PMATH 442 Lecture 1: September 12, 2011

David McKinnon
PMATH 442/642

NSERC & OGS scholarship info meeting
Thursday Sept. 15 10–12 noon DC 1302 Refreshments
Office hours are cancelled this Wednesday.

`http://www.student.math.uwaterloo.ca/~pmat442`

Definition: A homomorphism of rings is a function $f\colon R \to S'$ such that

1. $f(a+b) = f(a) + f(b)$
2. $f(ab) = f(a)f(b)$
3. $f(1) = 1$

Definition: Let R be a ring. There is a unique homomorphism $\phi\colon \mathbb{Z} \to R$ given by $\phi(n) = n$, called the characteristic homomorphism. Since $\mathbb{Z}$ is a PID, there is a unique nonnegative $n \in \mathbb{Z}$ such that $\ker \phi = (n)$. The characteristic of R is n.

Definition: An extension of fields is a pair of fields L, K such that $K \subset L$. It's written L/K.

The degree of L/K is the dimension of L as a K-vector space.
Recall: Let F be a field, R a non-zero ring, $\phi\colon F \to R$ a homomorphism. Then ϕ is 1–1.

If $p(x) \in F[x]$ is irreducible, then $F[x]/(p(x))$ is a field. As an extension of F, it has degree $\deg(p)$, with basis

$$\{1, x, \dots, x^{\deg(p)-1}\}.$$

Definition: Let K be a field. A K-algebra is a ring R that contains K.
Definition: A K-algebra homomorphism is a function $f\colon R \to S$ that is a ring homomorphism satisfying $f(a) = a$ for all $a \in K$.

$$f(ab) = f(a)f(b)$$
$$f(cv) = cf(v)$$

Note that a K-algebra homomorphism is also, equivalently, a ring homomorphism that is also a K-linear transformation.

Theorem: Let L/K be an extension of fields, $p(x) \in K[x]$ an irreducible polynomial, $\alpha \in L$ an element satisfying $p(\alpha) = 0$. Then $\phi\colon K[x]/(p(x)) \to K(\alpha)$ given by $\phi(f(x)) = f(\alpha)$ is a K-algebra isomorphism.
Proof: Not doing it. $\square$
So $\{1, \alpha, \alpha^2, \dots, \alpha^{\deg(p)-1}\}$ is a basis for $K(\alpha)$ over K.
Definition: In this context, $p(x)$ is called a minimal polynomial for α over K. It is unique to multiplication by a nonzero element of K.
Theorem: Let $p(x)$ be a minimal polynomial for α over K. If $f(x) \in K[x]$ satisfies $f(\alpha) = 0$, then $p(x) \mid f(x)$.
Proof: Not doing it. $\square$

PMATH 442 Lecture 2: September 14, 2011

Definition: Let K be a field, L an extension of K, $a \in L$ an element. Then α is algebraic over K *iff* there is a polynomial $p(x) \in K[x]$, $p(x) \not\equiv 0$, such that $p(\alpha) = 0$. (Otherwise, α is transcendental over K.) We say L/K is algebraic *iff* every element of L is algebraic over K.

L/K is finite *iff* $[L : K]$[1)] $< \infty$.

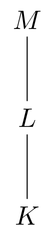
Theorem: Let L/K be a finite extension. Then L/K is algebraic.
Proof: Let $\alpha \in L$ be any element. Let $n = [L : K]$. The $n+1$ vectors 1, α, α^2, …, α^n are linearly dependent,

[1)] $= \dim_K L$

so there exist $a_0, a_1, \ldots, a_n \in K$ such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, but not all of the a_is are 0. So α is algebraic over K, since it's a root of $p(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$. $\square$

Example: $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \ldots)$ is algebraic over $\mathbb{Q}$, but not finite.

Theorem: (KLM)



$$[M:K] = [\underset{m}{M:L}][\underset{l}{L:K}]$$

Proof: Let $\{a_1, \ldots, a_l\}$ be a basis for L/K, $\{b_1, \ldots, b_n\}$ be a basis for M/L. Consider $\{a_ib_j\}_{\substack{i\in\{1,\ldots,l\}\\ j\in\{1,\ldots,m\}}}$.

Show that this set is a basis for M/K, from which the theorem immediately follows.

Linear independence: Assume $\sum_{i,j} \gamma_{i,j}a_ib_j = 0$ for some $\gamma_{ij} \in K$. Then $\sum_j \left(\sum_i \gamma_{ij}\alpha_i\right)b_j = 0$.

Since $\{b_j\}$ is linearly independent over L, we get $\sum_i \gamma_{ij}a_i = 0$ for all j. Since $\{a_i\}$ is linearly independent over K, we conclude that $\gamma_{ij} = 0$, for all i, j.

Spanning: Choose $\alpha \in M$. Then

$$\alpha = \sum_j c_jb_j,$$

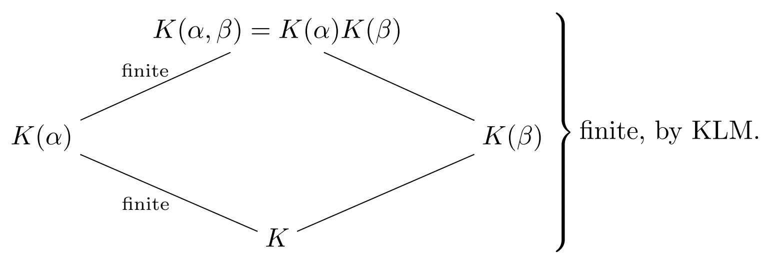
for some $c_j \in L$. For each j, there are γ_{ij} in K such that $c_j = \sum_i \gamma_{ij}\alpha_i$. Then:

$$\alpha = \sum_{i,j} \gamma_{ij}a_ib_j,$$

and we're done. $\square$

Let L/K be an extension of field. Let L^{alg} be the set of elements of L algebraic over K.

Theorem: L^{alg} is a field.
Proof: Let $\alpha \in L^{\text{alg}}$ be any element. Then $K(\alpha)/K$ is finite, because its degree is the degree of a minimal polynomial for α/K, which exists because α/K is algebraic. If $\beta \in L^{\text{alg}}$ is any other element, then $K(\beta)/K$ is finite too.



So $K(\alpha, \beta)$ is also finite. It contains $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and α/β (if $\beta \neq 0$), so all these must be in L^{alg}. $\square$

The field L^{alg} is called the algebraic closure of K in L.

Definition: Let M/K be an extension. Let E, $F \subset M$ be subfields of M containing K. The compositum (composite) of E and F over K is EF, defined to be the smallest subfield of M that contains E and F.

If $E = K(\alpha_1, \ldots, \alpha_n)$, $F = K(\beta_1, \ldots, \beta_m)$, then $EF = K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$.

Splitting Fields
Let L/K be an extension, $p(x) \in K[x]$ a non-constant polynomial. Then L is a splitting field for $p(x)$ over K *iff*:

(1) $p(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ for some c, $\alpha_i \in L$, *and*

(2) $L = K(\alpha_1, \ldots, \alpha_n)$.

Example: A splitting field for $x^4 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$.
Example: A splitting field for $x^3 + x + 1$ over $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ is $\mathbb{F}_2(a_1, a_2, a_3) = \mathbb{F}_8$, the field with 8 elements. (Note a_1, a_2, a_3 are the roots of $x^3 + x + 1$ in $\mathbb{F}_8$.)

PMATH 442 Lecture 3: September 16, 2011

Splitting Fields
Let K be a field, $p(x) \in K[x]$ a non-constant polynomial *A* splitting field for $p(x)$ over K is a field L such that:

(1) $p(x) = c(x-a_1)\cdots(x-a_n)$ for some c, a_1, $\ldots$, $a_n \in L$ *and*

(2) $L = K(a_1, \ldots, a_n)$

Fact: Up to isomorphism, there is exactly one splitting field for a given $p(x)$ over K.
Definition: A finite field extension L/K is normal *iff* L is the splitting field for some $p(x) \in K[x]$.
Note:

$$\left.\begin{array}{c} K(a_1, \ldots, a_n) \\ \vdots \\ \Big|{\scriptstyle \leq n-1} \\ K(a_1) \\ \Big|{\scriptstyle \leq n} \\ K \end{array}\right\} \text{degree} \leq n!$$

Definition: Let K be a field. An algebraic closure of K is a field K such that:

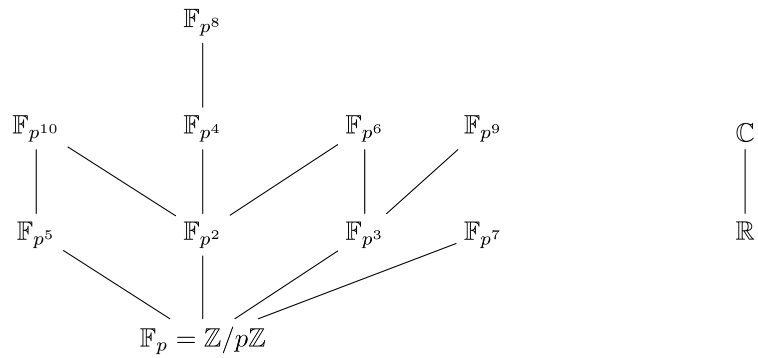
(1) L/K is algebraic

(2) Every non-constant polynomial $p(x) \in K[x]$ splits into linear factors in $L[x]$.

Fact: Up to isomorphism, there is exactly one algebraic closure of K.
Definition: A field K is algebraically closed *iff* every non-constant $p(x) \in K[x]$ splits into linear factors in $K[x]$.

Theorem: Any algebraic closure of a field K is algebraically closed.
Proof: Let L be an algebraic closure of K, and let $p(x) \in L[x]$ be any non-constant polynomial. Proceed by induction on $\deg(p)$. The base case $\deg(p) = 1$ is trivial.
Assume every polynomial of deg $\leq n$ splits, and let $\deg(p) = n+1$. If p is reducible, we're done. If not, let M/L be a splitting field for $p(x)$ over L.
Any root $\alpha \in M$ of $p(x)$ is algebraic over L. But L is algebraic over K, so M is also algebraic over K. Let $q(x) \in K[x]$ be a minimal polynomial for α over K. Then since $q(x) = 0$, we get $p(x) \mid q(x)$, and $q(x)$ splits into linear factors over K, so $p(x)$ does too. $\square$

Example: Union is $\overline{\mathbb{F}_p}$



Definition: Let K be a field, $p(x) \in K[x]$ a non-constant polynomial. We say that $p(x)$ is separable over K *iff* $\gcd(p, p') = 1$.
Definition: The derivative of $a_0 + a_1x + \cdots + a_nx^n$ is $a_1 + 2a_2x + \cdots + na_nx^{n-1}$.
Theorem:

$$\begin{aligned}(pq)' &= p'q + pq' \\ (p \pm q)' &= p' \pm q' \\ (cp)' &= cp' \text{ if } c \in K\end{aligned}$$

Proof: As if. □

Theorem: Let $p(x) = c\prod_i (x - a_i)^{n_i}$ for distinct $a_i \in K$. Then $x - a_i \mid p'(x)$ *iff* $(x - a_i)^2 \mid p(x)$.
Proof: Backwards: $p(x) = (x - a_i)^2q(x)$, so $p'(x) = 2(x - a_i)q(x) + (x - a_i)^2q'(x)$ which has a factor of $x - a_i$.

$$\begin{aligned}\text{Forwards: } p'(x) &= (x - a_i)q(x) \\ \implies p'(x) &= q(x) + (x - a_i)q'(x) \\ \implies 0 &= p'(a_i) = q(a_i)\end{aligned}$$

so $x - a_i \mid q(x) \implies (x - a_i)^2 \mid p(x)$ □

So $p(x)$ is separable *iff* it has no multiple roots in any extension of K.
Definition: Let L/K be an extension, $\alpha \in L$, α algebraic over K. Then α is separable over K *iff* its minimal polynomial over K is separable.

PMATH 442 Lecture 4: September 19, 2011

Fact: $p(x)$ is separable *iff* $\gcd(p, p') = 1$.
Definition: Let L/K be a field extension, $\alpha \in L$ an algebraic element. Then α is separable over K *iff* the minimal polynomial for α/K is separable. We say L/K is separable *iff* every $\alpha \in L$ is separable over K.
Definition: A field K is perfect *iff* every finite extension of K is separable.
Theorem: If $\operatorname{char} K = 0$, then K is perfect.
Proof: Let L/K be an extension, $\alpha \in L$ an algebraic element, $p(x) \in K[x]$ its minimal polynomial over K. Then $p(x)$ is irreducible in $K[x]$. If $\alpha \in K$, then α is trivially separable over K.
If not, then $p'(x)$ is non-constant, of degree smaller than $\deg(p)$. So $\deg(\gcd(p, p')) < \deg(p)$. Since p is irreducible, we conclude $\gcd(p, p') = 1$. □
What kind of polynomial has 0 derivative? Say $\operatorname{char} K = l$.

$$\begin{aligned}p(x) &= a_0 + a_1x + \cdots + a_nx^n \\ \implies p'(x) &= a_1 + 2a_2x + \cdots + na_nx^{n-1}\end{aligned}$$

If $p' = 0$ then $ia_i = 0$ for all i. This is equivalent to demanding $a_1 = 0$ for all i prime to p.
So $p'(x) = 0$ *iff*

$$p(x) = a_0 + a_lx^la_{2l}x^{2l} + \cdots + a_{nl}x^{nl}$$

Definition: Let K be a field of characteristic $l \neq 0$. Define the Frobenius homomorphism

$$\mathrm{Frob}_l \colon K \to K$$

by $\mathrm{Frob}_l(a) = a^l$.
Theorem: If $\operatorname{char} K = l \neq 0$, then $(a+b)^l = a^l + b^l$ for all $a, b \in K$.

Proof:
$$(a+b)^l = \sum_{i=0}^{l} \binom{l}{i} a^i b^{l-i}$$

If $i \neq 0, l$, $\binom{l}{i} = \frac{l!}{(l-i)!i!}$ is divisible by l, so:

$$= a^l + b^l \quad \square$$

Theorem: Let K be a field of characteristic $l \neq 0$. Then K is perfect *iff* $\mathrm{Frob}_l \colon K \to K$ is onto (is an isomorphism).
Proof: Backwards: Assume Frob_l is onto, and let α be any algebraic element in an extension L/K. Let $p(x)$ be a minimal polynomial for α/K.

If $p'(x) \neq 0$, then $\gcd(p, p') = 1$, and so α is separable over K. If $p'(x) = 0$, then:

$$\begin{aligned} p(x) &= a_0 + a_l x^l + \cdots + a_{nl} x^{nl} \\ \text{(since } \mathrm{Frob}_l \text{ is onto)} \quad &= (b_0)^l + (b_1)^l x^l + \cdots + (b_n)^l x^{nl} \\ &= (b_0 + b_1 x + \cdots + b_n x^n)^l \end{aligned}$$

which is reducible. This is impossible, so $p' \neq 0$.

Forwards: Since Frob_l is not onto, there is some $a \in K$ such that $a \neq b^l$ for any $b \in K$. Consider $x^l - a$, and let F/K be a splitting field for $x^l - a$. There is some root $\alpha \in F$ of $x^l - a$:

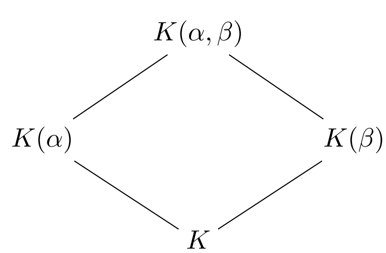
$$\alpha^l - a = 0$$
$$\implies x^l - a = x^l - \alpha^l = (x - \alpha)^l$$

Since $\alpha \notin K$, its minimal polynomial $p(x)$ over K has degree at least 2, and it's a factor of $(x-\alpha)^l$. So $p(x)$ isn't separable. $\square$

Theorem: Every finite field is perfect.
Proof: Frob_l, on a finite field is a 1–1 function from a finite set to itself. It's therefore onto. $\square$
Example: $\mathbb{F}_l(T)$ is imperfect, since T is not the lth power of any rational function, for degree reasons.

$$\mathbb{C}(x) = \left\{ \tfrac{p(x)}{q(x)} : {}^{p,q \in \mathbb{C}[x]}_{q \neq 0} \right\}$$
$$\mathbb{F}_l(T) = \left\{ \tfrac{p(T)}{q(T)} : {}^{p,q \in \mathbb{F}_l[T]}_{q \neq 0} \right\}$$

Definition: Let L/K be a finite extension. The separable closure of K in L is the set of all elements of L that are separable over K.
Theorem: The separable closure of K in L is a field.
Proof: Let K^{sep} be the separable closure of K in L. Let α, $\beta \in K^{\mathrm{sep}}$ be elements.



PMATH 442 Lecture 5: September 21, 2011

Cyclotomic extensions
Let n be an integer, $\zeta_n \in \mathbb{C}$ a primitive root of unity; *i.e.*, $\zeta_n = (e^{2\pi i/n})^a$ for some integer a prime to n. The nth cyclotomic extension of $\mathbb{Q}$ is $\mathbb{Q}(\zeta_n)$. Note that this is independent of a.

n	$\mathbb{Q}(\zeta_n)$	degree over $\mathbb{Q}$
1	$\mathbb{Q}$	1
2	$\mathbb{Q}$	1
3	$\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$	2
4	$\mathbb{Q}(i)$	2
5		4
6	$\mathbb{Q}(\sqrt{-3})$	2
$\vdots$		$\vdots$
n		$\phi(n)$

Definition: The group μ_n is the group of nth roots of unity with respect to multiplication.
We have $\mu_n \cong C_n$ (or $\mathbb{Z}/n\mathbb{Z}$), with generator $e^{2\pi i/n}$, via:

$$e^{2\pi i a/n} \mapsto a \bmod n$$

Note $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\mu_n)$.
Note that if $d \mid n$, then $\mu_d \subset \mu_n$.
Definition: The nth cyclotomic polynomial is

$$x^n - 1 = \prod_{\alpha \in \mu_n} (x - \alpha) = \prod_{a=1}^{n} (x - e^{2\pi i a/n})$$
$$\phi_n(x) = \prod_{(a,n)=1} (x - e^{\pi i a/n})$$

Note that $x^n - 1 = \prod_{d|n} \phi_d(x)$
Note $\phi_n(x)$ has degree $\phi(n) = \#$ integers prime to n between 0 and n.

