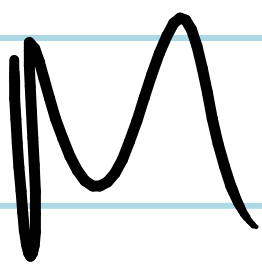
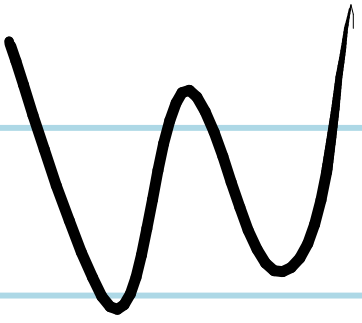
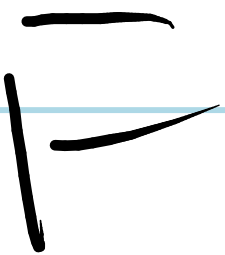






PMATH 348 **Post-Eisenstein**

11 Jan 2016 Recall **Prop 3.** Let $R$ be an integral domain and $P$ a prime ideal. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$, with $n \geq 1$. Suppose $a_n \notin P$ but $a_0, \ldots, a_{n-1} \in P$ and $a_0 \notin P^2$. Then $f(x)$ is irreducible in $R[x]$.

**Cor 4.** If $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ with $n \geq 1$ and $p \nmid a_n$, $p \mid a_0, \ldots, a_{n-1}$ and $p^2 \nmid a_0$ for $p$ a prime, then $f(x)$ is irreducible in $\mathbb{Z}[x]$ and hence also $\mathbb{Q}[x]$ by Gauss' Lemma.

**E.g** Let $p$ be a prime and consider the $p$-th cyclotomic polynomial $\Phi_p(x) = \frac{x^p - 1}{x - 1}$. Eisenstein's criterion does not immediately imply $\Phi_p(x)$ is irreducible. But consider

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1} \in \mathbb{Z}[x].$$

This satisfies Eisenstein's criterion, so $\Phi_p(x+1)$ is irred and so is $\Phi_p(x)$.

**Prop 5.** (Rational Root Theorem) Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. If $\frac{c}{d} \in \mathbb{Q}$ is a root of $f(x)$ and $\gcd(c,d) = 1$, then $c \mid a_0$ and $d \mid a_n$.

**Pf** $0 = f(\frac{c}{d}) = a_n(\frac{c}{d})^n + a_{n-1}(\frac{c}{d})^{n-1} + \cdots + a_1\frac{c}{d} + a_0$, so we have

$$a_nc^n + a_{n-1}c^{n-1}d + \cdots + a_ic^id^{n-i} + \cdots + a_1cd^{n-1} + a_0d^n = 0.$$

$c, d \mid 0$ so $c \mid a_0$ and $d \mid a_n$. $\square$

## §3. Field Extensions

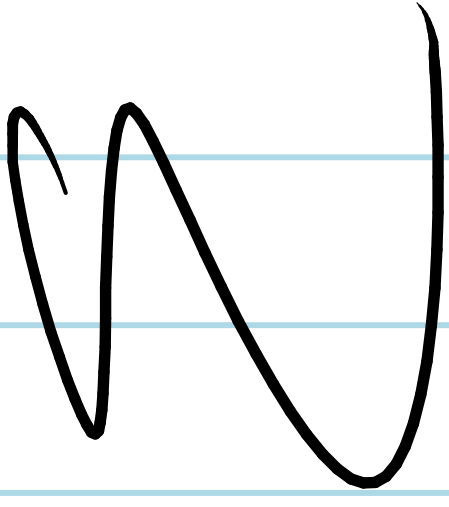
**Def** If $E$ is a field containing another field $F$, say $E$ is a **field extension** of $F$, and denote this by $E/F$. This is not a quotient of rings. If $E/F$ is a field extension, we can view $E$ as a vector space over $F$. The **degree** of $E/F$, denoted $[E:F]$, is the dimension of $E$ as a vector space over $F$, $\dim_F E$. If $[E:F] < \infty$, $E/F$ is a **finite extension**, else it is **infinite**.

**E.g** $[\mathbb{C}:\mathbb{R}] = 2$. $[F(x):F] = \infty$ for any field $F$.

**Thm 6.** If $E/K$ and $K/F$ are finite extensions, then $E/F$ is finite. Furthermore, $[E:F] = [E:K][K:F]$. **Pf** $E_{/F} \cong E_{/K} \otimes K_{/F}$ as vector spaces. $\square$

**Def** Let $E/F$ be a field extension. $\alpha \in E$ is **algebraic** over $F$ if there exists nonzero $f(x) \in F[x]$ such that $f(\alpha) = 0$ — else, $\alpha$ is **transcendental** over $F$. E.g. $5$, $\sqrt{2}$, and $\sqrt[3]{7} \in \mathbb{Q}$ are algebraic over $\mathbb{Q}$ (Exer.) but $e$ (Hermite 1873) and $\pi$ (Lindemann 1882) are transcendental over $\mathbb{Q}$.

**Def** Let $E/F$ be a field extension, $\alpha, \beta \in E$. Let $F[\alpha]$ denote the smallest subring of $E$ containing both $F$ and $\alpha$, and let $F(\alpha)$ denote the smallest subfield containing both. Define $F[\alpha, \beta]$ and $F(\alpha, \beta)$ and so on similarly. If $E = F(\alpha)$ for some $\alpha \in E$, say $E$ is a **simple extension** of $F$.



PMATH 348 # More on Field Extensions

15 Jan 2015 Recall if $\alpha \in E/F$ an extension, $\alpha$ is algebraic iff $[F(\alpha):F] < \infty$.

**Thm 10** Let $E/F$ be a finite extension. Then there exist $\alpha_1, \dots, \alpha_n \in E$ such that

$$F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq \cdots \subsetneq F(\alpha_1, \dots, \alpha_n) = E.$$

To wit, to understand finite extensions it suffices to understand simple extensions.

