$.
WLOG suppose $d \in \mathbb{N}$, $d > 1$ (or we're done). so $d = p_1 \cdots p_s$ where p_i are primes. Consider $I = (p_1)$ & reduce.
$\overline{0} = \overline{a_1(x)} \cdots \overline{a_k(x)}$. WLOG $\overline{a_1(x)} = \overline{0}$ ~~and repeat all the way down?~~
~~Then we're done~~ QED.

So $a_1^* = p_1 a_1^{**}(x)$

Notice that $A_i(x)$ & $a_i^{**}(x)$ are multiples by an integer. ~~[illegible]~~

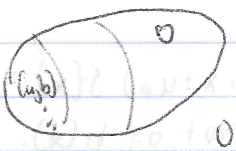
do
proofs
your
own.
more
practice.

read up on this

not naturals necessarily.

Field of Fractions

Let R be an integral domain. Want $R \hookrightarrow Q$, a field. So we want to construct $Q \ni$ no proper subfield Q' of Q containing R.



$\{(a,b) \in R \times R ;\ b \neq 0$ Define $\sim \ni$ $(a,b) \sim (c,d)$ if $ad = bc$.

Observe that $\sim$ is reflexive & symmetric.

Suppose $(a,b) \sim (c,d)$ & $(c,d) \sim (e,f)$ so

$ad = bc$ & $cf = ed$.

We want. $af = be$. ↓ we have

$cfad = edbc$

So $cd(fa) = cd(be)$. Since R an int. dom. $d \neq 0$, $c(fa) = c(be)$. Argue that if $c = 0$, then a must also be 0, so we're good. If c is nonzero, then by integral domain $af = be$.

- Denote equivalence class of (a,b) by $\frac{a}{b}$. Want to define a ring. Want to define addition, multiplication, 0, ...

- Observe if $y \in R - \{0\}$ $\frac{a}{b} = \frac{ya}{yb}$ & if w & z are nonzero R, then $\frac{a}{w} = \frac{a}{z}$.

Let $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$ & $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

☆ We still need to check that it's well defined.

$\frac{ac}{bd}$ vs $\frac{a'c}{b'd}$ ... $acb'd = a'bcd$. So we're good there.

In the text we can find well-definedness of $+$

We have a mult. identity $\frac{1}{1} = \frac{m}{m}$, $m \neq 0$

$\frac{1}{1} \cdot \frac{a}{b} = \frac{a}{b}$

$\frac{0}{m} + \frac{a}{b} = \frac{a}{b}$.

Then we check associativities, distributivity, commutivities, & lastly if $\frac{a}{b} \neq 0$ $\frac{a}{b} \cdot x = 1$.

- Observe that Q has no proper subfield isomorphic to R.

- also observe if F is a field $\Rightarrow \phi: R \to \phi(R) \hookrightarrow F$ then the least subfield of F containing $\phi(R)$ is isomorph. to Q so

$$\begin{array}{ccc} R & \xrightarrow{\phi} & \phi(R) \\ \downarrow & \overset{\sim}{\searrow} & \downarrow \\ Q & \dashrightarrow & F \end{array}$$

then ϕ & $\hat{\phi}$ are both isomorphisms.

- Let's reprove Gauss's Lemma ... again

Let R be a UFD w/ a field of fractions Q. Then if $p(x) \in R[x]$ & factors ~~into irreducibles~~ $p(x) = A_1(x) \cdots A_m(x)$ into irreducibles $Q[x]$, then $p[x] = a_1(x) \cdots a_m(x)$ in $R[x]$ where $A_i(x)$ & $a_i(x)$ are associate in $Q[x]$

Proof:

Same arguments as before, ~~do~~ $d\,p(x) = a_1^*(x) \cdots a_m^*(x)$ since R is a UFD, $d = p_1 \cdots p_s$ into a product of irreducibles. Now working in $R/(p)$ (which is a field), & after taking reduction homomorphism in $R/(p)[x]$ .. then proceed as we did before.

- R is a UFD $\Rightarrow R[x]$ is a UFD

Proof:

Use that $Q[x]$ is a UFD. Let $p(x) \in R[x]$ be a non-unit, non-0. If $p(x) = a_k x^k + \cdots + a_0$ & $\gcd(a_k, \ldots, a_0) = j$, look at $\frac{1}{j} p^*(x) = p(x)$. We'll factor $p^*(x)$ in $Q[x]$.

$p^*(x) = A_1(x) \cdots A_m(x)$. Convert into an R-factorization using Gauss's Lemma. So

$$p^*(x) = a_1(x) \cdots a_m(x)$$

Suppose $j = p_1 \cdots p_r$. Reconstitute, $p(x) = p_1 \cdots p_r a_1(x) \cdots a_m(x)$ a factorization into irreducibles.

Now we also need uniqueness: If ~~$p_1 \cdots p_r a_1(x) \cdots a_m(x)$~~ $p_1 \cdots p_r a_1(x) \cdots a_m(x) = q_1 \cdots q_s\, b_1(x) \cdots b_n(x)$, another R factorization.

Idea now is that $a_1(x)$ corresponds up to associate to some $b_i(x)$,

$b(x) = a_m x^m + \dots + a_0$

- **Corollary**: $b(x) \in R[x]$ $\gcd(a_0, \dots, a_m) = 1$. Then $b(x)$ is irred. in $Q[x]$, iff $b(x)$ is irred in $R[x]$.

  Proof:
  If $b(x)$ is irred. in $R[x]$, it can't reduce in $Q[x]$ ("over Q") by Gauss's Lemma.
  If is irred. over Q & the gcd of it's coeffs. is 1, then if there is a reduction in $R[x]$, ($2x$ is reducible in $Z[x]$ & irred in $Q[x]$) then $b(x)$ factors into a product of R-polynom of strictly lower degrees & a contradiction arises. QED

Proof is incomplete the rest is up to us.

- Recall our big Thm that we proved last time.
  R is a UFD $\Rightarrow$ $R[x]$ is a UFD. Some questions on this:
  1) T or F?
     R is an int. dom. & $R[x]$ is a UFD. Then R UFD?
     True: as a subring $R \hookrightarrow R[x]$, R consists of deg. 0 poly's. So if $b \in R \hookrightarrow R[x]$ is non-unit & nonzero, it factors into $R[x]$ irred. But into a prod. of deg. 0 irred.

  2) If R is a UFD, is $R[x,y]$?
     Yes, b/c $R \hookrightarrow R[x] \hookrightarrow (R[x])[y]$.

Proof is wrong in the book?

- **Eisenstein's Criterion**
  $b(x) \in R[x]$ where R is a UFD, $b(x) = x^m + b_{m-1}x^{m-1} + \dots + b_1 x + b_0$
  P is a prime ideal of R & $b_0, \dots, b_{m-1} \subseteq P$, & $b_0 \notin P^2$.
  Then $b(x)$ is irred. over R.

  Proof: Suppose $b(x)$ reduces to $c(x)e(x)$ in $R[x]$. Now we reduction thm working in $\frac{R}{P}[x]$, an integral domain: ~~from~~ ~~$\frac{R}{P}[x]$, $\overline{x}^m = \overline{b(x)} = \overline{c(x)e(x)} = \overline{c(x)}\,\overline{e(x)}$~~
  Let $c(x) = c_j x^j + \dots + c_0$ & $e(x) = e_k x^k + \dots + e_0$. So
  $b(x) = c(x)e(x)$ & $c_0 e_0 = b_0$. Since $b_0 \in P - P^2$.
  WLOG $c_0 \in P$ & $e_0 \notin P$, using that P is a prime ideal. (Is proof

cont

We WTJ all coeffs. of $c(x)$ are in P, leading to a contradiction, namely that leading coeff. of $b(x)$ is 1. Not. $c_0 e_1 + e_0 c_1 = b_1 \in P$. So $c_0 e_1 \& e_0 c_1 \in P$, then $c_1 \in P$. By an inductive argument, the leading coefficient $c_j \in P$, which is a contradiction. QED.

- **Application**: $\Phi(x) = x^{p-1} + x^{p-2} + \dots + 1 \in \mathbb{Z}[x]$ where p is a prime. Observe that $(x-1)\Phi(x) = x^p - 1$. Observe also that $b(x) \in \mathbb{Z}[x]$, $b(x)$ is irred. in $\mathbb{Z}[x]$ iff $\forall\, c \in \mathbb{Z}$ $b(x-c)$ is irred. Now consider

$$\Phi(x+1) = \frac{(x+1)^p - 1}{x+1-1} = \frac{x^p + pu(x) + px}{x}$$

$= x^{p-1} + pv(x) + p$, which satisfies Eisenstein's Thm.

So $\Phi(x)$ is irred. in $\mathbb{Z}[x]$. But also irred over $\mathbb{Q}$ since it's monic.

- **Modules & vector spaces**

R is a ring. A (left) R-module is a set M s.t. $(M, +)$ is an Abelian group, R "acts" on M $\forall\, r \in R$ & $\forall\, m \in M$, $rm \in M$.

$\forall\, r, s \in R$ & $\forall\, m, q \in M$,

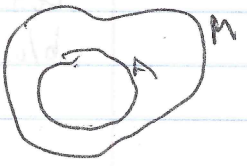
i) $(rs)m = r(sm)$ iii) $(r+s)m = rm + sm$

ii) $r(m+q) = rm + rq$ iv) if R has a unity, $1m = m$, $\in$ "unital module"

- Special attention to ii). Each $r \in R$ determines an Abelian homomorph. $r: M \to M$ (an endomorphism).

Ex] R_R Let $n \in \mathbb{N}$, R^n_R. Let R be a field... then R modules are vector spaces over R.

Ex] An R-submodule A of R-module M → when A closed under subtraction & $\forall\, r \in R$, $rA \subseteq A$.



- An R-module map $\phi: M \to Q$ is an R-module homomorph. if it respects the operation. $\ker \phi = \{m \in M \mid \phi(m) = 0\}$. If ϕ onto, $\phi(M) \cong \frac{M}{\ker \phi}$ → cosets of $\ker \phi$.