Theorem: $\phi_n(x) \in \mathbb{Z}[x]$, and is primitive. **Proof:** By induction on n. If $n = 1$, $\phi_n(x) = x - 1$ and we're done.
Now assume $\phi_k(x) \in \mathbb{Z}[x]$ for all $k < n$, and consider $\phi_n(x)$. We have

$$\begin{aligned} x^n - 1 &= \prod_{d|n} \phi_d(x) \\ &= \phi_n(x) \prod_{\substack{d|n \\ d \neq n}} \phi_d(x) \end{aligned}$$

Since $x^n - 1$, $\phi_d(x) \in \mathbb{Z}[x]$ for $d < n$, we deduce $\phi_n(x) \in \mathbb{Q}[x]$. Since $\mathbb{Z}$ is a UFD and since $\prod \phi_d(x)$ is primitive (by Gauss' Lemma), we conclude by Gauss' Lemma that $\phi_n(x) \in \mathbb{Z}[x]$. $\phi_n(x)$ is primitive because it's monic. □

Theorem: $\phi_n(x)$ is irreducible over $\mathbb{Q}$.
Proof: By Gauss' Lemma, it suffices to show that $\phi_n(x)$ is irreducible over $\mathbb{Z}$. Assume $\phi_n(x) = f(x)g(x)$ for irreducible $f(x)$ over $\mathbb{Q}$, $f(x), g(x) \in \mathbb{Z}[x]$. Let ζ_n be come primitive nth root of unity. Note that if p is prime, $p \nmid n$, then $\phi_n(\zeta_n^p) = 0$. $f(\zeta_n) = 0$
Since $x^n - 1$ is separable, so is $\phi_n(x)$, so there are 2 cases:
Case I: $g(\zeta_n^p) = 0$ for some prime p. Then ζ_n is a root of $g(x^p)$. Since $f(\zeta_n) = 0$ and f is irreducible, we get

$$g(x^p) = f(x)h(x)$$

for some $h(x) \in \mathbb{Z}[x]$. Reducing mod p:

$$\begin{aligned} g(x^p) &\equiv f(x)h(x) \bmod p \\ \implies g(x)^p &\equiv f(x)h(x) \bmod p \end{aligned}$$

so $\gcd(f, g) \not\equiv 1 \bmod p$.
So $\phi_n(x) = f(x)g(x)$ has a multiple root mod p. But this is impossible, since $\phi_n(x) \mid x^n - 1$ and $x^n - 1$ is separable mod p (since $p \nmid n$). So we are in:
Case II: $g(\zeta_n^p) \neq 0$ for all primes $p \nmid n$. In this case, $g(\zeta_n^a)$ for all a prime to n. Since $g \mid \phi_n(x)$, this means $g(x)$ is constant and $\phi_n(x)$ is irreducible. $\square$

So ζ_n has minimal polynomial $\phi_n(x)$ over $\mathbb{Q}$. Since $\deg(\phi_n(x)) = \phi(n)$, we conclude:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$$

If $n = p$ is prime, then $\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$.

PMATH 442 Lecture 6: September 23, 2011

Let K/F be a field extension. Then $\mathrm{Aut}_F(K)$ is the set of F-algebra isomorphisms $\phi\colon K \to K$.
Example: $\mathrm{Aut}_K(K) = \{1\}$[2)]
(An automorphism is an isomorphism of an object with itself.)
Example: $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{1, \sigma\}$ where σ is complex conjugation.
Example: $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = \{1, \sigma\}$ where $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$.
Example: If $\sqrt{D} \notin F$, then $\mathrm{Aut}_F(F(\sqrt{D})) = \{1, \sigma\}$, where $\sigma(a + b\sqrt{D}) = a - b\sqrt{D}$.

$$\begin{aligned} i^2 = -1 &\implies \sigma(i^2) = \sigma(-1) \\ &\implies \sigma(i)^2 = -1 \end{aligned}$$

Theorem: Let $p(x) \in F[x]$ be any polynomial, E/F an extension, $\sigma \in \mathrm{Aut}_F(E)$. If $\alpha \in E$ is a root of $p(x)$, then so is $\sigma(\alpha)$.
Proof: Let $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ for $a_i \in F$. Then:

$$\begin{aligned} a_0 + a_1\alpha + \cdots + a_n\alpha^n &= 0 \\ \implies \sigma(a_0 + \cdots + a_n\alpha^n) &= 0 \\ \implies \sigma(a_0) + \cdots + \sigma(a_n)\sigma(\alpha)^n &= 0 \\ \implies a_0 + \cdots + \sigma(\alpha)^n &= 0 \\ \implies p(\sigma(\alpha)) &= 0 \quad \square \end{aligned}$$

Since σ is 1–1, it follows that it permutes the roots of $p(x)$.
Example: $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{1\}$, because $\sigma(\sqrt[3]{2})^3 = 2 \implies \sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ since $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$.

Theorem: Let $S \subset \mathrm{Aut}_F(K)$ be any subset. Let $E = \{\, \alpha \in K : \sigma(\alpha) = \alpha \text{ for all } \sigma \in S \,\}$.
(E is called the fixed field of S.)
Then E is a field.
Proof: It suffices to show 0, $1 \in E$ (clear) and that E is closed under $+$, $-$, $\cdot$, and $\div$. Thus, pick any a, $b \in E$. Then for all $\sigma \in S$, $\sigma(a) = a$ & $\sigma(b) = b$, so $\sigma(a + b) = \sigma(a) + \sigma(b)$, and similarly for the rest. $\square$

Theorem: Let $T \subset K$ be any subset. Let $H = \{\, \sigma \in \mathrm{Aut}_F(K) : \sigma(\alpha) = \alpha \text{ for all } \alpha \in T \,\}$.
Then H is a subgroup of $\mathrm{Aut}_F(K)$.
Proof: It suffices to show $1 \in H$ (clear) and H closed under composition and inversion. This is easy:

$$\sigma_1 \in H,\ \sigma_2 \in H \implies \sigma_i(\alpha) = \alpha \text{ for } i = 1, 2$$

so $\sigma_1^{-1}(\alpha) = \alpha$ and $\sigma_1(\sigma_2(\alpha)) = \sigma_1(\alpha) = \alpha$ $\square$

[2)] id

$\text{Aut}_F(K)$	K/F
S $\longrightarrow$	fixed field, $F \subset E \subset K$
fixing automorphisms H subgroup $\longleftarrow$	T

Notice that the fixed field of S is the same as the fixed field of the subgroup generated by S.
Notice also that if $T \subset K$ is any subset, then the automorphisms fixing T are the same as the automorphisms fixing $F(T)$.

In particular, if $\alpha \in K$ is any element, then the F-algebra homomorphisms of K fixing α are precisely the F-algebra homomorphisms fixing $F(\alpha)$.

For instance, $\sigma \in \text{Aut}_{\mathbb{Q}}(\mathbb{C})$ fixes $\sqrt{2}$ *iff* it fixes $\mathbb{Q}(\sqrt{2})$.

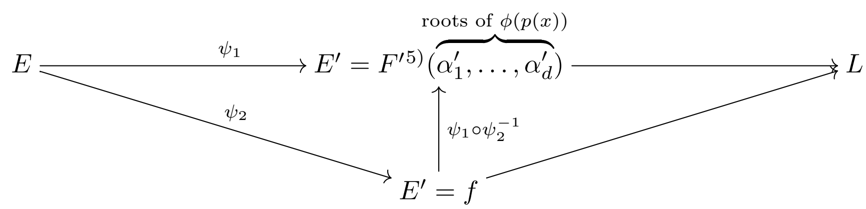
If $H_1 \subset H_2$, then $\text{fix}(H_2) \subset \text{fix}(H_1)$. If $E_1 \subset E_2$, then H_2[3] $\subset H_1$[4].

$\text{Aut}_{\mathbb{R}}(\mathbb{C})$	$\mathbb{C}/\mathbb{R}$
$\{1\}$	$\mathbb{C}/\mathbb{R}$
$\{1, \sigma\}$	$\mathbb{R}/\mathbb{R}$

For which field extensions K/F is this correspondence a bijection?
Answer: Splitting fields. Almost.

PMATH 442 Lecture 7: September 26, 2011

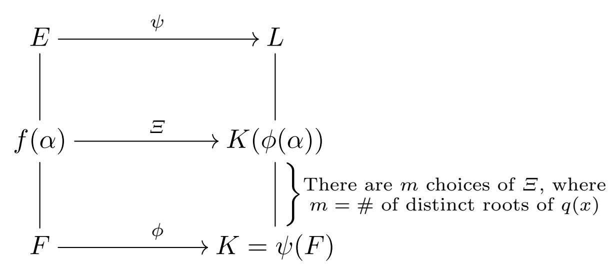
Theorem: Let E/F be a field extension of degree n, and assume that E is the spitting field of a polynomial $p(x) \in F[x]$. Let L be a field, $\phi\colon F \to L$ a homomorphism, and assume that $\phi(p(x))$ splits into linear factors in $L[x]$. Then there is a homomorphism $\psi\colon E \to L$ extending ϕ, and there are at most n such extensions ψ, with equality *iff* $p(x)$ is separable.



$$E' = \psi_1(E) = \psi_2(E)$$

Proof: The existence of ψ follows from the existence & uniqueness of splitting fields up to isomorphism.

Induce on n. Base case $n = 1$ is trivial, so assume the theorem for extensions of degree $\leq n-1$. Let $q(x)$ be an irreducible factor of $p(x)$ of degree at least 2. Let $\alpha \in E$ be a root of $q(x)$. Then:



E is the splitting field for $p(x)$ over $f(\alpha)$. By induction, there are at most $[E : F(\alpha)]$ choices of ψ for any given Ξ, with equality *iff* $p(x)$ has distinct roots. The number of choices of Ξ is at most $\deg(p(x))$, with equality *iff* $q(x)$ has distinct roots. So the number of choices of ψ in total is:

$$[E : F(\alpha)][F(\alpha) : F] = [E : F] = n,$$

[3] $\text{Aut}_{E_2}(K)$
[4] $\text{Aut}_{E_1}(K)$
[5] $\phi(F)$

with equality *iff* $p(x)$ is separable. $\square$

Corollary: If E is a splitting field of some polynomial over F, then $\#\operatorname{Aut}_F(E) \leq [E:F]$, with equality *iff* $p(x)$ is separable.

Definition: A finite extension E/F is Galois *iff* $\#\operatorname{Aut}_F(E) = [E:F]$.
Corollary: Splitting fields of separable polynomials are Galois.
Definition: If E/F is Galois, then $\operatorname{Gal}(E/F) = \operatorname{Aut}_F(E)$ is the Galois group of E/F.
Example: $\operatorname{Gal}(K/K) = \{1\}$.
Example: $\operatorname{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$, $\sigma =$ complex conjugation
Example: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois! Because $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$, but $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{1\}$.

PMATH 442 Lecture 8: September 28, 2011

Shuntaro Yamagishi

If E is a splitting field for a separable polynomial in $F[x]$, then E/F is Galois. If F is perfect (e.g., if $\operatorname{char} F = 0$ or F is finite) then every splitting field over F is Galois.
Example: $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$:
To determine a homomorphism from $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ to itself, it is enough to figure out where $\sqrt{2}$ & $\sqrt{3}$ go.
Clearly $\substack{\sqrt{2}\mapsto\pm\sqrt{2} \\ \sqrt{3}\mapsto\pm\sqrt{3}}$ are the only possibilities.

		$\sqrt{3}$: +	$\sqrt{3}$: −
$\sqrt{2}$	+	id	σ_2[6]
	−	σ_3	σ_6[7]

All four possibilities work, if you check them, so $\#\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \geq 4$. Since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}] = 4$, we conclude that $\#\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) = 4$, and $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is Galois.

$$\operatorname{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

This group has 5 subgroups.

$$\begin{array}{ccc} \{1\} & \longleftrightarrow & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ \{1, \sigma_3\} & \longleftrightarrow & \mathbb{Q}(\sqrt{3}) \\ \{1, \sigma_2\} & \longleftrightarrow & \mathbb{Q}(\sqrt{2}) \\ \{1, \sigma_6\} & \longleftrightarrow & \mathbb{Q}(\sqrt{6}) \\ \{1, \sigma_2, \sigma_3, \sigma_6\} & \longleftrightarrow & \mathbb{Q} \end{array}$$

Example: $\mathbb{F}_{343}/\mathbb{F}_7$
$\mathbb{F}_{343} =$ splitting field of $x^{343} - x$ over $\mathbb{F}_7$. Since $x^{343} - x$ is separable, $F_{343}/\mathbb{F}_7$ is Galois. Let $\sigma = \operatorname{Frob}_7 \colon \mathbb{F}_{343} \to \mathbb{F}_{343}$. It's an $\mathbb{F}_7$-automorphism of $\mathbb{F}_{343}$.

$$\mathbb{F}_{343} \cong \mathbb{F}_7[x]/(x^3 - 2) \cong \mathbb{F}_7(\sqrt[3]{2})$$

Let Larry, Curly and Moe be the three cube roots of two $\mathbb{F}_{343}$.

$$\begin{aligned} \sigma(\text{Larry}) &= \text{Curly} \qquad \text{(wlog)} \\ \sigma(\text{Curly}) &= \text{Moe} \\ \sigma(\text{Moe}) &= \text{Larry} \end{aligned}$$

So $\{1, \sigma, \sigma^2\}$ are three different $\mathbb{F}_7$-automorphisms of $\mathbb{F}_{343}$. So $\mathbb{F}_{343}/\mathbb{F}_7$ is Galois.

[6] $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$
[7] $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$

Example: $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. Degree 4.

$$\mathbb{Q}(\sqrt[4]{2})$$
$$2 \left| \right\} \text{Galois: } \begin{cases} \text{id} \\ a+b\sqrt[4]{2} \overset{\sigma}{\mapsto} a-b\sqrt[4]{2} \\ a,b\in\mathbb{Q}(\sqrt{2}) \end{cases}$$
$$\mathbb{Q}(\sqrt{2})$$
$$2 \left| \right\} \text{Galois: } \begin{cases} \text{id} \\ a+b\sqrt{2} \mapsto a-b\sqrt{2} \\ a,b\in\mathbb{Q} \end{cases}$$
$$\mathbb{Q}$$

$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2})) = \{\mathrm{id}, \sigma\}$ which is too small! So $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not Galois.

Definition: Let G be a group, K a field, V a (finite-dimensional) K-vector space, $\mathrm{GL}(V)$ the group of invertible K-linear transformations $V \to V$. (e.g., $V = K^n$, $\mathrm{GL}(V) = M_n(K)$.)
A representation of G with values in V is a homomorphism $\rho\colon G \to \mathrm{GL}(V)$.

PMATH 442 Lecture 9: September 30, 2011

Shuntaro Yamagishi
shuntaroy@hotmail.com

Definition: G a group, K a field, V a K-vector space. A representation of G in V is a homomorphism $\rho\colon G \to \mathrm{GL}^{8)}(V)$

$$\dim \rho = \dim V$$

We'll work with 1-dimensional representations, called characters:
Example: Dirichlet characters:

$$\rho\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$$
$$\rho(m) = e^{2\pi i m/n}$$

Example: K, L fields, $\phi\colon K \to L$ a homomorphism. Then $\phi|_{K^*}$ is a 1-dim representation of K^* in L.