**Pf** If $[E:F]=1$, $E=F$ and there is nothing to prove. Proceed by induction on $[E:F]$. Take $\alpha \in E \setminus F$. By Thm 6, $[E:F] = [E:F(\alpha)][F(\alpha):F] > [E:F(\alpha)]$. By the inductive hypothesis, there exist $\alpha_2, \dots, \alpha_n \in E$ such that

$$F(\alpha) \subsetneq F(\alpha)(\alpha_2) = F(\alpha, \alpha_2) \subsetneq F(\alpha, \alpha_2, \alpha_3) \subsetneq \cdots \subsetneq F(\alpha, \alpha_2, \dots, \alpha_n) = E$$

and furthermore $F \subsetneq F(\alpha)$. □

**Def** A field extension $E/F$ is algebraic if every $\alpha \in E$ is algebraic over $F$. Otherwise, the extension is transcendental.

**Thm 11.** Let $E/F$ be a field extension. If $[E:F] < \infty$, then $E/F$ is algebraic.

**Pf** Suppose $[E:F]=n$. Consider $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ for $\alpha \in E$ — this set is linearly dependent, so there exists a linear combination $f_0 + f_1\alpha + f_2\alpha^2 + \cdots + f_n\alpha^n = 0$ for $f_i \in F$ not all zero. Hence $\alpha$ is algebraic. □

**Thm 12.** Let $E/F$ be a field extension. Define $L = \{\alpha \in E \mid [F(\alpha):F] < \infty\}$. Then $L$ is an intermediate field of $E/F$.

**Pf** If $\alpha, \beta \in L$, we need to show $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in L$. Well, all of $F(\alpha+\beta)$, $F(\alpha-\beta)$, $F(\alpha\beta)$, and $F(\alpha/\beta)$ are subfields of $F(\alpha, \beta)$, so showing $[F(\alpha,\beta):F] < \infty$ will suffice. Since the minimal polynomial of $\alpha$ over $F(\beta)$ divides the minimal polynomial of $\alpha$ over $F$, we see $[F(\alpha,\beta):F(\beta)] \leq [F(\alpha):F]$, so by Thm 6,

$$[F(\alpha,\beta):F] = [F(\alpha,\beta):F(\beta)][F(\beta):F] \leq [F(\alpha):F][F(\beta):F] < \infty. \quad \square$$

**Def.** Let $E/F$ be a field extension. $\{\alpha \in E \mid [F(\alpha):F] < \infty\}$ is called the algebraic closure of $F$ in $E$.

**Rem.** The converse to Thm 11 is false — consider $\overline{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

**Def** A field $F$ is algebraically closed if for any algebraic extension $E/F$, $E=F$.

**E.g.** By the fundamental theorem of algebra, $\mathbb{C}$ is algebraically closed. Note $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$ (in any superfield of $\mathbb{C}$) and we have $[\mathbb{C}:\mathbb{R}]=2$.

## §4. Splitting Fields

**Def.** Let $E/F$ be a field extension. $f(x) \in F[x]$ splits over $E$ if $E$ contains all roots of $f(x)$, i.e. $f(x)$ is a product of linear factors in $E[x]$. If $f(x)$ splits over $E$ but not over any proper subfield, then $E$ is a splitting field of $f(x)$.

PMATH 348 **Splitting Fields**

18 Jan 2016 Recall $\tilde{E}/F$ ext and $E$ splitting field of $f(x) \in F[x]$ in $\tilde{E}$ if $f(x)$ splits in $E$ but not in any subfield of $E$. We will now discuss existence of splitting fields.

**Thm 13.** Let $p(x) \in F[x]$ be irreducible. The quotient ring $F[x]/(p(x))$ is a field containing $F$ and a root of $p(x)$.

**Pf.** Since $p(x)$ is irreducible, $I=(p(x))$ is maximal so $E = F[x]/I$ is a field. Consider the map $\psi: F \to E$ given by $\psi(a) = a+I$ — it is an embedding since it is not the zero map. So $E$ contains $F$. Let $\alpha = x+I$. Then $p(\alpha) = p(x)+I = \overline{0}$, so $\alpha$ is a root of $p(x)$. □

**Thm 14 (Kronecker)** Let $f(x) \in F[x]$. There exists a field $E/F$ such that $f(x)$ splits over $E$.

**Pf.** Proceed by induction on the degree of $f$. WLOG $\deg f > 1$ and $f(x)$ is reducible. Then $f(x) = p(x)q(x)$ for $p(x), q(x) \in F[x]$, $p(x)$ irreducible. By the previous theorem, there exists $K/F$ such that $p(x)$ has a root $\alpha \in K$. Then $f(x) = (x-\alpha)q(x)g(x)$. $\deg qg$ is strictly less than $\deg f$, so by induction we are done. □

**Thm 15.** Every $f(x) \in F[x]$ has a splitting field, which is a finite extension of $F$.

**Pf.** By Thm 14, there exists $E$ such that $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ splits over $E$. Consider $F(\alpha_1, \ldots, \alpha_n)$. This is the splitting field of $f(x)$ in $E$ because it is the minimal field containing the necessary roots. Further, $F(\alpha_1, \ldots, \alpha_n)/F$ is finite because each $\alpha_i$ is algebraic over $F$. □

We will now discuss uniqueness of splitting fields.

**Def.** Let $\phi: R \to S$ be a ring hom and $\Phi: R[x] \to S[x]$ be the unique hom such that $\Phi|_R = \phi$ and $\Phi(x) = x$. Then $\Phi$ extends $\phi$. More generally, if $R \subseteq R'$ and $S \subseteq S'$, any hom $\Phi: R' \to S'$ with $\Phi|_R = \phi$ extends $\phi$.