• Let F be a field, $p(x) \in F[x]$, $\deg p(x) \leq 3$ is non constant. Then $p(x)$ is irred. in $F[x] \iff p(x)$ has no root in F.

Proof:

If c is a root of $f(x)$, then by the Division alg., $f(x) = (x-c)\,q(x)$.

If $f(x)$ has no root in F & $f(x) = a(x)\,b(x)$ then the factorization has to be trivial, otherwise, WLOG, $a(x)$ has degree one $\Rightarrow$ we would have a root.

• More formal def. of module:

An R-module M is a set w/ an Abelian group under addition and on which a ring R "acts" via various axioms: (these axioms on previous page)

- Submodules

B is a submodule of M, if $B \neq 0$ &

a) B is closed under subtraction

b) $\forall\, r \in R$ & $\forall\, b \in B$, $rb \in B$.

- Homomorphism

Let M & N be R-modules. & $\phi : M \to N$. Then ϕ is an R-module homomorphism if

a) $\forall\, u, v \in M$, $\phi(u+v) = \phi(u) + \phi(v)$

b) $\forall\, r \in R$ & $m \in M$, $\phi(rm) = r\,\phi(m)$.

- Quotient Modules

Let B be a sub module of M. Let's look at $\frac{M}{B}$. $\frac{M}{B}$ is an R-module b/c if we had the coset $m+B$ & $r(m+B) = rm+B$.

cont.

- 1st Isomorphism Thm - can find in book
- Here's a nice class of modules

Let $\mathbb{R}^3$ be itself, & $R=\mathbb{R}[x]$. Fix a 3×3 matrix A. We'll have $\mathbb{R}[x]$ acton $\mathbb{R}^3$ as follows. For $g(x)\in\mathbb{R}[x]$ & $v\in\mathbb{R}^3$ w/ $g(x)\cdot v = g(A)v$.

Vector spaces (Special Modules)

Note: (Here we will use F as a field)

Ex] $\mathbb{R}^3$ is an $\mathbb{R}$-module. Ex] $\mathbb{Z}_2^n$ where $n\in\mathbb{N}$

Ex] $\mathbb{R}^n$ generalizes the previous one

Ex] $\mathbb{R}$ is a vector space over $\mathbb{Q}$. ($\mathbb{Q}$-module or $\mathbb{Q}$ vector space)

Ex] $\mathbb{C}$ is a vector space over $\mathbb{Q}$ Ex] $\{q_0+q_1\sqrt{2} \mid q_0,q_1\in\mathbb{Q}\}$ over $\mathbb{Q}$

Ex] $\mathbb{C}$ is a vector space over $\mathbb{R}$.

Ex] $F[x]$ is a vector space over F.

Ex] $F[x]$, $p(x)\in F[x]$, $\deg(p(x))=n\in\mathbb{N}$. $\frac{F[x]}{(p(x))} = \{\alpha_{n-1}x^{n-1}+\dots+\alpha_0+(p(x)) \mid$ α's are in $F\}$

- Idea: Span of set, linear independence of a set, & bases (of a vector space)
  - Let V be a vector space, over a field F & let $A=\{v_1,\dots,v_n\}\subseteq V$. The span of A ($sp(A)$) is $\{\sum_{i=1}^{n}\alpha_i v_i \mid \alpha_i$'s are in $F\}$ (set of all linear combinations). Not difficult to see $Sp(A)$ is an F subspace of V.
    - Other properties
      - $Sp(Sp(A))=Sp(A)$.
      - If $B\subseteq Sp(A)$, then $Sp(B)\subseteq Sp(A)$

  - $\{v_1,\dots,v_n\}$ is linearly independent over F if $\alpha_1v_1+\dots+\alpha_nv_n=0$, then $\alpha_1=\dots=\alpha_n=0$.

  Ex] Any set w/ 4 or more elts of $\mathbb{R}^3$ is linearly dependent.

    - Other properties
      - $\{v_1,\dots,v_n\}$ is linearly indep. $\Rightarrow$ if $v\in Sp\{v_1,\dots,v_n\}$, $v=\alpha_1v_1+\dots+\alpha_nv_n$, & v is represented by $\beta_1v_1+\dots+\beta_nv_n$, then $\forall\ i=1,\dots,n$, $\alpha_i=\beta_i$.

cont.

- $A = \{v_1, \dots, v_n\}$ is a basis for V over F if A is linearly indep. & $sp(A) = V$.

- Lemma: If $A = \{v_1, \dots, v_n\}$ spans V & no proper subset of A spans V, then A is linearly indep. So A is a basis for V.

Proof: By way of contradiction,

If $0 = \alpha_1 v_1 + \dots + \alpha_n v_n$ w/ at least one $\alpha_i \neq 0$. WLOG, let $\alpha_1 \neq 0$. So $-\alpha_1 v_1 = \alpha_2 v_2 + \dots + \alpha_n v_n$

$\Rightarrow v_1 = -\frac{\alpha_2}{\alpha_1} v_2 + \dots + -\frac{\alpha_n}{\alpha_1} v_n$

$\Rightarrow v_1 \in sp\{v_2, \dots, v_n\} \Rightarrow sp\{v_2, \dots, v_n\} = sp\{v_1, \dots, v_n\} = V$

which gives us our contradiction. QED.

- Prop: Suppose we have a vector space V & $\{v_1, \dots, v_n\}$ is a basis for V & $\{w_1, \dots, w_m\}$ is a linearly independent subset of V. Then $\exists$ an ordering of $\{v_1, \dots, v_n\}$ s.t. $\forall\ m \geq k \geq 0$, $\{v_1, \dots, w_k, v_{k+1}, \dots, v_n\}$ is a basis of V.

Proof: Ran out of time, but it's by induction.

rewriting of this:

- Prop: V is a vector space over a field F w/ $\{w_1, \dots, w_m\}$ that's linearly independent. & $\{v_1, \dots, v_n\}$ is a basis for V over F. Then for $j = 0, \dots$ where $m \geq k \geq 0$, the set $\{v_1, \dots, v_n\}$ can be ordered so that $\{w_1, \dots, w_j, v_{j+1}, \dots, v_n\}$ is a basis for V over F.

Proof:

By induction on j. w/ $j = 0$ we have nothing to show. Assume an induction hypothesis. The statement holds for $i \leq j$ for some $j \in \mathbb{N}$. Now we prove it for $j+1$. Well, $w_{j+1} \in V$.

$w_{j+1} = \beta_1 v_1 + \dots + \beta_j v_j + \alpha_{j+1} v_{j+1} + \dots + \alpha_n v_n$. Observation... at least one $\alpha_{j+1}, \dots, \alpha_n$ is not 0, otherwise $\{w_1, \dots, w_m\}$ is not linearly indep. WLOG assume $\alpha_{j+1} \neq 0$. Solve for v_{j+1} in terms of $w_1, \dots, w_j, v_{j+2}, \dots, v_n$. Claim: $\{w_1, \dots, w_j, w_{j+1}, v_{j+2}, \dots, v_n\}$ is a basis for V.

Cont.

proof cont.
Surely the span $\{v_1,\dots,v_j,w_{j+1},v_{j+2},\dots,v_n\}$ is V. Since that span contains v_{j+1} so that span contains $\{w_1,\dots,v_j,w_{j+1},\dots,v_n\}$ where by induction hypothesis it is a basis ... it spans.
Suppose $\beta_1 v_1 + \dots + \beta_{j+1} v_{j+1} + \alpha_{j+2} v_{j+2} + \dots + \alpha_n v_n = 0$ where β's & α's are in F. Substitute v_{j+1}...

You know what? read this on in the book.

- Corollary: If $\{v_1,\dots,v_n\}$ is a basis & $\{w_1,\dots,v_m\}$ are linearly independent. ① Then $n \geq m$. ~~② $n=m$~~ ③ Using that $m \leq n$, $\{w_1,\dots,v_n\}$ can be ~~Corollary: If $\{v_1,\dots,v_n\}$ is linearly indep~~ extended to a basis of X_i ④ So if V has a finite basis, then V has a dimension: The size of each basis.

Ex) $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$. We've shown it's a field.
The book writes "$K/\mathbb{Q}$" means K is a field extension of $\mathbb{Q}$. Observe that K is a vectorspace over $\mathbb{Q}$, what is dimension of K over $\mathbb{Q}$?
"$[K:\mathbb{Q}]$" or "$\dim(K/\mathbb{Q})$". Observe $\mathrm{sp}\{1,\sqrt{2}\} = K$ (over $\mathbb{Q}$), moreover $\{1,\sqrt{2}\}$ is lin. indep. over $\mathbb{Q}$ b/c $\sqrt{2}$ is irrational.

→ — Question:
$\mathbb{Q}(2^{1/3})$ ... by def. the smallest subfield $\mathbb{Q}$ in $\mathbb{C}$ that contains $2^{1/3}$

- Fact:
If $\{F_\alpha : \alpha \in I\}$ is a collection of subfields of K (a field) Then $\bigcap_{\alpha\in I} F_\alpha$ is a subfield, Clearly it's a sub ring & if $\beta \in \bigcap_{\alpha\in I} F_\alpha - \{0\}$, β has an inverse since it has an inverse in each F_α & the inverse is unique in K.

- Def: Let K be a field. The prime subfield of K is the least subfield contained in K.
- Interestingly, The prime subfield of any field K is either isomorphic to $\mathbb{Q}$ or to $\mathbb{Z}_p$ where p is prime.

- Def: The characteristic of a field K is $\begin{cases} n \text{ s.t. } n \text{ is the min. such } n\cdot 1_K = 0 \text{ if min exists} \\ 0 \text{ otherwise} \end{cases}$

Ex) $\mathbb{Q}$ has characteristic 0 & $\mathbb{Z}_p$ has characteristic p.

- **Lemma:** If K is a field, it's characteristic is 0 or p which is prime.