Theorem: Let G be a group, L a field, $\chi_1, \ldots, \chi_r$ a set of distinct characters of G over L. Then $\{\chi_1, \ldots, \chi_r\}$ are linearly independent over L.
Proof: Assume not, and let (after possibly renumbering) $\{\chi_1, \ldots, \chi_t\}$ be an L-linear dependent subset of minimal size. Then there are $a_1, \ldots, a_t \in L$ such that

$$a_1\chi_1(g) + \cdots + a_t\chi_t(g) = 0$$

for all $g \in G$. Note $t \geq 2$, and choose $\gamma \in G$ such that $\chi_1(\gamma) \neq \chi_t(\gamma)$. Then

$$\begin{aligned} & a_1\chi_1(\gamma)\chi_1(g) + \cdots + a_t\chi_t(\gamma)\chi_t(g) = 0 \\ \textit{and} \quad & a_1\chi_t(\gamma)\chi_1(g) + \cdots + a_t\chi_t(\gamma)\chi_1(g) = 0 \\ \implies & (\text{nonzero})\chi_1(g) + \cdots + (\text{something})\chi_{t-1}(g) = 0 \end{aligned}$$

so $\{\chi_1, \ldots, \chi_{t-1}\}$ is linearly dependent, which is a contradiction. $\square$

Theorem: Let K/E be a field extension, F and E-subfield of K. Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be E-automorphisms of K whose fixed field is F. If G is a group, then

$$\#G = [K : F].$$

Proof: Let $m = [K : F]$, $\{w_1, \ldots, w_n\}$ an F-basis of K. Define

$$\boldsymbol{v}_i = \begin{pmatrix} \sigma_i(w_1) \\ \vdots \\ \sigma_i(w_m) \end{pmatrix} \in K^m$$

8) invertible K-linear transformation $V \to V$

There are n vectors in $\boldsymbol{v}_i$. If we show that the $\boldsymbol{v}_i$s are K-linear independent it will follow that $n \leq m$. Thus, say $a_1, \ldots, a_n \in K$ satisfy:

$$a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n = \mathbf{0}.$$

We want to show $a_i = 0$ for all i. Well:

$$a_1\sigma_1(w_j) + \cdots + a_n\sigma_n(w_j) = 0$$

for all j. Since $\{w_1, \ldots, w_m\}$ is a basis for K/F, and since the σ_i are all F-linear transformations, we get

$$a_1\sigma_1(\alpha) + \cdots + a_n\sigma_n(\alpha) = 0$$

for any $\sigma \in K$. Since the σ_is are characters of K^* in K, they're K-linearly independent so $a_i = 0$ for all i. So $\#G \leq [K : F]$. Let $\alpha_1, \ldots, \alpha_{n+1} \in K$ be any elements. If we show it's linearly independent over F, then $\dim_F K \leq n$. Define

$$\boldsymbol{u}_i = \begin{pmatrix} \sigma_1(\alpha_i) \\ \vdots \\ \sigma_n(\alpha_i) \end{pmatrix} \in K^n.$$

There are $n+1$ of the $\boldsymbol{u}_i$s, so they are linearly dependent over K.
Choose $\beta_1, \ldots, \beta_{n+1} \in K$ such that

(1) $\beta_1\boldsymbol{u}_1 + \cdots + \beta_{n+1}\boldsymbol{u}_{n+1} = \mathbf{0}$

(2) A minimal # of β_i are 0.

and (3) $\beta_1, \ldots, \beta_t$ are nonzero, $\beta_{t+1}, \ldots, \beta_{n+1} = 0$, $\beta_t = 1$.

If all β_i are in F, then $\{\alpha_1, \ldots, \alpha_{n+1}\}$ is linearly dependent over F, by looking at first coordinate of (1).

If not, assume without loss of generality that $\beta_1 \notin F$. Choose σ (in G) such that $\sigma(\beta_1) \neq \beta_1$. Then:

$$\sigma(\beta_1)\sigma(\boldsymbol{u}_1) + \cdots + \sigma(\beta_t)\sigma(\boldsymbol{u}_t) = \mathbf{0}$$

But σ acts on each $\boldsymbol{u}_i$ by permuting the coordinates in the same way. So:

$$\sigma(\beta_1)\boldsymbol{u}_1 + \cdots + \sigma(\beta_t)\boldsymbol{u}_t = \mathbf{0}$$

Subtraction with (1) gives:

$$[\beta_1 - \sigma(\beta_1)]\boldsymbol{u}_1 + \cdots + [\beta_t - \sigma(\beta_t)]^{9)}\boldsymbol{u}_t = \mathbf{0}$$

So this relation has fewer nonzero terms, which is a contradiction. So $\beta_i \in F$ for all i, and we're done.

PMATH 442 Lecture 10: October 3, 2011

Theorem: Let K/F be a Galois extension. If $p(x) \in F[x]$ is irreducible and has a root in K, then $p(x)$ splits into linear factors in $K[x]$, and $p(x)$ is separable.
Proof: Let $G = \mathrm{Gal}(K/F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, $\sigma \in K$, $p(\alpha) = 0$. Let $\alpha_i = \sigma_i(\alpha)$ be the conjugates of α. Define $f(x) = \prod_i{}^{10)}(x - \alpha_i)$. Then G acts on the roots of $f(x)$ by permutation, so the coefficients of $f(x)$ are fixed by G.
The fixed field of G is a field that contains F and of which K is a degree n extension, so it *is* F.
Now, $f(\alpha) = 0$, so $p(x) \mid f(x)$. Since $p(\alpha_i) = 0$ for all i, we get $f(x) \mid p(x)$, and so $f(x)$ is also irreducible (it's a constant times $p(x)$). Furthermore, $p(x)$ has all its roots in K, and it's separable (because $f(x)$ is). □

Theorem: Let K/F be a finite extension. Then K/F is Galois *iff* K is the splitting field for a separable polynomial in $F[x]$.
Proof: Let $\{w_1, \ldots, w_n\}$ be an F-basis of K. Let $p_i(x)$ be a minimal polynomial for w_i over F. Let $g(x) = \mathrm{lcm}(p_i(x))$. Then since each $p_i(x)$ is separable, so is $g(x)$. Since each $p_i(x)$ splits in K, so does $g(x)$. Since $K = F(w_1, \ldots, w_n)$, K is a splitting field for $g(x)$ over F.

9) zero!
10) *distinct* α_i

Theorem: Let K/F be a finite extension. Then K/F is Galois *iff* it is normal and separable.
Proof: Forwards: Galois $\longrightarrow$ normal, done.
If $\alpha \in K$, then its minimal polynomial $p(x) \in F[x]$ is separable, so K/F is separable.
Backwards: Follows immediately from previous theorem. $\square$

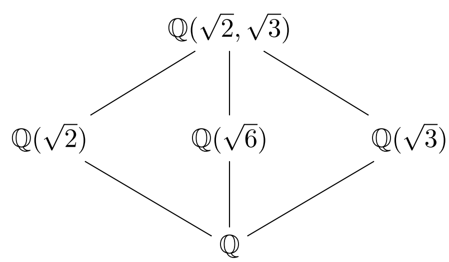
Theorem: (The Fundamental Theorem of Galois Theory).
Let K/F be a finite Galois extension, $G = \mathrm{Gal}(K/F)$. Then there is a bijection between subgroups of G and F-subfields of K given by:

$$E \longmapsto \{\sigma \in G \text{ such that } \sigma(\alpha) = \alpha \text{ for all } \alpha \in E\}$$
$$\left\{\begin{matrix}\alpha \in E \text{ such that} \\ \sigma(\alpha)=\alpha \\ \text{for all } \sigma \in H\end{matrix}\right\} \longleftarrow H$$

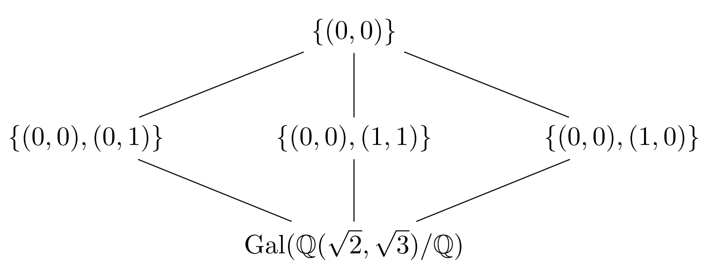
Moreover, if E_1, $E_2 \longleftrightarrow H_1$, H_2, then:

F-subfields of K		Subgroups of G
$E_2 \subset E_1$	$\longleftrightarrow$	$H_1 \subset H_2$
$[K : F]$	$=$	$\#H$
$[E : F]$	$=$	$\lvert G : H\rvert$
$\mathrm{Gal}(K/E) = \mathrm{Aut}_E K$	$\cong$	H
$\mathrm{Hom}_F(E, K)$[11]	$\cong$	G/H[12]
$\left\{\begin{matrix}E/F \text{ is Galois} \\ \mathrm{Gal}(E/F)\end{matrix}\right.$	$\overset{\textit{iff}}{\longleftrightarrow}$	$\left.\begin{matrix}H \text{ is normal in } G \\ G/H\end{matrix}\right\}$
$E_1 \cap E_2$	$\longleftrightarrow$	$H_1 H_2$
$E_1 E_2$	$\longleftrightarrow$	$H_1 \cap H_2$

Example: $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
The Fundamental Theorem says that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has five $\mathbb{Q}$-subfields.



$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{(0,0), (0,1), (1,0), (1,1)\}$$



PMATH 442 Lecture 11: October 5, 2011

Theorem: (FTGT)

---

[11] pointed set
[12] pointed set

Let K/F be a Galois extension, $G = \mathrm{Gal}(K/F)$. Then there is a bijection

$$\left\{\begin{smallmatrix}F\text{-subfields}\\ E \text{ of } K\end{smallmatrix}\right\} \longleftrightarrow \left\{\begin{smallmatrix}\text{Subgroups}\\ H \text{ of } G\end{smallmatrix}\right\}$$

$$E \longmapsto \left\{\begin{smallmatrix}\sigma \in G \text{ such that}\\ \sigma(\alpha)=\alpha \quad \forall \alpha\in E\end{smallmatrix}\right\}$$

$$\left\{\begin{smallmatrix}\alpha \in K \text{ such that}\\ \sigma(\alpha) = \alpha \text{ for}\\ \text{all } \sigma \in H\end{smallmatrix}\right\} \longleftarrow H$$

F-fields		Subgroups
$E_1 \subset E_2$	$\longleftrightarrow$	$H_2 \subset H_1$
$[K : E]$	$=$	$\#H$
$[E : F]$	$=$	$\#G/H = \lvert G : H\rvert$
$\mathrm{Gal}(K/E) = \mathrm{Aut}_E(K)$	$=$	H
$\mathrm{Hom}_F(E, K)$	$\cong$	G/H
E/F Galois	$\longleftrightarrow$	H is normal
(in the case $\mathrm{Gal}(E/F)$	$\cong$	G/H)
$E_1 \cap E_2$	$\longleftrightarrow$	H_1H_2
E_1E_2	$\longleftrightarrow$	$H_1 \cap H_2$

Proof: We will show that if H_1 and H_2 are subgroups of G with the same fixed field E, then $H_1 = H_2$. Then E is also the fixed field of H_1H_2, so

$$[K : E] = \#H_1 = \#H_2 = \#H_1H_2$$

so $H_1 = H_2$.

Now let $E \subset K$ be any F-subfield. Then $[K : E] = \#\,\mathrm{Gal}(K/E)$ because K/E is Galois.
But $\mathrm{Gal}(K/E)$ is a subgroup of G, so:

(1) $E \subset$ fixed field of $\mathrm{Gal}(K/E)$

and (2) $[K : \text{fixed field}] = [K : E]$

so E is the fixed field of $\mathrm{Gal}(K/E)$.

So the given correspondence is a bijection, as desired.

The inclusion-reversing property is clear.

We already proved $[K : E] = \#H$. KLM and $\#H(\#G/H) = \#G$ suffice to show $[E : F] = \#G/H$. We already showed $\mathrm{Gal}(K/E)$ is equal to H.

We will now show that $\mathrm{Hom}_F(E, K) \cong G/H$ as pointed sets.

Definition: A pointed set is an ordered pair (S, x) where $x \in S$.

Definition: Let F be a field, A_1, A_2 F-algebras. Then

$$\mathrm{Hom}_F(A_1, A_2) = \left\{\begin{smallmatrix}F\text{-algebra homomorphism}\\ \phi\colon A_1 \to A_2\end{smallmatrix}\right\}$$

Remarks: $\mathrm{Hom}_F(A_1, A_2)$ is, in general, just a set. If $A_1 \subset A_2$, then $\mathrm{Hom}_F(A_1, A_2)$ is a pointed set, with distinguished element $i\colon A_1 \hookrightarrow A_2$ the inclusion.

Define $\phi\colon G \to \mathrm{Hom}_F(E, K)$ by $\phi(\sigma) = \sigma|_E$[13)]
This maps the distinguished element of G (namely id) to that of $\mathrm{Hom}_F(E, K)$ (namely inclusion $E \hookrightarrow K$).

We know ϕ is onto because we proved that if K/E is Galois, then homomorphisms from $E \to K$ always extend to all of K.
If $\phi(\sigma_1) = \phi(\sigma_2)$, then $\sigma_1|_E = \sigma_2|_E$, so $\sigma_1\sigma_2^{-1}|_E = \mathrm{id}_E$. This implies that $\sigma_1\sigma_2^{-1} \in H = \mathrm{Gal}(K/E)$, so for any $f \in \mathrm{Hom}_F(E, K)$ the set

$$\{\, \sigma \in G : \phi(\alpha) = f \,\}$$

[13)] the restriction of σ to E

is a left coset of H. So we've shown that $G/H \cong \mathrm{Hom}_F(E, K)$ as pointed sets.
We have the following lemma:
Lemma: Say K/F is normal, $F \subset E \subset K$ fields. Then E/F is normal *iff* $\operatorname{im}\phi = E$ for all homomorphisms $\phi\colon E \to K$.

PMATH 442 Lecture 12: October 7, 2011

Office hours Tuesday Oct. 11 moved to 3:30–4:30.

Lemma: Let K/F be a finite normal field extension. E an F-subfield of K. Then E/F is normal *iff* $\operatorname{im}\phi = E$ for all F-homomorphisms $\phi\colon E \to K$.
Proof of lemma: Write $E = F(\alpha_1, \ldots, \alpha_n)$.
Forwards: Assume E/F normal. Then we can choose the α_is so that $p(x) = (x - \alpha_1)\cdots(x - \alpha_n)$ is in $F[x]$. For each i, $\phi(\alpha_i)$ is a root of $p(x)$, so since ϕ is injective, it permutes the roots of $p(x)$, so:

$$\begin{aligned} \operatorname{im}\phi = \phi(E) &= F(\phi(\alpha_1), \ldots, \phi(\alpha_n)) \\ &= F(\alpha_1, \ldots, \alpha_n) \\ &= E \end{aligned}$$

Backwards: Assume that E/F is not normal. Then there is an irreducible $p(x) \in F[x]$ such that $p(x)$ has a root $\alpha \in E$, but $p(x)$ does not split in E. Since $p(x)$ splits in K, there is a root β of $p(x)$ with $\beta \in K$. Since K/F is normal, and since $p(x)$ splits in K, we can extend the isomorphism $F(\alpha) \cong F(\beta)$ to a homomorphism $\psi\colon K \to K$. Let $\phi = \psi|_E$. Then $\phi(\alpha) = \beta \notin E$, so $\operatorname{im}\phi \not\supset E$. □

We now return to our quest to show that E/F is Galois *iff* H is a normal subgroup of G.

The lemma implies that E/F is Galois *iff* $\mathrm{Hom}_F(E, K) \cong \mathrm{Aut}_F(E)$ as pointed sets.

Let $\sigma \in \mathrm{Aut}_F(E)$. The subgroup of G fixing $\sigma(E)$ is $\sigma H \sigma^{-1}$. So $\sigma(E) = E$ for all $\sigma \in G$ *iff* $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$. So E/F is Galois *iff* H is normal in G.

In that case, the map $\psi\colon G \to \mathrm{Gal}(E/F)$, $\psi(\sigma) = \sigma|_E$, is an onto homomorphism $\ker\psi = H$, so induces an isomorphism $G/H \to \mathrm{Gal}(E/F)$.

We just need to show $E_1 \cap E_2$ corresponds to H_1H_2, and that E_1E_2 corresponds to $H_1 \cap H_2$.

If $\sigma \in H_1H_2$, then certainly σ fixes $E_1 \cap E_2$. Conversely, let E be the fixed field of H_1H_2. Then $E_1 \cap E_2 \subset E$, and since H_1H_2 is the smallest subgroup of G containing H_1 & H_2, it follows that E is the largest F-subfield of K contained in E_1 and E_2. But $E_1 \cap E_2$ is the largest F-subfield of K contained in E_1 & E_2, so $E = E_1 \cap E_2$.

Similarly, E_1E_2 is the smallest F-subfield of K containing E_1 & E_2 so it corresponds to the largest subgroup of G contained in H_1 & H_2, namely $H_1 \cap H_2$. □

Example: $\mathbb{Q}(\sqrt[3]{2}, \gamma) = K$, $\gamma = e^{2\pi i/3}$. What is $\mathrm{Gal}(K/\mathbb{Q})$, and what are the $\mathbb{Q}$-subfields of K?

$\mathrm{Gal}(K/\mathbb{Q})$: ϕ	$\phi(\sqrt[3]{2})$	$\phi(\gamma)$
id	$\sqrt[3]{2}$	γ
	$\gamma\sqrt[3]{2}$	γ
	$\gamma^2\sqrt[3]{2}$	γ
	$\sqrt[3]{2}$	γ^2
	$\gamma\sqrt[3]{2}$	γ^2
	$\gamma^2\sqrt[3]{2}$	γ^2

Since ϕ is determined by $\phi(\sqrt[3]{2})$ and $\phi(\gamma)$, and since $[K : \mathbb{Q}] = 6$, we know these six rows are all represented by elements of $\mathrm{Gal}(K/\mathbb{Q})$.

PMATH 442 Lecture 13: October 12, 2011

$\mathbb{Q}(\sqrt[3]{2}, \gamma)/\mathbb{Q}$, $\gamma = e^{2\pi i/3}$
$S = \{\underset{a}{\sqrt[3]{2}}, \underset{b}{\gamma\sqrt[3]{2}}, \underset{c}{\gamma^2\sqrt[3]{2}}\}$

$G = \text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \gamma)/\mathbb{Q})$
G acts on S by permutations, and this action is an isomorphism of G with S_3.

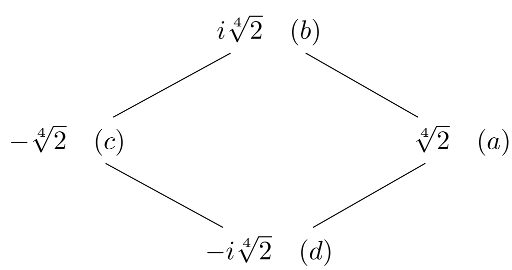
Subgroups of G	$\mathbb{Q}$-subfield
$\{1\}$	$\mathbb{Q}(\sqrt[3]{2}, \gamma)$
$\{1, (ab)\}$	$\mathbb{Q}(\gamma^2 \sqrt[3]{2})$
$\{1, (ac)\}$	$\mathbb{Q}(\gamma \sqrt[3]{2})$
$\{1, (bc)\}$	$\mathbb{Q}(\sqrt[3]{2})$
$\{1, (abc), (acb)\}$	$\mathbb{Q}(\gamma)$
G	$\mathbb{Q}$

Example: Compute the Galois group of $x^4 - 2$.
Solution: The splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$ which has degree 8 over $\mathbb{Q}$.