**Thm 16.** Let $\phi: F \xrightarrow{\sim} F'$ be an iso of fields and $f(x) \in F[x]$. Let $\Phi: F[x] \to F'[x]$ extend $\phi$. Let $g(x) = \Phi(f(x))$, and $E/F$ and $E'/F'$ be the splitting fields of $f(x)$ and $g(x)$, resp. Then there exists an iso $E \xrightarrow{\sim} E'$ extending $\phi$.

**Cor 17.** The splitting field of $f(x) \in F[x]$ is unique up to isomorphism. □

* * * TO BE CONTINUED * * *

PMATH 348 Something

20 Jan 2016 Recall Thm 16. Let $\phi: F \xrightarrow{\sim} F'$ be an iso of fields and $f(x) \in F[x]$. Let $\Phi: F[x] \to F'[x]$ extend $\phi$. Let $g(x) = \Phi(f(x))$ and $E/F$ and $E'/F'$ be splitting fields of $f(x)$ and $g(x)$, respectively. Then there exists $\psi: E \to E'$ extending $\phi$.

Pf. Proceed by induction on $[E:F]$. Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ with degree $\geq 2$ and let $q(x) = \Phi(p(x))$. Let $\alpha \in E$ and $\alpha' \in E'$ be roots of $p(x)$ and $q(x)$, resp. By Thm 8, we have an $F$-iso $F(\alpha) \cong F[x]/(p(x))$ by $\alpha \mapsto x + (p(x))$ and likewise there is an $F$-iso $F'(\alpha') \cong F'[x]/(q(x))$ by $\alpha' \mapsto x + (q(x))$. Now, since $\Phi$ is an iso and $p(x)$ is the image of $p(x)$ under $\Phi$, we have

$$F(\alpha) \cong F[x]/(p(x)) \cong F'[x]/(q(x)) \cong F'(\alpha').$$

since $F[x]/(p(x)) \xrightarrow{\sim} F'[x]/(q(x))$ by $\Phi$ will also extend $\phi$. Since $\deg p \geq 2$, $[E:F(\alpha)] < [E:F]$. By induction the result follows. $\square$

Thm 18. Let $F$ be a field and $f(x) \in F[x]$ with $\deg f = n \geq 1$. If $E/F$ is the splitting field of $f(x)$, then $[E:F] \mid n!$

Pf. Proceed by induction on $n$. Either $f$ is irreducible or it is not. Suppose it is irreducible. Then if $\alpha \in E$ is a root of $f(x)$, $F(\alpha) \cong F[x]/(f(x))$ and $[F(\alpha):F] = n$ by Thm 8. In $F(\alpha)$, $f(x) = (x-\alpha)g(x)$ and by induction, $[E:F] = [E:F(\alpha)]\, n \mid n!$. Now suppose $f(x)$ is reducible, i.e. $f(x) = g(x)h(x)$ for $\deg g = m \geq 1$ and $\deg h = n-m \geq 1$. Let $K$ be the splitting field of $g(x)$ over $F$. By induction, $[K:F] \mid m!$. Since $E$ is the splitting field of $h(x)$ over $K$, by induction $[E:K] \mid (n-m)!$. Thus

$$[E:F] = [E:K][K:F] \mid m!(n-m)! \mid n!$$

since $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ is an integer. $\square$

## §5. Finite Fields

Def. The prime field of a field $F$ is the intersection of all subfields of $F$.

Thm 19. If $F$ is a field, then its prime field is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ for $p$ a prime number.

Pf. Consider $\chi: \mathbb{Z} \to F$ sending $1 \mapsto 1$, i.e. $\chi(n) = n \cdot 1$. Let $I = \ker \chi$. Since $\mathbb{Z}/I \cong \operatorname{im} \chi \leq F$, it is an integral domain, so $I$ is prime. Hence either $I = (0)$, in which case $\mathbb{Z} \cong \operatorname{im} \chi \leq F$, so $F$ contains $\mathbb{Q}$, the smallest field containing $\mathbb{Z}$; or $I = (p)$ for $p$ a prime and $\operatorname{im} \chi \cong \mathbb{Z}/(p) = \mathbb{Z}_p$.

Def. Given a field $F$, if its prime field is iso to $\mathbb{Q}$ (resp. $\mathbb{Z}_p$), say $F$ has characteristic $0$ ($p$) denoted $\operatorname{ch}(F)$.

PMATH 348 **Characteristic**

22 Jan 2016 Recall Thm 19, every field has zero or prime characteristic.

Note that if $ch(F)=p>0$, for $a,b\in F$ we have

$$(a+b)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + \binom{p}{p}b^p = a^p + b^p.$$

**Prop 20** Let $F$ be a field, $ch(F)=p>0$, $n\in\mathbb{N}$. Then $\psi: F\to F$ given by $u\mapsto u^{p^n}$ is an injective $\mathbb{Z}_p$-homomorphism of fields. If $F$ is finite, $\psi$ is an isomorphism. (Exer.)

**Def** Let $F$ be a field. The monomials $\{1, x, x^2, \dots\}$ form a basis for $F[x]$. Define the operator $D: F[x]\to F[x]$ by $D(1)=0$ and $D(x^n)=nx^{n-1}$ for $n\geq 1$. Then for $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n\in F[x]$, we have $Df(x)=a_1+2a_2x+\cdots+na_nx^{n-1}$. Note that $D$ is a linear map, and satisfies the Leibniz rule: $D(fg)=(Df)g+f(Dg)$. We call $Df=f'$ the formal derivative of $f$.

**Thm 21** Let $F$ be a field and $f(x)\in F[x]$. If $ch(F)=0$, then $f'(x)=0$ iff $f(x)=c\in F$. If $ch(F)=p>0$, then $f'(x)=0$ iff $f(x)=g(x^p)$ for some $g(x)\in F[x]$.