  Proof:

  Suppose $\text{char}(K) = n$ where $n \in \mathbb{N}$ & $n = st \ni \{s,t\} \subseteq \mathbb{N}$.
  So $st = n = 0$ in K & since K is an integral domain, s or t is already 0 by minimality of n, s or $t = n$. Thus the $\text{char}(K) \neq 0$, $\text{char}(K)$ is a prime. QED

- If $\text{char}(K) = p$, then $\exists$ an isomorphic copy of $\mathbb{Z}_p$ in K.
  $\langle 1_K \rangle = (1_K)$. If ~~char~~ $\text{char}(K) = 0$, $\exists$ a copy of $\mathbb{Z}$ in K... $\mathbb{Q}$.

- **Extensions & roots**

  Suppose $p(x) \in F[x]$, $p(x)$ is irred. So $p(x)$ has no roots in F.

- **Prop:** $\exists$ an extension field K/F in which $p(x)$ has a root.

  Proof:

  Consider $K = \frac{F[x]}{(p(x))}$, a field (why $p(x)$ is irred). Note that F is naturally embedded in $F[x]/(p(x))$. Consider $x + (p(x)) \in F[x]/(p(x))$. Apply $p(x)$ to $x + (p(x))$: let $p(x) = x^n + \dots + a_0 \in F[x]$. So

  $$p(x + (p(x))) = (x + (p(x)))^n + a_{n-1}(x + (p(x)))^{n-1} + \dots + a_0 + (p(x))$$
  $$= p(x) + (p(x)) = (p(x)) = 0,$$ so we have a root.

- **Notation**

  $\theta \to x + (p(x))$. So elts. $\frac{F[x]}{(p(x))}$ are polys in θ w/ coeffs. in F, moreover reducing "mod $p(\theta) = 0$".

• **Double extension**: $F \subseteq K \subseteq L$

Is a double extension of vector spaces, ie $\frac{K}{F}$ (K field exten. of F) & $\frac{L}{K}$.

Ex] $\mathbb{Q} = F \quad K = \mathbb{Q}(\sqrt{2})$

$L = (\mathbb{Q}(\sqrt{2}))(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$\dim\left(\frac{K}{L}\right) = [K:L] = 4 = 2 \cdot 2$

Prop: In notation above, $[L:F] = [L:K][K:F]$. (finiteness assumed)

Proof: Assume $\{v_1, \dots, v_n\}$ is a basis for L over K, & $\{w_1, \dots, w_m\}$ is a basis for K over F. **Claim**: $\{v_i w_j \mid 1 \le i \le n, 1 \le j \le m\}$ is a basis for L over F.

Proof of Claim: Let $v \in L$. By hypothesis, $\exists\ \alpha_1, \dots, \alpha_n \in K \ni$

$v = \alpha_1 v_1 + \dots + \alpha_n v_n = (\beta_{11} w_1 + \dots + \beta_{1m} w_m) v_1 + \dots + (\beta_{n1} w_1 + \dots + \beta_{nm} w_m) v_n$. Now expand & see v as an F combination of $\{v_i w_j \mid \dots\}$. Now suppose $0 = \sum f_{ij} v_i w_j$ where the f_{ij}'s are in F.

So $0 = \left(\sum_{j=1}^{m} f_{1j} w_j\right) v_1 + \dots + \left(\sum_{j=1}^{m} f_{nj} w_j\right) v_n$. So each parenthesized expression is 0 b/c basis l.i. stuff. Since each $\{w_1, \dots, w_m\}$ is l.i. over F & each is equal to 0, each $f_{ij} = 0$ as well. QED.

• **Prop**: F is a field, $p(x)$ is irred over F, $\deg(p(x)) = n \in \mathbb{N}$. Then $\exists$ a field extension K of $F \ni p(x)$ has a root in K. (did this last time).

In fact w/ $K = \frac{F[x]}{(p(x))}$ (a field since $p(x)$ is irred over F).

$x + (p(x)) \in K$, is root of $p(x)$, & $[K:F] = n$

Proof last time

Ex] $\mathbb{Z}_2 = F$, $x^2 + x + 1 \in \mathbb{Z}_2[x]$ is irred over $\mathbb{Z}_2$ b/c $x^2 + x + 1$ has $2 \le 3$ & no root in $\mathbb{Z}_2$

Cont.

$cis(x) = \cos(x) + i\sin(x)$

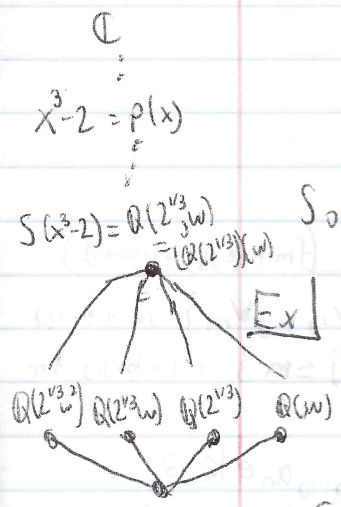
Ex $\frac{\mathbb{Z}_2[x]}{(x^2+x+1)} = K$ contains a root, $x + (x^2+x+1) = \theta$. Note

$\left|\frac{\mathbb{Z}_2[x]}{(x^2+x+1)}\right| = 4$

·	0	1	θ	$\theta+1$
0	0	0	0	0
1	0	1	θ	$\theta+1$
θ	0	θ	$\theta+1$	1
$\theta+1$	0	$\theta+1$	1	θ

x^2+x+1 has more than one root in K. Find it.

So K splits x^2+x+1 into a product of K linear factors.



Ex $\mathbb{Q}[x]$, $x^3-2 \in \mathbb{Q}[x]$, working in $\mathbb{C}$. We have 3 roots, none in $\mathbb{Q}$.

$w = cis\left(\frac{2\pi}{3}\right)$

$2^{1/3}w$ & $2^{1/3}w^2$

So no root of $x^3-2 \in \mathbb{Q}[x]$ in $\mathbb{Q}$ & $\deg = 3$. it's irred. So $\frac{\mathbb{Q}[x]}{(x^3-2)}$ would have a root.

Notes from last time are electronic. Taking a step ahead:

- $p(x)$ is irred. over F. So $\frac{F[x]}{(p(x))}$ has a root $\theta = x + (p(x))$
- Claim: $\frac{F[x]}{(p(x))} \cong F(\alpha)$ where $p(x) \in F[x]$, $\alpha = \deg(p) = n$.

  Proof: $\Gamma : F[x] \to F(\alpha) = F(\alpha)$ (the second $F(\alpha)$ is "stays on to")

  $u(x) \mapsto u(\alpha)$

  $\ker \Gamma = (p(x))$. Using 1st isomorphism thm, we're done.

  QED

read this stuff here

Note: $\left[\frac{F[x]}{(p(x))} : F\right] = \deg(p(x)) = n$

Recall: $K/F \Rightarrow K$ extends F.

• K/F & $\alpha \in K$. α is <u>algebraic</u> over F if $\exists$ $p(x) \in F[x]$ that has α as a root.

<u>Ex</u> $2^{1/3} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$

<u>nonEx</u> Only countably poly's in $\mathbb{Q}[x]$ so only countably many algebraic elts in $\mathbb{C}$ over $\mathbb{Q}$.

<u>Ex</u> $\mathbb{Q}(t) = \left\{ \frac{p(t)}{q(t)} \mid p(t) \in \mathbb{Q}[t],\ q(t) \in \mathbb{Q}[t],\ q(t) \neq 0 \right\}$.
t is <u>not</u> algebraic in $\mathbb{Q}(t)$ over $\mathbb{Q}$

- <u>Defn</u>: $\alpha \in K/F$ is algebraic. Let $m_{\alpha,F}(x)$ be a monic polynomial in $F[x]$ of least degree having α as a root. ← <u>minimal poly.</u>

<u>Ex</u> $2^{1/3}$ in $\mathbb{C}/\mathbb{Q}$

$m_{2^{1/3},\mathbb{Q}}(x) = x^3 - 2$.

- Observation: $m_{\alpha,F}(x)$ is <u>irreducible</u> over $F[x]$

- Now α is algebraic over K/F & $m_{\alpha,F}(x)$ is minimal poly, $F(\alpha) \cong \frac{F[x]}{(m_{\alpha,F}(x))}$

• <u>Lemma</u>: If K/F is finite, then every elt. in K is algebraic over F.

<u>Proof</u>: Let $\beta \in K/F$. Let $n = [F:K] \in \mathbb{N}$
$\Rightarrow [F(\beta):F] \leq n$. Consider $\{1, \alpha, \alpha^2, \ldots, \alpha^n\} \subseteq K$. So $\exists$ $c_0, \ldots, c_n \in F$ $\ni$ $c_0 + c_1\alpha + \ldots + c_n\alpha^n = 0$, all at least one $c_i \neq 0$.
Let $v(x) = c_n x^n + \ldots + c_0$, so $v(\alpha) = 0$. QED

• <u>Lemma</u>: $F \leq K \leq L$. If K is algebraic over F, L is algebraic over K, Then L is algebraic over F.

[<u>Defn</u>: K/F is <u>algebraic</u> if every elt. in K is algebraic over F]

<u>Proof</u>:
Let $\beta \in K$. Since L is alg over K, $\exists$ $s(x) \in K[x]$ & $s(\beta) = 0$, $s(x) = s_m x^m + \ldots + s_0$. The s_i's are in K. Consider $F(s_0, \ldots, s_m)$ & since K is alg over F, $[F(s_0, \ldots, s_m) : F]$ is finite; "inductively" & $[F(\alpha, s_0, \ldots, s_m) : F]$ is finite. Now $F(\alpha, s_0, \ldots, s_m)$ is algebraic over F. So α is algebraic over F. QED

Read Emil Artin Bio

• Prop: K/F. The algebraic elts of K over F, $Alg(K/F)$, form a subfield of K.

Proof: Let $\alpha, \beta \in Alg(K/F)$. Consider $F(\alpha,\beta) = (F(\alpha))(\beta)$ which by double extension thm, is in our F.