Any $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt[4]{2}, i)$ takes $i \mapsto \pm i$ and $\sqrt[4]{2}$ to $\pm\sqrt[4]{2}$ or $\pm i\sqrt[4]{2}$, and any $\mathbb{Q}$-automorphism is completely determined by its action on $\sqrt[4]{2}$ and i. This gives at most 8 automorphisms, so since $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ is Galois of degree 8, they are *all* realised by actual automorphisms.

Let $G = \text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$. Then G acts on $S = \{\underset{a}{\sqrt[4]{2}}, \underset{b}{i\sqrt[4]{2}}, \underset{c}{-\sqrt[4]{2}}, \underset{d}{-i\sqrt[4]{2}}\}$ by permutations. So there is a homomorphism $\psi\colon G \to S_4$ which is injective because if $\sigma \in \ker\psi$ then $\sigma(i) = i$ & $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$. The homomorphism ψ is given by:

$\mathbb{Q}$-Automorphism	Permutation of S
$(i, \sqrt[4]{2})$	1
$(-i, \sqrt[4]{2})$	(bd)
$(i, i\sqrt[4]{2})$	$(abcd)$
$(-i, i\sqrt[4]{2})$	$(ab)(cd)$
$(i, -\sqrt[4]{2})$	$(ac)(bd)$
$(-i, -\sqrt[4]{2})$	(ac)
$(i, -i\sqrt[4]{2})$	$(adcb)$
$(-i, -i\sqrt[4]{2})$	$(ad)(bc)$



Note that every permutation in $\psi(G)$ preserves this square, so $G \overset{\psi}{\hookrightarrow} D_4$. But $\#G = \#D_4 = 8$, so in fact ψ induces an isomorphism of G with D_4.

One can, as in the previous case, use this to find all the $\mathbb{Q}$-subfields of $\mathbb{Q}(\sqrt[4]{2}, i)$.

Theorem: Let K be the splitting field of a separable polynomial $f(x)$ over a field F. Then $\text{Gal}(K/F)$ acts transitively on the roots of $f(x)$ if $f(x)$ is irreducible.
Proof: Let $\alpha \in K$ be a root of $f(x)$. Define:

$$p(x) = \prod_{\substack{\sigma \in G \\ \text{distinct } \sigma(x)}} (x - \sigma(x))$$

Then the coefficients of $p(x)$ lie in the fixed field of G since $p(x)$ is fixed by G. So $p(x) \in F[x]$. But $p(x) = 0$, so $f(x) \mid p(x)$. However, since $p(x)$ is separable and every root of $p(x)$ is a root of $f(x)$, we get $p(x) \mid f(x)$. So $p(x) = cf(x)$ for some $c \in F$. Since G acts transitively on the roots of $p(x)$, it acts transitively on the roots of $f(x)$. $\square$

PMATH 442 Lecture 14: October 14, 2011

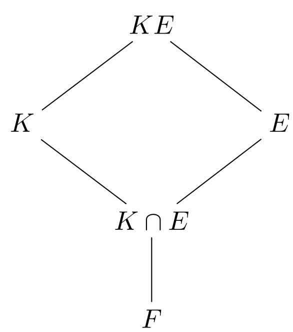
Galois Theory of Finite Fields
Say F is a finite field. Then F has p^n elements for some prime p and integer $n \geq 1$. We write $F = \mathbb{F}_{p^n}$. A finite extension of F is also a finite field, with p^{kn} elements for some integer $k \geq 1$. Let $E = \mathbb{F}_{p^{kn}}$. Then

$$[E : F] = [\mathbb{F}_{p^{kn}} : \mathbb{F}_{p^n}] = k$$

Consider $\text{Frob}_p \colon \begin{matrix} \mathbb{F}_{p^{kn}} \to \mathbb{F}_{p^{kn}} \\ E \to E \end{matrix}$.
It's an isomorphism, with fixed field $\mathbb{F}_p$. In general, Frob_p only fixes $\mathbb{F}_{p^n}$ is $n = 1$, so Frob_p is *not* in $\text{Aut}_F(E)$. However, $\alpha^{p^n} = \alpha$ *iff* $\alpha \in F = \mathbb{F}_{p^n}$, so $\mathbb{F}_{p^n}$ is the fixed field of $(\text{Frob}_p)^n$, the n-fold composition of Frob_p with itself.

So let $\pi = (\text{Frob}_p)^n$. Then for each $a \in \{1, \ldots, k\}$, the a-fold composition π^a is an automorphism of $\mathbb{F}_{p^{kn}} = E$ whose fixed field is $\mathbb{F}_{p^{an}} \cap E = \mathbb{F}_{p^{gn}}$ where $g = \gcd(a, k)$. So π is an F-automorphism of E of order k. So E/F is Galois with $\text{Gal}(E/F) = \{1, \pi, \ldots, \pi^{k-1}\} \cong \mathbb{Z}/k\mathbb{Z}$.

Theorem: Say K/F is a finite Galois extension, E/F any finite extension.



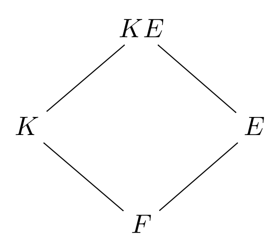
Then KE/E is Galois, and

$$\text{Gal}(KE/E) \cong \text{Gal}(K/K \cap E) \text{ and } [KE : F] = \frac{[K : F][E : F]}{K \cap E : F}.$$

Proof: First, note that the formula follows formally from the isomorphism of Galois groups:

$$\begin{aligned} [KE : F] &= [E : F][KE : E] \\ &= [E : F][K : K \cap E] \\ &= [E : F]\frac{[K : F]}{[K \cap E : F]} \end{aligned}$$

It therefore suffices to prove the theorem for $F = K \cap E$.

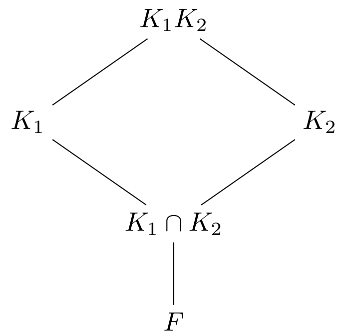


K is the splitting field for some separable polynomial $p(x) \in F[x]$. So KE is the splitting field for $p(x) \in E[x]$ over E, and therefore KE/E is Galois.

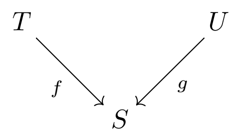
Define $\psi \colon \text{Gal}(KE/E) \to \text{Gal}(K/F)$ by $\psi(\sigma) = \sigma|_K$, which is well defined because K/F is Galois, so $\text{im}(\sigma|_K) = K$. ψ is a homomorphism. If $\sigma \in \ker \psi$, then $\sigma|_K = \text{id}$. Since $\sigma \in \text{Gal}(KE/E)$, $\sigma|_E = \text{id}$ too, so $\sigma_{KE} = \text{id}$. So ψ is injective.

Consider $\operatorname{im}\psi$. Its fixed field is, say, L. Then $L \subset K$, and every element of $\operatorname{Gal}(KE/E)$ fixes L, so $L \subset E$. But $F \subset L$, so $L = K \cap E = F$. Therefore $\operatorname{im}\psi = \operatorname{Gal}(K/F)$, and ψ is onto. ☐

Theorem: Say K_1K_2 are Galois extensions of F. Then $K_1 \cap K_2$ and K_1K_2 are Galois over F, and $\operatorname{Gal}(K_1K_2/F)$ is isomorphic to the fibre product of $\operatorname{Gal}(K_1/F)$ and $\operatorname{Gal}(K_2/F)$ over $\operatorname{Gal}(K_1 \cap K_2/F)$.



Definition: Let S, T, U be sets, with functions



The fibre product of T and U over S is:

$$T \times_S U = \{\, (t,u) \in T \times U : f(t) = g(u) \,\}$$

PMATH 442 Lecture 15: October 17, 2011

Definition: Let $\phi\colon G \to \operatorname{Sym}(S)$ be a group action of G on a set S. Then ϕ is transitive *iff* for every a, $b \in S$, there is a $g \in G$ such that $[\phi(g)](a) = b$.

Theorem: Let K_1, K_2 be Galois extensions of F. Then $K_1 \cap K_2$ and K_1K_2 are Galois extensions of F, and

$$\operatorname{Gal}(K_1K_2/F) \cong \operatorname{Gal}(K_1/F) \times_{\operatorname{Gal}(K_1\cap K_2/F)} \operatorname{Gal}(K_2/F) = \left\{ (\sigma,\tau) : \substack{\sigma\in\operatorname{Gal}(K_1/F) \\ \tau\in\operatorname{Gal}(K_2/F)} \quad \sigma|_{K_1\cap K_2} = \tau|_{K_1\cap K_2} \right\}$$

Proof: $K_1 \cap K_2$ is Galois over F because it's contained in K, (& so is separable) and if $p(x) \in F[x]$ is irreducible & has a root in K_i, then by normality of K_i/F it splits into linear factors in $K_i[x]$, and hence in $(K_1 \cap K_2)[x]$. So $K_1 \cap K_2/F$ is normal.

K_1K_2/F is Galois because it's a splitting field for $\operatorname{lcm}(f_1, f_2)$ over F, where K_i is a splitting field for $f_i(x)$ over F.

Define $\psi\colon \operatorname{Gal}(K_1K_2/F) \to G$ by $\psi(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2})$. It's clearly a homomorphism, and its image clearly lives in G because $(\sigma|_{K_1})|_{K_2} = (\sigma|_{K_2})|_{K_1}$. It's also injective because σ is determined by its values on K_1 & K_2.

$$\begin{aligned}
\#\operatorname{Gal}(K_1K_2/F) &= \frac{[K_1 : F][K_2 : F]}{[K_1 \cap K_2 : F]} \\
&= \frac{\#\operatorname{Gal}(K_1/F)\#\operatorname{Gal}(K_2/F)}{\#\operatorname{Gal}(K_1 \cap K_2/F)} \\
&= \#\operatorname{Gal}(K_1/F)\#\operatorname{Gal}(K_2/K_1 \cap K_2) \\
&= \#G
\end{aligned}$$

because there are $[K_2 : K_1 \cap K_2]$ ways to extend $\sigma|_{K_1\cap K_2}$ to K_2.

Therefore ψ is surjective and hence an isomorphism. $\square$

In particular, if $K_1 \cap K_2 = F$, then

$$\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$$

Definition: Let K/F be a separable extension, and let L/F be a Galois extension containing K/F. The Galois closure of K in L is the intersection of all Galois extensions of F that contain K/F & are contained in L.

Note: The Galois closure of K is a Galois extension of F.

Other notes: Say K/F is finite & separable. Then $K = F(\alpha_1, \dots, \alpha_n)$, so a splitting field for the lcm of the minimal polynomials over F of the α_is is a Galois extension of F containing K. In fact, this field is a Galois closure of K over F. Any Galois closure of K is isomorphic to this one.

$$\begin{gathered}
\mathbb{F}_{25} \cong \mathbb{F}_5(\sqrt{2}) \\
(2\sqrt{2})^2 = (3\sqrt{2})^2 = -2 \\
(\sqrt{a})(\sqrt{b}) \neq \sqrt{ab} \\
1 = 1 \\
\implies 1 \cdot 1 = (-1)(-1) \\
\left.\begin{aligned}\implies \sqrt{1 \cdot 1} = \sqrt{(-1)(-1)} \\ \implies \sqrt{1}\sqrt{1} = \sqrt{-1}\sqrt{-1}\end{aligned}\right\} \text{WRONG!} \\
\implies 1 = -1
\end{gathered}$$

PMATH 442 Lecture 16: October 19, 2011

Theorem: (Primitive Element) Let K/F be a finite, separable field extension. Then $K = F(\alpha)$ for some $\alpha \in K$.

Proof: First, note that is enough to show that $K = F(\alpha)$ *iff* K/F has finitely many subextensions. To see this, assume we had proven that $K = F(\alpha)$ *iff* K has finitely many F-subfields. Then since K/F is separable, there is a Galois extension L/F with $K \subset L$. By the Fundamental Theorem, L has only finitely many F-subfields, so K also has only finitely many F-subfields. By our presumed fact, $K = F(\alpha)$ for some $\alpha \in K$.

Forwards: Assume $K = F(\alpha)$, and let $E \subset K$ be an F-subfield. Let $p(x) \in F[x]$ be the monic minimal polynomial for α/F. Let $p(x) = p_1(x) \cdots p_n(x)$ be a factorization of $p(x)$ into monic irreducibles in $E[x]$. Let E' be the F-field generated by the coefficients of the $p_i(x)$. Note that $K = E(\alpha) = E'(\alpha)$ and α has the same minimal polynomial over E and E', so $[K : E] = [K : E']$, and hence $E = E'$ (since $E' \subset E$).

Backwards: Assume K has only finitely many F-subfields.

Case I: F is infinite. Then it is enough to show that for any α, β in K, $F(\alpha, \beta) = F(\gamma)$ for some $\gamma \in K$. Since F is infinite, and since K has only finitely many F-subfields there exist $c_1, c_2 \in F$ such that $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$ & $c_1 \neq c_2$.

$$\begin{gathered}
\text{Then } \beta = \frac{(\alpha + c_1\beta) - (\alpha + c_2\beta)}{c_1 - c_2} \in F(\alpha + c_1\beta) \\
\text{and } \alpha = (\alpha + c_1\beta) - c_1\beta \in F(\alpha + c_1\beta)
\end{gathered}$$

so we may take $\gamma = \alpha + c_1\beta$.

Case II: F finite, so K finite. By the classification of finite abelian groups, $K^* = K \setminus \{0\} \cong (\mathbb{Z}/n\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n\mathbb{Z})$ with $n_i \mid n_{i+1}$ for all $i < r$. If $r \geq 2$, then there are at least n_1^2 elements of K^* with order dividing n_1. This corresponds to at least n_1^2 different roots of $x^{n_1} - 1$. This is a problem if $n_1 > 1$, so we deduce that $r = 1$ & K^* is cyclic.

So $K = F(\alpha)$ where α is a generator of the cyclic group K^*. $\square$

Let's compute $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

$$\zeta_n = \text{primitive } n\text{th root of unity}$$

$$
\begin{aligned}
\text{Well, } [\mathbb{Q}(\zeta_n) : \mathbb{Q}] &= \phi(n) \\
&= \#(\mathbb{Z}/n\mathbb{Z})^* \\
&= \#\{\, a \in \{1, \dots, n\} : \gcd(a, n) = 1 \,\}
\end{aligned}
$$

We will find $\phi(n)$ automorphisms of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, which will imply that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois.

Let $\zeta_n(x) = n$th cyclotomic polynomial. The roots of $\zeta_n(x)$ are the primitive nth roots of unity. They are all powers of ζ_n, so $\mathbb{Q}(\zeta_n)$ is the splitting field for $\zeta_n(x)$ over $\mathbb{Q}$, and so $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois.

Claim: $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$

$$
\begin{aligned}
\text{via } \sigma \overset{\psi}{\mapsto} & \frac{\log \sigma(\zeta_n)}{\log \zeta_n} \\
&= a, \text{ where } \sigma(\zeta_n) = \zeta_n^a
\end{aligned}
$$

Proof of claim: It is easy to check that ψ is a homomorphism. If $\psi(\sigma) = 1$, then $\sigma(\zeta_n) = \zeta_n \implies \sigma = \mathrm{id}$, so ψ is 1–1. Since $\#\,\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \#(\mathbb{Z}/n\mathbb{Z})^* = \phi(n)$, we see that ψ is onto. □ claim

PMATH 442 Lecture 17: October 21, 2011

Computing Galois Groups

Given a polynomial $f(x) \in F[x]$, find the Galois group of a splitting field for $f(x)$ over $F[x]$. Assume $f(x)$ is separable.

If $F = \mathbb{F}_q$ and $f(x)$ is irreducible, then splitting field is $\mathbb{F}_{q^d}$, where $d = \deg(f)$, so $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) \cong \mathbb{Z}/d\mathbb{Z}$.

If $F = \mathbb{Q}$, the problem is much, much harder, in general.
Say $\deg(f(x)) = 2$, $f(x)$ irreducible. Then a splitting field has degree $\le 2!$, so it has degree 2. Therefore its Galois group is $\mathbb{Z}/2\mathbb{Z}$.
Now say $\deg(f(x)) = 3$, f irreducible. Let K be the splitting field for $f(x)$ over $\mathbb{Q}$. Then $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the three roots of $f(x)$, giving a homomorphism $\psi\colon \mathrm{Gal}(K/\mathbb{Q}) \to S_3$. Moreover, ψ is 1–1 because ψ is completely determined by its values on the roots of $f(x)$. The transitive subgroups of S_3 are:

A_3 (cyclic of order 3)
S_3

Let F be a field, and let $K = F(a_1, \dots, a_n)$ for indeterminates a_i. S_n acts on K by permuting the a_i.
Let $M =$ fixed field of S_n. Then $[K : M] = n! = \#S_n$.
Consider $f(x) = (x - a_1) \cdots (x - a_n)$. The coefficients of $f(x)$ all lie in M. They are:

$$
s_i = \text{sum of all products of } i \text{ dinstinct } a_i\text{s},
$$

up to multiplication by ± 1. The polynomial s_i is called the ith elementary symmetric polynomial.