**Pf** In characteristic zero, clearly $Dc=0$ for $c\in F$. Conversely, suppose $f(x)=a_0+a_1x+\cdots+a_nx^n$ satisfies $f'(x)=a_1+2a_2x+\cdots+na_nx^{n-1}=0$. $k\neq 0$ for all $k\geq 1$, so $a_k=0$ for these $k$. Thus $f(x)=a_0\in F$. In characteristic $p>0$, take $g(x)=b_0+b_1x+\cdots+b_mx^m$ and consider $f(x)=g(x^p)=b_0+b_1x^p+\cdots+b_mx^{mp}$. Then

$$f'(x)=pb_1x^{p-1}+2pb_2x^{2p-1}+\cdots+mpb_mx^{mp-1}=0.$$

Conversely, suppose $f'(x)=a_1+2a_2x+\cdots+na_nx^{n-1}=0$, so $ka_k=0$ for $1\leq k\leq n$. Hence, $a_k=0$ unless $p\mid k$, so that $f(x)=a_0+a_px^p+\cdots+a_{(n/p)p}x^{(n/p)p}=g(x^p)$ for $g(x)\in F[x]$. $\square$

**Def** Let $E/F$ be an ext. and $f(x)\in F[x]$. $\alpha\in E$ is a repeated root of $f(x)$ if $f(x)=(x-\alpha)^2g(x)$ for some $g(x)\in E[x]$.

**Thm 22** Let $E/F$ be an ext. and $f(x)\in F[x]$. Then $\alpha\in E$ is a repeated root iff $x-\alpha$ divides both $f$ and $f'$, i.e. $x-\alpha\mid \gcd(f,f')$.

**Rem** Note $\gcd(f,f')\neq 1$ iff $x-\alpha\mid\gcd(f,f')$ for $\alpha$ in some extension of $F$. As a consequence of Thm 22, $f(x)$ has no repeated root in any extension iff $\gcd(f,f')=1$.

**Pf** Suppose $f(x)=(x-\alpha)^2g(x)$. Then

$$f'(x)=(D(x-\alpha)^2)g(x)+(x-\alpha)^2Dg(x)=(x-\alpha)(2g(x)+(x-\alpha)g(x))$$

so $x-\alpha$ divides $f$ and $f'$. Conversely, suppose $x-\alpha$ divides $f$ and $f'$. Write $f(x)=(x-\alpha)g(x)$ for $g(x)\in E[x]$. Then $f'(x)=g(x)+(x-\alpha)g'(x)$, and so $g(\alpha)=f'(\alpha)-(\alpha-\alpha)g'(\alpha)=0$. Thus $g(x)=(x-\alpha)h(x)$ for some $h(x)\in E[x]$. $\square$

## Finite Fields

**Prop 23** If $F$ is a finite field, $ch(F)=p>0$ and $|F|=p^n$ for $n\geq 1$.

**Pf** Since $F$ is finite, its prime field cannot be $\mathbb{Q}$, so it is $\mathbb{Z}_p$ for prime $p$. Then $F$ is a finite-dimensional vector space over $\mathbb{Z}_p$, so $F\cong\mathbb{Z}_p^{\oplus n}$ for $n\geq 1$. $\square$

**Thm 24.** Let $F$ be a finite field. Then any subgroup of $F^*$, the group of units, is cyclic.

In particular, $F^*$ is cyclic, so taking a generator $u$, we see $F\cong\mathbb{Z}_p(u)$ (Cor. 25).

PMATH 348 # More on Finite Fields

25 Jan 2016 Recall Thm 24. Any finite subgroup of the group of units of a field is cyclic.

Pf. Take a finite group $G \leq F^*$. $G$ is finite and abelian, and WLOG non-trivial, so

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

where $n_1 \mid n_2 \mid \cdots \mid n_r$. Since $n_r G = 0$, it follows every $u \in G$ is a root of $x^{n_r} - 1 \in F[x]$. Since the polynomial has at most $n_r$ distinct roots, $r = 1$ so $G$ is cyclic. □

Cor 25 If $F$ is a finite field, $F = \mathbb{Z}_p(u)$ for $p$ prime and some $u \in F$. □

Prop 26 Let $p$ be a prime and $n \in \mathbb{N}$. Then $F$ is a finite field of order $p^n$ iff $F$ is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

Consequently, finite fields are determined up to iso by their order. (Cor 27 (EH Moore).)

Pf. Suppose $|F| = p^n$. Then $|F^*| = p^n - 1$, so every $u \in F^*$ satisfies $u^{p^n - 1} = 1$. Then each $u \in F$ is a root of $x(x^{p^n - 1} - 1) = x^{p^n} - x$. Conversely suppose $F$ is the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. $f'(x) = -1$ since $ch(F) = p$, so $f(x)$ has no repeated roots, i.e. $p^n$ distinct roots. Let $E$ be the set of roots. Consider $\varphi : F \to F$ given by $\varphi(u) = u^{p^n}$. For $u \in F$, $u$ is a root of $f(x)$ iff $\varphi(u) = u$. Thus the set $E$ is a subfield of $F$ of order $p^n$ and contains $\mathbb{Z}_p$. $f(x)$ splits over $E$, so $F \subseteq E$. □

## Separable Polynomials

Def. Let $F$ be a field and $f(x) \in F[x]$ nonzero. If $f(x)$ is irreducible, say $f(x)$ is separable over $F$ if it has no repeated roots in any extension $E$ of $F$. A general $f(x)$ is separable if each irreducible factor is.

E.g. Consider $f(x) = x^n - a \in F[x]$ for $n \geq 2$. If $\gcd(f, f') = 1$, $f(x)$ has no repeated roots, so it is separable. Note that if $a = 0$, the only irreducible factor of $f(x)$ is $x$, which is separable. If $a \neq 0$, note $f'(x) = nx^{n-1}$. If $ch(F) = 0$, $\gcd(f, f') = 1$. If $ch(F) = p > 0$ and $p \nmid n$, gcd is still 1. However, if $p \mid n$, $f'(x) = 0$ so $\gcd(f, f') \neq 1$. Supposing for now $n = p$ we need to find the irreducible factors of $f(x)$ to determine the separability of $f(x)$. Define $F^p = \{b^p \mid b \in F\}$, which is a subfield of $F$. If $a \in F^p$, $a = b^p$ for some $b$ so $f(x) = x^p - a = x^p - b^p = (x - b)^p \in F[x]$, and each $x - b$ factor is separable.