By Lemma 1, $F(\alpha,\beta)$ is algebraic. $\alpha^{-1} \in F(\alpha,\beta)$, $\alpha - \beta \in F(\alpha,\beta)$

- Def: A field K is <u>algebraically closed</u> if every polynomial $f(x) \in K[x]$ "splits" into linear finite factors in $K[x]$

- Given a field F, does there exist an extension of K/F which is algebraically closed?

Yes. Proof is due to Artin

Proof's in book, →

<u>Beginning of Proof:</u>

F is a field. To every poly, $p(x) = a_n x^n + \dots + a_0 \in F[x]$. . . . .

Info on splitting fields in electronic notes.

• Thm: F is a field, then $\exists$ an algebraically closed field containing F

proof is also in book →

<u>Proof:</u>

$\forall$ degree (monic) for greater polynomial $f(x) \in F[x]$ form a variable x_f. Look in $F[\dots, x_f, \dots]$.

Let $I := (\dots, f(x_f), \dots)$ ← ideal.

ranging over all monic deg > 0 poly's f.

Claim is that I is proper in $F[\dots, x_f, \dots]$.

Proof claim: contradiction. Otherwise $\exists$ $g_1, \dots, g_k$ & $f_1(x_{f_1}), \dots, f_k(x_{f_k})$ so $1 = g_1 f_1(x_{f_1}) + \dots + g_k f_k(x_{f_k})$

By the abstract construction, $\exists$ a field $K = F(\theta_1, \dots, \theta_k)$ where θ_i are roots in f_i.

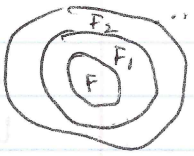
In K, $1 = 0$, so I is proper. Since $F[\dots, x_f, \dots]$ is ring w/ 1, we can use Zorn's Lemma to construct a maximal ideal $\mathfrak{M}$ containing I.

Form $F[\dots, x_f, \dots]/\mathfrak{m} := F_1$. Let $f(x)$ be a poly in $F[x]$.

cont.

Proof cont.

Consider $x_1 + I$. What is $f(x_1 + I)$?
$f(x_1 + I) = f(x_1) + I$ b/c $f(x_1) \in I$. $(x^n + \dots + a_0)(x_1 + I) = f(x_1) + I$
$= 0$. All polys in F have roots in F_1, which is a field.
Repeat $F_1 \hookrightarrow F_2 \hookrightarrow \dots$ Form K, taking union b/c



Now let $s(x) = x^n + \dots + k_1 x + k_0 \in K[x]$.
$\exists\, n \in \mathbb{N} \ni \{k_0, k_1, \dots, k_{n-1}\} \subseteq F_n$ & has roots in $F_{n+1} \subseteq K$.
QED.

- Separable:

A poly $a(x) \in F[x]$ is separable over F if $a(x)$ splits into distinct linear factors.

- Def: $D_x(a(x))$ when $a(x) = a_n x^n + \dots + a_0$
  $= n a_n x^{n-1} + a_{n-1}(n-1) x^{n-2} + \dots + a_1$ (derivative)
  So $D_x(f+g) = D_x(f) + D_x(g)$
  $D_x(fg) = D_x(f)\, g + D_x(g) f$

- Lemma: (1) $a(x)$ is separable iff all roots α of $a(x)$, α is not a root of $D_x(f)$
  (2) $a(x)$ is irred & separable iff $\gcd(a(x), D_x(a(x))) = 1$.

- A bit of review, but important & possibly on test
- K/F is an extension. $b \in K$. Lemma: b is algebraic iff $[F(b):F]$ is finite.
  Proof: b is alg. over F, it has a minimal poly $m_{b,F}(x)$, an irreducible, say of degree n. So $[F(b):F] = n \in \mathbb{N}$. Conversely if $[F(b):F] = n \in \mathbb{N}$, then $\{1, b, \dots, b^n\}$ is lin. dept. So $\exists$ $c_0, \dots, c_n \in F$, $c_0 + \dots + c_n b^n = 0$ & form $a(x) = c_0 + \dots + c_n x^n$ which kills b, witnessing that b is algebraic.
  QED.

Cont.

~~Lemma 2: If K is alg. over F, L is alg. over K~~

Lemma 2: L/K is alg, K/F is alg. $\Rightarrow$ L/F is alg.

Proof: Let $b \in L$. Since b is alg over K, $\exists$
$x^m + k_{m-1}x^{m-1} + \dots + k_1 x + k_0 = a(x)$ having b as a root.
Now coeffs of $a(x)$ are alg. over F, & by ~~a~~ an earlier Lemma, $[F(k_0):F]$ is finite. Inductively,
$[F(k_0,\dots,k_{m-1}):F]$ is finite. Now consider b is alg. over $F(k_0,\dots,k_{m-1})$, & now $[F(k_0,\dots,k_{m-1})(b):F(k_0,\dots,k_{m-1})]$ is finite.
So $[F(k_0,\dots,k_{m-1},b):F]$ is finite, so b is alg. over F by Lemma 0.

- Recall $D_x(f)$ (the derivative of x).

Lemma: α is a repeated root of $f(x)$ iff α is a root of $D_x(f)$.

Proof: ($\Rightarrow$) α is a repeated root of f.
$f(x) = (x-\alpha)^2 g(x)$ so
$D_x(f) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$
($\Leftarrow$) Conversely if $D_x(f)$ has a root at α, we have
$f(x) = (x-\alpha)h(x)$. Now $D_x(f) = h(x) + (x-\alpha)h'(x)$
So $h(\alpha) = 0$. So f has a double root at α. QED

Observation: f is separable if $(f, D_x(f)) = 1$

Corollary: If F has char. 0, then every irreducible poly over F is separable.

What about when F has char p where p is prime?
Our corollary won't work. It's bad when $f(x) = a_m x^{pk_m} + \dots + a_1 x^{pk_1} + \dots$

Review before we proceed w/ this thought:
on next page.

Frobenius map ϕ

1) p is prime then $p \mid \binom{p}{i}$, $0 < i < p$. Proof is old from 500 level.

2) R is comm w/ 1, char p. Consider $\phi(x) = x^p$, Note $\phi(x+y) = (x+y)^p = x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i + y^p$, Middle part cancelled by 1) Of course, $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$.
If R is a field, $\ker \phi = \{0\}$ ie. ϕ is injective. If R is a finite field, then R finite $\Rightarrow$ ϕ is a field automorphism.

Now back to our thought. Assume F is a finite field. Note $\phi(x) = x^p$ is bijective. $\forall\, b \in F\ \exists\, c \in F \ni b = c^p$.
So when $f(x) = a_m x^{pk_m} + \dots + a_1 x^{pk_1} + a_0$,

$f(x) = f_1(x^p)$ where

$f_1(x) = a_m x^{k_m} + \dots + a_1 x^{k_1} + a_0$. Also

$f(x) = (f_2(x))^p$ when $b_i^p = a_i$ works b/c char $F = 0$.

$D_x(f) = 0$ if f is not irrel.

Proof in book $\Rightarrow$ — Corollary: If F has char 0, or is finite, then every irrel. poly. is separable.

— Side: K/F. Where K is a separable extension, then $\mathrm{Aut}_F(K)$ is called the Galois group of K/F.

Fact: If $a(x), b(x)$ are monic & irreducible in $F[x]$, they contain no common root in the extension of F.

Proof:

Since $a(x), b(x)$ are monic irred, & different, $(a(x), b(x)) = 1$.
So since $F[x]$ is a Euclidean domain $\exists\, s(x), t(x) \in F[x] \ni$
$1 = s(x)a(x) + t(x)b(x)$. If c was a common root of $a(x)$ & $b(x)$ in an extension of K/F, then $0 = 1$ since cont.

$1 = s(c)a(c) + t(c)b(c) = 0 + 0$. QED.

- In "our" setting (char = 0 or finite field), splitting field of $f(x) = p_1(x) \cdots p_r(x)$, [distinct irred factors] is formed by adding $\deg p_1 + \cdots + \deg p_r$ distinct roots.

- Finite Fields

Fact: $K/F \Rightarrow K$ is a vectorspace over F

- K is a finite field so $\exists$ prime p, $n \in \mathbb{N}$ s.t. $|K| = p^n$. $|K^*| = p^n - 1$, $K^* = K - \{0\}$ (K^* is multiplicative group).

We know from Lagrange that any finite group G, all $a \in G$, $a^{|G|} = e$, the identity. So $b \in K - \{0\}$, $b^{p^n - 1} = 1$.

So all $c \in K$, $c^{p^n} = c$. So every elt. $c \in K$ is a root of $f(x) = x^{p^n} - x$. Also $Dx(f(x)) = -1 \neq 0$ so $f(x)$ is separable.

So K splits $f(x) = x^{p^n} - x$ & since $f(x)$ is separable, any proper subfield of K can't split $f(x)$. So K is a splitting field of $f(x)$ over $\mathbb{Z}_p$.
Up to isomorphism, there's only one splitting field of $f(x)$.

Corollary: There is a unique field up to isomorphism of order p^n where p is prime & $n \in \mathbb{N}$.

Review:
K^* is cyclic
Cyclic groups
G is cyclic: 1) Then every subgroup of G is cyclic
2) If G is finite, $|G| = n$
Therefore every $d \mid n$, $\exists$ a unique subgroup $H \leq G$, $|H| = d$
If $G = \langle g \rangle$, to get unique, $H \leq G$, $|H| = d$, $H = \langle g^{n/d} \rangle$.

Subfields of a finite field K, $|K| = p^n$?

$|J^*| \mid p^n - 1$

$|J^*| = p^k - 1$ for some $k \in \mathbb{N}$, $p^k - 1 \mid p^n - 1$. (iff $k \mid n$) — proof in homework

- $\phi(x) = x^p$ (Frobenius map) is in $\mathrm{Aut}_{F_p} K$ b/c $a \in F_p$ so $a^p = a$.
  $\phi^j(x) = x^{p^j}$ so $\phi^n(x) = id_K$ b/c $|K| = p^n$.

Notation: $\mathrm{Aut}_F(K) = \mathrm{Aut}(K/F)$.