Now, K is a splitting field for $f(x)$ over M, and also K is a splitting field for $f(x)$ over $F(s_1, \dots, s_n) \subset M$. By comparing degrees, we see that $M = F(s_1, \dots, s_n)$.

This action of S_n descends to $F[a_1, \dots, a_n]$. If E/F is a splitting field for a separable polynomial $p(x) \in F[x]$, then we get a homomorphism

$$
\begin{aligned}
\psi\colon\ & \mathrm{Gal}(E/F) \to \mathrm{Gal}(K/M) \\
& \sigma \mapsto \text{permutation corresponding to action of } \sigma \text{ on roots of } p(x)\text{, ordered.}
\end{aligned}
$$

ψ is injective because σ is determined by its values on the roots of $p(x)$, so we can pretend $\mathrm{Gal}(E/F)$ is a subgroup of $\mathrm{Gal}(K/M)$.

A_n is a normal subgroup of S_n, of index 2. Its fixed field is therefore a quadratic extension of M. What is this fixed field?

Definition: Let R be a ring, $r_1, \ldots, r_n$ elements of R. The discriminant of $r_1, \ldots, r_n$ is:

$$\mathrm{Disc}(r_1, \ldots, r_n) = \prod_{i<j} (r_i - r_j)^2$$

This is symmetric in $r_1, \ldots, r_n$. The fixed field of A_n in K is $M(\sqrt{\mathrm{Disc}(a_1, \ldots, a_n)})$. So $\mathrm{Gal}(E/F)$ fixes $F(\sqrt{\mathrm{Disc}(\alpha_1, \ldots, \alpha_n)})$ *iff* $\psi(\mathrm{Gal}(E/F)) \subset A_n$. This happens *iff* $\sqrt{\mathrm{Disc}(\alpha_1, \ldots, \alpha_n)} \in F$.

PMATH 442 Lecture 18: October 26, 2011

Assume that $2 \neq 0$.

$$\begin{array}{c} F(a_1, \ldots, a_n) \\ \Big| \;{\scriptstyle \mathrm{Gal}=G\cong S_n} \\ F(s_1, \ldots, s_n) \end{array}$$

$s_i = i$th elementary symmetric polynomial in a_is.
This is the splitting field for

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

If E/F is Galois, then $\mathrm{Gal}(E/F)$ embeds in $\mathrm{Gal}(F(a_1, \ldots, a_n)/F(s_1, \ldots, s_n)) \cong S_n$ by numbering the roots $\alpha_1, \ldots, \alpha_n$ of $p(x)$ over F.

$$\begin{aligned} \text{Define } D(f(x)) &= \prod_{i<j} (a_i - a_j)^2 \\ &\in F(s_1, \ldots, s_n) \end{aligned}$$

$F(s_1, \ldots, s_n, \sqrt{D})$ is the fixed field of A_n.

Definition: Let $p(x) \in F[x]$ be any polynomial $p(x) = t_n \prod_{i=1}^{n} (x - \alpha_i)$. The discriminant of $p(x)$ is

$$\mathrm{Disc}(p(x)) = t_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

Notice that this corresponds to $D(f(x))$ if $p(x)$ is monic.

So $F(\sqrt{D})$ is the fixed field of $\mathrm{Gal}(E/F) \cap A_n$, where we view $\mathrm{Gal}(E/F)$ as a subgroup of S_n using the correspondence described earlier (permutation action on the roots of $p(x)$).

Say $p(x)$ has degree 3, E/F a splitting field. Assume $3 \neq 0$. Then $\mathrm{Gal}(E/F)$ is either isomorphic to A_3 or to S_3. So $\mathrm{Gal}(E/F) \cong A_3$ *iff* $F = F(\sqrt{D})$ *iff* D is a square in F.

How can we compute D without knowing the roots of $p(x)$?

Definition: Let $f(x)$, $g(x)$ be polynomials in $F[x]$ for some field F, with $f(x) = t_n x^n + \cdots + t_0$, $g(x) = u_m x^m + \cdots + u_0$. The resultant of f and g is:

$$\mathrm{Res}(f, g) = \det \begin{pmatrix} t_n & t_{n-1} & \cdots & t_0 & & & \\ & t_n & t_{n-1} & \cdots & t_0 & & \\ & & \ddots & & & \ddots & \\ & & & t_n & t_{n-1} & \cdots & t_0 \\ u_m & \cdots & \cdots & \cdots & u_0 & & \\ & \ddots & & & & \ddots & \\ & & u_m & \cdots & \cdots & \cdots & u_0 \end{pmatrix} {}^{14)}$$

[14] m rows on top, n rows on bottom, main diagonal pointed out

$$\operatorname{Res}(x^2+x+1, x^3-2x+2) = \det \begin{pmatrix} 1 & 1 & 1 & & \\ & 1 & 1 & 1 & \\ & & 1 & 1 & 1 \\ 1 & 0 & -2 & 2 & \\ & 1 & 0 & -2 & 2 \end{pmatrix}$$

Claim: $\operatorname{Disc}(p(x)) = \frac{\operatorname{Res}(p,p')}{t_n}$

Theorem: Let $f(x) = t_n \prod_{i=1}^n (x-\alpha_i)$, $g(x) = u_m \prod_{i=1}^m (x-\beta_i)$ be polynomials in $F[x]$. Then:

$$\operatorname{Res}(f,g) = t_n^m u_m^n \prod_{i,j} (\alpha_i - \beta_j)$$

Proof: Write $\phi(x) = T_n \prod_i (x-a_i)$, $\psi(x) = U_m \prod_i (x-b_i)$, where all these a_is, b_is, T_n, U_m are indeterminants over F. It suffices to prove the theorem for ϕ & ψ.

Note that t_n divides all the coefficients of $\phi(x)$, and u_m divides all the coefficients u_i of $\psi(x)$, so

$$\operatorname{Res}(\phi,\psi) = t_n^m u_m^n (\text{sym poly in } a_i\text{s \& } b_i\text{s})$$

PMATH 442 Lecture 19: October 28, 2011

Let $f(x) = t_n x^n + \cdots + t_0$. Then

$$\operatorname{Disc}(f) = \frac{(-1)^{n(n-1)/2} \operatorname{Res}(f,f')}{t_n}$$

This is what we will prove, eventually.

Lemma:

$$f(x) = t_n \prod_{i=1}^n (x-\alpha_i)$$
$$g(x) = u_m \prod_{i=1}^m (x-\beta_i)$$

Then $\operatorname{Res}(f,g) = t_n^m u_m^n \prod_{i,j} (\alpha_i - \beta_j)$

Proof of lemma: We showed $\operatorname{Res}(f,g) = t_n^m u_m^n(\text{symmetric polynomial in } \alpha_i,\ \beta_j)$ by showing that

$$\phi(x) = T_n \prod (x-a_i)$$
$$\psi(x) = U_m \prod (x-b_i)$$

satisfy $\operatorname{Res}(\phi,\psi) = T_n^m U_m^n \cdot (\text{some polynomial symmetric in } a_i \text{ and } b_j)$

Next, we will show that $\operatorname{Res}(f,g) = 0$ *iff* $\gcd(f,g) \neq 1$. To see this, note that $\gcd(f,g) \neq 1$ *iff* there are polynomials $p(x)$, $q(x)$ of degrees at most $m-1$, $n-1$, respectively, such that $fp = gq$.

This is equivalent to saying that $\{f, xf, \ldots, x^{m-1}f, g, xg, \ldots, x^{n-1}g\}$ is linearly dependent. Writing this out in terms of the basis $\{1, x, \ldots, x^{n+m-1}\}$, we see that $\gcd(f,g) \neq 1$ *iff*

$$\det \begin{bmatrix} t_n & t_{n-1} & \ldots & t_0 & & \\ & t_n & \ldots\ldots\ldots & t_0 & & \\ & & \ddots & & \ddots & \\ & & & t_n & \ldots\ldots\ldots & t_0 \\ u_m & u_{m-1} & \ldots\ldots\ldots & u_0 & & \\ & \ddots & & & \ddots & \\ & & u_m & \ldots\ldots\ldots\ldots & & u_0 \end{bmatrix} = 0 = \operatorname{Res}(f,g)$$ [15]

[15] m rows, n rows

Therefore, $\mathrm{Res}(\phi, \psi) = CT_n^m U_m^n \prod_{i,j}(a_i - b_j)$ for some $C \in F$.

To find C, compute $\mathrm{Res}(x^n, x^m - 1)$.

$$= \det \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ 1 & & & -1 & & \\ & \ddots & & & \ddots & \\ & & 1 & \dots\dots\dots & & -1 \end{bmatrix} {}^{16)} = (-1)^n$$

$$\begin{aligned} \mathrm{Res}(x^n, x^m - 1) &= C \prod_{i=1}^{n} \prod_{j=1}^{m} (0 - \beta_j) \\ &= C \prod_{j=1}^{m} (-\beta_j)^n \\ &= C(-1)^{mn} \Big(\prod_{j=1}^{m} \beta_j \Big)^n \\ &= C(-1)^{mn} \big((-1)^{m+1} \big)^n \\ &= C(-1)^n \end{aligned}$$

$\implies C = 1$ ☐ lemma

$g(\alpha_i) = u_m \prod_j (\alpha_i - \beta_j)$

$$\begin{aligned} \implies \mathrm{Res}(f, g) &= t_n^m \prod_{i=1}^{n} g(\alpha_i) \\ &= (-1)^{nm} u_m^n \prod_{j=1}^{m} f(\beta_j) \end{aligned}$$

Now, $\mathrm{Disc}(f) = t_n^{2n-2} \prod_{i<j}(\alpha_i - \alpha_j)^2$, and $f'(\alpha_i) = \frac{\mathrm{d}}{\mathrm{d}x}\Big|_{x=\alpha_i} t_n \prod_{j=1}^{n}(x - \alpha_j) = \prod_{j \neq i}(\alpha_i - \alpha_j)$.

$$\begin{aligned} \text{So } \frac{\mathrm{Res}(f, f')}{t_n} &= t_n^{n-2} \prod_{i=1}^{n} f'(\alpha_i) \\ &= t_n^{n-2} t_n^n \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j) \\ &= (-1)^{n(n-1)/2 \, 17)} t_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{n(n-1)/2} \, \mathrm{Disc}(f, f') \end{aligned}$$

This proves the claim!

[16] m rows, n rows

[17] one factor of -1 for each pair (i, j), $i \neq j$

Example: $f(x) = x^2 + bx + c$

$$\begin{aligned}
\implies \operatorname{Disc}(f) &= -\operatorname{Res}(f, f') \\
&= -\operatorname{Res}(x^2 + bx + c, 2x + b) \\
&= -\det \begin{bmatrix} 1 & b & c \\ 2 & b & 0 \\ 0 & 2 & b \end{bmatrix} \\
&= -(b^2 + 4c - 2b^2) = b^2 - 4c
\end{aligned}$$

This looks familiar:

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

PMATH 442 Lecture 20: October 31, 2011

$$\operatorname{Disc}(f) = \frac{(-1)^{n(n-1)/2}\operatorname{Res}(f, f')}{\text{lead coeff. of } f} = \prod_{i \neq j} (\alpha_i - \alpha_j)^2 \text{[18)]}$$

If we add c to all the α_i, the product won't change. In other words, $\operatorname{Disc}(f(x)) = \operatorname{Disc}(f(x + c))$ for all constants c.

$\operatorname{Disc}(x^3 + ax^2 + bx + c)$
$a = -\alpha_1 - \alpha_2 - \alpha_3$
If we subtract $\frac{a}{3}$ from each α_i, their sum will become zero:

$$\begin{aligned}
(x - \tfrac{a}{3})^3 + a(x - \tfrac{a}{3})^2 + b(x - \tfrac{a}{3}) + c &= x^3 - \cancel{ax^2} + \tfrac{a^2}{3}x - \tfrac{a^3}{27} + \cancel{ax^2} - \tfrac{2a^2}{3}x + \tfrac{a^3}{9} + bx - \frac{ab}{3} + c \\
&= x^3 + (b - \frac{a^2}{3})x + (\tfrac{2a^3}{27} - \tfrac{ab}{3} + c)
\end{aligned}$$

This has the same discriminant & Galois group as our original polynomial, and roots that only differ by $\frac{a}{3}$ from the original roots.

So, we can calculate a "general" discriminant of degree 3 by:

$$\begin{aligned}
\operatorname{Disc}(x^3 + ax + b) &= (-1)^{3(3-1)/2}\operatorname{Res}(f, f') \\
&= -\operatorname{Res}(f, f') \\
&= -\det \begin{bmatrix} 1 & 0 & a & b & \\ & 1 & 0 & a & b \\ 3 & 0 & a & & \\ & 3 & 0 & a & \\ & & 3 & 0 & a \end{bmatrix} \\
&= -\det \begin{bmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 0 & 0 & -2a & -3b & 0 \\ 0 & 0 & 0 & -2a & -3b \\ 0 & 0 & 3 & 0 & a \end{bmatrix} \\
&= -(4a^3 + 27b^2)
\end{aligned}$$

$$= -4a^3 - 27b^2$$

18) α_i are roots of f, with multiplicity

Example: Compute the Galois group of $x^3 + 3x^2 + 3$, $x^3 + 3x^2 - 3$

$$\begin{aligned} &\rightsquigarrow (x-1)^3 + 3(x-1)^2 + 3 \\ &= x^3x - 1 - 6x + 3 + 3 \\ &= x^3 - 3x + 5 \\ \text{Disc} &= -4(-3)^3 - 27(5)^2 \\ &= 108 - 675 \\ &= -567 \end{aligned}$$

Not a square, so

Galois group $\cong S_3$

$$\begin{aligned} &\rightsquigarrow x^3 - 3x - 1 \\ \text{Disc} &= -4(-3)^3 - 27(-1)^2 \\ &= 108 - 27 \\ &= 81 \\ &= 9^2 \\ \implies &\text{Gal} \cong A_3 \end{aligned}$$

Q: What are the transitive subgroups of S_4? Possible orders:

~~1~~	~~2~~	~~3~~	4	~~6~~	8	12	24
			C_4		D_4	A_4	S_4
			$C_2 \times C_2$				

	In A_4?
C_4: group generated by 4-cycle	No
$C_2 \times C_2$: group of double-flips	Yes
D_4: generated by double flips & one 4-cycle	No
A_4: even permutations	Yes
S_4: all of 'em	No

Let G be a finite group, S a finite set on which G acts. Then:

$$\#G = \sum_{a \in S} (\# \text{ orbits of } a)(\text{stab}(a))$$

If S has 1 G-orbit, then $\#(\text{orbit}) \mid \#G$.

PMATH 442 Lecture 21: November 2, 2011

Question #6: Assume f & g are monic.
Tuesday November 8 4:30 MC 2065
Info session for Waterloo Math Grad School
Refreshments/Snacks

Galois Groups of degree 4 polynomials (irreducible):

	Disc a square?	Gal group of resolvent
$C_2 \times C_2$	Yes	$\{1\}$ (factors completely)
C_4	No	S_2 (linear · quadratic)
D_4	No	S_2 (linear · quadratic)
A_4	Yes	A_3 (irreducible)
S_4	No	S_3 (irreducible)

Resolvent cubic:
Let $\alpha_1, \ldots, \alpha_4$ be the roots of $f(x)$. Then $\text{Gal}(f(x))$ permutes the following three elements of the splitting field:

$$\begin{aligned} \theta_1 &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\ \theta_2 &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \\ \theta_3 &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) \end{aligned}$$

So $p(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3)$ has coefficients in the ground field F.

If $f(x) = x^4 + ax^3 + bx^2 + cx + d$, then its discriminant and resolvent cubic are heinous. Substituting $x = x - \frac{a}{4}$ will eliminate the x^3 term without changing the discriminant, galois group, or galois group & splitting behaviour of the resolvent cubic.

So we assume $a = 0$. In that case:

$$= 16b^4d - 4b^3c^2 - 128b^2d^2 + 144bc^2d - 27c^4 + 256d^3$$

& resolvent cubic is:

$$x^3 - 2bx^2 + (b^2 - 4d)x + c^2$$

Example: Find Galois group of $x^4 + 2x^2 - x + 3$ over $\mathbb{Q}$.
Solution: Disc = not a square
Resolvent cubic:

$$x^3 - 4x^2 - 8x + 1 \qquad \text{irreducible over } \mathbb{Q} \text{ (rational roots theorem)}$$

$\implies$ Gal $\cong S_4$.

Example: Same for $x^4 + 2x^2 + 4$.

Solution:

$$\begin{aligned}\text{Disc} &= 16 \cdot 2^4 \cdot 4 - 128 \cdot 2^2 \cdot 4^2 + 256 \cdot 4^3 \\ &= 2^{10} - 2^{13} + 2^{14} \\ &= 2^{10}(1 - 8 + 16) \\ &= 2^{10} \cdot 9 \\ &= (3 \cdot 2^5)^2\end{aligned}$$

Resolvent: $x^3 - 4x^2 - 12x = x(x-6)(x+2)$
Therefore Gal $\cong C_2 \times C_2$

Theorem: Let $f(x)$ be an irreducible polynomial in $\mathbb{Z}[x]$, primitive. Let $p \in \mathbb{Z}$ be a prime such that $f(x)$ is separable mod p, and p does not divide the leading coefficient of $f(x)$. If $f(x)$ factors mod p as $f(x) = m_1(x) \cdots m_r(x)$, $\deg(m_i) = d_i$, then Gal(f) over $\mathbb{Q}$ contains a permutation with cycle structure $(d_1) \cdots (d_r)$.

