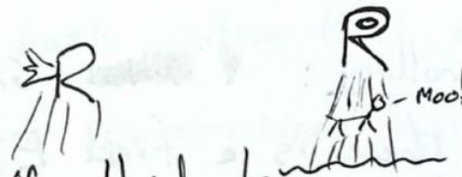
Field Theory



Defn: A ring R is a **PID** iff all ideals are principal and R is an ID.

Prop: If R is a PID, $I \subseteq R$ ideal, $I \neq 0$, I prime $\Rightarrow I$ maximal

Proof: Say $I \neq 0$ is prime, then say I is not maximal.

$I = (p) \subseteq J = (q)$ so $q = ap$ $\sum a \in R$. If $j \in J \setminus I$, then

$j = bq$ $\sum b \in R$ but $j = bq = (ba)p \in (p) = I$ $\not\in$,

So $J = I$ and I is maximal. ∎

Defn: $x \in R$ a **unit** $\iff \exists\, y \quad xy = 1$

$x \in R$ **prime** $\iff x \mid ab \Rightarrow x \mid a$ or $x \mid b$

$x \in R$ **irreducible** $\iff x = uv \Rightarrow u$ or v a unit

In PID, prime $\iff$ irreducible

Theorem: PID $\Rightarrow$ UFD

Theorem: Say F is a field, $p \in F[x]$, $p \neq 0$. Then there is $E \supseteq F$ such that $\exists\, \alpha \in E \quad p(\alpha) = 0$

Proof: Since $F[x]$ is a PID, there exists $r(x) \in F[x]$ irreducible such that $r(x) \mid p(x)$. Consider $I = (r)$.

I is prime b/c r irreducible $\Rightarrow r$ prime $\Rightarrow (r)$ prime.

Define $E = \frac{F[x]}{I}$.

Since I prime, $F[x]$ PID, then I maximal, so E is a field. Consider E a subfield of F by $f \mapsto f + I$.

Then $p(x + I) = 0$ in E. ∎

Corollary: Given a field F, and any $p \in F[x]$, there is a field $E \geq F$ such that all roots of $p(x)$ are in E.

Fact: If $a(x), b(x) \in F[x]$, then there are $q(x), r(x) \in F[x]$ s.t. $a = bq + r$, and $\deg(r) < \deg(b)$.

Prop: Let F be a field, $p \in F[x]$. Then
$$|\{\alpha \in F : p(\alpha) = 0\}| \leq \deg(p).$$

Proof: Inductively divide by $(x - \alpha)$, lowers degree and continue. Can only divide at most $\deg(p)$ many times, each time has remainder zero.

Defn: Let $p \in F[x]$, and $E \geq F$ [is the smallest field] such that all roots of p are in E. Then E is called a splitting field of p over F.

(1) E contains all roots of p

(?) → (2) If K is a field such that $F \leq K \leq E$ then $K = E$. (satisfying (1))

Theorem: For every field F and each $p \in F[x]$, there exists $E \geq F$ a splitting field of p over F.

Proof: Take E^* a splitting field by previous theorem, $E^* \geq F$. Take $E = \bigcap \{E^* \mid E^* \geq F, p \text{ splits in } E^*\}$,

Theorem: If E_1 and E_2 are both splitting fields of p over F, then there is $\phi: E_1 \to E_2$ an isomorphism such that $\phi \restriction F = id_F$.

Proof will take a while to get to.

Basic idea of Galois:

Given $p \in F[x]$ let E_p be its splitting field,

$$Gal(p) := Aut(E_p/F) = \{\phi: E_p \xrightarrow{\sim} E_p \mid \phi \restriction F = id_F\}$$

Galois group of p over F.

Fundamental Theorem of Algebra: For all $p \in \mathbb{C}[x]$, $\deg(p) \geq 1$, there is $\alpha \in \mathbb{C}$ such that $p(\alpha) = 0$.

Defn: A Field F is algebraically closed if $\forall p \in F[x]$, $\deg(p) \geq 1$, there is $\alpha \in F$ such that $p(\alpha) = 0$.

Question: given a field F, can we find $E \geq F$ algebraically closed?

Prop: If E is algebraically closed, then E must be infinite.

Proof: Otherwise, let $\alpha_1, \ldots, \alpha_n$ be the nonzero elements of E.

Define $p(x) = \prod_i (x - \alpha_i) + 1$. Then p has no root in F. ∎

Theorem: For each field F, there is $E \geq F$ that is algebraically closed.

Proof: uses transfinite induction or Zorn's Lemma. Next Time.

Defn: Let E be a field. E is called an algebraic closure of F provided that E is algebraically closed and if $F \leq K \leq E$ is algebraically closed and $K = E$.

Theorem: If E_1 and E_2 are both algebraic closures of F, there is an isomorphism between them that is the identity on F.

Last time:

Theorem: For every field F there exists $E \geq F$ algebraically closed. $(\forall p \in E[x] \quad \exists \alpha \in E \quad p(\alpha) = 0)$

Main Lemma: For every field K there exists a field $K^* \geq K$ such that $\forall p \in K[x], \exists \alpha \in K^* \quad p(\alpha) = 0$

Proof of Theorem: (assumming main lemma)

For each $n \in \mathbb{N}$ define the field F_n such that $F_n = F_{n-1}^*$ and $F_0 = F$, using the lemma.

Now let $E = \bigcup_{n \in \mathbb{N}} F_n$, since $F_{n+1} \geq F_n$, then $E \geq F$.

Furthermore, given $\alpha, \beta \in E$ as $F_n \leq F_k$ for all $k \geq n$, there is $n_0 \in \mathbb{N}$ with $\alpha, \beta \in F_{n_0}$. Since F_{n_0} is a field then $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta^{-1}$, $\alpha\beta \in F_{n_0} \subseteq E$.

E is also algebraically closed, because given $p \in E[x]$ there are $a_0, \dots, a_m \in E$ s.t. $p = \sum_{i=0}^{m} a_i x^i$

Since $\{a_0, \dots, a_m\}$ is a finite subset of E, there is n_0 such that $\{a_0, \dots, a_m\} \subseteq F_{n_0}$. Namely $p \in F_{n_0}[x]$

Using the lemma, F_{n_0+1} contains α such that $p(\alpha) = 0$. p has only finitely many roots, so we can find all roots of p in some F_{n_0+k}. ∎

Proof of Main Lemma: Let $S = K[x]$, $R = K[S]$

Define $A = \{p(y_p) \mid p \in K[x], \deg(p) \geq 2\}$

Let I be the ideal of R generated by A

Claim: $I \neq R$.

If $1 \in I$, then there are $a_0, \ldots, a_n \in A$ and $r_0, \ldots, r_n \in R$ such that $1 = \sum_{i=1}^{n} a_i r_i \in K[S]$, and in particular

$1 \in K[W]$ for some $W \subseteq S$, W finite.

For each i, there is $p_i \in K[x]$ such that $a_i = p_i(y_{p_i})$

There exists $E \geq K$ such that $\exists\ \alpha_0, \ldots, \alpha_n \in E$ such that $p_i(\alpha_i) = 0$.

Consider the equation $1 = \sum a_i r_i$ in $E[S]$; replacing y_{p_i} by α_i.

$$1 = \sum_{i=0}^{n} p_i(\alpha_i)\, r_i = 0 \quad \not\equiv$$

So I is a proper ideal. Extend to a maximal ideal $J \supseteq I$.

Let $K^* = R/J$, which gives the desired field.

Identify K with its image under $K \hookrightarrow K[S] \hookrightarrow \frac{K[S]}{J}$.

Claim: $y_p + J$ is a root of $p \in K[x]$.

If $p = \sum a_k x^k$, then $p(y_p + J) = p(y_p) + J = J = 0_{R/J}$

since $p(y_p) \in A$.

Gives alternative proof for existence of splitting field.

Theorem: Suppose $p \in F[x]$, irreducible of degree n, $E = \frac{F[x]}{(p)}$

Let $\alpha = x + (p) \in E$. Then E is an n-dimensional F-vector space where $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for E.

Proof:

Claim 1: E is generated by $\{\alpha^k : k<n\}$

Claim 2: $\{\alpha^k : k<n\}$ is linearly independent.

Proof of 1: Let $I=(p)$. Given $B\in E$ there is $q\in F[x]$ s.t. $B=q+I$. Divide q by p; $\exists\, a,b\in F[x]$, $q=ap+b$ and $\deg(b)<\deg(p)=n$

$$B=b+I.$$

Since $\deg(b)<n$, $b=\sum_{k<n} c_k x^k \Rightarrow B=\sum_{k<n} c_k \alpha^k \in \operatorname{span}\{\alpha^k \mid k<n\}$

Proof of 2:

Say $\sum_{k<n} b_k \alpha^k = 0$. Let $q(x)=\sum_{k<n} b_k x^k$.

Since $q(x+I)=\sum_{k<n} b_k \alpha^k = 0$, then $q(x)\in I$

So $q\in(p) \Rightarrow q=f\cdot p$ for some $f\in F[x]$.

Hence, since $\deg(q)<\deg(p)$, then we must have that $\deg(f)<0 \Rightarrow f\equiv 0$. Hence $q\equiv 0$, and so $b_k=0$ for all k. Then $\{\alpha^k : k<n\}$ is a linearly independent set. ∎

Theorem: If $F\le K\le E$, then $[E:F]=[E:K][K:F]$.

Ruler + Compass Constructions:

Basic questions: can you construct a square with side lengths $\sqrt{\pi}$? That is, "square the circle?"

Can you trisect an angle?

Which complex numbers can be constructed?

Can make everything in $\mathbb{Q}(i)$.

Suppose we perform a finite construction and obtain $z_1, \dots, z_n \in \mathbb{C}$. Consider $F = \mathbb{Q}(z_1, \dots, z_n)$.

Theorem: $[F:\mathbb{Q}] = 2^k$ for some k.

$F = \left(\dots\left(\left(\mathbb{Q}(z_1)\right)(z_2)\right)\dots\right)(z_n)$, so proof by induction on n.

Adding a single $z \in \mathbb{C}$ gives either a degree 1 or 2 extension, depending on whether or not z is a root of a degree 1 or degree 2 rational polynomial. Then

$$[F:\mathbb{Q}] = \prod_{i=1}^{n} [\mathbb{Q}(z_1, \dots, z_i) : \mathbb{Q}(z_1, \dots, z_{i-1})] . \quad \blacksquare$$

Defn: Suppose $F \leq E$. $\alpha \in E$ is algebraic over F provided that there exists $p \in F[x]$, $p \neq 0$ s.t. $p(\alpha) = 0$.

$\alpha \in E$ is transcendental (over F) if α is not algebraic.

Question: Are there any transcendental numbers?

Mid 19th century: Louiville proved $\alpha := \sum_{k=1}^{\infty} 10^{-k!}$ is transcendental.

1874: Cantor proved that almost every real number is ~~uncountable, and~~ transcendental, and the set of ~~uncount~~ transcendental numbers is uncountable.

Fact: π and e are transcendental.

Recall: $E \geq F$ $\alpha \in E$ is algebraic over $F \iff \exists\, p \in F[x]$, $p \neq 0$, $p(\alpha) = 0$.

Remark: Notice that for all $\alpha \in F$, α is algebraic over F

We will show If $E \geq F$, $K := \{\alpha \in E \mid \alpha \text{ algebraic over } F\}$, then $F \leq K \leq E$

Given a group G and $A \subseteq G$, the <u>subgroup generated by A</u> is

$$\langle A \rangle := \bigcap_{\substack{A \subseteq H \\ H \leq G}} H = \left\{ \prod_{i=n} a_i^{\varepsilon_i} \mid n \in \mathbb{N}, a_i \in A, \varepsilon_i \in \{-1, 1\} \right\}$$

<u>Notation</u>: Suppose $F \leq E$, $A \subseteq E$.

$F(A)$ is the subfield of E generated by A over F,

$$F(A) := \bigcap_{\substack{K \leq E \\ K \geq A \cup F}} K .$$

When $F \leq E$ and there is a finite $A \subseteq E$ such that $F(A) = E$, then E is <u>finitely generated</u> over F.

When $A = \{a\}$, $a \in E$, we write $F(a) := F(\{a\})$

$F(a)$ is called a <u>simple extension</u> of F. (E.g: $\mathbb{C} = \mathbb{R}(i)$)

<u>Defn:</u> $Aut_F(E) := \{\varphi \in Aut(E) \mid \varphi \restriction F = id_F\}$

$Aut_F(E) \leq Aut(E)$ as a group.

<u>Recall:</u> $p \in F[x]$ irreducible, $n = \deg(p)$, $E := \frac{F[x]}{(p)}$, $\alpha = x + (p)$

We showed $[E:F] = n$, and as an F-vector space $E = \text{span}\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$

As $\alpha \in E$ clearly $F(\alpha) \leq E$ and $[F(\alpha):F] \leq n$.

(1) <u>Theorem:</u> Suppose $F \leq E$, $\alpha \in E$. Then the following are equivalent:

(1) α is algebraic over F

(2) $[F(\alpha):F]$ is finite

To prove this, we will need

<u>Theorem 2:</u> Suppose $F \leq E$, $p \in F[x]$ irreducible, $\alpha \in E$, $p(\alpha) = 0$. Then $F(\alpha) \cong \frac{F[x]}{(p)}$ by an isomorphism φ such that $\varphi \restriction F = id_F$.

<u>Proof:</u> Define $\psi : F[x] \to F(\alpha)$, $\psi(\overline{p}) = \overline{p}(\alpha)$. $\ker \psi = (p)$ and $\text{im}\, \psi = F(\alpha)$ so therefore by 1st IM thm ψ gives

IM $\frac{F[x]}{(p)} \cong F(\alpha)$ ∎

~~Proof of (1):~~

Suppose $F \leq E$ fields, $\alpha \in E$

$F[\alpha] := \{p(\alpha) : p \in F[x]\} \leq F(\alpha)$ subring

$$F(\alpha) := \bigcap_{\substack{K \leq E \\ K \supseteq F \cup \{\alpha\}}} K = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; \substack{f,g \in F[x] \\ f(\alpha), g(\alpha) \neq 0} \right\} \leq E$$

Theorem: Suppose $p \in F[x]$ irreducible, $E \geq F$, $\alpha \in E$, $p(\alpha) = 0$.
There exists an isomorphism $\phi: \frac{F[x]}{(p)} \cong F(\alpha)$, s.t. $\phi \upharpoonright F = id_F$ and $F(\alpha) = F[\alpha]$

Proof: Consider $\psi: F[x] \to F[\alpha]$ defined by $\psi(f) = f(\alpha)$, $\forall f \in F[x]$.
Check ψ is HM, $\ker(\psi)$ [illegible], $\operatorname{im}\psi = F[\alpha]$
[illegible] by 1st IM Theorem, $\frac{F[x]}{\ker\psi} \cong F[\alpha]$

[illegible]

Since E is a field, $F[\alpha]$ subring of E, then $F[\alpha]$ is ID.
Hence $\ker(\psi)$ is a prime ideal, but $F[x]$ is a PID so $\ker(\psi)$ most be maximal. Hence $\frac{F[x]}{\ker(\psi)}$ is a field, so then $F[\alpha]$ is a field containing α.
We know $F[\alpha] \subseteq F(\alpha)$, and $F(\alpha)$ is smallest field containing α, so since $F[\alpha]$ is a field, then $F(\alpha) \subseteq F[\alpha] \Rightarrow F[\alpha] = F(\alpha)$.

Since $F[x]$ is a PID, $\ker(\psi) = (q)$. Since $p \in \ker(\psi)$, $p \in (q) \Rightarrow p = fq$ $\exists f \in F[x]$. But p is irreducible, so f must be a unit, so $f \in F$. So $(p) \supseteq (q)$, but q is maximal, so $(p) = (q) = \ker(\psi)$. So ψ is the desired IM. ∎

Corollary: $F \leq E$ fields, if α is algebraic over F, then there exists a monic irreducible $m_\alpha \in F[x]$ s.t. $m_\alpha = 0$ and
$F(\alpha) \cong \frac{F[x]}{(m_\alpha)}$ and $[F(\alpha) : F] = \deg(m_\alpha)$

Corollary: $F \leq E$. Then TFAE
1. $[F(\alpha) : F]$ is finite
2. α is algebraic over F

Proof of second corollary:

② $\Rightarrow$ ① easily

① $\Rightarrow$ ② Suppose $n \in \mathbb{N}$ s.t. $n = [F(\alpha) : F]$

Since $1, \alpha, \cdots, \alpha^n$ are $n+1$ elements of $F(\alpha)$, there is a nontrivial linear dependence among them. Hence,

$$\sum_{i=0}^{n} a_i \alpha^i = 0 \quad \text{where not all } a_i \text{ are zero.}$$

So let $p(x) = \sum_{i=0}^{n} a_i x^i$, and $p(\alpha) = 0$, $p \in F[x]$, so α alg. / F. ■

Question: If $F \leq E$ fields, $\alpha, \beta \in E$ algebraic over F, then is $\alpha + \beta$ algebraic over F? Yes.

Theorem: Say $F \leq E$, consider $K = \{\alpha \in E \mid \alpha \text{ algebraic over } F\}$. Then $K \leq E$.