- When $f(x)$ is separable, $f(x) \in F[x]$ & S is a splitting field of $f(x)$, then $\mathrm{Aut}(S/F)$ is the Galois group of $f(x)$.

read more on this

* Cyclotomic Polynomials

Recall that if p is prime, $x^p - 1 = (x-1)(x^{p-1} + \dots + x + 1)$ ↳ $\Phi_p(x)$

we showed $\Phi_p(x)$ is irred. using Eisenstein

$x^n - 1$ roots in $\mathbb{C}$. The nth roots of unity form a subgroup of $\mathbb{C}$, a cyclic subgroup generated by $e^{\frac{2\pi i}{n}}$. A primitive n^{th} root of unity: $\Psi \in \mu_n$ that are generators.

The 2^{th} roots of unity: 1 & -1

Def: $\Phi_n(x) = \prod (x - \Psi)$ where Ψ is primitive

Ex: $\Phi_2(x) = x + 1$

$\Phi_3(x) = (x - e^{\frac{2\pi i}{3}})(x - e^{\frac{2\pi i (2)}{3}}) \in \mathbb{Z}[x]$

Lemma: $\Phi_n(x) \in \mathbb{Z}[x] \quad \forall n \in \mathbb{N}$.

Proof:

$x^n - 1 = \Phi_n(x) \prod_{\substack{d \mid n \\ n > d}} \phi_d(x)$. Proof is by induction on n.

Base case: see $n = 2$

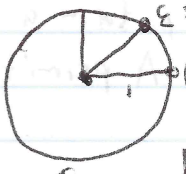
Look at ⊛ & see it is a factorization in $\mathbb{Q}(\varepsilon)[x]$, where ε is a primitive root of unity. So using the division thm, we can do long division. By the induction hypothesis, $\prod_{\substack{d \mid n \\ n > d}} \phi_d(x) \in \mathbb{Z}[x]$. So $\phi_n(x) \in \mathbb{Q}[x]$. By Gauss's Lemma, $\phi_n(x) \in \mathbb{Z}[x]$.

- Thm: $\Phi_n(x)$ is irred. over $\mathbb{Q}$. Proof next time.

• **Def:** When K is a field extension over F & $|Aut(K/F)| = [K:F]$, we say that K is Galois over F & denote $Aut(K/F)$ by $Gal(K/F)$.

Ex Is $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ Galois? No, why should $|Aut(\mathbb{Q}(2^{1/3})/\mathbb{Q})| < 3$? We know if $\alpha \in Aut(\mathbb{Q}(2^{1/3})/\mathbb{Q})$ & k is a root of a $\mathbb{Q}$ poly $m(x)$, then $\alpha(k)$ is a root of $m(x)$. So if $\alpha \in Aut(\mathbb{Q}(2^{1/3})/\mathbb{Q})$, what does it do to $2^{1/3}$? Sends it to a root of x^3-2 so to $2^{1/3}$, not in $\mathbb{Q}(2^{1/3}) \dots \mathbb{Q}(2^{1/3}) = \{k_0 + k_1 2^{1/3} + k_2 2^{2/3} \mid k_0, k_1, k_2 \in \mathbb{Q}\}$. What does α do? $\alpha(2^{1/3}) = 2^{1/3}$, so what is α on $\mathbb{Q}(2^{1/3})$? α is the identity then.

- $n \in \mathbb{N}$. $x^n - 1 \in \mathbb{Z}[x]$. nth roots of unity



The n roots of unit $\{cis\left(\frac{2\pi i k}{n}\right) \mid 0 \le k < n\}$, & it's a group. μ_n is cyclic $\{\mu_n = (cis\frac{2\pi i}{n})^j\}$.

The generators of μ_n are called primitive nth roots of unity. primitive 2nd roots: -1 primitive 4th roots: $i, -i$. If ε is primitive nth root of unity, then $|\{\varepsilon^j \mid (j,n) = 1, 0 \le j < n\}| = \varphi(n)$.

Def: $\Phi_n(x) = \prod_{\varepsilon \text{ prim}} (x - \varepsilon)$

so $\Phi_2(x) = x + 1$

$\Phi_4(x) = (x+i)(x-i) = x^2 + 1$

so $x^n - 1 = \prod_{\varepsilon^n = 1} (x - \varepsilon) = \Phi_n(x) \prod_{d \mid n, d < n} \Phi_d(x)$

($\Phi_n(x)$: $f(x)$; $\prod_{d \mid n, d < n} \Phi_d(x)$: $g(x)$) so

$\Phi_n(x) = f(x)\, g(x)$ in over $\mathbb{Q}(\varepsilon)[x]$ is the splitting field of $x^n - 1$.

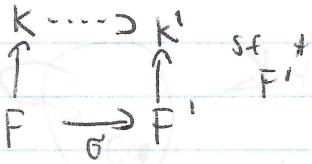
Note we are in Ch. 14.

- The division thm & Gauss's Lemma & in for that $\Phi_n(x) \in \mathbb{Z}[x]$.

• **Thm:** If $\Phi_n(x) \in \mathbb{Q}[x]$ is irred.

Proof: We'll use contradiction, $\Phi_n(x) = f(x)g(x)$. Can assume $f(x)$ is monic & irreducible, WLOG. Roots of $\Phi_n(x)$ are primitive n^{th} roots. Roots of unity partitioned is roots of $f \cup$ roots of g.
Rest of proof in book.
Just read chpter 14.

• K is a splitting field over F & $\exists$ some poly $t(x) \in F[x]$. Go back to the situation $\sigma: F \to F'$ & letting K' be an s.f of $t'(x)$.



s.f of $t'(x)$ over F'. Then $\exists$ an isomorphism $\tilde{\sigma}: K \to K'$ that extends σ.

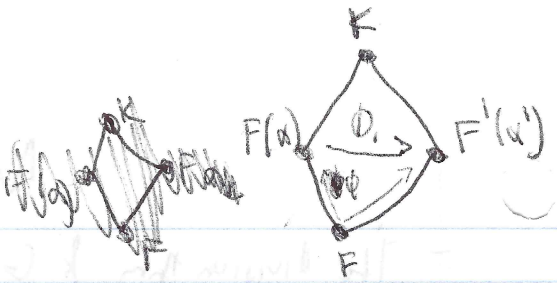
• We have these extensions - we showed they exist.

- Why not count how many such "extensions" there are. Assume $t(x)$ is separable. We'll do it inductively. $t(x) = p_1(x) \cdots p_s(x)$. $F(\alpha) \cong F'(\alpha') \cong F[x]/(p_1(x))$. Note that $K/F(\alpha)$ is a splitting field of $t(x)$ over $F(\alpha)$.

Prop: $t(x)$ is separable.
K is s.f. of $t(x)$ over F. Then the # of extensions is $[K:F]$. proof by induction: # of extensions from $F(\alpha)$ to K & $F'(\alpha')$ to K' is $[K:F(\alpha)] = [K' : F'(\alpha')]$ by induction hyp. (base case) $[K:F] = 1$. Notice that there are $\deg(p_1(x))$ extensions. $\sigma_1: F(\alpha) \to F'(\alpha')$ & t separable $\Rightarrow p_1$ separable. So there are $[F(\alpha):F] = \deg p_1$ maps σ_1. An extension $K_1 \xrightarrow{\sigma_2} K'$ can be found by "composing" two extensions: At least $[K:F]$ extensions.

Conversely any such extension "roots to roots" determines a map $\sigma: F(\alpha) \to F'(\alpha')$, concluding the proof:

Cor: $t(x)$ sep over F & K is the s.f. Then $|\mathrm{Aut}(K/F)| = [K:F]$ so K/F is Galois.
Proof on next page.

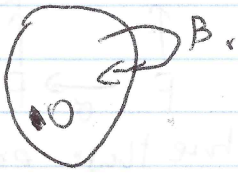


Proof cont:
Let $F \to F'$ w/ σ = identity. Applying thm $\rightsquigarrow$ $k = k'$.
Any extension we've constructed is an automorphism of K pointwise fixing F. By thm, $|Aut(K/F)| = [K:F]$

~~Stupid diagram~~
~~K is a splitting field of a separable poly $f(x)$ in $F[x]$.~~

Def: Let G be a finite group & L be a field. A map $\chi: G \to L$ is an injective group homomorphism is an L-character.

Ex] K is a field & $\beta \in Aut\ K$
$\beta(0) = 0$. So
$\beta: K^\times \to K$ so β is a character.



Lemma: Let G be finite group & L be a field. Then the characters of G over L are linearly independent.
Note: G is finite, order it: $(g_1, g_2, \ldots, g_n)$ where $g_1 = e$.
A function $f: G \to L$, $(f(g_1), \ldots, f(g_n)) \in L^n$. Every such function f is an element in L^n, a vector space over L. So the characters of G over L form a subset of the v-space $\oplus L^n$.
Proof:
next time:
☆ ✡ read in book ✡ ☆

★ look up Euler's function (ϕ).

Thm: Let K be a field, G a finite subgroup of $\mathrm{Aut}K$, & let F be the set $\{b \in K \mid \forall \sigma \in G, \sigma(b)=b\}$. (called the fixed field of G). Then $[K:F] = |G|$.

Proof:

Contradiction: $[K:F] \geq |G|$. Assume $|G| > [K:F]$. Let $\{v_1, \ldots, v_m\}$ be a basis for K over F.

Sketch:

Let $G = \{\sigma_1, \ldots, \sigma_n\}$.

$\sigma_1(v_1)x_1 + \ldots + \sigma_n(v_1)x_n = 0$

$\vdots$

$\sigma_1(v_m)x_1 + \ldots + \sigma_n(v_m)x_n = 0$; $\exists (\beta_1, \ldots, \beta_n)$ non trivial solution.

Let $(a_1, \ldots, a_m) \in F^n$.

★ Read book. Thm 9 ch 14. full proof there. ★

Proof: 2 Parts 1) $[K:F] \geq |G|$ 2) $[K:F] \leq |G|$

by contradiction.