Example: Compute Gal$(x^4 + 5x^2 + 11)$.
Previous techniques $\implies$ C_4 or D_4.
Mod 2: $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ ╳
Mod 3: $x^4 - x^2 - 1 = (x^2 + 1)^2$ ╳
Mod 5: $x^4 + 1 = (x^2 + 2)(x^2 - 2)$ ╳

PMATH 442 Lecture 22: November 4, 2011

Compute Gal$(x^4 + 5x^2 + 11)$
Reduce mod 17:

$$x^4 + 5x^2 + 11 = (x+1)(x-1)(x^2+6)$$

$\implies$ Gal contains a permutation with cycle structure (1)(1)(2), and so cannot be C_4.

When can the roots of a polynomial in x be expressed in terms of $+, -, \cdot, \div, \sqrt[n]{\cdot}$, and the coefficients?

Theorem: Let F be a field that contains all the nth roots of unity. Let $a \in F$. Then $F(\sqrt[n]{a})/F$ is Galois, with cyclic Galois group, provided char $F \nmid n$.
Proof: First, we may assume that $[F(\sqrt[n]{a}) : F] = n$, since otherwise we may replace n with

$$k = \min_i \{ (\sqrt[n]{a})^i \in F \}$$

and we will have $k \mid n$.

Write $x^n - a = (x - \sqrt[n]{a})(x - \zeta\sqrt[n]{a}) \cdots (x - \zeta^{n-1}\sqrt[n]{a})$ where ζ is a primitive nth root of unity. Therefore, since $\zeta \in F$, $F(\sqrt[n]{a})$ is a splitting field for $x^n - a$ over F. Since char $F \nmid n = [F(\sqrt[n]{a}) : F]$, we see that $F(\sqrt[n]{a})/F$ is separable, so it's Galois.

Let $\sigma \in \mathrm{Gal}(F(\sqrt[n]{a})/F)$ be such that $\sigma(\sqrt[n]{a}) = \zeta\sqrt[n]{a}$. Since $\zeta \in F$, $\sigma(\zeta) = \zeta$, so $\sigma(\zeta^r\sqrt[n]{a}) = \zeta^{r+1}\sqrt[n]{a}$. Therefore σ has order n and $\mathrm{Gal}(F(\sqrt[n]{a})/F) = \langle\sigma\rangle$ is cyclic. □

Theorem: Let F be a field containing the nth roots of unity. Let K/F be a finite Galois extension with cyclic Galois group. Then $K = F(\sqrt[n]{a})$ for some $a \in F$, $n = [K : F]$.[19]
Proof: Say $\alpha \in K$, ζ a primitive nth root of unity. Define

$$(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)$$

where $\mathrm{Gal}(K/F) = \langle a\rangle$. Then

$$\sigma((\alpha,\zeta)) = \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^n(\alpha)$$
$$\zeta^{-1}(\alpha,\zeta) = \zeta^{-1}\alpha + \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-2}\sigma^{n-1}(\alpha)$$

Since $\zeta^{-1}\alpha = \zeta^{n-1}\sigma^n(\alpha)$, we see that $\sigma((\alpha,\zeta)) = \zeta^{-1}(\alpha,\zeta)$.
In particular, $\sigma((\alpha,\zeta)^n) = (\sigma,\zeta)^n$, so $(\alpha,\zeta)^n \in F$. Furthermore, if $1 \le k \le n-1$, then $\sigma^k((\alpha,\zeta)) = \zeta^{-k}(\alpha,\zeta) \ne (\alpha,\zeta)$, so (α,ζ) does not lie in any proper subfield of K. So we may set $a = (\alpha,\zeta)^n$ to get $K = F(\sqrt[n]{a})$. □

Theorem: Assume F contains the nth roots of unity, $a, b \in F^*$. Then $F(\sqrt[n]{a}) \cong F(\sqrt[n]{b})$ *iff* $\langle a\rangle \equiv \langle b\rangle \bmod (F^*)^n$, where

$$(F^*)^n = \{\, \alpha^n : \alpha \in F^* \,\}$$

(that is, $a^k = b^l\alpha^n$ for some $\alpha \in F$, $1 \le k, l \le n-1$.)

PMATH 442 Lecture 23: November 7, 2011

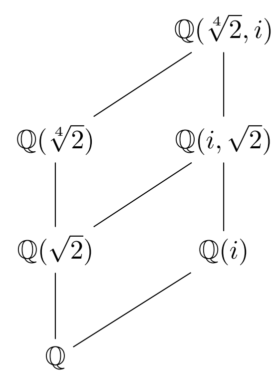
Definition: Let L/F be an extension, $\alpha \in L$ any element. Then α is solvable in radicals over F *iff* $\alpha \in K$ for some field K such that

$$F = K_0 = K_1 \subset K_2 \subset \cdots \subset K_n = K$$

where $K_i = K_{i-1}(\sqrt[r_i]{a_i})$ for some $a_i \in K_{i-1}$, and $r_i \in \mathbb{Z}_{>0}$, $\mathrm{char}\, F \nmid r_i$.

We say $p(x) \in F[x]$ non-constant is solvable in radicals *iff* all its roots are. We call an extension like K/F a solvable extension.

Theorem: Let $\alpha \in K$ be solvable in radicals over F. Then α is contained in a Galois solvable extension.
Proof: First, adjoin all the r_ith roots of unity to f;



this is an extension of solvable form. Next, notice that to compute the Galois closure of K over F, one need only adjoin elements of the form $\sqrt[r_i]{b_i}$ for some elements $b_i \in K_{i-1}$, although there may be several of them for each i. □

Definition: A group G is solvable *iff* there is a set of subgroups

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

[19] $\mathrm{char}\, F \nmid n$

such that G_{i-1} is a normal subgroup of G_i, with G_i/G_{i-1} an abelian group.

Say G is a group, $N \subset G$ a normal subgroup. Then G/N is abelian *iff* for all g, $h \in G$, we have $ghg^{-1}h^{-1} \in N$.

Definition: The commutator of g & h is $[g,h] = ghg^{-1}h^{-1}$. The commutator subgroup of G is the subgroup of G generated by the commutators of G. It's denoted $[G,G]$.
Notice that G/N is abelian *iff* $[G,G] \subset N$. Also notice that $[G,G]$ is a normal subgroup of G, because for any homomorphism f (like, say, conjugation by σ), $f(ghg^{-1}h^{-1}) = f(g)f(h)f(g)^{-1}f(h)^{-1} = [f(g), f(h)]$.

We can construct the commutator series of G:
$G^{(0)} = G$
$G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$
So $G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots$ and $G^{(i)}/G^{(i-1)}$ is abelian! If $G^{(n)} = \{1\}$ for some n, then G is solvable. Conversely, if G is finite, then if $G^{(n)} \neq \{1\}$ for all n, then G is not solvable.

Theorem: Let G be a finite solvable group. Then any subgroup or quotient group of G is also solvable.
Proof: Say H is a subgroup of G, and say $G_0 = \{1\} \subset G_1 \subset \cdots \subset G_n = G$ satisfy G_i/G_{i-1} abelian. Let $H_i = H \cap G_i$. Then H_i is a normal subgroup of H_{i+1} and $H_{i+1}/H_i \hookrightarrow G_{i+1}/G_i$, so H_{i+1}/H_i is abelian. Since $H_0 \subset G_0 = \{1\}$, we conclude that H is solvable.

Similarly, if N is a normal subgroup of G & $q\colon G \to G/N$ is the "reduce mod N" homomorphism, then the chain

$$q(G_0) \subset q(G_1) \subset \cdots \subset q(G_n)$$

shows that G/N is solvable. $\square$

PMATH 442 Lecture 24: November 9, 2011

Theorem: Let G be a group, N a normal subgroup. If N is solvable and G/N is solvable, then so is G.
Proof: G is solvable *iff* its commutator series $G^{(i)}$ satisfies $G^{(n)} = \{1\}$ for some n. Since $G^{(i)}$ mod $N = (G/N)^{(i)}$, we see that $G^{(n)} \subset N$ for some M (G/N is solvable). Since N is solvable, its subgroup $G^{(i)}$ is also solvable, so the groups $G^{(i)}$ satisfy $G^{(n)} = \{1\}$ for some n, as desired. $\square$
Theorem: Let F be a field of characteristic 0, $f(x) \in F[x]$ a non-constant polynomial. Then $f(x)$ is solvable in radicals *iff* $\mathrm{Gal}(f)$ over F is solvable.
Proof: Forwards: If $f(x)$ is solvable in radicals, then its splitting field admits subfields satisfying

$$F = K_0 \subset K_1 \subset \cdots \subset K_n = \text{splitting field}$$

and $K_i = K_{i-1}(\sqrt[n_i]{a_i})$. Moreover, we can insist that K_i/K_{i-1} is Galois for each i, by adjoining all relevant roots of unity first. This may make K_n larger than a splitting field for $f(x)$; this is OK & we'll consider it later.

So $\mathrm{Gal}(K_i/K_{i-1})$ is abelian for all i, making $\mathrm{Gal}(K_n/F)$ solvable. Since a splitting field K is contained in K_n, its Galois group over F is a quotient of $\mathrm{Gal}(K_n/F)$, and so is solvable.

Backwards: Let K/F be a splitting field for $f(x)$. Then since $\mathrm{Gal}(K/F)$ is solvable, we get a chain of subgroups $\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = \mathrm{Gal}(K/F)$ such that G_i/G_{i-1} is abelian. By refining this chain, we may assume that G_i/G_{i-1} is cyclic for all i. But if K_i corresponds to G_i, then G_i/G_{i-1} cyclic $\implies K_{i-1} = K_i(\sqrt[n_{i-1}]{a_{i-1}})$ for some $a_{i-1} \in K_{i-1}$, provided that K_i contains all (n_{i-1})th roots of unity. So if we adjoin a large finite number of roots of unity to F, then we can construct a chain of subfields of a suitable form to prove that $f(x)$ is solvable in radicals. $\square$

Question: Is every finite group solvable?
Answer: No. If $n \geq 5$, A_n has no nontrivial normal subgroups and is not abelian, and so is not solvable.

Furthermore, the only normal subgroups of S_n for $n \geq 5$ are $\{1\}$, A_n, and S_n. So if $n \geq 5$, then S_n isn't solvable.

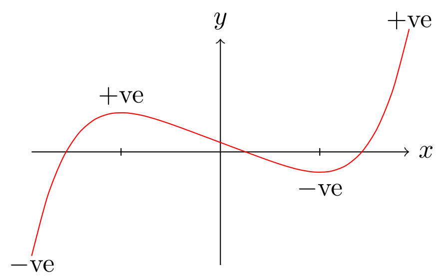
I'd like to thank my parents, God and L. Ron Hubbard.

$$S_3\colon \{1\} \subset \underset{\text{cyclic}}{A_3} \subset S_3 \text{ solvable } \checkmark$$

$$S_4\colon \{1\} \subset \underset{\substack{\text{double}\\\text{flips}}}{V_4} \subset A_4 \subset S_4$$

So S_4 is solvable too. But S_5 is *not* solvable.
Example: The Galois group of $x^5 - 15x + 5$ over $\mathbb{Q}$ is S_5.
Proof: The polynomial is irreducible by Eisenstein's Criterion using $p = 5$.

Since $x^5 - 15x + 5$ is irreducible of degree 5, its Galois group acts transitively on a 5-element set, so by orbit–stabilizer, the Galois group's order is divisible by 5. Let $G = \mathrm{Gal}(f(x)) = \mathrm{Gal}(x^5 - 15x + 5)$. By Cauchy's Theorem, G contains an element of order 5. So G must contain a 5-cycle.
$f'(x) = 5x^4 - 15$
Roots $x = \pm\sqrt[4]{3}$



We see that $f(x)$ has exactly 3 real roots. Therefore, the action of complex conjugation on the roots of $f(x)$ is as a transposition. So G contains a transposition.

A simple bubble sort shows that G must be all of S_5.

PMATH 442 Lecture 25: November 11, 2011

Definition: A valuation on a field K is a function $\phi\colon K \to \mathbb{R}_{\geq 0}$ satisfying:

$\forall a, b \in K$ (1) $\phi(ab) = \phi(a)\phi(b)$

(2) $\phi(a) = 0$ *iff* $a = 0$

(3) $\phi(a + b) \leq \phi(a) + \phi(b)$

Example: Let $K = \mathbb{Q}$, $p \in \mathbb{Z}$ prime. For $\frac{a}{b} \in \mathbb{Q}$ in lowest terms, define $\left|\frac{a}{b}\right|_p = 0$ if $a = 0$. If $a \neq 0$, write $\frac{a}{b} = p^r \frac{a'}{b'}$ for a', $b' \in \mathbb{Z}$, $p \nmid a'b'$, and let

$$\left|\frac{a}{b}\right|_p = \frac{1}{p^r}$$

(1) and (2) are clear. For (3), note that (if $r \leq t$ without loss of generality)

$$\begin{aligned}\left|p^r \tfrac{a_1}{b_1} + p^t \tfrac{a_2}{b_2}\right|_p &= p^{-r}\left|\tfrac{a_1}{b_1} + p^{t-r} \tfrac{a_2}{b_2}\right|_p \\ &\leq p^{-r}\end{aligned}$$

so $|a + b|_p \leq \max\{|a|_p, |b|_p\}$.

This is called the p-adic absolute value on $\mathbb{Q}$.
Example: $|\frac{8}{37}|_2 = \frac{1}{8}$, $|\frac{12}{17}|_3 = \frac{1}{3}$ $|\frac{12}{17}|_2 = \frac{1}{4}$
So $p^n \to 0$ p-adically.
Example: $1 + p + p^2 + \cdots = \sum_{i=0}^{\infty} p^i = \frac{1}{1-p}$ if $\sum_{i=0}^{\infty} p^i$ converges. If we interpret this sequence classically. $\sum p^i$ does not converge.

Theorem: Let $\sum_{i=0}^{\infty} a_i$ be an infinite series. Then $\sum_{i=0}^{\infty} a_i$ is Cauchy p-adically *iff* $|a_i|_p \to 0$. $(a_i \in \mathbb{Q})$
Proof: Forwards is clear. Backwards is harder. Say $|a_i|_p \to 0$. Then $|\sum_{i=0}^{n} a_i|_p \leq \max_{i \in \{1,\ldots,n\}}\{|a_i|_p\}$. So

$$\Big|\sum_{i=0}^{n} a_i - \sum_{i=0}^{m} a_i\Big|_p = \Big|\sum_{i=m+1}^{n} a_i\Big|_p \leq \max_{i \in \{m+1,\ldots,n\}}\{|a_i|_p\}$$

which is going to 0. So $\sum_{i=0}^{\infty} a_i$ induces a Cauchy sequence. □

So $\sum_{i=0}^{\infty} 2^i = -1$.

Is $\mathbb{Q}$ p-adically complete?
No: $3^2 \equiv 2 \bmod 7$ so 3 is 7-adically close to $\sqrt{2}$. Sort of, "$|3 - \sqrt{2}|_7 \leq \frac{1}{7}$".
Let's look for $a_2 \in \mathbb{Z}/7^2\mathbb{Z}$ such that $a_2^2 \equiv 2 \bmod 7^2$.

Say $a_2 \equiv 3 \bmod 7$. Then $a_2 \equiv 3 + 7k \bmod 7^2$

$$\begin{aligned}
&\implies (3+7k)^2 \equiv 9 + 42k \bmod 49 \\
&\implies 2 \equiv 9 + 42k \bmod 49 \\
&\implies -7 \equiv 42k \bmod 49 \\
&\implies -1 \equiv 6k \bmod 7 \\
&\implies k \equiv \bmod 7 \\
&\implies a_2 = 3 + 7 = 10 \text{ works!}
\end{aligned}$$

By iterating this procedure, we can find integers a_r such that $a_r^2 \equiv 2 \bmod 7^r$ for all $r \in \mathbb{Z}_{>0}$. So $\{a_r\}$ is a Cauchy sequence, whose limit if it exists is $\sqrt{2} \notin \mathbb{Q}$. Therefore $\mathbb{Q}$ is not 7-adically complete.

PMATH 442 Lecture 26: November 14, 2011

Let R be the ring of p-adic Cauchy sequences of rational numbers, with

$$\{a_i\} + \{b_i\} = \{a_i + b_i\}$$
$$\{a_i\}\{b_i\} = \{a_i b_i\}$$

It is easy to see that the sum & product of Cauchy sequences is again Cauchy.

Let $M = R$ be the set of null sequences in R; namely, the set of sequences whose limit exists and is 0. It is easy to see that M is an ideal of R, since it is closed under + & −, and multiplication by arbitrary Cauchy sequences.

Theorem: M is a maximal ideal of R.
Proof: We will show that every element of $R - M$ is a unit, so M is maximal. Say $\{a_i\}$ is a p-adic Cauchy sequence which does not converge to 0. Then there are only finitely many a_i such that $a_i = 0$, since $\{a_i\}$ is Cauchy & not null. After adding a null sequence, then, we may assume that $a_i \neq 0$ for all i. Consider $\{\frac{1}{a_i}\}$. It is clearly an inverse to $\{a_i\}$. Is it Cauchy? Yes: The sequence $\{|a_i|_p\}$ is also Cauchy, and therefore convergent. So if $\lim_{i\to\infty}|a_i|_p = L$, then $\{|\frac{1}{a_i}|_p\} \to \frac{1}{L} \neq 0$ and

$$\left|\frac{1}{a_n} - \frac{1}{a_m}\right|_p = \big|\underbrace{a_n}_{\to\frac{1}{L}}\big|_p^{-1}\big|\underbrace{a_m}_{\to\frac{1}{L}}\big|_p^{-1}\big|\underbrace{a_m - a_n}_{\to\text{small as you like}}\big|_p$$

so $\{\frac{1}{a_n}\}$ is Cauchy. □

$$|a_n|_p - |a_m|_p \leq |a_n - a_m|_p \text{ by } \triangle \text{ inequality}$$
$$|a_m|_p - |a_n|_p \leq |a_m - a_n|_p \text{ by } \triangle \text{ inequality}$$
$$a^{-1} = (a^{-1}(a)a_1^{-1}) = a_1^{-1}$$

So R/M is a field containing $\mathbb{Q}$. We call it $\mathbb{Q}_p$, the field of p-adic numbers.