Proof: Given $\alpha, \beta \in K$, by previous fact, enough to show $F(\alpha, \beta)$ is a finite dimensional F-vector space.

$$F(\alpha, \beta) = F(\alpha)(\beta) \Rightarrow [F(\alpha, \beta) : F(\alpha)]\,[F(\alpha) : F] = [F(\alpha, \beta) : F].$$

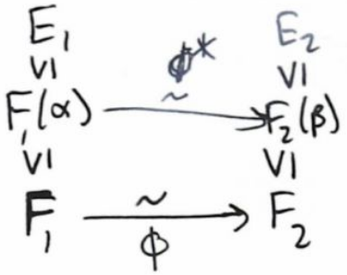
Since α algebraic over F, $[F(\alpha) : F]$ is finite.

Since β algebraic over F, $[F(\beta) : F]$ is finite

β algebraic over $F \Rightarrow$ β alg. / $F(\alpha) \Rightarrow$ $[F(\beta, \alpha) : F(\alpha)]$ finite. ■

Theorem (Kronecker's Lemma): $F_\ell \leq E_\ell$, where $\ell \in \{1, 2\}$.

If $\varphi : F_1 \cong F_2$, and let $\alpha \in E_1$, $\beta \in E_2$, and $p \in F_1[x]$ is irreducible such that $p(\alpha) = 0$. If $\varphi(p)(\beta) = 0$, then there is an IM $\varphi^* : F_1(\alpha) \cong F_2(\beta)$ where φ^* extends φ, and $\varphi^*(\alpha) = \beta$.



Fact: $E \geq F$, $\alpha \in E$, $p \in F[x]$ irreducible s.t. $p(\alpha) = 0$

Then $\frac{F[x]}{(p)} \cong F[\alpha] = F(\alpha)$ when $x + (p) \longmapsto \alpha$

Theorem (Kronecker's Lemma): Suppose $\phi: F_1 \cong F_2$, $E_1 \geq F_1$, $E_2 \geq F_2$

$\alpha \in E_1$, $\beta \in E_2$ $p \in F_1[x]$ irreducible s.t. $p(\alpha) = 0$ and

$\bar{\phi}(p)(\beta) := \sum_{i=0}^{\deg p} \phi(a_i)\beta^i = 0$ if $p = \sum_{i=0}^{\deg p} a_i x^i$

then $\exists$ [redacted] $\phi^*: F_1(\alpha) \cong F_2(\beta)$ s.t. $\phi^* \restriction F_1 = \phi$, $\phi^*(\alpha) = \beta$.

Prop 2: W/ same notation as above, if $\phi: F_1 \cong F_2$ and p irreducible in $F_1[x]$, then $\bar{\phi}(p)$ is irreducible over $F_2[x]$.

Proof of Kronecker's Lemma: Using fact, there is $\phi': F_1(\alpha) \cong \frac{F_1[x]}{(p)}$, where $\phi'(\alpha) = x + (p)$. Then $\psi: \frac{F_1[x]}{(p)} \cong \frac{F_2[x]}{(\bar{\phi}(p))}$. Then by the fact and proposition 2, $\psi': \frac{F_2[x]}{(\bar{\phi}(p))} \cong F_2(\beta)$ Compose these IMs to get $\psi' \circ \psi \circ \phi': F_1(\alpha) \cong F_2(\beta)$, and this IM extends ϕ. ∎

Corollary: Suppose $F \leq E$, and [redacted] $p \in F[x]$ irreducible, $\alpha, \beta \in E$. If $p(\alpha) = p(\beta) = 0$, then $\exists$ $\varphi: F(\alpha) \cong F(\beta)$ s.t. $\varphi(\alpha) = \beta$.

Recall:

Theorem: If F a field, $p \in F[x]$, there is $E \geq F$ splitting field of p over F.

That shows existence of a splitting field. Now we can prove uniqueness:

Theorem: Suppose that $F_1 \leq E_1$ and $F_2 \leq E_2$, $p \in F_1[x]$, p splits over E_1 and E_2. Then there is an IM $\psi: E_1 \cong E_2$ s.t.

$\phi: F_1 \cong F_2$ [redacted] $\psi = \phi$ on F_1

Proof: (Uniqueness of splitting field)

By induction on $n = \deg(p)$. If $n = 1$ then F contains all roots of P, and by minimality of splitting field ~~$E_1 = F_1 = F_2 = E_2$~~ $E_1 \cong F_1 \cong F_2 = E_2$

If $n > 1$, let $q \in F_1[x]$ s.t. q is irreducible, $q \mid p$.

As E_i are splitting fields for P, there are $\alpha \in E_1$, $q(\alpha) = 0$, $\beta \in E_2$, $\bar{\phi}(q)(\beta) = 0$.

By Kronecker's Lemma, there is $\phi^* : F_1(\alpha) \cong F_2(\beta)$, ϕ^* extending ϕ, and $\phi^*(\alpha) = \beta$.

Now consider $p' = p/q$, which has lesser degree than p. Hence, taking $p' = p/q$ as an element of $F_1'[x]$ where $F_1' = F_1(\alpha)$ and $F_2' = F_2(\beta)$. By induction, this gives an IM $\psi' : E_1 \cong E_2$, using $\phi' = \phi^*$, and ψ' extends ϕ' and so also ψ' extends ϕ. Hence ψ' is the desired map. ■

Defn: E is an algebraic closure of F iff E is algebraically closed and E is minimal among alg. closed fields containing F.

Theorem: If E_1, E_2 are both algebraic closures of F, then $\exists \phi : E_1 \cong E_2$ s.t. ϕ is the identity on F.

Fact: Suppose $F \leq E$ and $\alpha \in E$. Then TFAE

(a) α is algebraic over F

(b) $[F(\alpha) : F]$ is finite

Fact: $F \leq E$, let $K = \{\alpha \in E \mid \alpha \text{ alg. } \backslash F\}$

Then $F \leq K \leq E$.

Theorem (Transitivity of being algebraic):

Suppose $F \leq K \leq E$. Suppose

(1) K is algebraic over F

(2) $\alpha \in E$ is algebraic over K

Then α is algebraic over F.

Proof: Since α algebraic over K, $\exists\ p \in K[x]$ s/t $p(\alpha) = 0$, $p(x) = \sum_{i=0}^{n} b_i x^i$

$[F(b_0, \dots, b_n) : F]$ is finite. So then

$[F(\alpha) : F] = [F(\alpha) : F(b_0, \dots, b_n)]\,[F(b_0, \dots, b_n) : F]$ is finite, so α alg. $\setminus F$. ■

Corollary: For every field, there is a field extension which is an alg. closure of it.

Proof: By Zorn, take $E^* \geq F$ algebraically closed. Take

$\bar{E} = \{\alpha \in E^* \mid \alpha \text{ algebraic } / F\}$.

Claim: $\bar{E}$ is algebraic ~~closed~~ closure of F.

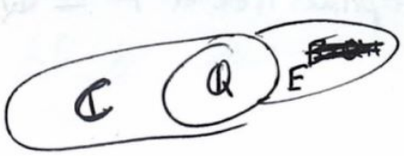
By previous ~~fact~~, $\bar{E} \leq E^*$ and $\bar{E} \geq F$

Let $E \geq F$. Clearly any alg. closed subfield of E must contain $\bar{E}$. So it suffices to show that $\bar{E}$ is algebraically closed. Given $p \in \bar{E}[x]$, since $\bar{E} \subseteq E^*$ and E^* is alg. closed, $\exists\ \alpha \in E^*$, $p(\alpha) = 0$. Since E^* alg. over $\bar{E}$ and $\bar{E}$ is alg. over F, then α is alg. over $F \Rightarrow \alpha \in \bar{E}$. ■

Counter example: intersection of alg. closed fields not alg. closed.

$E := \mathbb{Q} \cup \{(\pi, z) \mid z \in \mathbb{C} \setminus \mathbb{Q}\}$ identify z with (π, z) for $z \in \mathbb{Q}$

define $\alpha + \beta = (\pi, z_1 + z_2)$, etc. $E \cong \mathbb{C}$ and so alg. closed.



~~E = ℚ~~ So $E \cap \mathbb{C} = \mathbb{Q}$ is not alg. closed.

History of Zorn's Lemma:

- Zorn's Lemma named after Max Zorn in 1936 (?) (ish)
- Paper had applications to algebra of "Kuratowski's Principle" (1922)
- People started to call it Zorn's Lemma, but it was really from Kuratowski, however Zorn's Lemma was published in English, and Kuratowski's paper was not. People prefer English.
- Zorn never claimed credit for the Lemma.

Theorem: (Uniqueness of Algebraic Closure)
Suppose $\phi: F_1 \cong F_2$, E_1 alg. closure of F_1, E_2 alg. closure of F_2, then there is $\phi^*: E_1 \cong E_2$, ϕ^* extends ϕ.

Corollary: E_1, E_2 algebraic closures of F. Then $E_1 \cong E_2$ by an IM which fixes F.

Defn: Let F be a field. Char $F = \begin{cases} 0 & \text{if } \Sigma 1 \neq 0 \text{ ever} \\ \min\{p \mid \underbrace{1+1+\cdots+1}_{p \text{ times}} = 0\} & \text{otherwise} \end{cases}$

Lemma: Char F is either 0 or prime.

Question: Is there an infinite field with char $F \neq 0$?
Yes, $\mathbb{F}_p(x)$ is such a field, and char $\mathbb{F}_p(x) =$ char $\mathbb{F}_p$.

Remark: If $F \leq E$, then char $F =$ char E.

Defn: Given F, the prime field of F is the subfield of F generated by $1 = \{\frac{n}{k} \mid n, k \leq \text{char } F\}$

Proposition: If char $F = p$, then the prime field of F is IM/c to $\mathbb{F}_p$.
If char $F = 0$, then the prime field of $F \cong \mathbb{Q}$

Theorem (Uniqueness of Algebraic Closure):

Suppose $\phi: F_1 \cong F_2$, E_i the algebraic closure of F_i, then there is $\phi^*: E_1 \cong E_2$, ϕ^* extends ϕ.

Proof: Consider the poset $\mathbb{P} = \{\psi: K_1 \cong K_2 \mid F_\ell \leq K_\ell \leq E_\ell, \psi \geq \phi\}$. View $(\mathbb{P}, \subseteq)$ as a poset, with $\subseteq$ set inclusion on $\psi \subseteq K_1 \times K_2$.

Claim 1: If C is a chain in $\mathbb{P}$, it has an upper bound.

Let $b = \bigcup C$, $K_1^* =$ domain of b, $K_2^* =$ the image of b.

Verify $K_1^* \leq E_1$ and $K_1^* \geq F_1$, $F_2 \leq K_2^* \leq E_2$, b is an isomorphism, as $\psi \geq \phi$ for all $\psi \in C$, then $b \geq \phi$. So $b \in C$, and an upper bound. ∎

By Zorn, there is $\phi^* \in \mathbb{P}$ maximal.

Let $K_1 = \text{dom } \phi^*$, $K_2 = \text{im } \phi^*$. As $\phi^* \in \mathbb{P}$, then $\phi^* \geq \phi$.

Claim 2: $K_1 = E_1$ and $K_2 = E_2$.

Suppose for contradiction that $K_1 \subsetneq E_1$. Let $\alpha \in E_1 \setminus K_1$.

As E_1 is algebraic closure, α must be algebraic over F_1.

Trivially, α is algebraic over K_1. Take $p \in K_1[x]$ irreducible such that $p(\alpha) = 0$. Also $\overline{\phi^*}(p) \in K_2[x]$ is irreducible. Since E_2 is algebraically closed, there is $\beta \in E_2$ $\overline{\phi^*}(p)(\beta) = 0$.

Apply Kronecker's Lemma to $K_1, K_2, \phi^*, p, \alpha, \beta$ to get $\phi^{**}: K_1(\alpha) \cong K_2(\beta)$ such that $\phi^{**} \geq \phi^*$, with $\phi^{**}(\alpha) = \beta$.

As $\phi^{**} \geq \phi^*$, then $\phi^{**} \geq \phi$, and $F_1 \leq K_1(\alpha) \leq E_1$ and $F_2 \leq K_2(\beta) \leq E_2$, then $\phi^{**} \in \mathbb{P}$. However $K_1(\alpha) \supsetneq K_1$ and $K_2(\beta) \supsetneq K_2$, so $\phi^{**} \geq \phi^*$, so contradicts the maximality of ϕ^*. ✳. So $\phi^*: E_1 \cong E_2$.

∎

Last time: Every field has an algebraic closure which is unique up to isomorphism.

Question: Given p prime, $n \geq 1$, find F s.t. $|F| = p^n$.

Defn: Let F be a field. Then ϕ is an endomorphism if $\phi : F \to F$ is a field homomorphism.

Lemma: Suppose ϕ is an endomorphism. Then $K = \{a \in F \mid \phi(a) = a\}$ is a subfield of F.

Lemma: ϕ endomorphism $\Rightarrow$ ϕ monomorphism.

$\ker \phi$ is an ideal, $0 \neq 1 = \phi(1) \Rightarrow \ker \phi = 0 \Rightarrow \phi$ injective.

Corollary: If ϕ is an endomorphism of a finite field, then it is an automorphism.

~~[illegible]~~

$K_n := \{a \mid \phi^n(a) = a\} \leq F$.

Fact: (Binomial Theorem)

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Corollary (Freshman's Dream): If F has characteristic p, $(x+y)^p = x^p + y^p$. (p prime)

Theorem: If F is a field of characteristic $p > 0$, $\chi_p(x) = x^p$ is an endomorphism of F.

Called the Frobenius Endomorphism.

Defn: Let F be a field, $p \in F[x]$, let E_p be the splitting field of p over F. p has a multiple root iff $\exists \alpha \in E_p$ s.t. $(x-\alpha)^2 \mid p$.

Theorem: Let $p \in F[x]$. Then TFAE

(1) p has no multiple roots

(2) $\gcd(p, p') = 1$

Notation: Given F, its algebraic closure is $\overline{F}$.

Theorem: For every prime p, each $n \geq 1$, $n \in \mathbb{N}$, $\exists K$ a field, $|K| = p^n$.

Proof: Let $F = \overline{\mathbb{F}_p}$. Consider $K = \{a \in F \mid \varphi_p^n(a) = a\}$.

As φ_p is an endomorphism, $K \leq F$.

Let $q = \varphi_p^n(x) - x = x^{p^n} - x$. We have $K = \{a \in F \mid q(a) = 0\}$

$\deg q = p^n$, so we know $|K| \leq p^n$. Now we want to show that q has no multiple roots. By GCD theorem, above, enough to compute $\gcd(q, q') = \gcd(x^{p^n} - x, p^n x^{p^n - 1} - 1)$

In $\overline{\mathbb{F}_p}[x]$, $q' = p x^{p^n - 1} - 1 = -1$. Hence, $\gcd(q, q') = 1$. So q has no multiple roots, hence $|K| = p^n$. ■

Proof of GCD Theorem:

(1) $\Rightarrow$ (2) Suppose $\exists \alpha \in E_p$ (splitting field of p over F) s.t. $p = (x-\alpha)^2 q$ $\nexists\, q \in E_p[x]$

$p' = 2(x-\alpha) q + (x-\alpha)^2 q' = (x-\alpha)(2q + (x-\alpha) q') \Rightarrow (x-\alpha) \mid p'$

So $\mathrm{GCD}(p, p') \neq 1$.

(2) $\Rightarrow$ (1) Suppose $q \in E_p[x]$ is a nonconstant polynomial such that $q \mid p$ and $q \mid p'$. Let $\beta \in E_p$ s.t. $q(\beta) = 0$.

Since $q \mid p$ there is $f \in E_p[x]$ s.t. $p = qf$. Since $(x-\beta) \mid q$, let $q = (x-\beta) g$. $p' = q' f + (x-\beta) g f'$.

$q \mid p$ and $(x-\beta) \mid q' \Rightarrow (x-\beta) \mid p'$ and also $(x-\beta) \mid q \Rightarrow (x-\beta) \mid p$.

■

Miscellaneous Facts:

Lemma: $F \leq E$, $\alpha, \beta \in E$
$F(\alpha, \beta) = F(\alpha)(\beta)$.

Defn: $F \leq E$. $E \setminus F$ *is finite* iff $[E:F] < \infty$

Fact: E/F is finite $\Rightarrow \forall \alpha \in E$, α alg. $/F$.

Fact: E/F, $\alpha \in E$. α alg. $/F \iff [F(\alpha):F] < \infty$.

Lemma: If $E \setminus F$ is finite then $\exists\ \alpha_1, \ldots, \alpha_n$ alg. $/F$ s.t. $E = F(\alpha_1, \ldots, \alpha_n)$.

Defn: Suppose $F \leq E$, $F \leq K_1, K_2 \leq E$. The composite of K_1 and K_2, K_1K_2 is the smallest subfield of E containing K_1 and K_2

Lemma: If $K_1/F, K_2/F$ are both finite, then K_1K_2 is finite.
If $K_1 = F(\alpha_1, \ldots, \alpha_n)$ and $K_2 = F(\beta_1, \ldots, \beta_m)$, then $F(\alpha_1, \ldots \alpha_n, \beta_1, \ldots, \beta_m) = K_1K_2$.