1) Suppose $|G| > [K:F]$. $G = \{\sigma_1, \ldots, \sigma_n\}$ where $\{\alpha_1, \ldots \alpha_m\}$ is a basis for K/F where $n > m$. So

$\sigma_1(\alpha_1)x_1 + \ldots + \sigma_n(\alpha_1)x_n = 0$

$\vdots$

$\sigma_1(\alpha_m)x_1 + \ldots + \sigma_n(\alpha_m)x_n = 0$ .... again, it's in the book

Scott & I prove part 2

~~Suppose $[K:F]=n<\infty$. Let $G \leq Aut\, K$ & $G=\{\sigma_1, \ldots, \sigma_n\}$~~ where

* **Corollary** K/F is a finite extension. Then $[K:F] \geq |Aut(K/F)|$ w/ equality iff F is the fixed field $Aut(K/F)$.

  Proof:

  Let $G = Aut(K/F)$ & let F_1 be the fixed field of G. By Artin & Scott's Thm, $[K:F_1] = |G|$. Also $F \subseteq F_1$ i.e. $[K:F] \geq [K:F_1] = |G|$. Notice we have equality iff fixed field of $Aut(K/F)$ is F.

  Observation: K/F is finite, i.e. $[K:F]$ is finite. Then K/F is Galois iff the fixed field $Aut(K/F)$ is F.

  Ex] $\mathbb{Q}(2^{1/3})/\mathbb{Q}$. $Aut(\mathbb{Q}(2^{1/3})/\mathbb{Q}) = \{e\}$ so not Galois b/c $[\mathbb{Q}(2^{1/3}):\mathbb{Q}] = 3 > |Aut(\mathbb{Q}(2^{1/3})/\mathbb{Q})| = 1$. The fixed field $Aut(\mathbb{Q}(2^{1/3})/\mathbb{Q}) = \mathbb{Q}(2^{1/3})$, so the whole extension.

Let fixed field be $= F$ →

* **Corollary:** K is a field & H & G are finite subgroups of $Aut(K)$, then if the fixed field of H is equal to the fixed field of G, then $H = G$.

  Proof:

  Show that $Aut(K/F) = H = G$. Proof in book.

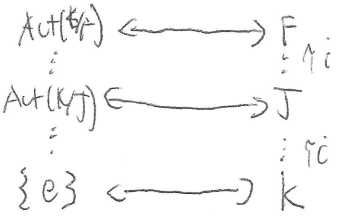
* To prove K/F Galois $\Rightarrow$ existence of $f(x) \in F[x] \ni K$ is s.f of $f(x) \in F[x]$ we'll show if $\gamma \in K - F$, all roots of $m_{\gamma,F}(x)$ are in K & $m_{\gamma,F}(x)$ is separable.

  Proof:

  Pick up γ, $m_{\gamma,F}(x)$ where $\gamma \in K-F$. Look at $\{\sigma_1, \ldots, \sigma_n\} = Aut(K/F)$ & apply each to γ, so $\gamma = \sigma_1(\gamma), \sigma_2(\gamma), \ldots, \sigma_n(\gamma)$.... Form a poly $f(x) = (x-\sigma_1(\gamma)) \cdots (x-\sigma_n(\gamma)) \in K[x]$.

  Observation: $Aut(K)$ acts on $K[x]$ ∋ each $\sigma \in Aut(K)$ acts as an automorphism of $K[x]$. If $\sigma \in Aut(K/F)$, $\sigma(f(x)) = (x-\sigma(\sigma_1(\gamma)))$ $\ldots (x-\sigma\sigma_n(\gamma)) = f(x)$. So the coeffs. of $f(x)$ are fixed by each elt. of $Aut(K/F)$. Since K/F is Galois, the fixed field of K/F is F. So $f(x) \in F[x]$. Note that γ is a root of $f(x)$, so $m_{\gamma,F}(x) \mid f(x)$.

cont.



Proof cont. If γ went to the splitting field of $m_{\gamma,F}(x)$, then $f(x) \mid m_{\gamma,F}(x)$. So $m_{\gamma,F}(x) = f(x)$. So $\sigma_i(\gamma) \in K$ & all roots of $m_{\gamma,F}(x)$ have been accounted for. So $m_{\gamma,F}(x)$ separable splits in K. So K/F is the splitting field for some $f(x) \in F[x]$ by an exercise. QED.

Read book. Fundamental Thm of Galois Theorem.

K is the splitting field for $f(x) \in F[x]$.

(1) There's a bijection between the subgroups of $Aut(K/F)$ & subfields $\{J : K \geq J \geq F\}$.

By one of the corollaries, $\exists$ a bijection $i : Sub(Aut(K/F))$. By the corollary, this is an injection. Let $J \in Subf(K/F)$. Consider $Aut(K/J) \leq Aut(K/F)$. Also K/J is Galois & is s.f of $f(x) \in J[x]$. By fixed field $i(Aut(K/J)) = J$. So i is a bijection.

(2) i maps normal subgroups to splitting fields ... splitting fields are mapped back to normal subgroups. "preserves indices"

Lemma: TFAE

1) J s.f over F
2) $\forall \sigma \in Aut(K/F)$, $\sigma(J) \subseteq J$ ($\sigma(J) = J$)
3) $Aut(K/J) = \sigma^{-1}(J)$ is normal in $G = Aut(K/F)$.

Proof:

1) $\Rightarrow$ 2) $\gamma \in J - F$, All roots of $m_{\gamma,F}(x)$ are in J. Now apply $\sigma \in Aut(K/F)$ to γ... roots-to-roots, completes 1) $\Rightarrow$ 2). QED.

- Reference: K/F is finite, TFAE:

1) K/F is Galois
2) $\gamma \in K$, then all roots of $m_{\gamma,F}(x)$ are in K.
3) Fixed field of $Aut(K/F)$ is F.
4) K is a splitting field of some poly $f(x) \in F[x]$.

Fund. Thm. of Galois: $G = Aut(K/F)$

Assume K/F is Galois. Then the map $i : Sub(G) \to Subf(K/F)$ is an order-reversing bijection, one that preserves "index".

Thm:

If J is an intermediate subfield (i.e. $F \leq J \leq K$), then J is a spl. field of some poly $u(x) \in F[x]$ iff $\mathrm{Aut}(K/J) \trianglelefteq \mathrm{Aut}(K/F)$

$\downarrow$ $\mathrm{Aut}(J/F) \cong \frac{\mathrm{Aut}(K/F)}{\mathrm{Aut}(K/J)}$.

Proof (first part)

TFAE, i) J/F is Galois, ii) $\forall \sigma \in \mathrm{Aut}(K/F)$, $\sigma(J) = J$ & iii) $\mathrm{Aut}(K/J) \trianglelefteq \mathrm{Aut}(K/F)$.

Proof of TFAE bizness:

i $\Rightarrow$ ii

Use 2 from references (on previous page). Let $\gamma \in J$ w/ $m_{\gamma,F}(x)$ its min poly. Let $\sigma \in \mathrm{Aut}(K/F)$, so σ maps roots of $m_{\gamma,F}(x)$ to roots of $m_{\gamma,F}(x)$. Since J/F is Galois, all roots of $m_{\gamma,F}(x)$ are in J. So $\sigma(\gamma) \in J$. Since γ & σ were arbitrary, then we've proven this for all $\sigma \in \mathrm{Aut}(K/F)$, $\sigma(J) \subseteq J$. We get equality from the fact that $\mathrm{Aut}(K/F)$ is finite, so $\sigma(J) = J$.

ii $\Leftrightarrow$ iii

Let $\alpha \in \mathrm{Aut}(K/J)$, $\sigma \in \mathrm{Aut}(K/F)$ & $\gamma \in J$. Consider $\sigma^{-1}\alpha\sigma(\gamma)$. If $\sigma(\gamma) \in J$, then $\sigma^{-1}\alpha\sigma(\gamma) = \sigma^{-1}\sigma(\gamma) = \gamma$. If $\sigma^{-1}\alpha\sigma \in \mathrm{Aut}(K/J)$, then $\sigma^{-1}\alpha\sigma(\gamma) = \gamma$, so $\alpha(\sigma(\gamma)) = \sigma(\gamma)$. If ii) holds, then we're good. But K/J is Galois. So we're still good without ii. but now all "$\sigma(\gamma)$'s" are fixed by $\mathrm{Aut}(K/J)$ so are in J.

ii $\Rightarrow$ i

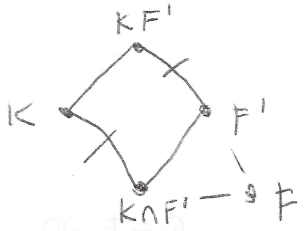
Let $\gamma \in J$ & consider $m_{\gamma,F}(x)$. If γ' is another root of $m_{\gamma,F}(x)$. But $\mathrm{Aut}(K/F)$ acts transitively on roots of irreducible polys, so $\exists\, \sigma \in \mathrm{Aut}(K/F)$ w/ $\sigma(\gamma) = \gamma'$. But $\sigma(J) = J$ which places γ' in J.

last part of proof: WTS if J/F is Galois, $\mathrm{Aut}(J/F) \cong \frac{\mathrm{Aut}(K/F)}{\mathrm{Aut}(K/J)}$.

$\sigma|_J$ is σ restricted by J.

Let $\sigma \in \mathrm{Aut}(K/F)$. Consider $\Gamma : \mathrm{Aut}(K/F) \to \mathrm{Aut}(J/F)$. $\Gamma(\sigma) = \sigma|_J$; well defined by TFAE part. It's clear Γ is a group homo. It's surjective using a ladder argument. The kernel of Γ is $\mathrm{Aut}(K/J)$. So by 1st iso thm we're done.

QED.