* * * TO BE CONTINUED * * *.

PMATH 348 **Separable Polynomials Continue**

27 Jan 2016 Recall $f(x) \in F[x]$ is separable if all irreducible factors have no repeated roots in any extension of $F$. E.g. Consider $f(x) = x^n - a$ for $n \geq 2$. We have determined that in characteristic zero, $f(x)$ is separable, and in characteristic $p > 0$, if $p \nmid n$ then $f(x)$ is separable. Now suppose $n = p$. If $a \in F^p = \{u^p \mid u \in F\}$, $f(x)$ is separable, so suppose $a \notin F^p$. Claim: $f(x) = x^p - a$ is irred in $F[x]$.

Pf. Cl. Write $f(x) = g(x)h(x)$ for $g(x), h(x) \in F[x]$. Let $E/F$ be an ext where $x^p - a$ has a root, say $\beta \in E$. $\beta \notin F$ since $\beta^p = a \notin F^p$. Now, $x^p - a = x^p - \beta^p = (x-\beta)^p$, so $g(x) = (x-\beta)^r$ and $h(x) = (x-\beta)^s$ for $r+s = p$. Write $g(x) = (x-\beta)^r = x^r - r\beta x^{r-1} + \cdots$. Then $r\beta \in F$ and $\beta \notin F$, so as an element of $F$, $r = 0$. Then $r = 0$ or $r = p$, and it follows $f(x)$ is irreducible. □

Thus we find $x^p - a$ is not separable in this case. In fact, since $f(x) = (x-\beta)^p \in E[x]$, all the roots of $f(x)$ are the same, $f(x)$ is purely inseparable.

Def. A field $F$ is perfect if every (irreducible) polynomial in $F[x]$ is separable over $F$.

Thm 28. Let $F$ be a field. If $F$ has characteristic zero, it is perfect. If $F$ has characteristic $p > 0$, then $F$ is perfect iff $F^p = F$.

Rem. We have already shown that if $F^p \neq F$, $F$ is not perfect.

Pf. Let $r(x) \in F[x]$ be irreducible. Then $\gcd(r, r')$ is either $1$ or $r(x)$. In fact,

$$\gcd(r, r') = \begin{cases} 1 & \text{if } r' \neq 0 \\ r(x) & \text{if } r' = 0 \end{cases}.$$

Suppose $r(x)$ is not separable. Then by (the remark of) Thm 22, $\gcd(r, r') \neq 1$, so $r'(x) = 0$. If $F$ has characteristic zero, by Thm 21, $r'(x) = 0$ implies $r(x)$ is constant, so it is not irreducible — contradiction. If $F$ has characteristic $p > 0$ then by Thm 21, $r(x) = a_0 + a_1 x^p + \cdots + a_n x^{np}$. By the remark, we may assume $F^p = F$. Then $a_i = b_i^p$, so

$$r(x) = b_0^p + b_1^p x^p + \cdots + b_n^p x^{np} = (b_0 + b_1 x + \cdots + b_n x^n)^p$$

$r(x)$ is not irreducible and again there is a contradiction. □

Cor 29. Every finite field is perfect.

Pf. Every finite field is the splitting field of $x^{p^n} - x$ for some $p, n$. Thus, for any $a \in F$, $a = a^{p^n} = (a^{p^{n-1}})^p$, so $F^p = F$ and $F$ is perfect.

PMATH 348 # Return to Group Theory

29 Jan 2016 Recall a group action of a group $G$ on a set $S$ is a function $G \times S \to S$ denoted $(g,x) \mapsto gx$ such that for all $x \in S$, $ex = x$ for $e \in G$ the identity, and for all $g, h \in G$, $g(hx) = (gh)x$. If $G$ acts on $S$, the orbit of $x \in S$ is $\bar{x} = \{gx \mid g \in G\}$ and the stabilizer is $G_x = \{g \in G \mid gx = x\} \leq G$. Recall $|\bar{x}| = [G : G_x]$.

E.g. Let $G$ act on itself by conjugation $(g,h) \mapsto ghg^{-1}$. Then for $x \in G$, the stabilizer

$$C_G(x) = G_x = \{g \in G \mid gxg^{-1} = x\}$$

is called the centralizer of $x$ in $G$. Let $C(G) = \bigcap_{x \in G} C_G(x)$ be the center of $G$.

E.g. Let $S$ be the set of all subgroups of $G$, and let $G$ act on $S$ by conjugation. Then for $H \in S$, the stabilizer

$$N_G(H) = G_H = \{g \in G \mid gHg^{-1} = H\}$$

is called the normalizer of $H$ in $G$.

Recall also the class equation of $G$, $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$, for $x_i \in G \setminus C(G)$ such that the orbits $\bar{x}_i$ are distinct non-central conjugacy classes.

Lem 30 Let $H$ be a group of order $p^n$ for $p$ prime acting on a finite set $S$, and let

$$S_0 = \{x \in S \mid hx = x \text{ for all } h \in H\}.$$

Then $|S| \equiv |S_0| \bmod p$

Pf. For $x \in S$, $|\bar{x}| = 1$ iff $x \in S_0$. So $S = S_0 \cup \bar{x}_1 \cup \cdots \cup \bar{x}_n$ for some choice of $x_i$ with $|\bar{x}_i| > 1$. By Orbit-Stabilizer, $|\bar{x}_i| = [H : H_{x_i}] \mid p^n$ so $p \mid |\bar{x}_i|$ and $|S| = |S_0| + |\bar{x}_1| + \cdots + |\bar{x}_n| \equiv |S_0|$. □

Thm 31. (Cauchy) Let $p$ be a prime and $G$ a finite group. If $p \mid |G|$, then $G$ contains an element of order $p$.