It is easy to see that $\mathbb{Q}_p$ is complete. The absolute value of $\mathbb{Q}_p$ is

$$|\{a_n\}|_p = \lim_{n\to\infty} |a_n|_p.$$

$\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ via $x \mapsto \{x\}$.

So what the heck *is* $\mathbb{Q}_p$? Some elements of $\mathbb{Q}_p$ include:

$$1 + p + p^2 + \cdots$$
$$2 + 3p^2 - 4p^3 + p^4 + \cdots$$

More generally, if $0 \le a_i \le p-1$, $a_i \in \mathbb{Z}$, then $\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Q}_p$. In fact, for any $n \in \mathbb{Z}$, the series $\sum_{i=n}^{\infty} a_i p^i$ is in $\mathbb{Q}_p$.

We will show that every elements of $\mathbb{Q}_p$ is of the form $\sum_{i=n}^{\infty} a_i p^i$ for $0 \le a_i \le p-1$, a_i, $n \in \mathbb{Z}$.

Theorem: Let $\alpha \in \mathbb{Q}_p^*$. Then α can be written uniquely as $\alpha = p^r u$ for $|u|_p = 1$.
Proof: $|\alpha|_p = p^{-r}$ for some r. So $|p^{-r}\alpha|_p = 1$, so $\alpha = p^r(p^{-r}\alpha)$. If $\alpha = p^k u$, then $|\alpha|_p = p^{-r} \implies k = r$, and then $u = p^{-r}\alpha$. □

Definition: The ring of p-adic integers is $\mathbb{Z}_p = \{\, \alpha \in \mathbb{Q}_p : |\alpha|_p \le 1 \,\}$. This is a ring because of $|a + b|_p \le \max\{|a|_p, |b|_p\}$. It's not a field, since $p \in \mathbb{Z}_p$ but $\frac{1}{p} \notin \mathbb{Z}_p$. Note $\mathbb{Z}_p^* = \{\, \alpha \in \mathbb{Q}_p : |\alpha|_p = 1 \,\}$. So $\mathbb{Q}_p^* = \{\, p^r u : u \in \mathbb{Z}_p^* \,\}$. In particular, $\mathbb{Q}_p$ is the fraction field of $\mathbb{Z}_p$.

PMATH 442 Lecture 27: November 16, 2011

Theorem: $\mathbb{Z}_p =$ the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.
Proof: If $\{x_i\}$ is a Cauchy sequence of integers $x_i \in \mathbb{Z}$, then $|\{x_i\}|_p \le 1$ because $|x_i|_p \le 1$ for all i. So $\overline{\mathbb{Z}} \subset \mathbb{Z}_p$.

Conversely, say $\{x_i\} \in \mathbb{Z}_p$. Then $\lim_{i\to\infty} |x_i|_p \le 1$. If $\lim_i |x_i|_p = 0$, then $\{x_i\} = 0 \in \overline{\mathbb{Z}}$. Otherwise, we have $|x_n|_p = \lim_i |x_i|_p$ for all large enough n. Write $x_n = p^r \frac{a_n}{b_n}$ for $p \nmid a_n b_n$. Then for every positive integer m, there is an integer $\alpha_{n,m}$ such that

$$\alpha_{n,m} \equiv x_n \bmod p^m \iff |\alpha_{n,m} - x_n|_p \le p^{-m}$$

So up to messing around with finitely initial terms, the sequence $\{\alpha_{n,n}\} \in \overline{\mathbb{Z}}$ is equal in $\mathbb{Q}_p$ to $\{x_n\}$, so $\{x_n\} \in \overline{\mathbb{Z}}$. □

Theorem: $\mathbb{Z}_p/p^r\mathbb{Z}_p \cong \mathbb{Z}/p^r\mathbb{Z}$.
Proof: Consider $\phi\colon \mathbb{Z} \to \mathbb{Z}_p/p^r\mathbb{Z}_p$. It is clear that $\ker\phi = p^r\mathbb{Z}$. So there is an injection $\phi\colon \mathbb{Z}/p^r\mathbb{Z} \to \mathbb{Z}_p/p^r\mathbb{Z}_p$. It is onto because any $\alpha \in \mathbb{Z}_p$ satisfies

$$|\alpha - n|_p \le p^{-r} \text{ for some } n \in \mathbb{Z}, \iff \alpha \equiv n \bmod p^r\mathbb{Z}_p \iff \alpha \equiv \phi(n)\checkmark \quad \square$$

Say $\alpha \in \mathbb{Q}_p$. If $\alpha = 0$, then α is clearly of the form $\alpha = \sum_{i=n}^{\infty}$ for $0 \le a_i \le p-1$. If $\alpha \ne 0$, write $\alpha = p^r \frac{a}{b}$, where $p \nmid ab$. It suffices to write $\frac{a}{b} = \sum_{i=n}^{\infty} a_i p^i$.

But $\frac{a}{b} \in \mathbb{Z}_p$, so for each $r \ge 1$, we can find $m_r \in \mathbb{Z}$ such that $\frac{a}{b} \equiv m_r \bmod p^r\mathbb{Z}_p$. So if we choose $m_r \in \{0, \dots, p-1\}$, we write m_r in base p_i and get

$$\frac{a}{b} = a_0 + a_1 p + \cdots + a_{r-1}p^{r-1} + Ep^r$$

for $0 \le a_i \le p-1$. Moreover, note that $m_{r+t} \equiv m_r \bmod p^r$. So we get a well defined series

$$\frac{a}{b} = \sum_{i=0}^{\infty} a_i p^i$$

where $a_i \in \{0, \dots, p-1\}$. So $\mathbb{Q}_p$ really is

$$\mathbb{Q}_p = \left\{ \sum_{i=n}^{\infty} a_i p^i : a_i \in \{0, \dots, p-1\} \right\}$$

$$\begin{array}{r} \not{0}\not{0}\not{0}\overset{7}{0} \\ -1 \\ \hline \dots 666 \text{ in } \mathbb{Q}_7 \end{array}$$

$$= \sum_{n=0}^{\infty} 6 \cdot 7^n$$

Define $R \subset (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times \cdots$ by

$$R = \left\{ (a_1, a_2, \dots) : a_i \equiv a_{i+r} \bmod p^i,\ a_i \in \mathbb{Z}/p^i\mathbb{Z} \right\} = H$$

Theorem: $\mathbb{Z}_p \cong R$.
Proof: Define $\phi\colon \mathbb{Z}_p \to H$ by $\phi(\alpha) = (\alpha \bmod p, \alpha \bmod p^2, \cdots)$. Clearly $\operatorname{im}\phi \subset$, so $\phi\colon \mathbb{Z}_p \to R$. Since $\ker\phi = \{0\}$, ϕ is injective. For surjectivity, say $(n_1, n_2, \dots) \in R$. If we choose $n_i \in \{0, \dots, p^i - 1\}$, then writing n_i in base p will have a consistent set of ith order p-adic approximations $\sum_{i=0}^{\infty} a_i p^i$, where $n_i = \sum_{j=0}^{i-1} a_j p^j$. So $(n_1, n_2, \dots) \in \operatorname{im}\phi$. □

PMATH 442 Lecture 28: November 18, 2011

Definition: A valuation on a field K is a function $\phi\colon K \to \mathbb{R}$ such that:

(1) $\phi(x) \geq 0$, $\phi(x) = 0$ *iff* $x = 0$

(2) $\phi(xy) = \phi(x)\phi(y)$

(3) $\phi(x+y) \leq \phi(x) + \phi(y)$

If ϕ also satisfies $\phi(x+y) \leq \max\{\phi(x), \phi(y)\}$ then we say ϕ is non-archimedean.

Assume K is a field complete with respect to a non-archimedean valuation $|\cdot|_v$.
Definition: The valuation ring of K is $O = \{ x \in K : |x|_v \leq 1 \}$. It is easy to see that O is a ring.
Definition: The maximal ideal of O is $M = \{ x \in O : |x|_v < 1 \}$.
It is easy to see that M is the set of non-units of O, and is therefore the unique maximal ideal of O.
Definition: The field O/M is called the residue field of O (or K).
Theorem (Hensel's Lemma): Let K be complete with respect to a non-archimedean valuation $|\cdot|_v$. Let $f(x) \in O[x]$, $f \not\equiv M$. Say $\overline{f} = \overline{g}\overline{h}$ in $(O/M)[x]$, where $\overline{g}$, $\overline{h} \in (O/M)[x]$ are relatively prime. Then $f = gh$, where $g \equiv \overline{g} \bmod M$, $h \equiv \overline{h} \bmod M$, and $\deg g = \deg \overline{g}$, and g, $h \in O[x]$.

Example: Say $K = \mathbb{Q}_7$, $O = \mathbb{Z}_7$, $f(x) = x^2 - 2$. Then

$$x^2 - 2 \equiv (x+3)(x-3) \bmod 7 \text{ in the residue field } \mathbb{Z}/7\mathbb{Z}.$$

Helsel $\implies \exists g, h \in \mathbb{Z}_7[x]$ such that $\deg g = \deg h = 1$ and

$$x^2 - 2 = g(x)h(x).$$

But $\deg g = \deg h = 1 \implies gh$ has two roots in $\mathbb{Z}_7$,

$$\pm\sqrt{2} \in \mathbb{Z}_7 \subset \mathbb{Q}_7.$$

PMATH 442 Lecture 29: November 21, 2011

K complete with respect to a non-archimean valuation $|\cdot|_v$. Let $O = \{ a \in K : |a|_v \leq 1 \}$ be the valuation ring. $M \subset O$ the maximal ideal $\{ a \in K : |a|_v < 1 \}$.

$$K = \mathbb{Q}_p$$
$$O = \mathbb{Z}_p$$
$$M = p\mathbb{Z}_p$$

Theorem: (Hensel's Lemma)
Let $f(x) \in O[x]$ be non-constant, $f \not\equiv 0 \bmod M$. Assume $\overline{f} = \overline{g}\overline{h} \bmod M$, where $\overline{f}$ is the reduction of f mod M, and that $\overline{g}$, $\overline{h}$ are relatively prime in $(O/M)[x]$. Then $f = gh$ in $\theta[x]$, where $g \equiv \overline{g}$ and $h \equiv \overline{h} \bmod M$, and $\deg(g) = \deg(\overline{g})$.

Proof: Pick g_0, $h_0 \in O[x]$ willy-nilly so that $\deg(g_0) = \deg(\overline{g})$, $\deg(h_0) \leq \deg(\overline{h})$, $g_0 \equiv \overline{g}$, $h_0 \equiv \overline{h} \bmod M$. Since $\overline{h}$, $\overline{g}$ are coprime in $(O/M)[x]$, there are $a(x)$, $b(x) \in O[x]$ such that $ag_0 + bh_0 \equiv 1 \bmod M$.
Amongst the coefficients of $f - g_0h_0$ and $ag_0 + bh_0 - 1$, there is (at least) one with smallest valuation. Call it π.
We show: $f \equiv g_rh_r \bmod \pi^{r+1}$.
If $r = 0$, we're already done. Proceed by induction. Say $f \equiv g_{r-1}h_{r-1} \bmod \pi^r$, with $\deg g_{r-1} = \deg \overline{g}$, $\deg h_{r-1} \leq \deg \overline{h}$. We're looking for g_r and h_r.
Write $\left\{ \begin{smallmatrix} g_r = g_{r-1} + p_r\pi^r \\ h_r = h_{r-1} + q_r\pi^r \end{smallmatrix} \right.$, for p_r, $q_r \in O[x]$. Then:

$$f - g_rh_r \equiv \pi^r(g_{r-1}g_r + h_{r-1}p_r) \bmod \pi^{r+1}$$
$$\implies \underbrace{\frac{1}{\pi^r}(f - g_rh_r)}_{f_r :=} \equiv g_{r-1}g_r + h_{r-1}p_r \bmod \pi$$

Now, $q_r = af_r$ and $p_r = bf_r$ works because $g_r \equiv g_0 \bmod M$, $h_r \equiv h_0 \bmod M$. However, this choice may not satisfy the degree constraints $\deg g_r = \deg \overline{g}$ and $\deg h_r \leq \deg \overline{h}$. So write: $bf_r = Qg_0 + R$ for $\deg R \leq \deg g_0$, and set $p_r = R$. The leading coefficient of g_0 is not in M, so it's a unit in O. The Euclidean Algorithm will show that Q, $R \in O[x]$. So:

$$\begin{aligned} g_0(af_r + h_0Q) + h_0p_r &\equiv ag_0f_r + g_0h_0Q + h_0p_r \\ &\equiv ag_0f_r + h_0(bf_r - p_r) + h_0p_r \\ &\equiv ag_0f_r + bh_0f_r \\ &\equiv f_r \bmod \pi \end{aligned}$$

PMATH 442 Lecture 30: November 23, 2011

Theorem: (Hensel's Lemma) Let K be a complete field with respect to a non-archedmedian valuation, O is valuation ring, $M \subset O$ the maximal ideal. Let $f(x) \in O[x]$, and assume $\overline{f} \equiv \overline{g}\overline{h} \bmod M$ for $\gcd(\overline{g}, \overline{h}) = 1$. Then $f = gh$ in $K[x]$, where $g \equiv \overline{g} \bmod M$, $h \equiv \overline{h} \bmod M$, $\deg(g) = \deg(\overline{g})$.
Proof: (continued)

$$g_0(af_r + h_0Q) + h_0(p_r) \equiv f_r \bmod \pi$$
$$\text{and } \deg(p_r) \leq \deg f - \deg h_0 = \deg(g_0)$$

So after deleting terms in $af_r + h_0Q$ of too high degree (because they're 0 mod π), we find q_r.

$$\begin{aligned} \text{So } g_{r+1} &= g_r + p_r\pi^r \\ h_{r+1} &= h_r + q_r\pi^r \\ \text{satisfies } f &\equiv g_rh_r \bmod \pi^{r+1} \\ \deg(g_{r+1}) &= \deg(\overline{g}) \\ \deg(h_{r+1}) &\leq \deg(\overline{h}) \\ \left.\begin{aligned} g_{r+1} &\equiv \overline{g} \\ h_{r+1} &\equiv \overline{h} \end{aligned}\right\} &\bmod M \end{aligned}$$

So $\{g_r\}$ & $\{h_r\}$ are Cauchy sequences of polynomials in $K[x]$, that must converge to g & h, respectively, satisfying $f = gh$, $\deg g = \deg \overline{g}$, $g \equiv \overline{g}$, $h \equiv \overline{h}$. ☐

Example: $\sqrt{2} \notin \mathbb{Q}_5$, because if not, then $|\sqrt{2}|_5^2 = |2|_5 = 1$, so $\sqrt{2} \in \mathbb{Z}_5$. But $x^2 - 2$ is irreducible in the residue field $\mathbb{F}_5$, so $\sqrt{2} \notin \mathbb{Z}_5$.
Example: $x^{p-1} - 1$ splits completely in $\mathbb{F}_p[x]$: $x^{p-1} - 1 = \prod_{i=1}^{p-1}(x - i)$. By Hensel's Lemma, $x^{p-1} - 1$ splits completely in $\mathbb{Q}_p[x]$, too. So if $n \mid p - 1$, then $\zeta_n \in \mathbb{Q}_p$.

Definition: Let L/K be a finite extension, $\alpha \in L$ any element. The norm of α over K is $\det(m_\alpha)$, where

$$m_\alpha \colon L \to L \text{ is } m_\alpha(x) = \alpha x$$
$$N_{L/K}(\alpha) = \det(m_\alpha)$$
$$N_{L/K}(\alpha) = (-1)^{[L:K]}(\text{constant term in characteristic polynomial})$$

Since α is a root of the monic characteristic polynomial (by Cayley–Hamilton Theorem), the minimal polynomial of α ($m(x)$) is a factor of the characteristic polynomial of m_α ($\chi(x)$). But every root of $\chi(x)$ is a root of $m(x)$, so $\chi(x) = m(x)^d$, where $d = [L : K(\alpha)]$. Comparing constant terms gives $(m(0))^d = \chi(0)$.

$n = [L : K]$
$L = 1 \cdot K + \alpha \cdot K + \cdots + \alpha^{n-1} \cdot K$
if $L = K(\alpha)$

$$[m_\alpha] = \begin{bmatrix} 0 & 0 & & & -a_0/a_n \\ 1 & 0 & & & -a_1/a_n \\ 0 & 1 & & & -a_2/a_n \\ \vdots & & \ddots & & \vdots \\ 0 & \dots & 0 & 1 & -a_{n-1}/a_n \end{bmatrix}$$
$$m(x) = a_0 + a_1 x + \cdots + a_n x^n$$
$$\implies \alpha^n = -\frac{a_0}{a_1} - \frac{a_1}{a_n}\alpha - \cdots - \frac{a_{n-1}}{a_n}\alpha^{n-1}$$
$$\det[m_\alpha] = (-1)^{n-1}\frac{-a_0}{a_n} = (-1)^n a_0$$
$$N_{L/K}(\alpha) = (-1)^{[L:K]}(\text{constant term of monic minimal polynomials})^{[L:K(\alpha)]}$$

Say $K/\mathbb{Q}_p$ is a finite extension. Define
$$|\alpha|_v = \sqrt[n]{|N_{K/\mathbb{Q}_p}(\alpha)|_p}$$
where $n = [K : \mathbb{Q}_p]$. This is a non-archedmedian valuation:

(1) $|\alpha|_v \geq 0$, equality *iff* $\alpha = 0$ ✓

(2) $|\alpha\beta|_v = |\alpha|_v |\beta|_v$ ✓

(3) $|\alpha + \beta|_v \leq \max\{|\alpha|_v, |\beta|_v\}$

We will justify (3) next time.