Prop: $F \leq K_1, K_2 \leq E$, E/F finite, then
$[K_1K_2 : F] \leq [F : K_1][F : K_2]$

Proof: Let α_i, β_j be as above. Then $[K_1K_2 : K_1] \leq m$, and

$$[K_1K_2 : K_1][K_1 : F] \leq [K_1K_2 : F] \Rightarrow [K_1K_2 : F] \leq mn.$$

Gives equality when $\{\beta_j\}$ independent over K_1.

Proof that $\forall n \geq 1$, p prime, $\exists$ a field F w/ $|F| = p^n$.

Proof: Let E_p be the splitting field of $q(x) = x^{p^n} - x$ over $\mathbb{F}_p$.

E_p must contain all roots of q but since $(q, q') = 1$, then $q(x)$ has no multiple roots, p^n distinct ones, so

$|E_p| \geq p^n$. Let $F = \{\alpha \in E_p \mid q(a) = a\} \subseteq E_p$ w/ p^n many elements. By minimality of splitting field, $E_p = F$. ∎

Group Theory — G acts on S

Orbit of $x \in S$ = $Orb(x) = \{g \cdot x \mid g \in G\}$

Stabilizer of $x \in S$: $Stab(x) = G_x = \{g \in G \mid g \cdot x = x\}$

Orbit-Stabilizer Theorem: $|Orb(x)| = [G : G_x]$

If G is finite, $|Orb(x)||G_x| = |G|$.

Claim: $p \in F[x]$, $E \geq F$, $a \in E$, $p(a) = 0$.
$f \in Aut_F(E)$, then $f(a)$ is also a root of p.

Proof: Suppose $p(x) = \sum_{k=0}^{n} b_k x^k$. Since $p(a) = 0$, then $\sum b_k a^k = 0$

$$f(p) = \sum_{k=0}^{n} f(b_k) x^k = \sum_{k=0}^{n} b_k x^k = p(x).$$

In particular, $f(0) = 0$, so

$$0 = f(p(a)) = f\left(\sum b_k a^k\right) = \sum b_k f(a^k) = \sum b_k f(a)^k = p(f(a)).$$ ∎

Automorphisms taking F to F move roots of a polynomial to another root.

If $G = Aut_F(E)$, then G acts on $E = F(\alpha_1, \ldots, \alpha_n)$ the splitting field of p, $\{\alpha_1, \ldots, \alpha_n\}$ are the roots of p, then elements of G are permutations of $\{\alpha_1, \ldots, \alpha_n\}$.

Lemma: Suppose G is a finite group acting on a finite set S, p a prime number, $S_0 := \{x \in S \mid \forall g \in G,\ g \cdot x = x\}$. If there is $n \geq 1$ s.t. $|G| = p^n$, then $|S| \equiv |S_0| \pmod{p}$.

Proof: Orbits partition the set S, so there is $S^* \subseteq S \setminus S_0$ which is a complete set of representatives for the orbits of S, namely

$$S = \left(\bigcup_{x \in S^*} \mathrm{orb}(x)\right) \cup S_0$$

$x \in S_0 \Rightarrow |\mathrm{orb}(x)| = 1$

$x \in S^* \Rightarrow |\mathrm{orb}(x)| \geq 2$.

$$|S| = \sum_{x \in S^*} |\mathrm{orb}(x)| + |S_0| = \sum_{x \in S^*} [G : \mathrm{Stab}(x)] + |S_0|$$

($[G : \mathrm{Stab}(x)]$: orbit stabilizer)

$$= \sum_{x \in S^*} p^{k_x} + |S_0|$$

(p^{k_x}: Lagrange $\Rightarrow [G:H] \mid |G|$ and $|\mathrm{orb}(x)| > 1$)

$\Rightarrow |S| \equiv |S_0| \pmod{p}$ ∎

Lemma: If G is a p-group (i.e. $|G| = p^k$) acting on S, then $|S| = |S_0| \bmod p$.

Cauchy's Theorem: If G is finite, p prime, $p \mid |G|$ then $\exists\ H \leq G$, $|H| = p$.

Corollary: If G is a p-group then $Z(G) \neq \{e\}$

Proof: G acts on itself by conjugacy $|S_0| \equiv |S| = |G| \equiv 0 \bmod p$

$S_0 = \{x \in G \mid \forall g \in G,\ gxg^{-1} = x\} = Z(G)$

S_0 $|S_0| \equiv p^n \equiv 0 \bmod p \Rightarrow |Z(G)| \geq p \geq 2$ since Z nonempty. ∎

Corollary: If p is prime and m a natural number s.t. $\gcd(m, p) = 1$, then

$$\binom{p^k m}{p^k} \equiv m \bmod p.$$

Sylow's First Theorem: Suppose G is a finite group, p prime, $p \mid |G|$. Let $k, m \in \mathbb{Z}$ such that $|G| = p^k m$ and $\gcd(m, p) = 1$. Then there is $P \leq G$ such that $|P| = p^k$.

Proof of Sylow's 1st theorem:

Consider $S = \{X \subseteq G \mid |X| = p^k\}$

G acts on S by $gX = \{gx : x \in X\} \in S$.

Let $S^* \subseteq S$ be a complete set of representatives of the orbits.

We have $|S| = \sum_{x \in S^*} |Orb(x)|$ and by orbit-stabilizer,

$|S| = \sum_{x \in S^*} [G : G_x]$ Now $|S| = \binom{mp^k}{p^k} \equiv m \mod p$.

Since $p \nmid m$, there is $X \in S^*$ such that $p \nmid [G : G_X]$

By LaGrange, $[G : G_X] = \frac{|G|}{|G_X|} \Longrightarrow \exists\, m' \leq m,\ |G_X| = p^k m'$.

Claim: $|G_X| = p^k$, so this is the Sylow subgroup.

pf: Pick $a \in X$, consider $f(g) = ga$, $f : G_X \longrightarrow X$.

$f(g_1) = f(g_2) \Longrightarrow g_1 a = g_2 a \Rightarrow g_1 = g_2$.

So f is injective, hence $|G_X| \leq |X| = p^k$

But we know $|G_X| = m' p^k$, so $m' = 1$ and $|G_X| = p^k$. ∎

Proof of Corollary 2:

Let $G = \frac{\mathbb{Z}}{p^k \mathbb{Z}}$, $A = \{1, 2, \ldots, m\}$.

$S = \{X \subseteq G \times A : |X| = p^k\}$. Clearly $|S| = \binom{p^k m}{p^k}$

Given $g \in G$, $X \in S$, consider $g \cdot X = \{(g + a, b) \mid (a, b) \in X\}$.

This is a group action. By Lemma, $|S| \equiv |S_0| \mod p$.

What is S_0?

$$S_0 = \{\{(a + g, b) \mid (a, b) \in X\} = X \ \forall g \in G\}$$

As $g_1 + a = g_2 + a \Rightarrow g_1 = g_2$ and $|G| = p^k = |X|$, there is $b \in \{1, \ldots, m\}$ such that $X = G \times \{b\}$.

So $S_0 = \{G \times \{i\} \mid i \in A\} \Longrightarrow |S_0| = m$.

Hence $|S| \equiv |S_0| \mod p \Longrightarrow \binom{p^k m}{p^k} \equiv m \mod p$. ∎

Question: Suppose $P_1, P_2 \in Syl_p(G)$. Is there $f \in Aut(G)$ s.t. $f(P_1) = P_2$?

Yes, Sylow's Second Theorem.

Questions: How big is $Syl_p(G)$?

Sylow's Third Theorem: $|Syl_p(G)| \equiv 1 \bmod p$.

Theorem: (Sylow's 2nd Theorem)
Suppose $|G| = p^k m$, p prime, $\gcd(p, m) = 1$.
If $P_1, P_2 \in Syl_p(G)$ then $\exists g \in G$ $gP_1g^{-1} = P_2$.

Proof: Consider $S = \{gP_1 \mid g \in G\}$. P_2 acts on S by left multiplication. So $|S| \equiv |S_0| \bmod p$

$|S| = [G : P_1] = \frac{p^k m}{p^k} = m$. So $|S_0| > 0$, hence nonempty, so pick $g \in G$ s.t. $gP_1 \in S_0$.

$gP_1 \in S_0 \iff \forall h \in P_2 \quad hgP_1 = gP_1$
$\iff \forall h \in P_2 \quad g^{-1}hgP_1 = P_1$
$\iff$ [redacted] $g^{-1}P_2g = P_1 \iff P_2 = gP_1g^{-1}$. ∎

Review:

- $\forall q \in F[x]$, there is $E \geq F$, $\alpha \in E$ s.t. $q(\alpha) = 0$.
- Given $F \leq E$, $\alpha \in E$. If α algebraic over F, there is unique monic $m_\alpha \in F[x]$ s.t. $\phi: F(\alpha) \cong \frac{F[x]}{(m_\alpha)}$ where $\phi|_F = id_F$ $\phi(\alpha) = x + (m_\alpha)$

  $[F(\alpha) : F] = \deg(m_\alpha)$

- Defn: $p \in F[x]$ $E \geq F$ is splitting field for p over F iff p factors into linear terms, $p(x) = a\prod(x - \alpha_i)$ and if $F \leq K \leq E$ s.t. p factors over K, then $K = E$.
- Defn: E is algebraic closure of F if ~~$\forall p \in E[x]$~~, $\forall p \in F[x]$, p splits into linear factors over $E[x]$, and E minimal among all algebraically closed fields containing F.

Defn: If $H \leq G$, $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is the normalizer of H in G.

Facts: (1) $H \subseteq N_G(H)$

(2) $N_G(H) \leq G$ → as the stabilizer of the conjugacy action on subgroups

Lemma: When G is finite, $H \leq G$, $[N_G(H) : H] \equiv [G : H] \bmod p$.

Proof: $S = \{gH : g \in G\}$ Consider action of H on S by left multiplication.

$|S| \equiv |S_0| \bmod p$, and $S = [G : H]$

$gH \in S_0 \iff \forall h \in H,\ hgH = gH \iff g^{-1}hg\,H = H$

$\iff g^{-1}hg \in H\ \forall h$

$\iff g^{-1}Hg = H.$

So $g \in N_G(H)$

So $S_0 = \{gH \mid g \in N_G(H)\}$

$|S_0| = [N_G(H) : H]$

Use lemma from few lectures ago. ∎

Corollary: G finite, $H \leq G$, H is p-group
$p \mid [G:H] \Rightarrow N_G(H) \supsetneq H$.

Sylow's Third Theorem: G finite, p prime, $p \mid |G|$. Then
(1) $|Syl_p(G)| \equiv 1 \bmod p$ and
(2) $|Syl_p(G)| \mid |G|$

Proof: Recall any two p-Sylow subgroups are isomorphic by conjugation.
Pick $P_1 \in Syl_p(G)$. Let G act on $Syl_p(G)$ by conjugacy. Then,

$$|Syl_p(G)| = |orb(P_1)| = [G : Stab_G(P_1)] \quad \text{by orbit-stabilizer}$$
$$= [G : N_G(P_1)] \quad Stab_G(P) = N_G(P) \text{ for conjugacy action}$$

Hence, by previous lemma, $[G:N_G(P_1)] \mid |G|$, gives (2).

Consider the action of P_1 on $S = Syl_p(G)$ by conjugacy.
Enough to show $|S_0| = 1$, since $|S| \equiv |S_0| \bmod p$.

Claim: $S_0 = \{P_1\}$

pf: $P_2 \in S_0 \iff \forall g \in P_1 \quad g P_2 g^{-1} = P_2$ so $g \in N_G(P_2)$
$\iff P \neq P_1 \subseteq N_G(P_2)$.

Trivially, $P_2 \leq N_G(P_2)$.

P_1, P_2 are p elements of $Syl_p(N_G(P_2))$.

Apply Sylow's second theorem to P_1, P_2 and $N_G(P_2)$, so
$\exists g \in N_G(P_2)$, then $g P_2 g^{-1} = P_1$. Since $P_2 \trianglelefteq N_G(P_2)$, then $P_2 = P_1$.

Hence, $S_0 = \{P_1\}$, and therefore $|Syl_p(G)| \equiv 1 \bmod p$.

Theorem: If G is finite, $P \in Syl_p(G)$, then

$$N_G(N_G(P)) = N_G(P).$$

Proof: Trivially, $N_G(N_G(P)) \supseteq N_G(P)$. Let $N = N_G(P)$.

Note $P \in Syl_p(N)$ and by definition of normalizer, $P \trianglelefteq N$.

Consider $x \in N_G(N)$, so $xNx^{-1} = N \Rightarrow xPx^{-1} \leq N$

Since $P \trianglelefteq N$, then $x \in N_G(P)$. ■

→ $xPx^{-1} = P$ only because $|Syl_p(N)| = 1$, so P is only element of $Syl_p(N)$ $\Rightarrow xPx^{-1} = P$ since P-sylow subgroups are conjugate.

Question: if $\varphi \in Aut(\mathbb{R})$, then $\varphi = id_{\mathbb{R}}$.

Answer: Get rationals essentially for free.

Then $x < y \iff z^2 = y - x$ for some $z \in \mathbb{R}$.

So $\phi(z^2) = \phi(x-y) \Rightarrow \phi(z)^2 = \phi(x) - \phi(y) \Rightarrow \phi(x) < \phi(y)$.

Defn: Composite of subgroups: $H, K \leq G$ HK is the composite of H and K, the subgroup of G generated by HuK.

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

Lemma: If $H \leq G$ and $K \trianglelefteq G$, Then $HK = HK = KH$.

Proof: Clearly, $KH \subseteq K \vee H$. Enough to show $KH \leq G$. Clear. ■

Second Isomorphism Theorem: $H \leq G$, $K \trianglelefteq G \Rightarrow K \cap H \trianglelefteq H$ and $\frac{HK}{K} \cong \frac{H}{K \cap H}$

Proof: Consider $\phi: G \to G/K$ the natural H/M. Let $\psi = \phi \restriction H$.

$\ker \psi = \{h \in H \mid \psi(h) = K\} = \{h \in H \mid h \in K\} = H \cap K$, $\operatorname{im} \psi = HK/K$

1st IM thm: $H/\ker \psi \cong \operatorname{im} \psi \Rightarrow \frac{H}{H \cap K} \cong HK/K$. ■

Third Isomorphism Theorem: $N \leq K$ and $N \trianglelefteq G$ and $K \trianglelefteq G \Rightarrow \frac{(G/N)}{(K/N)} \cong \frac{G}{K}$.

Proof: $\phi: G/N \to G/K$ defined by $\phi(gN) = gK$. Well-defined.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K/N & \longrightarrow & G/N & \longrightarrow & \frac{G/N}{K/N} & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & K & \longrightarrow & G & \longrightarrow & G/K & \longrightarrow & 0 \end{array}$$

exact. (1st IM Thm). ■

exact

"Quotient by N" exact functor, $\frac{G/K}{N} \cong G/K$ since $N \leq K$.

Theorem: If G is a finite group, abelian and $p \mid |G|$ then there is $H \leq G$ such that $[G:H] = p$.

Proof: $|G| = \prod_{i=1}^{k(G)} p_i$, p_i prime. $k(G)$ is number of primes.

By Cauchy, a subgroup of order p, call it N. Let $G^* = G/N$.

$k(G^*) = k(G) - 1$, $|G^*| = \frac{|G|}{p}$. By induction there is $H^* \leq G^*$ with $[G^*:H^*] = p$, let $\phi: G \to G^*$ be the natural HM.

Not guaranteed that $p \mid |G^*|$!

Define $H = \phi^{-1}(H^*)$. $|H| = p|H^*| \Longrightarrow [G:H] = [G^*:H^*] = p$.

Correct Proof: $|G| = \prod_{i=1}^{k(G)} p_i$, p_i prime, not necessarily distinct.

Base case $k(G) = 1$, pick $H = \langle e \rangle$.

If $k(G) > 1$, let q be another prime that divides $|G|$. By Cauchy, a subgroup of order q, call it N. Let $G^* = G/N$, $k(G^*) = k(G) - 1$, $|G^*| = \frac{|G|}{q}$. By induction there is $H^* \leq G^*$ with $[G^*:H^*] = p$, since $p \mid |G^*|$. Define $H = \phi^{-1}(H^*)$ where ϕ is natural HM.

$|H| = p|H^*| \Longrightarrow [G:H] = [G^*:H^*] = p$. ∎

Defn: G a group. It's commutator subgroup is the subgroup of G generated by $\{xyx^{-1}y^{-1} \mid x, y \in G\}$, $G' = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle$.

Lemma: If ϕ is an endomorphism, then $\phi(G') \leq G'$.

Corollary: G' is a characteristic subgroup of G. (Invariant under automorphism).

Hence $G' \trianglelefteq G$, take $\psi_g(x) = gxg^{-1}$, an automorphism, so G' invariant under ψ_g.

Theorem: Suppose $N \trianglelefteq G$. Then G/N is abelian $\iff N \supseteq G'$.

Proof: G/N abelian $\iff \forall a, b \in G \quad (aN)(bN) = (bN)(aN)$

$\iff abN = baN \quad \forall a, b \in G$

$\iff aba^{-1}b^{-1} \in N \quad \forall a, b \in G.$

$\iff G' \subseteq N.$ ∎

Defn: G is solvable if $\exists n \geq 1$ s.t. $G^{(n)} = \{e\}$, where

$G^{(0)} = G'$

$G^{(n)} = \left(G^{(n-1)}\right)'$ if $n > 0$

↑ commutator subgroup of $G^{(n-1)}$

Solvable means there is a sequence

$$G \rhd G' \rhd G'' \rhd \cdots \rhd G^{(n)} \rhd G^{(n+1)} = \{e\}.$$

Theorem 1: If G is solvable and $H \leq G$, then H is solvable.