Pf. (J. McKay) Define $S = \{(a_1, a_2, \ldots, a_p) \in G^p \mid a_1 a_2 \cdots a_{p-1} a_p = e\}$. $|S| = |G|^{p-1}$, so since $p \mid |G|$, $|S| \equiv 0 \bmod p$. Let $\mathbb{Z}_p$ act on $S$ by $(k, (a_1, \ldots, a_p)) \mapsto (a_{k+1}, \ldots, a_p, a_1, \ldots, a_k)$. Defining $S_0$ as above, we see $(a_1, \ldots, a_p) \in S_0$ iff $a_1 = a_2 = \cdots = a_p$. $(e, \ldots, e) \in S_0$ so $|S_0| \geq 1$. But by the lemma, $|S_0| \equiv |S| \equiv 0 \bmod p$, so $p \mid |S_0|$ and thus there exists $a \in G \setminus \{e\}$ such that $(a, \ldots, a) \in S_0$. But $S_0 \subseteq S$ so $a \cdots a = a^p = e$. □

Def. Let $p$ be a prime. A group in which every element's order is a nonnegative power of $p$ is called a $p$-group.

Cor 32 A finite group $G$ is a $p$-group iff $|G|$ is a power of $p$.

Def. Let $N$ be a subgroup of $G$. If $gNg^{-1} = N$ for all $g \in G$, $N$ is normal. Write $N \trianglelefteq G$

Lem 33 The center of a nontrivial finite $p$-group is nontrivial.

Pf. Using the class equation, $p \mid p^n = |G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$, and $p \mid [G : C_G(x_i)]$ for each $x_i$, since $[G : C_G(x_i)] \mid |G| = p^n$ and $[G : C_G(x_i)] > 1$ since $x_i \notin C(G)$. Thus $p \mid |C(G)|$ since $C(G) \ni e$. □

PMATH 348 **Sylow Theorems**

1 Feb 2016 Recall Lem 30. If $H$ of order $p^n$ acts on $S$ then $S_0 = \{x \in S \mid hx = x \ \forall h \in H\}$ satisfies $|S| \equiv |S_0| \bmod p$. Recall also Thm 31. If $p \mid |G|$, $G$ contains an element of order $p$.

**Lem 34.** If $H$ is a $p$-subgroup of a finite group $G$, $[N_G(H) : H] \equiv [G : H] \bmod p$.

**Pf** Let $S$ be the set of left cosets of $H$ in $G$, and let $H$ act on $S$ by left translation. Then $|S| = [G : H]$. Then constructing $S_0$ as in Lem 30, we have for $x \in G$,

$$xH \in S_0 \iff hxH = xH \ \forall h \in H \iff x^{-1}hxH = H \ \forall h \in H \iff x^{-1}Hx = H \iff x \in N_G(H),$$

so $|S_0|$ is the number of cosets that have representatives in $N_G(H)$, i.e.

$$[N_G(H) : H] = |S_0| \equiv |S| = [G : H] \bmod p. \ \square$$

**Cor 35.** If $H$ is a $p$-subgroup of finite $G$ such that $p \mid [G : H]$ then $N_G(H) \neq H$. $\square$

**Thm 36.** (First Sylow Thm) Let $G$ be a subgroup of order $p^n m$ for $p$ prime, $n \geq 1$, $\gcd(p, m) = 1$. Then $G$ contains a subgroup of order $p^k$ for all $1 \leq k \leq n$ and each subgroup of order $p^k$ for $k < n$ is normal in some subgroup of $p^{k+1}$.

[take $H$ a subgroup of order $p^k$]

**Pf** Cauchy's Thm gives $k = 1$. Proceed by induction on $k$. $p \mid [G : H]$, so consider the normalizer $N_G(H) \supseteq H$. $p \mid [N_G(H) : H]$ by Cor 35 so $N_G(H)/H$ contains a subgroup $H_1 = H_1/H$ of order $p$. Then $H \trianglelefteq H_1 \leq N_G(H)$, and $|H_1| = |H|[H_1 : H] = p^{k+1}$. $\square$

**Def** $P \leq G$ is a **Sylow $p$-subgroup** if it is a maximal $p$-subgroup of $G$.

**Cor 37** Let $G$ have order $p^n m$, $p$ prime, coprime to $m$. A $p$-subgroup is Sylow iff its order is $p^n$. Also, every conjugate of a Sylow $p$-subgroup is Sylow. Finally, if the Sylow $p$-subgroup is unique, it is normal in $G$. $\square$

**Thm 38.** (Second Sylow Thm) If $H$ is a $p$-subgroup of $G$ and $P$ is a Sylow $p$-subgroup, then there exists a $g \in G$ such that $H \subseteq gPg^{-1}$. In particular, all Sylow $p$-subgroups are conjugate to each other.

**Pf** Let $S$ be the set of left cosets of $P$ in $G$, and let $H$ act on $S$ by left translation. By Lem 30, $|S_0| \equiv |S| = [G : P] \bmod p$. But $p \nmid [G : P]$, so $S_0 \ni xP$ for some $x \in G$.

$$xP \in S_0 \iff hxP = xP \ \forall h \in H \iff x^{-1}hxP = P \ \forall h \in H \iff x^{-1}Hx \subseteq P \iff H \subseteq xPx^{-1}. \ \square$$

# PMATH 348 More Sylow Theorems

3 Feb 2016

Recall Thm 38 (Second Sylow Thm) If $H$ is a $p$-subgroup of $G$ and $P$ is any Sylow $p$-subgroup of $G$, there exists $g \in G$ such that $H \leq gPg^{-1}$. In particular, all Sylow $p$-subgroups of $G$ are conjugate.

Thm 39 (Third Sylow Thm) If $G$ is a finite group and $p$ is a prime, the number of Sylow $p$-subgroups of $G$ divides $|G|$ and is $1 \bmod p$.