• Thm: K/F is Galois, Let have another field F' where $F \subseteq F'$. WTS KF'/F' is Galois & $Aut(KF'/F') \cong Aut(K/K\cap F')$

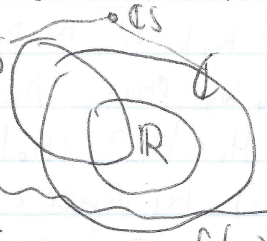
Proof: ⊛

K/F is Galois. So it's s.f. for $f(x) \in F[x]$ & $K = F(r_1,\dots,r_n)$ where $\{r_1,\dots,r_n\}$ are roots of $f(x)$. KF' is smallest subfield containing K & F'. So $KF' = F'(r_1,\dots,r_n)$; $F'(r_1,\dots,r_n)$ is s.f over ~~K~~ F'. Now let $\sigma \in Aut(KF'/F')$, So σ permutes the roots & fixes F' (and thus fixes F), so $\sigma(K) \subseteq K$. Then using finiteness, $\sigma(K) = K$.
Let $\Gamma : Aut(KF'/F') \to Aut(K/K\cap F')$. So $\Gamma(\sigma) = \sigma|_K$. Γ is a well defined onto homo. If $\Gamma(\sigma) = id_K$, then σ fixes K & F' pointwise, so $\sigma = id_{KF'}$ completing the proof. QED.

• Fundamental Thm of Algebra:

If $f(x) \in \mathbb{C}[x]$, it has a root in $\mathbb{C}$.

Reduction: We can assume $f(x)$ has real coefficients, ie. $f(x) \in \mathbb{R}[x]$ by considering $f \cdot \overline{f}(x)$.
We'll argue by contradiction:



Formula s.f of $f(x)$ (S).
$\mathbb{C} = \mathbb{R}[i]$

Proof: Contradiction, Suppose $f(x) \in \mathbb{C}[x]$ but has no root in $\mathbb{C}$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ & let $\overline{f}(x) = x^n + \overline{a_{n-1}}x^{n-1} + \dots + \overline{a_0}$. If $f(x)$ has no roots in $\mathbb{C}$, then $\overline{f}(x)$ has no roots in $\mathbb{C}$. Let $u(x) = f(x)\overline{f}(x)$. Notice $\overline{u}(x) = u(x)$ i.e. $u(x) \in \mathbb{R}[x]$. But also $u(x)$ has no roots in $\mathbb{C}$. Assume $f(x) \in \mathbb{R}[x]$.

Complex conjugation.

Extend $\mathbb{R}$ to a s.f. of $f(x)$, We rely heavily on the fundamental thm of Galois Theory, ie. $G = Aut(K/\mathbb{R}) \dashrightarrow \mathbb{R}$

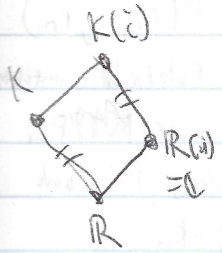
Consider a Sylow 2 subgroup of G, call it H, so $|G| = 2^k m$ where $(2,m) = 1$ & $|H| = 2^k$. Let $[G:H] = n$. So by Fund. Thm of Galois, $[E:\mathbb{R}] = m$. So m is odd.

$H \dashrightarrow E$ (index m)
$\{e\} \longrightarrow K$

Cont.

Proof cont:

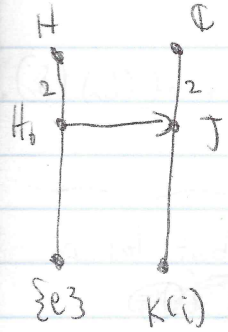
If $n>1$, take $\gamma \in E - \mathbb{R}$ then $[\mathbb{R}(\gamma):\mathbb{R}]$ is odd & greater than 1. So $m_{\gamma,\mathbb{R}}(x)$ has odd degree, so $m_{\gamma,\mathbb{R}}(x)$ has a 0 in $\mathbb{R}$ (Intermediate Value Thm). Use this type of argument to show $f(x)$ has a root in $\mathbb{R}$ (contradiction).



So, $n=1 \Rightarrow H=G \Rightarrow G$ is a 2-group (i.e. $|G|=2^k$).
So by last time's thm H, 2-group, $H \cong \mathrm{Aut}(K(i)/\mathbb{C})$.

Lemma: If A is a p-group, then w/ $|A|=p^j$ where $j \in \mathbb{N}$, then for every $j \geq k \geq 0$ $\exists$ a subgroup B of A w/ $|B|=p^k$.

Induction on proof: We know since A is a p-group, A has a non trivial center $Z(A)$. This is proven w/ the class eqn. Note every subgroup of $Z(A)$ is a normal subgroup b/c $Z(A)$ is Abelian. By Cauchy-for-Abelian, $Z(A)$ has a subgroup of order p, say C. C is normal in A.
Proceed by induction. Consider A/C ... $|A/C|=p^{j-1}$. Apply hypothesis. Find a subgroup of $\overline{D}$ of $A/C \ni |\overline{D}|=p^{k-1}$.
Pull back $\overline{D}$ to $D \leq A$ so $|D|=p^k$.



Back to by proof, $\mathrm{Aut}(K(i)/\mathbb{C}) \cong H$, $|H|=2^s$ where $s \in \mathbb{N}$.
Choose $H_0 \leq H \ni |H_0|=2^{s-1}$. $\exists\ \gamma \in J - \mathbb{C}$ whose min. poly $m_{\gamma,\mathbb{C}}(x)$ has degree 2. QED.

Lemma: $\exists$ a least splitting field L containing K [known as "Galois closure of K"].

Proof:

Assume $\exists$ some Galois extension of K, E, the set of Galois extensions of K is non empty. Let L be the intersection of all such Galois extensions.

Claim: L is Galois over F.

Pf: Recall an extension B/A is Galois iff whenever $\gamma \in B$, all roots of $m_{\gamma,A}(x)$ are in B. So let $\beta \in L$. Now all roots of $m_{\beta,F}(x)$ are in each of the Galois extensions of F. So all are in L.

QED.

• Simple extensions: K/F is a simple extension if $\exists\ \theta \in K \ni F(\theta) = K$.

Ex| If K is a finite field char p (so $|K| = p^n$) we saw that K^* (the multiplicative group of units of K) is cyclic. Say $\langle \theta \rangle = K^*$.
So $K = \mathbb{F}_p(\theta)$

– We've shown every finite field is a simple extension over $\mathbb{F}_p$

• Prop: K/F is Galois & F is infinite. Then K is a simple extension.

Proof:
We'll exploit that there are finitely many subfields $J \ni \{J : F \subseteq J \subseteq K\}$. (b/c of the bijection between $\mathrm{Aut}(K/F)$ between the subfields). It suffices to show then that if $\alpha, \beta \in K$, then $\exists\ \gamma \in K \ni F(\alpha, \beta) = F(\gamma)$ where $F \subseteq \dots \subseteq F(\alpha,\beta) = F(\gamma) \subseteq \dots \subseteq K$. It's sufficient b/c there's only a finite # of subfields. Consider all elts. of the form $\alpha + c\beta$ when $c \in F$. The set $\{\alpha + c\beta : c \in F\}$ is infinite. But there are only finitely many intermediate fields so for some $c_1 \neq c_2$ in F, $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$ (pigeon hole principle). So $\alpha + c_1\beta \in F(\alpha + c_2\beta)$. It's not hard to show from here that but α & β are in $F(\alpha + c_1\beta)$, & so $F(\alpha,\beta) = F(\alpha + c_1\beta)$
QED.

• Radical extensions: ✓ this is it.

– $F = K_0 \subseteq K_1 \subseteq \dots \subseteq K_i \subseteq K_{i+1} \subseteq \dots$
$\forall\ i$, $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ where $a_i \in K_i$ & $n_i \in \mathbb{N}$.

Ex| The s.f. of $x^3 - 2$ over $\mathbb{Q}$,
$\mathbb{Q} \subseteq \mathbb{Q}(2^{1/3}) \subseteq \mathbb{Q}(2^{1/3})(\omega)$

– K/F is a cyclic extension if K/F is Galois & $\mathrm{Gal}(K/F) = \mathrm{Aut}(K/F)$ is cyclic. K/F is Abelian if Galois & $\mathrm{Gal}(K/F)$ is Abelian.

For next time:

• Thm: $K/\mathbb{Q}$ is Galois has roots in a radical extension only if $\mathrm{Gal}(K/\mathbb{Q})$ is solvable.

• A bit of review:

Cyclic $\subseteq$ Abelian $\subseteq$ Nilpotent $\subseteq$ Solvable.

These containments are all proper.

- Nilpotent: A finite group G is nilpotent if $\exists$ a sequence that terminates w/ G as follows:

$$\{e\} \leq Z(G) \leq Z(G/Z(G)) \leq \dots \leq G$$

Ex] Any p group is Nilpotent, b/c it's center is non-trivial & it's non trivial, & it's images are p groups.

- Solvable: A composition series (increasing) for G is a finite sequence

$\{e\} \leq H_1 \leq H_2 \leq \dots \leq H_i \leq H_{i+1} \leq \dots \leq H_n = G$

$\ni H_i \trianglelefteq H_{i+1}$ $\forall i$ & H_{i+1}/H_i is simple.

Recall A is a simple group if it's non-trivial & has exactly 2 normal subgroups

Ex] A is Abelian & simple iff $A \cong \mathbb{Z}_p$ where p is prime.

Thm: The factors (H_{i+1}/H_i) are invariant ie, any composition series for G has the same factors including the multiplicities

Def: A finite group G is solvable if it's factors are cyclic.

Ex] S_3

non abelian, but solvable. $\{e\} \leq A_3 \leq S_3$.

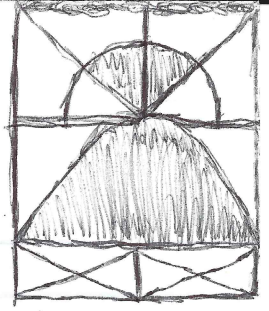
not nilpotent. $Z(S_3) = \{e\}$

better def:

A group G is solvable if it has a composition series all of whose factors $\{G_i/G_{i-1} \mid i = 1, \dots, k\}$ are cyclic.

Ex] - every finite Abelian group is solvable.

- Every finite group G has a comp. series.