Theorem 2: If G is solvable, $\phi: G \to G^*$, then $\text{im}(\phi)$ is solvable.

} follow from lemma, below

Lemma:

(1) $H \leq G \Rightarrow H' \leq G'$

(2) $\phi: G \to G^*$ HM $\Rightarrow \phi(G)' \geq \phi(G')$

Theorem: If $N \lhd G$, N, G/N solvable, then also G is solvable.

Proof: Let $k, m \geq 1$ s.t. $N^{(k)} = 0$ and $(G/N)^{(m)} = 0$ ← trivial group. (should be 1)

Consider $\phi: G \to G/N$ the natural HM.

$$(G/N)^{(n)} = \phi(G)^{(n)} \geq \phi(G^{(n)}) \Longrightarrow \phi(G^{(m)}) \leq \phi(G)^{(m)} = 0$$

So therefore, $G^{(m)} \subseteq N$

Hence $(G^{(m)})^{(k)} \subseteq N^{(k)} = 0 \Rightarrow G^{(m+k)} = 0$ ■

Defn: G is simple iff the only proper, normal subgroups are trivial.

Fact: If $n \geq 5$, then A_n is simple.

Corollary: If $n \geq 5$, S_n is not solvable.

Proof: We know $A_n \lhd S_n$, and $[S_n : A_n] = 2$. If S_n is solvable, then A_n is solvable too. So since A_n is not abelian, so $A_n' \neq 1$, clearly $A_n' \lhd A_n$, which means $A_n' = A_n$ by simpleness. Contradicts solvability. ■

3/17/14

Defn: A group G is nilpotent provided there is $n \geq 1$ s.t. $C_n(G) = G$.

Defn: $\{C_n(G) \mid n \in \mathbb{N}\}$ is an ascending central series of G provided

$n = 0$: $C_0(G) = \{1\}$

$n > 0$: Let $\phi: G \to G/C_n(G)$ be the natural HM.

$$C_{n+1}(G) := \phi^{-1}\left(Z(G/C_n(G))\right)$$

↑ center

$$C_0 \leq C_1 \leq \cdots \leq C_n \leq C_{n+1} \leq \cdots \leq G$$

$$C_n(G) \trianglelefteq G.$$

Remark: G abelian $\Leftrightarrow C_1(G) = Z(G)$

Every abelian group is nilpotent.

Theorem: If $|G| = p^n$, p prime, then G is nilpotent.

Proof: by a previous fact, $Z(G)$ is nontrivial, if G is a p-group, $|G| = p^n \; \forall n \in \mathbb{N}$

If $C_n(G) \lneq G$ always, then $|G / C_n(G)| = p^k$ for some $k \in \mathbb{N}$.

So its center is non-trivial, so $C_{n+1}(G) \supsetneq C_n(G)$

As G is finite, the process of computing $C_m(G)$ will terminate as m increases. ∎

Theorem: If H, K are nilpotent groups then also $H \times K$ is nilpotent.

Claim: $C_n(H \times K) = C_n(H) \times C_n(K)$

Proof: (by induction on n)

$n = 1$: $C_1(H \times K) = Z(H \times K) = Z(H) \times Z(K) = C_1(H) \times C_1(K)$ direct computation

$n > 1$: Consider the HMs (both natural). Let $G = H \times K$

$\pi_K : K \longrightarrow K / C_n(K)$

$\pi_H : H \longrightarrow H / C_n(H)$

Define $\pi : G \longrightarrow H/C_n(H) \times K/C_n(K)$, $\pi = \pi_K \times \pi_H$.

$\psi : H/C_n(H) \times K/C_n(K) \longrightarrow \dfrac{H \times K}{C_n(H) \times C_n(K)} = \dfrac{H \times K}{C_n(H \times K)} = \dfrac{G}{C_n(G)}$

↑ induction hypothesis

Let $\phi = \psi \circ \pi$, $\phi : G \longrightarrow \dfrac{G}{C_n(G)}$. ϕ is the natural HM.

$$C_{n+1}(G) = \phi^{-1}\left(Z\left(G/C_n(G)\right)\right) = \pi^{-1} \circ \psi^{-1}\left(Z\left(G/C_n(G)\right)\right)$$

(ψ is isomorphism)

$$= \pi^{-1} \circ \psi^{-1}\left(Z\left(\frac{H \times K}{C_n(H \times K)}\right)\right) = \pi^{-1}\left(Z\left(\frac{H}{C_n(H)}\right) \times Z\left(\frac{K}{C_n(K)}\right)\right)$$

(definition of π)

$$= \pi_H^{-1}\left(Z\left(\frac{H}{C_n(H)}\right)\right) \times \pi_K^{-1}\left(Z\left(\frac{K}{C_n(K)}\right)\right)$$

$$= C_{n+1}(H) \times C_{n+1}(K)$$

∎

The claim easily implies the lemma.

∎

Main Theorem: Suppose G is a finite Group. Then G is nilpotent if and only if G is a direct product of its p-sylow subgroups.

Proof: ($\Longleftarrow$) Theorems from earlier.

($\Longrightarrow$) Needs some lemmas.

Fact: If $P \in Syl_p(G)$, then $N_G(P) = N_G(N_G(P))$ ← from last time

Lemma: Suppose G is nilpotent; if $H \lneq G$, then $H \lneq N_G(H)$.

pf: Let $n = \max\{n \in \mathbb{Z} \mid C_n(G) \subseteq H\}$. n exists because G is finite, nilpotent.
Let $g \in C_{n+1}(G) \setminus H$. Enough to show as $g \notin H$ $g \in N_G(H)$.

Given any $h \in H$, $C_n(G)gh = (C_n(G)g)(C_n(G)h)$

Since $g \in C_{n+1}(G)$, then $gC_n(G)$ is in the center of $G/C_n(G)$, by defn.

Hence $(C_n(G)g)(C_n(G)h) = (C_n(G)h)(C_n(G)g) = C_n(G)hg$.

So $C_n(G)gh = C_n(G)hg \Rightarrow ghg^{-1} \in hC_n(G)$

but $C_n(G) \subseteq H \Rightarrow ghg^{-1} \in H$. Hence $g \in N_G(H)$, and thus $g \in N_G(H) \setminus H$.

Proof of Main Theorem: If $G = P$ and P is a P-group, we're done. Let $k \geq 2$. ∎

Otherwise, as G is finite suppose $|G| = \prod_{i=1}^{k} p_i^{n_i}$, where p_i is prime. By Sylow's first theorem, $\exists\, P_i \in Syl_{p_i}(G)$ for all p_i, with $|P_i| = p_i^{n_i}$

Claim: $P_i \trianglelefteq G$ $\forall p_i$.

pf: As $k \geq 2$ then $P \lneq G$. Since G is nilpotent, apply key lemma to get $P \lneq N_G(P)$. If $N_G(P) = G$, done. Else $N_G(P) \lneq G$, so again by key lemma $N_G(P) \lneq N_G(N_G(P))$ ⚡ fact above.
Hence $N_G(P) = G$. ∎

Claim: If $i \neq j$, then $P_i \cap P_j = \{1\}$.

pf: Given $a \in P_i$, then $|a| = p_i^x$ $\exists\, x \in \mathbb{N}$.
Given $b \in P_j$, then $|b| = p_j^y$ $\exists\, y \in \mathbb{N}$

So if $c \in P_i \cap P_j$, $|c| = p_i^x = p_j^y \Rightarrow x = y = 0$ and $c = 1$. ∎

Claim 3: $i \neq j \Rightarrow \forall x \in P_i, y \in P_j, xy = yx$

pf: $P_i \trianglelefteq G$, $P_j \trianglelefteq G$ by first claim. Let $x \in P_i$, $y \in P_j$.

So $yxy^{-1} \in P_i \Rightarrow yxy^{-1}x^{-1} \in P_i$

$xyx^{-1} \in P_j \Rightarrow yxy^{-1}x^{-1} \in P_j$

$\Rightarrow yxy^{-1}x^{-1} = 1$ by previous claim.

Hence $yx = xy$. ■

Denote by H_i the group $P_1 P_2 \cdots P_{i-1} P_{i+1} \cdots P_k \leq G$

if $a \in H_i$, then there are $e_1, \ldots, e_k \geq 0$ such that $|a| = p_1^{e_1} p_2^{e_2} \cdots p_{i-1}^{e_{i-1}} p_{i+1}^{e_{i+1}} \cdots p_k^{e_k}$.

If $a \in P_i$, then since $|a|$ does not divide $|P_i|$ and $p_i \nmid |a|$, necessarily $a = 1$.

So $H_i \cap P_i = \{1\}$.

Now consider $H^* = P_1 P_2 \cdots P_k \leq G$. $|H^*| = \prod_{i=1}^{k} |P_i| = \prod_{i=1}^{k} p_i^{n_i} = |G| \Rightarrow |H^*| = |G|$ and $H^* = G$.

Corollary: Suppose G is finite. If G is nilpotent and $k \mid |G|$ then $\exists H \leq G$ with $|H| = k$. ■

Proof: Follows from the following fact about p-groups.

Fact: If $|G| = p^n$, then for all $k \leq n$, $\exists H_k \leq G$ with $|H_k| = p^k$. ■

Corollary: If F is a finite field, then F^* is cyclic.

Proof: Let $G = F^*$. Since G is abelian, then it is nilpotent.

$|G| = \prod_{i=1}^{k} p_i^{n_i}$, p_i prime. Let $P_i \in Syl_{p_i}(G)$ have order $p_i^{n_i}$.

$G = \bigoplus_{i=1}^{k} P_i$. $a \in P_i \Rightarrow a^{p_i^{n_i}} = 1$. Thinking about the polynomial $x^{p_i^{n_i}} - 1$ in F, it has all of its roots, at most $p_i^{n_i}$, but if it is a root, it is of order $p_i^{n_i}$ and hence in P_i, so $a^{p_i^{n_i}} = 1 \Rightarrow a \in P_i$.

Let $Q_i \subsetneq P_i$ such that $|Q_i| = p_i^{n_i - 1}$. By the above,

$P_i = \{\alpha \in F \mid \alpha \text{ root of } x^{p_i^{n_i}} - 1\}$

$Q_i = \{\alpha \in F \mid \alpha \text{ root of } x^{p_i^{n_i - 1}} - 1\}$

Let $a_i \in P_i \setminus Q_i$. Then $|a_i| \mid p_i^{n_i}$. Since p_i is prime, $|a_i| = p_i^m$ $\exists\, m \leq n$

However, since $a \notin Q_i$, then $m > n_i - 1 \Rightarrow m = n_i$. So $|a_i| = p_i^{n_i}$, thus $\langle a_i \rangle = P_i$.

Since G is the direct sum of P_i, P_i cyclic, G is cyclic too. $(G = \langle \prod a_i \rangle)$. ■

Consequences:

$\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n}-x$ over $\mathbb{F}_p$.

By corollary, $\exists\, \alpha \in \mathbb{F}_{p^n}$ such that $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$.

There is irreducible polynomial such that α is its root.

3/[illegible]/14

Theorem: If F is a finite field, there is a prime p and integer $n>0$ such that $F \cong \mathbb{F}_{p^n}$ and $\exists\, \alpha \in F$ s.t. $F = \mathbb{F}_p(\alpha)$. ← α is called the primitive element of $F/\mathbb{F}_p$.

Proof: F finite $\Rightarrow \exists\, p = \text{char } F$ and $\exists n \geq 1$ s.t. $|F| = p^n$, by linear algebra.
Now consider $G = F^*$. By Lagrange, since $|G| = p^n - 1$, $a \in G \Rightarrow a^{p^n-1} = 1$.
$\Rightarrow \forall a \in F\ \ a^{p^n} - a = 0$. Let $q(x) = x^{p^n} - x$. We know $F = \{a \in F \mid a \text{ root of } q\}$.
Hence, since $\mathbb{F}_{p^n}$ is the splitting field of $q(x)$, then $F \cong \mathbb{F}_{p^n}$. ■
By a previous theorem, there is some $\alpha \in F^*$ such that $\langle \alpha \rangle = F^*$.
Clearly $F \subseteq \mathbb{F}_p(\alpha) \subseteq F$. ■
(since $\mathbb{F}_p, \{\alpha\} \subseteq F$.)

Defn: $F \leq E$. $Aut(E/F) = Aut_F(E) = \{\sigma \in Aut(E) \mid \sigma \upharpoonright F = id_F\}$.

Remark: $Aut_F(E) \leq Aut(E)$ as a group under composition.

Defn: Given a field E, let $G := Aut(E)$. If $H \leq G$, then <u>the fixed field of H</u> is $E^H := \{a \in E \mid \forall \sigma \in H,\ \sigma(a) = a\}$

Lemma: $E^H \leq E$.

Proof: $E^H := \bigcap_{\sigma \in H} E^\sigma$ where $E^\sigma = \{a \in E \mid \sigma(a) = a\}$. Enough to show $E^\sigma \leq E$.

Given $a, b \in E^\sigma$, $\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = a \pm b$ $\quad \sigma(0) = 0,\ \sigma(1) = 1$

$\sigma(ab) = \sigma(a)\sigma(b) = ab$

Goal: to prove

Theorem 1: If E is finite, then $Aut(E) \cong \frac{\mathbb{Z}}{n\mathbb{Z}}$ as a group.

In particular, $Aut(E) = \{x_p^k \mid k < n\}$

Remark: $\sigma \in Aut_{\mathbb{F}_p}(\mathbb{F}_{p^n}) \Longrightarrow \sigma \wedge \mathbb{F}_p = id_{\mathbb{F}_p}$. So by the theorem 1 above $|Aut_{\mathbb{F}_p}(\mathbb{F}_{p^n})| = n$.

Theorem 2: If E is a splitting field of $q(x) \in F[x]$ then $|Aut_F(E)| \leq [E:F]$
Moreover, when q has no multiple roots then $|Aut_F(E)| = [E:F]$

Lemma: Suppose $E_1 \geq F_1$, $E_2 \geq F_2$ $\phi: E_1 \to E_2$ is IM s.t. $\phi \wedge F$ is an isomorphism from F_1 to F_2, then if $p \in F[x]$, $\alpha \in E_1$ root of p, then $\phi(\alpha)$ is root of $\phi(f)$.

Proof of Theorem 1: Let $\alpha \in \mathbb{F}_{p^n}$ be such that $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. Consider $G := Aut(\mathbb{F}_{p^n})$.

Since $[\mathbb{F}_{p^n}:\mathbb{F}] = n$ and $\mathbb{F}_{p^n}$ is a simple extension of $\mathbb{F}_p$. We know that as an $\mathbb{F}_p$-vector space, $\mathbb{F}_{p^n}$ is generated by $\{\alpha^k \mid k < n\}$. Also $\exists q \in \mathbb{F}_p[x]$ irreducible of degree n such that $q(\alpha) = 0$.

Given $\sigma \in G$, as $\mathbb{F}_{p^n} = Span\{\alpha^k \mid k < n\}$, the value of $\sigma(\alpha)$ determines σ, since σ leaves $\mathbb{F}_p$ fixed. By lemma, we know $\sigma(\alpha)$ is a root of $\sigma(q) = q$ as well. (↑ b/c σ leaves base field $\mathbb{F}_p$ alone.)

Since q has at most n roots, there are at most n choices for $\sigma(\alpha)$, and hence $|G| \leq n$.

Now we show that $|G|$ is $\geq n$.

If $n = 1$, done. Else, $n > 1$, then $x_p \in Aut(\mathbb{F}_{p^n})$. Enough to show that $x_p^k \neq x_p^l$ for all $k, l \in n$, $k \neq l$. WLOG $k < l$. If $a \in \mathbb{F}_{p^n}$, then assume for contradiction $x_p^k(a) = x_p^l(a) \Longrightarrow x_p^{l-k}(a) = a$, for any $a \in \mathbb{F}_{p^n}$.

We find all elements of $\mathbb{F}_{p^n}$ are roots of $x^{p^{l-k}} - x$. Found a polynomial of degree $< p^n$ with p^n many distinct roots $\lightning$.

Hence $|G| \geq n$, so $|G| = n$. The above also shows $x_p^k \in G$ $\forall$ for any $k < n$, so $G = \{x_p^k \mid k < n\}$. ∎

3/26/14

Defn: χ is a character of G to F provided $\chi: G \to F^*$ is a homomorphism

Defn: Let $\chi_1, \dots \chi_n$ be characters from $G \to F$. We say they are linearly independent iff $\forall a_1, \dots, a_n \in F$, if $\forall g \in G$,

$$\sum_{i=1}^{n} a_i \chi_i(G) = 0 \implies a_1, \dots, a_n = 0$$

Lemma: Suppose $\chi_1, \dots \chi_n$ are characters from G to F. If $1 \le i \ne j \le n \implies \chi_i \ne \chi_j$ then $\{\chi_1, \dots, \chi_n\}$ are independent.