Pf. The Sylow $p$-subgroups are all conjugates of one Sylow $p$-subgroup $P$, and the number of conjugates $[G : N_G(P)] \mid |G|$. Now let $S$ be the set of Sylow $p$-subgroups and let $P$ act on $S$ by conjugation. Then $Q \in S_0$ iff $xQx^{-1} = Q$ for all $x \in P$, i.e. $P \subseteq N_G(Q)$. But then $Q \trianglelefteq N_G(Q)$ and $Q$ and $P$ are conjugate, so $Q = P$, $S_0 = \{P\}$, and $|S| \equiv |S_0| = 1 \bmod p$. □

Eg. If $G$ is a group of order 15 and $n_p$ be the number of Sylow $p$-subgroups. $15 = 3 \cdot 5$ so $1 \equiv n_3 \mid 15 \bmod 3$ and $1 \equiv n_5 \mid 15 \bmod 5$. Must have $n_3 = n_5 = 1$, so both $\mathbb{Z}_3$ and $\mathbb{Z}_5$ are normal in $G$. Thus, $G = \mathbb{Z}_3 \times \mathbb{Z}_5 = \langle (1,1) \rangle$ so $G$ is cyclic.

Eg. If $G$ is a group of order 21, $1 \equiv n_7 \mid 21 \bmod 7$ so $n_7 = 1$, but $1 \equiv n_3 \mid 21 \bmod 3$ can lead to either $n_3 = 1$ or $n_3 = 7$. In the former case $\mathbb{Z}_3$ is also normal and $G = \mathbb{Z}_3 \times \mathbb{Z}_7$, but in the latter, it is not as easy. Let $P_7 = \langle x \rangle$ be the 7-Sylow and $H = \langle y \rangle$ a 3-Sylow. $P_7 \trianglelefteq G$ so $yxy^{-1} = x^k$ for $0 \leq k < 7$. It follows $x = y^3 x y^{-3} = y^2 x^k y^{-2} = \cdots = x^{k^3}$ so $k^3 \equiv 1 \bmod 7$, i.e. $k \in \{1, 2, 4\}$. If $k = 1$, $yxy^{-1} = x$, so $yx = xy$ and $G$ is abelian, i.e. $G = P_7 \times H$. If $k = 2$, $yx = x^2 y$, and if $k = 4$, $yx = x^4 y$ which implies $y^2 x = x^{16} y^2 = x^2 y^2$. Mapping $y \mapsto y^2$ we have an iso from $k = 2$ to $k = 4$, and this is valid since $\langle y \rangle = \langle y^2 \rangle$. It follows that there are two isomorphism classes of groups of order 21, abelian and nonabelian.

PMATH 348 # Solvable Groups

5 Feb 2016

**Def.** A group $G$ is solvable if there exist subgroups $G_i$ such that

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1$$

and $G_i/G_{i+1}$ is solvable.

**Rem.** It is not necessary that $G_{i+1} \trianglelefteq G$ — but if that is the case, it implies $G_{i+1} \trianglelefteq G_i$

**Eg** $S_4 \trianglerighteq A_4 \trianglerighteq V_4 = \langle (12),(34) \rangle \cong \mathbb{Z}_2^2 \trianglerighteq 1$, and $S_4/A_4 \cong \mathbb{Z}_2$ and $A_4/V_4 \cong \mathbb{Z}_3$, so $S_4$ is solvable.

**Second Isomorphism Thm.** If $H \leq G \trianglerighteq N$ then $H/H\cap N \cong NH/N$,

**Third Isomorphism Thm.** If $N, H \trianglelefteq G$ and $N \subseteq H$, then $\frac{G/N}{H/N} \cong G/H$.

**Thm 40** If $G$ is a solvable group, every subgroup and quotient of $G$ is solvable. Conversely, if $N \trianglelefteq G$ is solvable and $G/N$ is too, then $G$ is also solvable.

**Pf** Suppose $G$ is solvable, so $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1$ with $G_i/G_{i+1}$ abelian. Then let $H \leq G$ and define $H_i = H \cap G_i$. Then $H = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m = 1$. Observe $H_i, G_{i+1} \leq G_i$ and $H_{i+1} = H \cap G_{i+1} = H_i \cap G_{i+1}$. So, by Second Iso,

$$H_i/H_{i+1} = H_i/H_i \cap G_{i+1} \cong H_i G_{i+1}/G_{i+1} \leq G_i/G_{i+1},$$

and so $H_i/H_{i+1}$ is abelian. Hence $H$ is solvable. Now let $N \trianglelefteq G$, and consider

$$G = G_0 N \geq G_1 N \geq \cdots \geq G_m N = 1 \quad \text{and} \quad G/N = G_0 N/N \geq G_1 N/N \geq \cdots \geq G_m N/N = 1.$$

$G_{i+1} \trianglelefteq G_i$ and $N \trianglelefteq G$, so $G_{i+1}N \trianglelefteq G_i N$ and hence $G_{i+1}N/N \trianglelefteq G_i N/N$. By Third Iso,

$$\frac{G_i N/N}{G_{i+1}N/N} \cong \frac{G_i N}{G_{i+1}N} \cong G_i/G_i \cap G_{i+1}N \hookrightarrow G_i/G_{i+1},$$

which is abelian, so $\frac{G_i N/N}{G_{i+1}N/N}$ is abelian and $G/N$ is solvable.

*** TO BE CONTINUED ***

**Def.** A nontrivial group $G$ is simple if its only normal subgroups are itself and 1.

**E.g** $A_5$ is simple and nonabelian, so it is not solvable. Nor is any group containing it as a subgroup, by Thm 40, so $S_n$ for $n \geq 5$ is not solvable.