PMATH 442 Lecture 31: November 25, 2011

$|\alpha|_v = \sqrt[n]{|N_{K/\mathbb{Q}_p}(\alpha)|_p}$
Theorem: $|\cdot|_v$ is a non-archimedean valuation on K.
Proof: All done except:
$$|\alpha + \beta|_v \leq \max\{|\alpha|_v, |\beta|_v\}.$$
Without loss of generality, say $|\beta|_v \geq |\alpha|_v$. Then it suffices to show:
$$\Big|\frac{\alpha}{\beta} + 1\Big|_v \leq \max\Big\{\Big|\frac{\alpha}{\beta}\Big|_v, 1\Big\}.$$

Lemma: Let L be a field that's complete with respect to a non-archimedean valuation ψ. Say $f(x) \in L[x]$ is irreducible, $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Then $\psi(a_i) \le \max\{\psi(a_0), \psi(a_n)\}$ for all i.
Proof of Lemma: Let O be the valuation ring. Let j be the smallest index such that $\psi(a_j) \ge \psi(a_i)$ for all i. Then $\frac{1}{a_j} f \in O[x]$ and

$$f \equiv x^j(a_j + \cdots + a_nx^{n-j}) \bmod M$$

where $M \subset O$ is the maximal ideal. By Hensel's Lemma, $f(x)$ factors as the product of 2 polynomials, one of $\deg j$ & the other of degree $n - j$. Since f is irreducible, either $j = 0$ or $n - j = 0$. ☐ lemma

By the lemma applied to $L = \mathbb{Q}_p$, we see that a monic irreducible polynomial in $\mathbb{Q}_p[x]$ lies in $\mathbb{Z}_p[x]$ *iff* its constant coefficient lies in $\mathbb{Z}_p$. So $N_{K/\mathbb{Q}_p}(\alpha) \in \mathbb{Z}_p$ *iff* monic minimal polynomial for α lies in $\mathbb{Z}_p[x]$. Since $|\frac{\alpha}{\beta}|_v \le 1$, we get $N(\frac{\alpha}{\beta}) \in \mathbb{Z}_p$ so monic minimal polynomial for $\frac{\alpha}{\beta}$ has coefficients in $\mathbb{Z}_p$. If $m(x)$ is the monic minimal polynomial for $\frac{\alpha}{\beta}$, then $m(x-1)$ is the monic minimal polynomial for $(\frac{\alpha}{\beta} - 1)$. So $m(x) \in \mathbb{Z}_p[x] \implies m(x-1) \in \mathbb{Z}_p[x]$, and hence $N(\frac{\alpha}{\beta} + 1) \in \mathbb{Z}_p$ &

$$\Big|\frac{\alpha}{\beta} + 1\Big|_v \le \max\Big\{\Big|\frac{\alpha}{\beta}\Big|_v, 1\Big\}$$

as desired.

PMATH 442 Lecture 32: November 28, 2011

Example: $K = \mathbb{Q}_3(\sqrt{2})$
Note that $[K : \mathbb{Q}_3] = 2$, because $|\sqrt{2}|_3 = \sqrt{|2|_3} = 1$. Since $\sqrt{2} \notin \mathbb{F}_3$, $\sqrt{2} \notin \mathbb{Z}_3$, so $\sqrt{2} \notin \mathbb{Q}_3$. Now,

$$|a + b\sqrt{2}|_3 \le \max\{|a|_3, |b|_3\}$$
$$= \sqrt{|N(a + b\sqrt{2})|_3} = \sqrt{|a^2 - 2b^2|_3}$$

If $|a|_3 \ne |b|_3$, then $|a + b\sqrt{2}|_3 = \max\{|a|_3, |b|_3\}$.
If $|a|_3 = |b|_3$, then $a + b\sqrt{2} = 3^r(a' + b'\sqrt{2})$, where a', $b' \in \mathbb{Z}_3^*$. In that case, $a' = \pm b' = \pm 1 \bmod 3$, so $(a')^2 - 2(b')^2 = -1 \bmod 3$, so $|a + b\sqrt{2}|_3 = |a|_3 = |b|_3$. So in general,

$$|a + b\sqrt{2}|_3 = \max\{|a|_3, |b|_3\}.$$

$K/\mathbb{Q}_p$ is a finite extension.
Then $\sqrt[n]{|N_{K/\mathbb{Q}_p}(\alpha)|_p}$ is an extension of $|\cdot|_p$ to K. It's the *only* such extension, and K is complete with respect to this extension.

$$\begin{aligned} O &= \text{valuation ring of } K \\ &= \{\, \alpha \in K : |\alpha|_p \le 1 \,\} \\ &= \{\, \alpha \in K : \text{monic minimal polynomial lies in } \mathbb{Z}_p[x] \,\} \end{aligned}$$

Note that O is Galois stable, *i.e.*, if $\alpha \in O$, $\sigma \in \mathrm{Aut}_{\mathbb{Q}_p}(K)$, then $\sigma(\alpha) \in O$.

Assume $K/\mathbb{Q}_p$ is Galois.

Recall that the residue field of K is $\overbrace{O/M}^{=k}$, where $M =$ maximal ideal of O. It's an extension of $\mathbb{F}_p$, and a finite one since $[K : \mathbb{Q}_p] < \infty$.
Define:

$$\psi\colon\ \mathrm{Gal}(K/\mathbb{Q}_p) \to \mathrm{Gal}(k/\mathbb{F}_p)$$

as follows:

Say $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$. Then $\sigma|_O\colon O \to O$ is also an automorphism. Since $|\cdot|_p$ is also Galois invariant, σ maps M to M. Thus, σ induces a homomorphism

$$\psi(\sigma)\colon \underbrace{O/M}_{=k} \to \underbrace{O/M}_{=k}.$$

$\psi(\sigma)$ is an automorphism because k is a finite field.
It is easy to check that ψ is a homomorphism of groups

$$\psi\colon \operatorname{Gal}(K/\mathbb{Q}_p) \to \operatorname{Gal}(k/\mathbb{Q}_p).$$

Say $k = \mathbb{F}_p(\overline{\alpha})$, $\overline{m}(x)$ a minimal polynomial for $\overline{\alpha}$ over $\mathbb{F}_p$. Then by Hensel's Lemma, any polynomial $m(x) \in \mathbb{Z}_p[x]$ with $m \equiv \overline{m} \bmod M$ and $\deg(m) = \deg(\overline{m})$ will also be irreducible and split completely in K. (α a root of $m(x)$, $\alpha \equiv \overline{\alpha} \bmod M$)
If $\overline{\sigma} \in \operatorname{Gal}(k/\mathbb{F}_p)$ and $\overline{\sigma}(\overline{\alpha}) = \overline{\beta}$, then if $\beta \in K$ is a root of $m(x)$ with $\beta \equiv \overline{\beta} \bmod M$, then any $\sigma \in \operatorname{Gal}(K/\mathbb{Q}_p)$ with $\sigma(\alpha) = \beta$ satisfies $\psi(\sigma) = \overline{\sigma}$.

The kernel of ψ is called the inertia (sub)group of $\operatorname{Gal}(K/\mathbb{Q}_p)$.

Definition: $K/\mathbb{Q}_p$ finite is unramified *iff* ψ is an isomorphism. Equivalently, if $[k : \mathbb{F}_p] = [K : \mathbb{Q}_p]$.

Definition: The inertia subfield of K is the fixed field of the inertia group.

$$K$$
$$\Big|\ [K : K^{\mathrm{ur}}] = \#I(K)$$
$$K^{\mathrm{ur}}$$
$$\Big|\ [K^{\mathrm{ur}} : \mathbb{Q}_p] = [k : \mathbb{F}_p]$$
$$\mathbb{Q}_p$$

Example:

$$\mathbb{Q}_3(\sqrt{2}, \sqrt{3})$$
$$\Big|\ \text{ramified}$$
$$\mathbb{Q}_3(\sqrt{2})$$
$$\Big|\ \text{ramified}$$
$$\mathbb{Q}_3$$

PMATH 442 Lecture 33: November 30, 2011

Theorem: If $K/\mathbb{Q}_p$ is a finite unramified extension, then it is also Galois.
Proof: By assumption, $[K : \mathbb{Q}_p] = [k : \mathbb{F}_p]$, where k is the residue field O/M of K. Write $k = \mathbb{F}_p(\overline{\alpha})$ for some $\overline{\alpha} \in k$. Choose $\alpha \in O \subset K$ such that $\alpha \equiv \overline{\alpha} \bmod M$. Then $\mathbb{Q}_p(\alpha)$ is an extension of $\mathbb{Q}_p$ of degree $n = [K : \mathbb{Q}_p] = [k : \mathbb{F}_p]$, because a minimal polynomial $\overline{m}(x) \in \mathbb{F}_p[x]$ for $\overline{\alpha}/\mathbb{F}_p$ is irreducible, and also it's the reduction of a minimal polynomial $m(x)$ for $\alpha/\mathbb{Q}_p$. Therefore $\mathbb{Q}_p(\alpha) = K$.

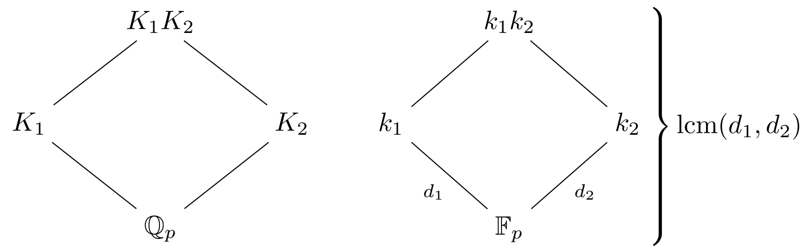
$\mathbb{Q}_p(\alpha)$ is clearly separable over $\mathbb{Q}_p$. But $\overline{m}(x)$ is separable, and splits completely (into linear factors) in $k(x)$. By Hensel's Lemma, since the factors are pairwise coprime, this means $m(x)$ factors completely in $K[x]$. So K is a splitting field for $m(x)$ over $\mathbb{Q}_p$, since $\mathbb{Q}_p(\alpha) = K$. So $K/\mathbb{Q}_p$ is Galois. $\square$

This means that if $K/\mathbb{Q}_p$ is unramified, then its Galois group is cyclic. Better yet, any two unramified extensions of $\mathbb{Q}_p$ of degree n are isomorphic, by Hensel's Lemma and previous theorem.

So extensions of $\mathbb{F}_p$ an unramified extensions of $\mathbb{Q}_p$ are in a natural 1–1 correspondence.

Consequences: The composition of 2 unramified extensions of $\mathbb{Q}_p$ is unramified.

Note that:



Let's find all quadratic extensions of $\mathbb{Q}_p$ for $p \neq 2$.
They are classified by $(\mathbb{Q}_p^*)/(\mathbb{Q}_p^*)^2$

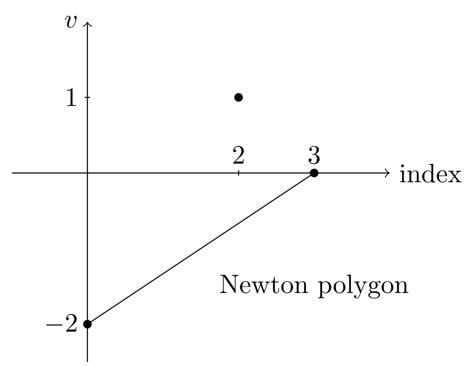
Any $\alpha \in \mathbb{Q}_p^*$ is, up to squares, an element of either $\mathbb{Z}_p$ or $p\mathbb{Z}_p$.

$$\mathbb{Z}_p \cong \{\, (a_1, a_2, a_3, \dots) : a_i \in \mathbb{Z}/p\mathbb{Z},\ a_1 \equiv a_{1+j} \bmod p^i\ \forall j \geq 0 \,\}$$

If $(a_1, \dots) \in (\mathbb{Q}_p)^2$, then $a_1 \in (\mathbb{F}_p)^2$.
So modulo squares, there are 2 choices for a_1. For all $i \geq 2$, there are again only 2 choices for a_i, up to squares, so there are exactly 2 units in $\mathbb{Z}_p$, up to squares.
Similarly, there are 2 elements of $p\mathbb{Z}_p$ up to squares. So $(\mathbb{Q}_p^*)/(\mathbb{Q}_p^*)^2$ has order 4. There are therefore 3 nontrivial quadratic extensions of $\mathbb{Q}_p$:

unramified: $\mathbb{Q}_p(\sqrt{a})$ $\leftarrow$ a non-residue mod p
ramified: $\mathbb{Q}_p(\sqrt{p})$
ramified: $\mathbb{Q}_p(\sqrt{ap})$

Newton Polygons
For $a_i \in \mathbb{Q}_p^*$, define $v(a) = -\log|a|_p$ = biggest power of p dividing a.
Let $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}_p[x]$ be a polynomial, $a_n \neq 0$. Plot all the points $(i, v(a_i))$ for $a_i \neq 0$. The Newton polygon of $f(x)$ is the lower convex hull of these points.
Example: $p = 3$, $f(x) = x^3 + \frac{3}{4}x^2 + \frac{7}{9}$
Plot: $(3, 0)$, $(2, 1)$, $(0, -2)$



PMATH 442 Lecture 34: December 2, 2011

Newton Polygons
$v(a) = -\log|a|_p$ for $a \in \mathbb{Q}_p^*$. Newton polygon of $a_0 + a_1x + \cdots + a_nx^n$ is lower convex hull of $\{(i, v(a_i))\}$.

Theorem: Let $f(x) = a_0 + \cdots + a_nx^n \in \mathbb{Q}_p[x]$ be a polynomial of degree n. Say $(r, v(a_r))$ and $(s, v(a_s))$ are the endpoints of a line segment in the Newton polygon of $f(x)$, of slope $-m$. Then $f(x)$ has (in some extension of $\mathbb{Q}_p$) $|r - s|$ roots α_i with $|a_i|_p = p^{-m}$.

Note: The Galois group of $f(x)$ does not change the valuation of roots of $f(x)$. Thus, this theorem tells us that line segments in the Newton polygon correspond to factors of $f(x)$ in $\mathbb{Q}_p[x]$.
Proof: Assume without loss of generality that $a_n = 1$.

Order the roots of $f(x)$ as follows:

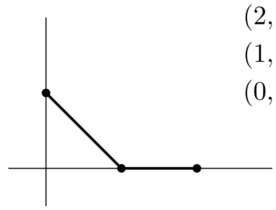
$$\begin{aligned} \alpha_1, \ldots, \alpha_{t_1} &\leftarrow v(\alpha_i) = m_1 \\ \alpha_{t_1+1}, \ldots, \alpha_{t_2} &\leftarrow v(\alpha_i) = m_2 \quad > m_1 \\ &\vdots \\ \alpha_{t_r+1}, \ldots, \alpha_n &\leftarrow v(\alpha_i) = m_{r+1} > m_r \\ \text{so } v(a_n) &= 0 \\ v(a_{n-1}) &\geq \min\{v(\alpha_i)\} = m_1 \\ v(a_{n-1}) &\geq \min\{v(\alpha_i\alpha_j)\} = 2m_1 \\ &\vdots \\ v(a_{n-t_1}) &= t_1 m_1 \\ v(a_{n-t_1-1}) &\geq t_1 m_1 + m_2 \\ &\vdots \\ v(a_{n-t_1-t_2}) &= t_1 m_1 + (t_2 - t_1) m_2 \end{aligned}$$

Continuing in this fashion, one sees that the Newton polygon of $f(x)$ has vertices

$$(n - t_0, t_1 m_1 + (t_2 - t_1) m_2 + \cdots + (t_c - t_{c-1}) m_c),$$

and has $r + 1$ segments of slopes $-m_1$, $-m_2$, $\ldots$, $-m_{r+1}$. □

Example: $x^2 + x - 6$, $\mathbb{Q}_3$.



$(2, 0)$
$(1, 0)$
$(0, 1)$

$= (x + 3)(x - 2)$

Theorem: Assume that the Newton polygon of $f(x)$ intersects $\mathbb{Z}^2$ in exactly two points. Then $f(x)$ is irreducible in $\mathbb{Q}_p[x]$.

Proof: Say $f(x) = g(x)h(x)$, and assume without loss of generality that f, g, h are all monic. We know that the Newton polygon of $f(x)$ is a single line segment of slope m, since the Newton polygon only has vertices at lattice points. Say $\deg(f) = n$.

So $v(\alpha) = m$ for all roots α of f, and thus for all roots of g and h, too. If $\deg(g) = d$, then $|g(0)|_p = p^{-dm}$ and $|h(0)|_p = p^{-(n-d)m}$. The Newton polygon joins $(n, 0)$ to $(0, nm)$, which contains the point $(d, (n - d)m)$. Thus, either $d = n$ or $d = 0$, and so $f(x)$ is irreducible. □

So $x^5 + 2x^4 + 4$ is irreducible over $\mathbb{Q}_2$, because its Newton polygon has exactly 2 lattice points, one at each end.