Proof: Otherwise, let m be the smallest number such that $\chi_1, \dots, \chi_m$ are distinct but linearly dependent. Then ~~for all $g \in G$~~, there are $a_1, \dots, a_n \in F$ not ~~all~~ zero,

$$\sum_{i=0}^{m} a_i \chi_i(g) = 0 \quad \text{for all } g \in G. \quad \text{Since } \chi_i(g) \ne 0, \text{ then } m \ge 2.$$

Since $\chi_1 \ne \chi_m$, there ~~are~~ is $g_0 \in G$ such that $\chi_1(g_0) \ne \chi_m(g_0)$. We know:

(1) $\forall g \in G, \sum_{i=1}^{m} a_i \chi_i(g) = 0 \implies \forall g \in G, \sum_{i=1}^{m} a_i \chi_i(g_0 g) = 0$ (2)

$$\implies \forall g \in G, \sum_{i=1}^{m} a_i \chi_i(g_0) \chi_i(g) = 0 \quad (3)$$

And multiplying (1) by $\chi_m(g_0)$, we get

(4) $\forall g \in G, \sum_{i=1}^{m} a_i \chi_i(g) \chi_m(g_0) = 0$

Subtract (3) from (4):

$$\left(\chi_m(g_0) - \chi_1(g_0)\right) a_1 \chi_1(g) + \dots + \left(\chi_m(g_0) - \chi_{m-1}(g_0)\right) a_{m-1} \chi_{m-1}(g) = 0 \quad (5)$$

Let $b_i = \left(\chi_m(g_0) - \chi_i(g_0)\right) \cdot a_i$

Rewrite (5)

$$\sum_{i=1}^{m-1} b_i \chi_i(g) = 0. \quad \text{Since } \chi_1, \dots, \chi_{m-1} \text{ linearly independent, then } b_i = 0 \ \forall i.$$

In particular, $b_1 = 0$, but $a_i \ne 0$, $\chi_m(g_0) - \chi_1(g_0) \ne 0$, ⚡.

■

Theorem: Let E be a field and suppose G is a finite subgroup of $\mathrm{Aut}(E)$. Let $F = E^G = \{a \in E \mid \forall \sigma \in G \ \sigma(a) = a\}$. Then $[E:F] = |G|$.

Last Time: $p \in F[x]$, E splitting field of p over F. Then $|\mathrm{Aut}(E/F)| \leq [E:F]$.

Corollary: Suppose $E \geq F$ is finite. Then if $G = \mathrm{Aut}(E/F)$ and $F = E^G$, E/F is Galois.

Defn: A field extension E/F is Galois iff E/F is finite and $[E:F] = |\mathrm{Aut}(E/F)|$.

Proof of Theorem: First, show that $[E:F] \geq |G|$. As G is finite fix $G = \{\sigma_1, \dots, \sigma_n\}$. Suppose for contradiction $[E:F] < n$. Let $m = [E:F]$ and fix an F-basis $\alpha_1, \dots, \alpha_m$ for E. Consider $\sum_{i=1}^{n} \sigma_i(\alpha_j) x_i = 0$ for $1 \leq j \leq m$. Since $m < n$, this is a system of m equations in n variables, by linear algebra, there is a non-trivial solution $\beta_1 \cdots \beta_m \in E$ for $x_1, \dots, x_m$, β_i not all zero.

We contradict the lemma by proving $\{\sigma_1, \dots, \sigma_n\}$ are linearly dependent characters of E^* into E^*.

As $\beta_i \neq 0$ for some i, enough to show $\forall \alpha \in E^*$, $\sum_{i=1}^{n} \beta_i \sigma_i(\alpha) = 0$.

Given $\alpha \in E^*$, $\alpha = \sum_{i=1}^{m} a_i \alpha_i$. So $\sigma(\alpha) = \sum_{i=1}^{m} \sigma(a_i)\sigma(\alpha_i)$. Since $a_i \in F$ and $F = E^G$, $\sigma(a_i) = a_i$. So $\sigma(\alpha) = \sum_{i=1}^{m} \sigma(\alpha_i)\, a_i$. (*)

Evaluate $\sum_{i=1}^{n} \beta_i \sigma_i(\alpha) = \sum_{i=1}^{n} \beta_i \left(\sum_{j=1}^{m} a_j \sigma_i(\alpha_j) \right) =$ sum of equations times coefficients $a_i = 0$.

■

3/28/14

Theorem: E a field, $G \leq Aut(E)$ finite. $F = E^G$. Then $[E:F] = |G|$.

Theorem A: E a field, $G \leq Aut(E)$, $G = \{\sigma_1 = 1, \sigma_2, \dots, \sigma_n\}$ $F = E^G$. Then $[E:F] \leq n$.

Theorem B: Same setup as above. $[E:F] \geq n$. (Proved Last Time)

Proof of A: Consider the linear system of homogenous equations.

Assume for contradiction $[E:F] > n$. Pick $\alpha_1, \dots \alpha_{n+1} \in E$ linearly independent over F. Gives system

$$\bigstar \quad \begin{cases} \sigma_1(\alpha_1)x_1 + \dots + \sigma_1(\alpha_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma_n(\alpha_1)x_1 + \dots + \sigma_n(\alpha_{n+1})x_{n+1} = 0 \end{cases}$$

has more variables than equations, so a nontrivial solution

$\exists\, \beta_1, \dots, \beta_{n+1} \in E$ with nontrivial solution.

Let $A = \begin{bmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_{n+1}) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_{n+1}) \end{bmatrix}$

System is $A\vec{x} = 0$

Claim: There is some i such that $\beta_i \notin F$.

pf: Suppose $\beta_i \in F$ for all i. Consider the first equation in $\bigstar$.

$\sigma_1(\alpha_1)\beta_1 + \dots + \sigma_1(\alpha_{n+1})\beta_{n+1} = 0$ Since $\sigma_1 = 1$, then this means

$\alpha_1\beta_1 + \dots + \alpha_{n+1}\beta_{n+1} = 0$. Since not all β_i are zero, nontrivial linear dependence among $\{\alpha_i\}$. Contradicts assumption of independence. $\#$

Let $k = \min\{k \mid \exists \beta_1, \dots, \beta_k \in E$ solution to $\bigstar$, $\exists X \subseteq \{\beta_i \mid 1 \leq i \leq k\}$ $|X| = k$, $\beta \in X \Rightarrow \beta \neq 0\}$

smallest number k such that there are k-many $\beta_i \neq 0$ in nontrivial solution

Fix $\vec{\beta} = (\beta_1, \dots, \beta_{n+1})$, a solution to the system of equations, such that $\vec{\beta}$ has exactly k many nonzero entries. We may assume $\vec{\beta} = (\beta_1, \dots, \beta_k, 0, \dots, 0)$ w/ $\beta_i \neq 0$ and $1 \leq i \leq k$. Further permute the labels on the α_i so that this is still a solution.

Also, $\left(\beta_1/\beta_k, \dots, \frac{\beta_{n+1}}{\beta_k}\right)$ is also a solution, so we may assume that $\beta_k = 1$. By claim, there is some i so that $\beta_i \notin F$. Since $1 = \beta_k, 0 \in F$, then $i < k$. Again permute the labels $\#$ such that $\beta_1 \notin F$, $\beta_k = 1$, $\beta_j = 0$ for $j > k$, $\beta_i \neq 0$ for $1 \leq i \leq k$.

So now $A\vec{\beta} = 0$, in particular $\sigma_j(\alpha_1)\beta_1 + \dots + \sigma_j(\alpha_{k-1})\beta_{k-1} + \sigma_j(\alpha_k) = 0$. $(**)$

proof continued:

Since $\beta_1 \notin F$, there is some $\sigma \in G$ s.t. $\sigma(\beta_1) \neq \beta_1$. There is some $k_0 \in \{2, \dots, n\}$ such that $\sigma_{k_0} = \sigma$. $\sigma_{k_0}(\beta_1) \neq \beta_1$. Apply σ_{k_0} to the equations $A\vec{\beta} = 0$, so (**) becomes

$$\sigma_{k_0} \circ \sigma_j(\alpha_1)\, \sigma_{k_0}(\beta_1) + \dots + \sigma_{k_0} \circ \sigma_j(\alpha_k)\, \underbrace{\sigma_{k_0}(\beta_k)}_{\beta_k = 1 \Rightarrow \sigma_{k_0}(\beta_k) = 1.} = 0$$

Let B be the matrix for this system, $B(\sigma_{k_0}(\vec{\beta})) = 0$.

Consider $\{\sigma_{k_0} \circ \sigma_j \mid 1 \le j \le n\} = G$. This is really a permutation of the system A.

The equations B defines are of the form

$$\sigma_j(\alpha_1)\, \sigma_{k_0}(\beta_1) + \dots + \sigma_j(\alpha_{k-1})\, \sigma_{k_0}(\beta_{k-1}) + \sigma_j(\alpha_k) = 0$$

~~Subtract B - A.~~ Subtract $A - B'$ ← permutation of B so that $\sigma_{k_0} \circ \sigma_j$ (row) corresponds to σ_j row of A

$$\sigma_j(\alpha_1)\,(\beta_1 - \sigma_{k_0}(\beta_1)) + \dots + \sigma_j(\alpha_{k-1})\,(\beta_{k-1} - \sigma_{k_0}(\beta_{k-1})) + \sigma_j(\alpha_k)(1-1) = 0$$

Let $\gamma_i = \beta_i - \sigma_{k_0}(\beta_i)$. Then $\vec{\gamma} = (\gamma_1, \gamma_2, \dots, \gamma_{k-1}, 0, 0, \dots, 0)$ a nontrivial solution to the original system! Also, $\vec{\gamma}$ has at most $k-1$ nonzero entries, which contradicts the minimality of k. ✳

So $[E:F] \le n$.

■

This shows that $[E:F] = |G|$ when $F = E^G$ for a finite subgroup $G \le \mathrm{Aut}(E)$.

3/31/14

Defn: $E \ge F$ fields. The extension E/F is Galois if $[E:F] = |\mathrm{Aut}(E/F)|$.

Fact: Suppose $p \in F[x]$. separable. If E is the splitting field of p over F, then E/F is galois. (separable: no multiple roots)

Theorem: Given E, $G \le \mathrm{Aut}(E)$ finite, $F = E^G$. Then E/F is galois.

Corollary: Suppose E/F is finite. Then $|\mathrm{Aut}(E/F)| \le [E:F]$ and E/F galois iff $F = E^{\mathrm{Aut}(E/F)}$.

Proof: Certainly $E^{\mathrm{Aut}(E/F)} \supseteq F$, so we need to show $E^{\mathrm{Aut}(E/F)} \subseteq F$.

Notice that if E/F is finite and $n := [E:F]$, then by choosing $\alpha_1, \dots, \alpha_n$ an F-basis for E, any permutation $\sigma \in \mathrm{Aut}(E/F)$ permutes $\{\alpha_i \mid 1 \le i \le n\}$. So $|\mathrm{Aut}(E/F)| \le n!$

→

Proof continued:

Let $F_1 := E^{Aut(E/F)}$. By theorem, $[E:F_1] = |Aut(E/F)|$. Trivially, $F \leq F_1 \leq E$, so by the product formula, $[E:F] = [E:F_1][F_1:F] = |Aut(E/F)|[F_1:F]$ (*)

$\Rightarrow |Aut(E/F)| \leq [E:F]$.

E/F galois $\iff [E:F] = |Aut(E/F)| \overset{(*)}{\iff} [F_1:F] = 1 \iff F_1 = F \iff F = E^{Aut(E/F)}$

■

(OLD)

Question: If $F \leq E$, $G = Aut(E/F)$, clearly $F \leq E^G \leq E$. When is $F = E^G$?

Answer: When E/F is Galois.

Corollary 2: Suppose $G \leq Aut(E)$ is finite, $F = E^G$, then E/F Galois and $G = Aut(E/F)$.

Proof: $[E:F] = |G| \leq |Aut(E/F)| \overset{\text{corollary 1}}{\leq} [E:F] \Rightarrow [E:F] = |Aut(E/F)|$. As $G \subseteq Aut(E/F)$, both finite of same cardinality, then $G = Aut(E/F)$. ■

Corollary 3: Let G_1, G_2 be two different finite subgroups of $Aut(E)$. Then $E^{G_1} \neq E^{G_2}$.

Proof: Suppose $E^{G_1} = E^{G_2}$. By corollary 2, $G_1 = Aut(E/E^{G_1}) = Aut(E/E^{G_2}) = G_2$ ⚡.

Theorem: Suppose E/F is finite. Then TFAE:

(1) E/F is Galois
(2) $\exists p \in F[x]$, p is separable (no multiple roots) and E is the splitting field of p over F.

Furthermore, for any $q \in F[x]$ irreducible, $\exists \alpha \in E$ $q(\alpha) = 0$, then q splits in E. Assuming (1)

Proof: (2) $\Rightarrow$ (1) from previous fact.

Proof (1)⇒(2): Suppose E/F Galois, $q \in F[x]$ irreducible, and $\exists \alpha \in E$ such that $q(\alpha)=0$. Then q splits in E → proven below

Let $G = \mathrm{Aut}(E/F)$, let $\alpha \in E$ be such that $q(\alpha)=0$.

Let $\{1, \sigma_2, \dots \sigma_n\}$ enumerate G. Consider $\{\sigma_i(\alpha)\}$, all roots of q, by Kronecker's Lemma. Let $k \leq n$ be such that $\{\alpha_1, \dots, \alpha_k\} = \{\alpha, \sigma_2(\alpha), \dots, \sigma_n(\alpha)\}$. (basically we want the $\sigma_i(\alpha)$ that are not repititions, all distinct roots from the set $\{\sigma_i(\alpha)\}$.)

Consider $p(x) = \prod_{i=1}^{k} (x-\alpha_i) \in E[x]$. Claim that $p \in F[x]$.

Since $\{1, \sigma_2, \dots, \sigma_n\} = G$, given $\tau \in G$, $\{\tau, \tau\circ\sigma_2, \dots, \tau\circ\sigma_n\} = G$.

Then $\tau(p) = \prod_{i=1}^{k} (x - \tau(\alpha_i)) = \prod_{i=1}^{k} (x-\alpha_i) = p$.

Thus, $p \in E^G[x] = F[x]$ since E/F is galois.

As q is irreducible, with root $\alpha \in E$, and p also vanishes at α, so an irreducible polynomial and another have a common root.

In $E[x]$, $(x-\alpha_i) \mid q$ for all i, so $p \mid q(x)$. ← also true in $F[x]$!

$\Rightarrow p = q$.

So q splits in E.

Remains to show (2).

by old fact, $\forall i$ $\exists q_i$

Fix a basis $\beta_1, \dots, \beta_n$ a basis for E/F. Pick $q_i \in F(x)$ irreducible such that $q_i(\beta_i)=0$. Consider $p = \prod_{i=1}^{n} q_i$, each factor of which splits in E.

Let $r(x)$ be the ~~largest~~ highest degree squarefree polynomial that divides p. Then E is its splitting field. ∎

04/02/14

Recall: E/F is Galois iff $[E:F] = |\mathrm{Aut}(E/F)|$.

Theorem: TFAE

(1) E/F is Galois

(2) $F = E^{\mathrm{Aut}(E/F)}$

(3) $\exists\ p \in F[x]$ separable such that E is the splitting field of p over F.

Proof: (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (3) from last lecture

(3) $\Rightarrow$ (1) Several lectures ago, like the uniqueness of splitting fields. ■

Main Lemma (used in (2) $\Rightarrow$ (3)): If E/F is Galois, and $q \in F[x]$ irreducible and $\exists\ \alpha \in E$ s.t. $q(\alpha) = 0$, then q factors into linear terms in E.

Idea of proof: Suppose $q(\alpha) = 0$, $G = \mathrm{Aut}(E/F) = \{1, \sigma_2, \dots, \sigma_n\}$. Then $A = \{\alpha, \sigma_2(\alpha), \dots, \sigma_n(\alpha)\}$ are the roots of $q(x)$. So if $\tau \in G$, τ is a permutation of A. Then if $f(x) = \prod (x - \alpha_i)$ where $\alpha_1, \dots, \alpha_k$ are the distinct elements of A, $\tau(f(x)) = f(\tau(x))$, and so since $F = E^G$, then $f \in F[x]$. So $f \mid q$, but q irreducible, so $f = q$. ■

(C.F. Atiyah & Macdonald Ch. 5 exercise 12)

Theorem (Galois Correspondence): Suppose E/F is Galois, let $G = \mathrm{Aut}(E/F)$. Then (1) There is a bijection between $\{K \leq E \mid F \leq K\}$ and $\{H \mid H \leq G\}$ given by $K \longmapsto \mathrm{Aut}(E/K)$ and $H \longmapsto E^H$, it's inverse.

(2) If $H \leq G$ then $[E:E^H] = |H|$ and $[E^H:F] = [G:H]$

(3) When $F \leq K \leq E$ then E/K is Galois, $\mathrm{Aut}(E/K) = H$ when $H \leq G$ s.t. $K = E^H$

(4) K/F is Galois $\iff H \trianglelefteq G$ when $K = E^H$ and $\mathrm{Aut}(K/F) \cong G/H$

"there is a god"

Consequences:

Theorem (Primitive Element Thm): If E is a finite extension of $\mathbb{Q}$, then there is $\alpha \in E$ such that $E = \mathbb{Q}(\alpha)$.