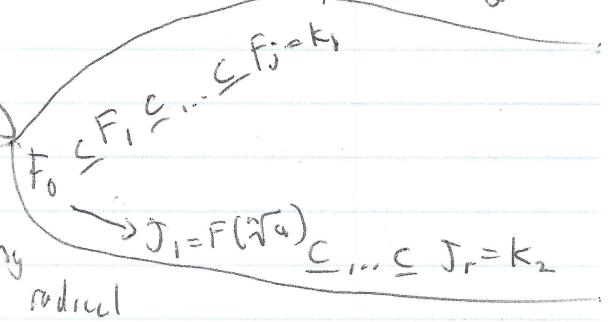
- **Thm: Jordan-Hölder Thm.**
G is a finite group, then the factors of any series are the same as a multiset: [Factors G_i/G_{i-1}, $i=1,\dots,k$].

These are big facts
- If G is solvable, then:
  a) Every subgroup of G is solvable
  b) Every hom of G is solvable.

- Idea for b).
Suppose $N \trianglelefteq G$. Consider G/N. Then:
i) There's a composition series of G containing N.

Induction:
Start w/ $\{e\} \leq N \leq G$. We take a comp. series for N.
$\{e\} \leq H_1 \leq \dots \leq H_{i-1} \leq N = H_i \leq G$. We know G/N has a comp. series: $\{e\} = N \leq K_1/N \leq K_2/N \leq \dots \leq K_j/N = G/N$.
Consider $N \leq K_1 \leq \dots \leq K_j = G$. Also $K_j/K_{j-1} \cong \frac{K_j/N}{K_{j-1}/N}$ by 3rd isom. Thm. So we're done.

- **Extension by roots $\Leftrightarrow$ radical extension.**
$F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_{i-1} \subseteq F_i \subseteq \dots \subseteq K$
where $F_i = F_{i-1}(\sqrt[n_{i-1}]{a_{i-1}})$ where $a_{i-1} \in F_{i-1}$.
α is in a radical extension. $f(x) \in F[x]$.
Now focusing on $f(x)$: all roots of $f(x)$ are contained in some radical extension of F. We'll assume that $\forall\, n_i$ that "occur" in the radical extension that all n_i^{th} roots of unity are in F.
Along similar lines, an observation we can "merge" into a simple radical extension from F to $K_1 K_2$. Given $f(x) \in F[x]$ assume each root α_i, $i=1,\dots,m$ has a radical extension K containing all α_i where $i=1,\dots,m$. Note that K splits $f(x)$. We don't know that K/F is Galois. cont.



-explanation cont.

But we proved that $\exists$ a Galois closure of K, i.e. a least extension J of K that is Galois.

Let $\sigma \in Gal(J/F)$. Consider $\sigma(F) \subseteq \sigma(F_1) \subseteq \dots \subseteq \sigma(F_{i-1}) \subseteq \sigma(F_i) \subseteq \dots \subseteq K$ is also a radical extension.

For various σ, merge these radical extensions to a single radical extension & observe that

$\bigcup_\sigma \sigma(K) = J$ so when we merge the radical extensions we get that J is a radical extension of F

Cb/c J is s.t. $\exists \prod_{r_i, F(x)} \ni K = F[\gamma_1, \dots, \gamma_m]$

So J is a radical extension of F containing all roots of $f(x)$.

$F \subseteq J_{i-1} \subseteq J_i \subseteq \dots \subseteq J_{n-1} \subseteq J_n = J$

$\subseteq$ S $\subseteq$ S is s.t. $\sigma(f(x)) \in F[x]$

$F \subseteq S \subseteq J$.

Look at $F \subseteq \dots \subseteq J_{i-1} \subseteq J_i \subseteq \dots \subseteq J$.

$G_{i-1} \supseteq G_i$

We'll show $J_i = J_{i-1}(\sqrt[n_{i-1}]{a_{i-1}})$

J_i / J_{i-1} is cyclic

So $F(\sqrt[n]{a})$ & the n^{th} roots of unity are in F_1 then $Gal(F(\sqrt[n]{a})/F)$ is cyclic.

Last day of Algebra.

Dawn of the Final Day

- Let K/F be an extension w/ F containing n^{th} roots of unity, & $a \in F$. Then K/F is cyclic & $[K:F] \mid n$.

Proof:

Let $K = F(\sqrt[n]{a})$. The roots of $x^n - a = f(x)$ are $\sqrt[n]{a}$, $\sqrt[n]{a}\,\varepsilon$, $\sqrt[n]{a}\,\varepsilon^2$, ..., $\sqrt[n]{a}\,\varepsilon^{n-1}$, where ε is the primitive n^{th} root of unity. So $\varepsilon \in F$, so all roots of $x^n - a = f(x)$ are in $F(\sqrt[n]{a})$ & it's clear $F(\sqrt[n]{a})$ is a s.f. for $f(x)$. Let $\sigma \in Gal(K/F) = G$. We have $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\,\varepsilon^i$, $i \in \{0, 1, \ldots, n-1\}$ [This is note 1 to roots idea] So $\sigma(\sigma(\sqrt[n]{a})) = \sigma(\sqrt[n]{a}\,\varepsilon^i) = (\sqrt[n]{a}\,\varepsilon^i)\varepsilon^i$. Morgenally, $\sigma(\sqrt[n]{a}\,\varepsilon^j) = \sqrt[n]{a}\,\varepsilon^i\varepsilon^j$. So σ is completely determined by $\sigma(\sqrt[n]{a})$.

If α & $\beta \in Gal(K/F)$, $\alpha\beta(\sqrt[n]{a}) = \alpha(\sqrt[n]{a}\,\varepsilon^k) = \sqrt[n]{a}\,\varepsilon^j\varepsilon^k$ where $\alpha(\sqrt[n]{a}) = \sqrt[n]{a}\,\varepsilon^j$ & $\beta(\sqrt[n]{a}) = \sqrt[n]{a}\,\varepsilon^k$. So, $\alpha\beta(\sqrt[n]{a}) = \beta\alpha(\sqrt[n]{a})$, so $Gal(K/F)$ is Abelian. We can also construct a map $\Gamma: Gal(K/F) \to \mathbb{Z}_n$. So $\Gamma(\beta) = k$, so Γ is an injection. Easy to prove Γ is a homomorphism compatible w/ multiplication in $Gal(K/F)$. Where by $\mathbb{Z}_n$ we mean the additive group. So $Gal(K/F)$ injected into $(\mathbb{Z}_n)$ makes it cyclic & $|Gal(K/F)| \mid n$.

QED.

• Suppose $A(x) \in F[x]$ & all roots of $A(x)$ are contained in a radical extension of F. We showed all roots are contained in a Galois extension J of F.

Proof: Done before.

Last time we showed that the Galois extension of K could also be represented as a radical extension:

$$F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_{i-1} \subseteq F_i \subseteq \dots \subseteq J$$
$$\downarrow \qquad\qquad \downarrow \quad \downarrow \qquad \downarrow$$
$$G = Gal(J_F) \qquad G_{i-1} \quad G_i \qquad \{e\}$$

F_i/F_{i-1} is Galois & cyclic (by previous proof)

J/F_{i-1} is Galois

So by Fund. Thm. of Galois Theory w/

$$\text{cyclic} \to Gal(F_i/F_{i-1}) \cong \frac{Gal(J/F_{i-1})}{Gal(J/F_i)}$$

So $Gal(J/F)$ is solvable. But we want to show that $Gal(S/F)$ is solvable.

Since S is Galois in J, we have $Gal(J/S)$ is normal & $Gal(S/F) \cong \frac{Gal(J/F)}{Gal(J/S)}$

In homework we will show the homomorphic image of a finite solvable group is solvable.

Prove if K/F is cyclic, then $K = F(\sqrt[n]{a})$ for some $a \in F$, some n.

$\Rightarrow$ K/F cyclic w/ $Gal(K/F) = \langle \sigma \rangle$, $[K:F] = n$, & F contains nth roots of unity. Let γ be primitive nth root of unity, & let $\langle \alpha, \gamma \rangle = \gamma^0 \sigma^0(\alpha) + \gamma^1 \sigma^1(\alpha) + \gamma^2 \sigma^2(\alpha) + \dots + \gamma^{n-1} \sigma^{n-1}(\alpha)$. Since $Gal(K/F)$ is lin. independent over K, $\exists \alpha \in K \ni \langle \alpha, \gamma \rangle \neq 0$. (Have $\alpha \in K$ Side.)

Consider $\sigma(\langle \alpha, \gamma \rangle) = \gamma^0 \sigma^1(\alpha) + \gamma^1 \sigma^2(\alpha) + \dots + \gamma^{n-1} \sigma^n(\alpha)$

$\gamma^{n-1} \sigma^0(\alpha)$.

Check that $\sigma(\alpha, \gamma) = \gamma^{n-1}(\alpha, \gamma)$

$\sigma((\alpha, \gamma)^n) = (\sigma(\alpha, \gamma))^n = (\gamma^{n-1}(\alpha, \gamma))^n = (\alpha, \gamma)^n$. So σ fixed $(\alpha, \gamma)^n$. So σ^k fixes $(\alpha, \gamma)^n$ $\forall k = 0, \dots, n-1$, i.e. $Gal(K/F)$ fixes $(\alpha, \gamma)^n$. So $(\alpha, \gamma)^n \in F$.

Proof cont.

This is our "a" i.e. $(\alpha,\gamma)^n = a \in F$. One last thing:
$\sigma^k(\alpha,\gamma) = \gamma^k(\alpha,\gamma)$, so $\sigma^k((\alpha,\gamma)^n) = (\alpha,\gamma)^n$ iff $\sigma^k = \text{identity}$.
Let B/A be Galois, & suppose $\gamma \in B - A$ & $\sigma \in Gal(B/A)$:
$\sigma(\gamma) = \gamma$ iff $\sigma = id_B$, then γ is not contained in any proper subfield of B.
Consider $J = A(\gamma)$ & it's associative group, $i^{-1}(J) = \{e\}$ so $J = B$.
Let $a = (\alpha,\gamma)^n$, so $K = F(\alpha,\gamma)$ & $(\alpha,\gamma) = \sqrt[n]{(\alpha,\gamma)}$. QED.