Holds for a finite field instead of $\mathbb{Q}$, but for different reasons. If F is finite, E finite extension, E^* is cyclic $\Longrightarrow \langle\alpha\rangle = E^*$ $\forall\ \alpha \in E$ and $E = F(\alpha)$.

Corollary of Galois Correspondence: Suppose E/F is Galois. Then $\{K \mid F \leq K \leq E\}$ is finite.

Proof: This set $\{K \mid F \leq K \leq E\}$ corresponds to subgroups $\{H \mid H \leq G\}$ and G is a finite group. ∎

Proof of Primitive Element Theorem: Fix $\beta_1, \dots, \beta_n \in E$ a basis over $\mathbb{Q}$. Let $q_1, \dots, q_n \in \mathbb{Q}[x]$ irreducible be such that $q_i(\beta_i) = 0$. Consider $p = \prod_{i=1}^{n} q_i \in \mathbb{Q}[x]$. Take E^* the splitting field of p over $\mathbb{Q}$. By Kronecker's Lemma, there is $\phi: E \longrightarrow E^*$ with $\phi \restriction \mathbb{Q} = 1_{\mathbb{Q}}$. We may assume $E^* \supseteq E$, considering $\phi: \mathbb{Q}(\beta_1, \dots, \beta_n) \cong \mathbb{Q}(\phi(\beta_1), \dots, \phi(\beta_n)) \subseteq E^*$. (Actually, $E \leq E^*$).

~~[illegible],~~

Claim: For all i, q_i is separable.

Pf: q_i is irreducible, and $\deg q_i' < \deg q_i$ and so q_i, q_i' share no roots. (q_i': derivative)

Therefore, p is separable by Main Lemma from earlier, and thus $E^*/\mathbb{Q}$ is galois. So argue by induction on n, so enough to show that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$ for any, $\alpha, \beta \in E$ and some $\gamma \in E$.

Consider $t \longmapsto \mathbb{Q}(\alpha + t\beta) \leq E^*$ for $t \in \mathbb{Q}$. As E^* has finitely many subfields, by Galois correspondence, we may pigeonhole such that for some infinite $S \subseteq \mathbb{Q}$, and $\mathbb{Q}^* \leq E^*$ so that $t \in S \Rightarrow \mathbb{Q}(\alpha + t\beta) = \mathbb{Q}^*$.

Take $t_1 \neq t_2$ s.t. $\mathbb{Q}(\alpha + t_1\beta) = \mathbb{Q}(\alpha + t_2\beta)$, use arithmetic to show $\alpha, \beta \in \mathbb{Q}^*$. So let $\gamma = \alpha + t_1\beta$ and $\mathbb{Q}^* = \mathbb{Q}(\gamma)$. ∎

04/04/14

The Primitive Element Theorem: If F has characteristic zero, E/F is a finite field extension, then $\exists\, \alpha \in E$ such that $F(\alpha) = E$.

More general, but same proof.

Fundamental Theorem of Algebra: $\mathbb{C}$ is algebraically closed.

~~Proof:~~

Facts: (1) $P \in \mathbb{R}[x]$, $\deg P$ odd $\Rightarrow \exists\, \alpha \in \mathbb{R}$, $p(\alpha) = 0$. (Intermediate Value Thm)

(2) $a \in \mathbb{R}$, $a > 0 \Rightarrow \exists\, b \in \mathbb{R}$ s.t. $b^2 = a$. (Okay)

Lemma: if $z \in \mathbb{C}$, then there is w such that $w^2 = z$. (Polar Coordinates)

Lemma: If $F \geq \mathbb{C}$, then $[F:\mathbb{C}] \neq 2$.

Proof: Take $\alpha \in F \setminus \mathbb{C}$, clearly $\{1, \alpha\}$ are linearly independent over $\mathbb{C}$, so $[\mathbb{C}(\alpha):\mathbb{C}] \geq 2$, but also $\mathbb{C}(\alpha) \leq F$ since $[F:\mathbb{C}] = 2$ we get $F = \mathbb{C}(\alpha)$. As $[\mathbb{C}(\alpha):\mathbb{C}] = 2$, $\exists\, p \in \mathbb{C}[x]$ irreducible of degree 2 s.t. $p(\alpha) = 0$. We can solve quadratics (i.e. p) for $p(x) = ax^2 + bx + c$, and its roots are in $\mathbb{C}$, so $[F:\mathbb{C}] \neq 2$. ∎

Proof of FTA: If $\mathbb{C}$ is not algebraically closed then $\exists\, F \geq \mathbb{C}$ s.t. $F/\mathbb{C}$ is finite. Suppose for contradiction that such F exists.

As $F/\mathbb{C}$ is finite, $[\mathbb{C}:\mathbb{R}] = 2$, then $F/\mathbb{R}$ is finite. Pick $\beta_1, \ldots, \beta_n \in F$ an $\mathbb{R}$-basis for F. Let $E \geq F$ such that $E/\mathbb{R}$ is Galois. So

$$\mathrm{Aut}(E/\mathbb{R}) \text{ is finite, and } |\mathrm{Aut}(E/\mathbb{R})| = [E:\mathbb{R}] = [E:\mathbb{C}][\mathbb{C}:\mathbb{R}] = 2[E:\mathbb{C}].$$

Hence $2 \mid |\mathrm{Aut}(E/\mathbb{R})|$. ~~By sylow's 1st theorem, $\exists\, H \leq \mathrm{Aut}(E/\mathbb{R})$ $|H| = 2^n$ $\frac{}{4}$.~~

Also by sylow's 1st theorem, $\exists\, H \leq \mathrm{Aut}(E/\mathbb{C})$ with $|H| = 2^n$ $\nexists\, n \in \mathbb{N}$, $[G:H]$ odd.

Claim: $H = \mathrm{Aut}(E/\mathbb{C})$.

Proof: By Galois correspondence, $[E:E^H] = |H|$ and $[E^H:\mathbb{R}] = [G:H]$ ← odd.

Since $[E^H:\mathbb{R}]$ is odd, then by primitive element theorem, $E^H = \mathbb{R}(\alpha)$ and α is a root of an irreducible $p \in \mathbb{R}[x]$ of odd degree $\Rightarrow p$ linear. →

Therefore, $[E^H : \mathbb{R}] = [G:H] = 1 \Rightarrow E^H = \mathbb{R}$.

$[E:E^H] = |H| = |G| = 2^n \Rightarrow H = G = Aut(E/\mathbb{C})$. (?)

04/07/14

Fundamental Theorem of Algebra

Facts: (1) There is no extension of $\mathbb{C}$ of degree 2.

(2) $p \in \mathbb{R}[x]$ $\deg(p)$ odd $\Rightarrow$ p has a root

Proof due to Artin

Proof (FTA): If $\mathbb{C}$ is not algebraically closed, then $\mathbb{C}$ has a finite extension. Find $E \geq \mathbb{C}$ such that E is a splitting field for a separable polynomial over $\mathbb{R}$.

$E/\mathbb{R}$ is galois, as a splitting field.

Consider $Aut(E/\mathbb{R})$. By Sylow's first theorem, $\exists P \leq Aut(E/\mathbb{R})$ $|P| = 2^n$ and $[Aut(E/\mathbb{R}) : P]$ odd.

Claim: $P = Aut(E/\mathbb{R})$

Proof: Let $F = E^P$. By Galois Correspondence $[F:\mathbb{R}] = [Aut(E/\mathbb{R}) : P]$ ← odd.

Hence by primitive element theorem, $F = \mathbb{R}(\alpha)$. Since $[Aut(E/\mathbb{R}) : P]$ is odd, then $[F:\mathbb{R}]$ is odd. $\exists q \in \mathbb{R}[x]$ irreducible and $q(\alpha) = 0$ and $\deg(q)$ is

$\deg(q) = [\mathbb{R}(\alpha) : \mathbb{R}]$ odd. By fact 2, $[\mathbb{R}(\alpha) : \mathbb{R}] = 1 \Rightarrow [F:\mathbb{R}] = 1 \Rightarrow F = \mathbb{R}$,

As E/F is galois, $E^P = E^{Aut(E/\mathbb{R})} \Rightarrow P = Aut(E/\mathbb{R})$. ∎

Trivially, $Aut(E/\mathbb{C}) \leq Aut(E/\mathbb{R})$ is also a 2-group, so $Aut(E/\mathbb{C}) = 2^m$.

If $m = 0$; then $|Aut(E/\mathbb{C})| = 1$ by galois's correspondence as $E/\mathbb{C}$ also galois.

So $[Aut(E/\mathbb{C})] = [E:\mathbb{C}] = 1 \Rightarrow E = \mathbb{C}$, Contradicts $E \neq \mathbb{C}$. We are done.

If $m > 0$: By a fact about P-groups, $\exists H \leq Aut(E/\mathbb{C})$ such that $|H| = 2^{m-1}$.

Namely, $[Aut(E/\mathbb{C}) : H] = 2$. Consider $K : E^H$. $\mathbb{R} \leq K \leq E$. By Galois Correspondence,

$[K:\mathbb{C}] = [Aut(E/\mathbb{C}) : H] = 2$. Found $K \geq \mathbb{C}$, $[K:\mathbb{C}] = 2$, contradicts Fact 1.

∎

Fact (A): If $G \leq Aut(E)$ is finite, then $[E:E^G] = |G|$

Fact (B): $G_1 \neq G_2 \leq Aut(E)$ finite $\Rightarrow E^{G_1} \neq E^{G_2}$.

Galois Correspondence Theorem: Let E/F be galois. Then if $G = Aut(E/F)$

(1) $\{K \leq E \mid F \leq K\}$ and $\{H \mid H \leq G\}$ are in bijection.

(2) If $H \leq G$ then $|H| = [E:E^H]$ and $[E^H:F] = [G:H]$

(3) When $F \leq K \leq E$, then E/K is galois, $Aut(E/K) = H$ when $H \leq G$ s.t. $K = E^H$.

Proof: By fact (B), $H \longmapsto E^H$ is injective. As E/F is galois, then $\exists p \in F[x]$ separable, E is splitting field of p/F. As E is a splitting field of p/K, since $F \leq K$, then E/K is galois, so we get (3).

Since E/K is Galois and $Aut(E/K) \leq Aut(E/F)$, using part (2) of the ~~correspondence~~ characterization theorem, $K = E^{Aut(E/K)}$.

We have proved: Given $F \leq K \leq E$ then there exists $H \leq Aut(E/F)$, $K = E^H$, (take $H := Aut(E/K)$). Thus $H \longmapsto E^H$ is also surjective.

The inverse of $H \longmapsto E^H$ is $K \longmapsto Aut(E/K)$.

To show (2), it is enough to show $[E:K] = |H|$ because using La Grange,

$[E:F] = [E:K][K:F]$ and $[Aut(E/F):H]\,|H| = |Aut(E/F)|$

this follows easily from Fact (A). ∎

04/09/14

Recall:

Main Lemma: For $F \leq E$, if $F = E^{Aut(E/F)}$, then for all $p \in F[x]$ irreducible, if $\exists \alpha \in E$, $p(\alpha) = 0$, then $p(x)$ splits in $E[x]$.

Theorem (Galois Correspondence) (part (iv) only): Suppose E/F is galois, $H \leq Aut(E/F)$, $K = E^H$. Then K/F is galois $\iff$ $H \lhd Aut(E/F)$ and if K/F is galois, then $Aut(K/F) \cong Aut(E/F)/H$.

Remark:

~~Proof:~~ Suppose E/F is finite, then we may assume $E \leq \bar{F}$. Consider $\bar{E}$. Certainly every polynomial in $F[x]$ has a root in $\bar{E}$.

Claim: $\alpha \in \bar{E} \Rightarrow \alpha$ alg $/F$

Proof: $p \in E[x]$, $p(\alpha) = 0$, coefficients of p alg/F since E alg./F.

So by uniqueness of algebraic closure, $\bar{E} \cong \bar{F} \Rightarrow E \leq \bar{E} \cong \bar{F}$. ∎

Proof:

Given $F \leq K \leq E$. Consider $\tau : K \to \bar{F}$, ~~$\tau \wedge F = id_F$~~ $\tau \wedge F = id_F$. Define

Embed $(K/F) = \{\tau \mid \tau : K \to \bar{F}$ and $\tau \wedge F = id_F\}$.

Claim: $\forall \tau \in$ Embed(K/F), $\exists \sigma \in Aut(E/F)$ extending τ.

Proof: Observe that $\tau \in$ Embed (K/F) means $\tau(K) \leq E$ ← supposing $E \leq \bar{F}$ by the remark

Given $\alpha \in K$ let $q_\alpha \in F[x]$ be its irreducible polynomial.

Since $\alpha \in K \subseteq E$, and E/F galois, by the main lemma q_α splits in $E[x]$, so E has all the roots of q_α. As $\tau \wedge F = id_F$, $\tau(\alpha)$ is also a root of q_α.

We get $\tau(\alpha) \in E$. $(\alpha \in K \Rightarrow \tau(\alpha) \in E \Rightarrow \tau(K) \leq E)$

Given $\tau \in$ Embed (K/F), we have $\tau : K \cong \tau(K)$. As E/F Galois, $\exists p \in F[x]$ separable, E is the splitting field of p/F.

As $F \leq K \leq E$, E is the splitting field of p/K as well As $\tau \wedge F = id_F$ and $\tau(p) = p$, E is the splitting field of $\tau(p)$ over $\tau(K)$. $\tau : K \cong \tau(K)$ (both $\leq E$)

By uniqueness of splitting fields, $\exists \sigma : E \cong E$, σ extends $\tau \Rightarrow \sigma \wedge F = id_F$.

We found $\sigma \in Aut(E/F)$ as desired. ∎ claim.

Proof continued:

Claim: $\mathrm{Embed}(K/F) = \mathrm{Aut}(K/F)$.

Proof: ~~As was just shown,~~ $\mathrm{Embed}(K/F) \geq \mathrm{Aut}(K/F)$ is clear.

Enough to show they have the same (finite) cardinality.

Given $\sigma_1, \sigma_2 \in \mathrm{Embed}(K/F)$, $\sigma_1 \restriction K = \sigma_2 \restriction K \iff \sigma_1^{-1} \circ \sigma_2 = \mathrm{id}_K$. $K = E^H$

$\iff \sigma_1^{-1} \circ \sigma_2 \in H$ ← (*)

$\iff \sigma_1 H = \sigma_2 H$

Given $\tau \in \mathrm{Embed}(K/F)$, define a map $\tau \mapsto \sigma_\tau H$, where σ_τ is an extension of τ to $\mathrm{Aut}(E/F)$. By (*), $\tau \mapsto \sigma_\tau H$ is a bijection.

Hence $|\mathrm{Embed}(K/F)| = [\mathrm{Aut}(E/F) : H] = [K:F] = |\mathrm{Aut}(K/F)|$ ■ claim

↑ galois correspondence part 2

~~But K/F is galois, so we know that~~

Given $\sigma \in \mathrm{Aut}(E/F)$, what subgroup of $\mathrm{Aut}(E/F)$ fixes $\sigma(K)$?

$$H_1 := \{\tau \in \mathrm{Aut}(E/F) \mid \tau(\sigma(K)) = \sigma(K)\} = \sigma H \sigma^{-1}$$

By the fact that there is a bijection between $\{H \leq \mathrm{Aut}(E/F)\}$ and $\{K : F \leq K \leq E\}$, this is precisely the group that fixes $\sigma(K)$:

$$\sigma(K) = E^{\sigma H \sigma^{-1}}$$

Again invoking the galois correspondence,

$$|H_1| = [E : \sigma(K)] = [E:K]$$

↑ GC; ↳ $\sigma \in \mathrm{Aut}(E/F)$.

We have proved:

Claim: $\forall \sigma \in \mathrm{Aut}(E/F)$, $\sigma(K) = K \iff \sigma H \sigma^{-1} = H$

And thus K/F is galois $\iff H \trianglelefteq \mathrm{Aut}(E/F)$.

Using the map $\tau \mapsto \sigma_\tau H$, we have a bijection $\mathrm{Aut}(K/F)$ onto $\frac{\mathrm{Aut}(E/F)}{H}$

■

04/14/14

Test Monday, April 28

Facts: (1) If F is finite, then $\#F^\times$ is cyclic.

(2) If F is finite, $\exists\, p, n$ s.t. $F \cong \mathbb{F}_{p^n}$.

(3) $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$

(4) $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \chi_p \rangle$ of order n, where $\chi_p(a) := a^p$

(5) $\exists\, \alpha \in \mathbb{F}_{p^n}$ s.t. $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$

Using the Galois Correspondence Theorem

Corollary: Let $E = \mathbb{F}_{p^n}$. If $F \leq E$, then there is some $d \mid n$ $F = \mathbb{F}_{p^d}$. The converse also holds.

Proof: ($\Longrightarrow$) By (2), $\exists\, d \leq n$ s.t. $F = \mathbb{F}_{p^d}$. As E is a vector space / F, suppose $[E:F] = k$. By product formula, $[E:\mathbb{F}_p] = [E:F][F:\mathbb{F}_p] \Longrightarrow n = kd$.

($\Longleftarrow$) We know $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois (it is the splitting field of a separable polynomial. By galois correspondence, $\forall\, H \leq \mathbb{Z}/n\mathbb{Z}$, there is $F = E^H$, and $\mathbb{F}_p \leq F \leq E$. Again by galois correspondence $[F:\mathbb{F}_p] = |H|$. Take $H \leq \mathbb{Z}/n\mathbb{Z}$ with $|H| = d$ $\forall$ divisor $d \mid n$. Then $[F:\mathbb{F}_p] = d \Longrightarrow F = \mathbb{F}_{p^d}$. ∎

Using the same proof as for fact 1, we can establish the following:

Theorem: If $G \leq F^\times$ is finite, then G is cyclic.

Proof: (Exercise).

Solvability by Radicals:

Defn: We say a polynomial of degree n is **solvable by radicals** over F provided there is a finite sequence of instructions consisting of statements of the form

$$\left.\begin{aligned} a &:= b \pm c \\ a &:= b \cdot c \\ a &:= b/c \\ a &:= (b)^{1/m} \end{aligned}\right\}$$ where b, c are either coefficients of the polynomial or results of previous operations, $m \geq 1$ an integer.

Denote by this progression $P(a_1, \ldots, a_n)$, where $a_1, \ldots, a_n \in F$. The result of $P(a_1, \ldots, a_n) = \alpha$, where $q(\alpha) = 0$, $q(x) = \sum_{k=0}^{n} a_k x^k$.

Idea: How we can solve $x^m - a$ for $a \in F$. Simplest form is when $a = 1$.

Defn: $\alpha \in F$ is an **n^{th} root of unity** if $\alpha^n = 1$. $U_n := \{\alpha \mid \alpha^n = 1\} \leq (\mathbb{Z}/n\mathbb{Z}, \times)$.

$\alpha \in U_n$ is **primitive** if it generates U_n.

Theorem: Suppose $F \leq E$, $\exists \alpha \in E$ is a primitive n^{th} root of unity ($n \geq 1$ and $E = F(\alpha)$). Then $\mathrm{Aut}(E/F)$ is abelian.

Proof: $\langle \alpha \rangle = U_n \Rightarrow E$ contains all roots of $x^n - 1 \Rightarrow E/F$ is the splitting field of $x^n - 1$. Given $\sigma \in \mathrm{Aut}(E/F)$, $\sigma(\alpha)$ also generates U_n. There exists $k_\sigma < n$ such that $\sigma(\alpha) = \alpha^{k_\sigma}$. $\gcd(k_\sigma, n) = 1$ (else not a generator).

Let $\psi : \mathrm{Aut}(E/F) \longrightarrow (\mathbb{Z}/n\mathbb{Z}, \times)$, $\psi(\sigma) = k_\sigma$. ψ is a homomorphism.

Since $E = F(\alpha)$, $\sigma \in \mathrm{Aut}(E/F)$ is determined by $k < n$ when $\sigma(\alpha) = \alpha^k$, so ψ is injective.

Hence $\mathrm{Aut}(E/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z}, \times)$, hence abelian. ∎

4/16/14

Last Time: $E = F(\alpha)$, α a primitive ($n>2$) n^{th} root of unity, then $Aut(E/F)$ is abelian.

And $Aut(E/F) \leq \frac{\mathbb{Z}}{n\mathbb{Z}}^{\times}$, injection given by $\psi(\sigma) = k_\sigma$ where $\sigma(\alpha) = \alpha^{k_\sigma}$.

Theorem: Suppose $\alpha \in F$ is a primitive n^{th} root of unity, $a \in F$ and $p(x) = x^n - a$. If E is the splitting field of p over F and $\phi: Aut(E/F) \to \left(\frac{\mathbb{Z}}{n\mathbb{Z}}^{*}, \cdot\right)$ is an injective HM, then p is irreducible $\iff$ ϕ is surjective.

Proof: Suppose $\beta \in E$ is a root of $p(x)$. The set of roots of p in E is $\{\beta, \beta\alpha, \beta\alpha^2, \ldots, \beta\alpha^{n-1}\}$. If $\sigma \in Aut(E/F)$ then $\exists!\, k_\sigma$ s.t. $k_\sigma < n$, $\sigma(\beta) = \beta\alpha^{k_\sigma}$.

Take $\phi(\sigma) := k_\sigma$. Why is ϕ an HM? Consider $\phi(\sigma\circ\tau)$.

$$\sigma(\tau(\beta)) = \sigma(\beta\alpha^{k_\tau}) = \sigma(\beta)\,\sigma(\alpha^{k_\tau}) = \sigma(\beta)\,\alpha^{k_\tau} = \beta\alpha^{k_\sigma + k_\tau}$$ (σ fixes F)

$$\phi(\sigma\circ\tau) = k_\sigma + k_\tau = \phi(\sigma) + \phi(\tau)$$ ∎

($\Rightarrow$) Suppose p is irreducible. By Kronecker, $\forall k<n$, $\exists \sigma \in Aut(E/F)$, $\sigma(\beta) = \beta\alpha^{k_\sigma}$. ∎

($\Leftarrow$) Suppose $p = fg$ (not irreducible). Since p has n-many distinct roots $\{\beta, \beta\alpha, \beta\alpha^2, \ldots, \beta\alpha^{n-1}\}$ then p is separable and we may assume $\gcd(f,g) = 1$. Since $p(\beta) = 0$, then $f(\beta) = 0$ or $g(\beta) = 0$. Assume $f(\beta) = 0$. Then there is k s.t. $f(\beta\alpha^k) \neq 0$ but $g(\beta\alpha^k) = 0$. Since ϕ is surjective, there is $\sigma \in Aut(E/F)$ with $\phi(\sigma) = k$. Namely $\sigma(\beta) = \beta\alpha^k$. Since $f(\beta) = 0$ and $\sigma \restriction F = id_F$, also $\sigma(\beta)$ is a root of $\sigma(f) = f$ in $F[x]$, which contradicts $f(\beta\alpha^k) \neq 0$, yet $f(\sigma(\beta)) = 0$, $\sigma(\beta) = \beta\alpha^k$. ∎

Corollary: Suppose $\alpha \in F$ is a primitive p^{th} root of unity. If $a \in F$, then $x^p - a$ either splits in F or is irreducible.

Proof: By previous theorem, there is $\phi: Aut(E/F) \hookrightarrow \left(\frac{\mathbb{Z}}{p\mathbb{Z}}, +\right)$

Since $H \leq \frac{\mathbb{Z}}{p\mathbb{Z}} \implies H = 0$ or $H = \mathbb{Z}/p\mathbb{Z}$, then if $x^p - a$ does not split, $E \supsetneq F$ we have $|Aut(E/F)| > 1 \implies im(\phi) = \mathbb{Z}/p\mathbb{Z} \implies \phi$ surjective $\implies x^p - a$ irreducible. →

Proof ctd.

else, if $\text{im}(\phi) = 0$, then ϕ is not surjective and $x^p - a$ is reducible. Since it has one root, β, then $\beta\alpha^k$ for $k < p$ are all n roots, so $x^p - a$ is irreducible. ∎

Defn: E/F is called a pure extension provided $\exists\, \alpha \in E$, $E = F(\alpha)$ and $\exists\, n > 1$, $\exists\, a \in F$ such that $\alpha^n = a$.

Defn: $p \in F[x]$ is solvable by radicals over F provided E is the splitting field of p/F and $\exists\, \{B_i \mid 1 \le i \le t\}$ s.t. $F \le B_i \lneq B_{i+1}$, $E \le B_t$ and B_{i+1}/B_i is a pure extension.

$$F = B_0 \lneq B_1 \lneq \cdots \lneq B_t \quad \text{and} \quad E \le B_t.$$

Main Theorem: $p \in F[x]$ separable, E splitting field of p over F, then if p is solvable by radicals, then $\text{Aut}(E/F)$ is solvable.

Prop: $p \in F$ solvable by radicals over F. Then $\exists\, \{B_i \mid i \le t\}$ such that $F = B_0 \le B_i \lneq B_{i+1}$ and $B_{i+1} = B_i(\alpha_i)$ where $\alpha_i^{p_i} - a_i = 0$ for some prime p_i and $a_i \in B_i$.

Proof: Clear because for pure extensions w/ $\alpha^n = a$, we can take $\alpha^n = (\alpha^p)^m$ for prime p, and $mp = n$.

Theorem: Let $q \in F[x]$ have $\deg(q) = n$. Suppose for any prime $p \mid n!$, F contains a primitive p^{th} root of unity. If q is solvable by radicals, then $\text{Aut}(E_q/F)$ is solvable, where E_q is the splitting field of q over F.

We will later remove the assumption about primitive pth roots.

4/18/14

F is smallest field containing coefficients of p.

$p \in F[x]$, E is its splitting field, p is solvable by radicals over F if $\exists \{B_i \mid i \le t\}$ s.t.

Fact:

If $p \in F[x]$ is solvable by radicals, then there is a chain $F = B_0 \le B_1 \le \dots \le B_t$ such that B_{i+1}/B_i is pure, and p splits in B_t.

We may assume $[B_{i+1} : B_i]$ is prime.

Recall (Galois Correspondence): $F \le K \le E$, E/F galois and K/F galois, then $Aut(E/K)$ is normal in $Aut(E/F)$ and $Aut(K/F) \cong \frac{Aut(E/F)}{Aut(E/K)}$.

Theorem: Let $q \in F[x]$, $n = \deg(q)$. Suppose for all prime factors p of $n!$, F contains a primitive p^{th} root of unity. If q is solvable over F, then $Aut(E_q/F)$ is solvable as a group, where E_q is the splitting field of q/F.

Fact: $a \in F$. If there is a primitive p^{th} root of unity $\alpha \in F$, then $x^p - a$ splits or is irreducible. (p is prime).

Proof: Suppose $\{B_i \mid i \le t\}$ s.t. $F = B_0 \le B_1 \le \dots \le B_t$, B_{i+1} pure over B_i, q splits in B_t. $[B_{i+1} : B_i] = p_i$ prime. Consider $G_i := Aut(B_t/B_i)$, then we have

$G_{i+1} \le G_i \le \dots \le G_0 = Aut(B_t/F)$. Let $\beta_{i+1} \in B_i$ s.t. β_{i+1} is a root of $x^{p_i} - a_i$ for some $a_i \in B_i$. Since F contains the p_i-th primitive root of unity by assumption, then B_{i+1} is the splitting field of $x^{p_i} - a$. Hence B_{i+1} is galois over B_i. As B_t is also a splitting field of some polynomial over B_0 (take product of polynomials), so B_t/B_0 is galois. Apply galois correspondence to see that

$$Aut(B_{i+1}/B_i) \cong \frac{Aut(B_t/B_i)}{Aut(B_t/B_{i+1})} = \frac{G_i}{G_{i+1}}$$

Also, $|G_i/G_{i+1}| = |Aut(B_{i+1}/B_i)| = [B_{i+1} : B_i] = p_i$ prime

So G_i/G_{i+1} is abelian, and therefore $G_{i+1} \supseteq G_i'$.

Fact: [redacted]
G/H abelian $\Rightarrow G' \subseteq H$.

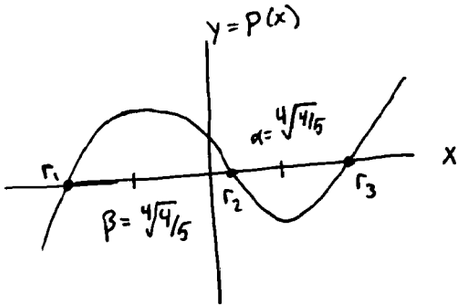
Fact: G solvable, $\phi: G \to H$ then $\phi(G)$ solvable.

Since $G_t = Aut(B_t/B_t) = \{1\}$, we proved that $G_0^{(t)} = 1 \Rightarrow Aut(B_t/F)$ is solvable.

Therefore, $Aut(E/F) \cong \frac{Aut(B_t/F)}{Aut(B_t/E)}$ and therefore solvable. ■

Abel-Ruffini Theorem: There is $p \in \mathbb{Q}[x]$ of degree 5 such that its galois group is not solvable.

Proof: Take $p(x) = x^5 - 4x - 2$. By eisenstein, p is irreducible, and let E be the splitting field of p over $\mathbb{Q}$. Say $\alpha \in E$ a root of q, so $[\mathbb{Q}(\alpha):\mathbb{Q}] = 5$, so $[E:\mathbb{Q}]$ is divisible by $5 \Longrightarrow 5 \mid [\mathrm{Aut}(E/\mathbb{Q})]$. By observing the graph, we see that p has three real roots, r_1, r_2, r_3. Let $z \in \mathbb{C}$ be another root, $z \in \mathbb{C} \setminus \mathbb{R}$. Also $\bar{z}$ a root.



Hence, roots of p are $\{r_1, r_2, r_3, z, \bar{z}\}$. Then $E = \mathbb{Q}(r_1, r_2, r_3, z, \bar{z})$. By Kronecker, any element of $\mathrm{Aut}(E/\mathbb{Q})$ is determined by a permutation of $\{r_1, r_2, r_3, z, \bar{z}\}$, hence $G \leq S_5$. Claim $G \cong S_5$. We identify elements of G with permutations of $\{r_1, r_2, r_3, z, \bar{z}\}$.

Define $\sigma = (r_1 r_2 r_3 z \bar{z})$ in permutation notation, and $\tau = (z\bar{z})$

Fact: $S_5 = \langle (12345), (ij) \rangle$ for $1 \leq i \neq j \leq 5$, that is, S_5 is generated by a 5-cycle and transposition.

Using this fact, $S_5 \leq G$, so $G \cong S_5$. Since S_5 is not solvable, then G is not solvable. ∎

04/21/14

Last time:

Theorem: If $q \in F[x]$, $n = \deg(q)$, E the splitting field of q over F, and F contains all p^{th} roots of unity for all $p \mid n!$ prime, then

q solvable by radicals $\Longrightarrow \mathrm{Aut}(E/F)$ solvable.

Theorem 2 (GC improved): Suppose $F \leq K \leq E$ s.t. K is a splitting field of $p \in F[x]$ over F. Then $\mathrm{Aut}(E/K) \trianglelefteq \mathrm{Aut}(E/F)$ and there exists a monomorphism $\psi: \dfrac{\mathrm{Aut}(E/F)}{\mathrm{Aut}(E/K)} \hookrightarrow \mathrm{Aut}(K/F)$ and if also E is a splitting field over K then ψ is surjective too.

→

First a **Lemma:** Suppose K is the splitting field of $p \in F[x]$ and $E \geq K$. If $\sigma \in Aut(E/F)$ then $\sigma|_K \in Aut(K/F)$.

Proof: If $\sigma \in Aut(E/F)$, $\sigma|_F = id_F$. Fix $\{\alpha_1, \dots, \alpha_n\} \leq K$ all the roots of p. So $K = F(\alpha_1, \dots, \alpha_n)$. By Kronecker, $\sigma(\alpha_i)$ is a root of p, so $\sigma(\{\alpha_1, \dots, \alpha_n\}) = \{\alpha_1, \dots \alpha_n\}$. Hence $\sigma(K) = K$, so $\sigma \in Aut(K/F)$ when restricted to K. ∎

Proof of Thm 2: Consider $\phi: Aut(E/F) \to Aut(K/F)$ given by $\phi(\sigma) = \sigma|_K$. Clearly ϕ is an HM. What is the kernel?

$$Ker(\phi) = \{\sigma \in Aut(E/F) \mid \sigma|_K = id_K\} = Aut(E/K).$$

So by first IM theorem, $\dfrac{Aut(E/F)}{Aut(E/K)} \hookrightarrow Aut(K/F)$. ∎

Suppose now that E is a splitting field of some polynomial over K. Given $\tau \in Aut(K/F)$, there is $\sigma: E \to E$ which extends τ, by uniqueness of splitting field. Since $\tau|_F = id_F$, then also $\sigma|_F = id_F$, so we found a $\sigma \in Aut(E/F)$ s.t. $\phi(\sigma) = \tau$. ∎

Theorem: Let $q \in F[x]$, and let E be its splitting field. If q is solvable (by radicals) over F then $Aut(E/F)$ is solvable.

Proof: Fix $\{B_i \mid i \leq t\}$ such that $F = B_0 \leq B_1 \leq \dots \leq B_t$ where $E \leq B_t$, and B_{i+1} is pure over B_i: (there is $x^{k_i} - a_i$, $a_i \in B_i$, $k_i \geq 1$ prime).

Let $k = \prod_{i=1}^{t} k_i$, and take $\alpha \in \bar{F}$ a primitive k^{th} root of unity.

Consider $F = B_0 \leq F(\alpha) \leq B_1(\alpha) \leq \dots \leq B_t(\alpha) = B^*$. Note that $B_{i+1}(\alpha)$ is also pure over $B_i(\alpha)$.

By theorem 2, $\dfrac{Aut(B^*/F)}{Aut(B^*/F(\alpha))} \leq Aut(F(\alpha)/F)$ (isomorphic to a subgroup of)

By a previous theorem, this is abelian b/c α a primitive root of unity.

Proof continued:

Let $G = Aut(B^*/F)$ and $N = Aut(B^*/F(\alpha))$. $\frac{G}{N}$ is abelian $\Rightarrow$ $\frac{G}{N}$ solvable.

Considering the chain

$F(\alpha) \subsetneq B_1(\alpha) \subseteq B_2(\alpha) \subseteq \dots \subseteq B_t(\alpha)$, then by the previous version of this theorem, N is solvable.

Furthermore, $N \lhd G$, and N is solvable, and G/N is solvable $\Rightarrow$ G solvable. ■

04/23/14 Transcendence Degree

Defn: Suppose M is an R-module. For any $X \subseteq M$, $span(X) = \left\{ \sum_{i=1}^{n} r_i m_i \mid r_i \in R, m_i \in X \right\}$.

(1) X generates $M \iff span(X) = M$

(2) X linearly independent $\iff \forall a \in X \quad a \notin span(X \setminus \{a\})$

(3) X is a basis $\iff$ (1) and (2) hold.

Facts:

(1) $Span(X) = Span(Span(X))$

(2) $X \subseteq Span(X)$

(3) $a \in Span(X) \Rightarrow \exists\, X_0 \subseteq X$ finite, then $a \in Span(X_0)$

(4) $Y \subseteq Span(X)$, $a \in Span(Y) \Rightarrow a \in Span(X)$ "transitivity"

(5) Exchange Principle

$a \in Span(X \cup \{b\}) \setminus Span(X) \Rightarrow b \in Span(X \cup \{a\})$

Only works if R is a division ring.

Proofs:

(1) through (4) trivial.

For (5), $a = \sum_{i=1}^{n} a_i x_i + a_{n+1} b \Rightarrow b = \frac{1}{a_{n+1}} \left(a - \sum a_i x_i \right) \in Span(X \cup \{a\})$

The theory of transendence degree was developed by E. Stienitz in 1910, and leads to the theorem:

Theorem: Given an uncountable cardinal $\lambda > \aleph_0$, and for all p either prime or $p = 0$, then there is a field F of cardinality λ and characteristic p, unique up to isomorphism.

Defn: Let W be a nonempty set, and let $cl: \mathbb{P}(W) \to \mathbb{P}(W)$

(W, cl) is a pre-geometry provided (1) $X \subseteq W \Rightarrow X \subseteq cl(X)$,

and (2) $a \in cl(X) \Rightarrow \exists\, X_0 \subseteq X$ finite, $a \in cl(X_0)$

and (3) $X, Y \subseteq W$ $a \in cl(Y)$ and $Y \subseteq cl(X) \Rightarrow a \in cl(X)$

and (4) $a \in cl(X \cup \{b\}) \setminus cl(X) \Rightarrow b \in cl(X \cup \{a\})$.

and (5) $cl(\emptyset) \subsetneq W$

"Van der Waarden Axioms"

Defn: Let W be nonempty, and $cl: \mathbb{P}(W) \to \mathbb{P}(W)$, then (W, cl) is a matroid provided that (W, cl) is a pregeometry and $\exists\, B \subseteq W$ finite such that $cl(B) = W$.

Notice that $(V, span)$ is a pre-geometry.

Example: Suppose $F \leq E$ fields, $X \subseteq E$. Then $F(X)$ denotes the subfield of E generated by $X \cup F$. $cl(X) = \{\alpha \in E \mid \alpha \text{ algebraic over } F(X)\}$. (E, cl) is a pre-geometry.

Defn: Suppose (W, cl) is a pre-geometry, $X \subseteq W$. Then

(1) X is independent if $a \notin cl(X \setminus \{a\})$ for all $a \in X$

(2) X generates W if $cl(X) = W$

(3) X is a basis for W if X is both independent and generates W.

The main results: (to be proved later)

Theorem 1: if W is a pre-geometry, $X \subseteq W$ nonempty, then TFAE:

(a) X is a basis.

(b) X is a minimal set of generators.

(c) X is a maximal independent set.

Theorem 2: if W is a pre-geometry, $X, Y \subseteq W$. Suppose that X is independent and Y generates W. Then there is $Y' \subseteq Y$ s.t. $X \cap Y' = \emptyset$ and $X \cup Y'$ is a basis.

Corollary: Any independent set can be extended to a basis.

Corollary: Every vector space has a basis.

Theorem 3: If B_1, B_2 are both bases for a pregeometry (W, cl) then $|B_1| = |B_2|$

Defn: the transendence degree of E over F is the dimension of the pregeometry in the example.

↑ dimension of W.

04/25/14

Lemma: (W, cl) is a pre-geometry, then $X \subseteq Y \subseteq W \Rightarrow cl(X) \subseteq cl(Y)$ Monotonicity

Lemma: $cl(Y) = cl(cl(Y))$ for $Y \subseteq W$ Idempotence

Theorem: TFAE for $X \subseteq W$

(1) X a basis
(2) X a minimal set of generators
(3) X is a maximal independent set

Proof:

(1) $\Rightarrow$ (2) enough to show $Y \subsetneq X \Rightarrow cl(Y) \subsetneq W$

Suppose $Y \subsetneq X$, and let $a \in X \setminus Y$ s.t. $a \notin cl(Y)$. Then because X is independent, $a \notin cl(X - \{a\})$, and $X \setminus \{a\} \supseteq Y$, so $a \notin cl(Y)$.

(2) $\Rightarrow$ (3) Suppose X is a minimal set of generators, $a \in X$.

Then X is independent, because $cl(X \setminus \{a\}) \subsetneq X$ by minimality $\Rightarrow a \notin cl(X \setminus \{a\})$

X is maximal: let $a \in W/X$. Enough to show ~~$a \in cl(X \setminus \{a\})$~~ $\hookrightarrow a \in cl(X \cup \{a\} \setminus \{a\}) = cl(X) = W$

(3) $\Rightarrow$ (1) Want to show $cl(X) = W$.

Take $a \in W \setminus cl(X) \Rightarrow a \notin X \Rightarrow X \cup \{a\}$ dependent $\Rightarrow \exists\, b \in X \cup \{a\}$ s.t. $b \in cl(X \cup \{a\} \setminus \{b\})$

(↑ lemma 1; ↑ maximality)

if $b = a$, we're done

if $b \neq a$, $b \in cl(X \setminus \{b\} \cup \{a\})$, and by independence, $b \notin cl(X \setminus \{b\})$

So by the exchange principle, $a \in cl(X \setminus \{b\} \cup \{b\}) \Rightarrow a \in cl(X)$. ■

Theorem 2: X independent, $cl(X) = W \Rightarrow \exists\, Y' \subseteq Y$ s.t. $X \cup Y'$ is a basis and $X \cap Y' = \emptyset$.

Proof: Consider the poset $\mathbb{P} = \{Y^* \subseteq Y \mid X \cup Y^* \text{ independent}, X \cap Y^* = \emptyset\}$ under $\subseteq$.

If Y' is a maximal element of $\mathbb{P}$, then claim $X \cup Y'$ is a basis, $B := X \cup Y'$

By $Y' \in \mathbb{P}$, B is independent. Take $a \in W$ since $cl(Y) = W$, and finite $Y_0 \subseteq Y$ such that $a \in cl(Y_0)$. By transitivity, it is enough to show $Y_0 \subseteq cl(B)$.

(↑ and independence,)

So suppose for contradiction that $\exists\, b \in Y_0 \setminus cl(B)$. Since ~~$b \in cl(B)$~~ $b \notin cl(B) \Rightarrow b \notin B$, so $b \notin X \cup Y^*$. By maximality of Y^*, $X \cup Y^* \cup \{b\}$ not independent, $b \in cl(X \cup Y^*)$. Contradiction.

We know that there is a maximal element of $\mathbb{P}$, by Zorn's Lemma.

4/30/14

Theorem 2: (W, cl) is a pregeometry, $X \subseteq W$ independent, $cl(X) = W$.
$\Longrightarrow \exists\ Y^* \subseteq Y$, $X \cup Y^*$ basis and $Y^* \cap X = \emptyset$.

Remains to show in the proof that Zorn's lemma applies, to the poset $\mathbb{P} = \{Y' \subseteq Y \mid X \cup Y' \text{ independent and } Y' \cap X = \emptyset\}$. Need to show that every chain has an upper bound in $\mathbb{P}$. Let $\mathcal{C}$ be a chain in $\mathbb{P}$.

Clearly (1) $Y' \in \mathcal{C} \Longrightarrow Y' \subseteq Y$

(2) $Y' \in \mathcal{C} \Rightarrow Y' \cap X \neq \emptyset$

(3) $Y' \subseteq \bigcup \mathcal{C}$ $\forall\ Y' \in \mathcal{C}$.

Claim: $X \cup (\bigcup \mathcal{C})$ is independent. Let $Y' = \bigcup \mathcal{C}$

otherwise, there is $a \in X \cup Y'$, $a \in cl(X \cup Y' \setminus \{a\})$. By finite character, $\exists\ X_0 \subseteq X$, $Y_0 \subseteq Y'$ finite. $a \in cl(X_0 \cup Y_0 \setminus \{a\})$. As $\mathcal{C}$ has no last element, $\exists\ Y'' \in \mathcal{C}$, $Y'' \supseteq Y_0$. We found $a \in cl(X_0 \cup Y'' \setminus \{a\})$, so therefore $a \in cl(X \cup Y'' \setminus \{a\}) \Longrightarrow X \cup Y'' \cup \{a\}$ not independent which means that [illegible] b/c $\exists\ y^* \supseteq Y'' \cup \{a\}$, $y^* \in \mathcal{C}$, then $Y^* \cup X$ not independent, contradicts $y^* \in \mathcal{C}$. ∎

Hence by Zorn's lemma, there is $y^* \in \mathbb{P}$ such that Y^* is maximal.

Claim: $X \cup Y^*$ is a basis.

By $Y^* \in \mathbb{P}$, we know $X \cup Y^*$ independent. Remains to show spanning. Enough to show $cl(X \cup Y^*) = W$.

Given $a \in W = cl(Y)$, $\exists\ Y_0 \subseteq Y$ finite, $a \in cl(Y_0)$. If $Y_0 \subseteq X \cup Y^*$ we are done. Else $\exists\ b \in Y_0 \setminus (X \cup Y^*)$, $b \notin X$ and $b \notin Y^* \Longrightarrow X \cup (Y^* \cup \{b\})$ independent, $(Y^* \cup \{b\}) \cap X = \emptyset$

So $Y^* \cup \{b\} \in \mathbb{P}$ and $Y^* \cup \{b\} \supsetneq Y$, so contradicts maximality of Y^*.
So $X \cup Y^*$ must span W. ∎

Stronger statement

Theorem 3: $X, B \subseteq W$, (W, cl) a pregeometry. If X is independent and B is a basis, then $|B| \geq |X|$.

Corollary: All bases have the same size.

Set Theory:

Theorem (Cantor-Bernstein): If $A \hookrightarrow B$ and $B \hookrightarrow A$, then there is a bijection $A \leftrightarrow B$. ($|A| \leq |B|$ and $|B| \leq |A| \Rightarrow |A| = |B|$.)

Cardinal Arithmetic: Suppose A, B disjoint.

$\lambda = |A|$, $\mu = |B|$, $\lambda + \mu = |A \cup B|$, $\lambda\mu = |A \times B|$ $\lambda^\mu = |\{f : B \to A\}|$

Note that because $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Z}|$, then $\aleph_0 + \aleph_0 = \aleph_0$, and ~~$\aleph_0 + \aleph_0$~~

because $|\mathbb{Z}| = |\mathbb{N}| = |\mathbb{Q}|$, $\aleph_0 \aleph_0 = \aleph_0$

Also because $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$, $2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0}$

Fact: If λ is an infinite cardinal, then $\lambda \cdot \lambda = \lambda$

Corollary: B a set of infinite cardinality λ, then $S = \{A \subseteq B : |A| < \aleph_0\}$ has cardinality λ.

Corollary: There are non-algebraic real numbers.

Proof: The cardinality of algebraic numbers is countable, yet $\mathbb{R}$ uncountable.

05/02/14

Theorem: Suppose $F \subseteq E$ are fields. Then $\{a \in E \mid \alpha \text{ algebraic over } F\}$ has cardinality $\leq |F| + \aleph_0$.

Proof: Let $S = F[x]$.

$$|S| \leq \sum_{n \in \mathbb{N}} (|F| + \aleph_0)^n = \sum_{n \in \mathbb{N}} |F| + \aleph_0 = \aleph_0 (|F| + \aleph_0) = \aleph_0 + |F|.$$

Now let $S_p = \{a \in E \mid p(a) = 0\}$. Know that $|S_p| \leq \deg p < \aleph_0$. Let $A = \{\alpha \in E \mid \alpha \text{ alg}/F\}$.

$$|A| = \left|\bigcup_{p \in S} S_p\right| \leq \sum_{p \in S} |S_p| \leq \sum_{p \in S} \aleph_0 \leq |S| \cdot \aleph_0 \leq (|F| + \aleph_0)\aleph_0 = |F| + \aleph_0. \quad \blacksquare$$

Corollary: If $\overline{F}$ is algebraically closed, then $|\overline{F}| = |F| + \aleph_0$

Proof: $|\overline{F}| \leq |F| + \aleph_0$ from previous theorem.

Also, $\overline{F}$ is necessarily infinite, so if $|F| < \aleph_0$

$$|\overline{F}| \leq \sum_{n \in \mathbb{N}} |F|^n \leq \sum_{n \in \mathbb{N}} \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0 \quad \text{but } \overline{F} \text{ infinite, so } |\overline{F}| > \aleph_0$$

if $|F| \geq \aleph_0$, then $|F| \geq |F| + \aleph_0$. ■

Theorem 3: If (W, cl) is a pre-geometry, B a basis and X independent, then $|X| \leq |B|$

Lemma: This holds for finite B.

Proof (Assuming Lemma:) Suppose for the sake of contradiction that $|X| > |B|$.

By finite character, for all $x \in X$, $\exists\, B_x \subseteq B$ finite s.t. $x \in cl(B_a)$.

Consider ~~$f: X \Rightarrow \{B_x \subseteq B : |B_x|$~~ $f: X \longrightarrow \{b \subseteq B : |b| < \aleph_0\}$ (= T) given by $f(a) = B_a$. By a ~~fact~~ from the previous lecture, the cardinality of T is $|B|$. As $|X| \geq |T|$, by pigeonhole there is $S \subseteq X$ infinite, such that $\exists\, b \in T$ s.t. $a \in S \Rightarrow f(a) = b \Rightarrow a \in cl(B)$. Because X is independent, S is also independent. We found a finite b s.t. $\forall a \in X$, $a \in cl(b)$, which contradicts the lemma.

Proof of lemma: Suppose X is independent, B a finite basis. ($m = |X \cap B|$) It is enough to show that there is B_1 with $|B_1| = |B|$ such that $|X \cap B_1| = m+1$. Then by iteration, the claim is proven.

Suppose $B = \{a_1, \ldots, a_n\}$ and $X \cap B = \{a_1, \ldots, a_m\}$. Also WLOG, X generates W by extending X to a basis, by Theorem 2. As B is a minimal set of generators, $cl(B \setminus \{a_{m+1}\}) \subsetneq W$. By monotonicity, $X \not\subseteq cl(B \setminus \{a_{m+1}\})$, since $cl(X) = W$. Take $c \in X \setminus cl(B \setminus \{a_{m+1}\})$. Define $B_1 = (\{a_1, \ldots, a_n\} \setminus \{a_{m+1}\}) \cup \{c\}$.

Clearly $|B_1 \cap X| = m+1$. Enough to show B_1 is a basis.

(1) B_1 independent: if $\exists a \in cl(B_1 \setminus \{a\})$, since $c \notin cl(B \setminus \{a_{m+1}\})$, then $c \notin cl(B \setminus \{a_{m+1}, a\})$. but $c \in cl(B \setminus \{a_{m+1}, a\} \cup \{c\}) \Rightarrow c \in cl(B \setminus \{a_{m+1}\})$ *.

→

proof continued:

(2) B_1 generates W. We are given $cl(B)=W$. Enough to show $a_{m+1} \in cl(B_1)$.

if $c \notin cl(B \setminus \{a_{m+1}\})$, we know $c \in cl(B) = cl(B \setminus \{a_{m+1}\} \cup \{a_{m+1}\})$

Exchange principle: $a_{m+1} \in cl(B \setminus \{a_{m+1}\} \cup \{c\}) = cl(B_1)$. ∎

So B_1 is a basis.

Theorem (Steinitz): If F, E are algebraically closed fields with char F = char E, and $|E| = |F| > \aleph_0$, then $E \cong F$.

Proof:

Claim: the transcendence degree of E over its prime field is $|E|$.

proof: Suppose $B \subseteq E$ is a basis, guaranteed by Theorem 3.

Let P be the prime field of E. Then $a \in E$ is algebraic over $P(B)$. By a previous theorem,

$$|E| \leq |P(B)| \leq \aleph_0 \cdot |B| \quad \text{so} \quad |E| > \aleph_0 \Rightarrow |B| = |E|. \quad ∎$$

By existence of basis, take $B_E \subseteq E$ and $B_F \subseteq F$ both transcendence bases. By lemma, $|E| = |F| \Rightarrow |B_E| = |B_F|$.

Simple algebra shows there is $\phi: P(B_E) \cong P(E_F)$ given any bijection from B_E to B_F. But as E is the algebraic closure of $P(B_E)$ and F an algebraic closure of $P(B_F)$. Uniqueness of algebraic closure $\Rightarrow$

$\exists\, \psi: E \cong F$ extending ϕ. ∎