PMATH 348 **Solvability**

8 Feb 2016 Recall Thm 40; it remains to prove that if $N \trianglelefteq G$ and $G/N$ are solvable, then so is $G$.

Pf. (cont) Since $N$ is solvable, we have $N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_m = 1$ with $N_i/N_{i+1}$ ab. For $N \leq H \leq G$, write $\bar{H} = H/N$. Then since $G/N$ is solvable, $G/N = \bar{G} = \bar{G}_0 \trianglerighteq \bar{G}_1 \trianglerighteq \cdots \trianglerighteq \bar{G}_r = 1$ with $\bar{G}_i/\bar{G}_{i+1} = (G_i/N)/(G_{i+1}/N) \cong G_i/G_{i+1}$ abelian, where $G_i$ is the preimage of $\bar{G}_i$ under the quotient-by-$N$ map. Thus we have

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_r = N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_m = 1$$

with all quotients abelian. □

Cor 41. $G$ is a finite solvable group iff there exists $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1$ with $G_i/G_{i+1}$ of prime order (and thus cyclic).

Pf. Let $A$ be a finite abelian group. Then $A \cong C_{k_1} \times C_{k_2} \times \cdots \times C_{k_m}$ (cyclic). Recall by Chinese Remainder Theorem, $C \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$. By the first Sylow Thm, we have for any $\mathbb{Z}/p^\alpha\mathbb{Z}$ the tower

$$\mathbb{Z}/p^\alpha\mathbb{Z} \trianglerighteq \mathbb{Z}/p^{\alpha-1}\mathbb{Z} \trianglerighteq \cdots \trianglerighteq \mathbb{Z}/p\mathbb{Z} \trianglerighteq 1$$

with quotients $\cong \mathbb{Z}/p\mathbb{Z}$. Hence, each $G_i \trianglerighteq G_{i+1}$ can be decomposed into a tower where the quotients have prime order. □

## Automorphism Groups

Def. Let $E/F$ be a field extension. If $\psi : E \xrightarrow{\sim} E$ is an automorphism and $\psi|_F = \mathrm{Id}$, then say $\psi$ is an $F$-auto or an auto of $E/F$. The set of $F$-autos on $E$ form a group denoted $\mathrm{Aut}_F(E) = \{\psi : E \xrightarrow{\sim} E \ F\text{-auto}\}$, the automorphism group of $E/F$.

Lem 42. Let $E/F$ be a field ext, $f(x) \in F[x]$, and $\psi \in \mathrm{Aut}_F(E)$. If $\alpha \in E$ is a root of $f(x)$, then so is $\psi(\alpha)$. Pf. $f(\psi(\alpha)) = \psi(f(\alpha)) = \psi(0) = 0$. □

Lem 43. Let $E = F(\alpha_1, \ldots, \alpha_n)/F$. For $\psi, \psi' \in \mathrm{Aut}_F(E)$, if $\psi(\alpha_i) = \psi'(\alpha_i)$ for all $\alpha_i$ then $\psi = \psi'$. □

Cor 44. If $E/F$ is a finite extension, $\mathrm{Aut}_F(E)$ is a finite group.

Pf. $E = F(\alpha_1, \ldots, \alpha_n)$ for $\alpha_i$ algebraic/$F$, by Thm 10. For $\psi \in \mathrm{Aut}_F(E)$, $\psi(\alpha_i)$ must be a root of the minimal poly of $\alpha_i$, so there are at most finitely many choices of image of $\alpha_i$. $\psi$ is determined by these images, so $\mathrm{Aut}_F(E)$ must be finite. □

PMATH 348 **Galois Groups Continued**

10 Feb 2016 Recall $\mathrm{Aut}_F(E) = \{\psi : E \xrightarrow{\sim} E \text{ fixes } F\}$.

**Cor 44** If $E/F$ is a finite extension, then $\mathrm{Aut}_F(E)$ is finite. □

**Rem** The converse is false: $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R}) \leq \mathrm{Aut}(\mathbb{R}) = 1$. (Exer.)

**Def** Let $F$ be a field and $f(x) \in F[x]$. If $E/F$ is the splitting field of $f(x)$, say $\mathrm{Aut}_F(E)$ is the automorphism group of $f(x)$ over $F$.

Recall **Thm 16.** $\phi : F \xrightarrow{\sim} F'$ and $f(x) \in F[x]$, $\Phi : F[x] \xrightarrow{\sim} F'[x]$ extending $\phi$, $E$ ($E'$) splitting field of $f(x)$ ($\Phi(f(x))$), then there exists $\psi : E \xrightarrow{\sim} E'$ extending $\phi$.

**Exer** Prove that the number of such $\psi$'s is at most $[E:F]$, with equality iff $f(x)$ is separable.

**Thm 45** Let $E/F$ be the splitting field of $f(x) \in F[x]$ nonzero. Then $|\mathrm{Aut}_F(E)| \leq [E:F]$, with equality iff $f(x)$ is separable. *Pf* Follows by exer. □

**E.g.** Let $F$ be a field of characteristic $p > 0$, and suppose $F^p \neq F$. Take $x^p - a \in F[x]$ with $a \in F \setminus F^p$, and let $E$ be its splitting field. $f(x) = (x-\beta)^p$ for $\beta \in E$ so $E = F(\beta)$. Since $\beta$ is the only root of $f(x)$, $\mathrm{Aut}_F(E) = 1 < p = \deg f = [E:F]$.

**Thm 46.** If $f(x) \in F[x]$ has $n$ distinct roots in the splitting field $E$, then $\mathrm{Aut}_F(E)$ is isomorphic to a subgroup of the symmetric group $S_n$. In particular, $|\mathrm{Aut}_F(E)| \mid n!$

*Pf.* Let $X = \{\alpha_1, \ldots, \alpha_n\}$ be the distinct roots of $f(x)$ in $E$. By Lem 42, if $\psi \in \mathrm{Aut}_F(E)$, then $\psi(X) = X$. Let $S_X \cong S_n$ be the symmetric group on $X$. Then

$$\mathrm{Aut}_F(E) \longrightarrow S_X \qquad \psi \longmapsto \psi|_X$$

is a group homomorphism, and injective by Lem 43. Hence, $\mathrm{Aut}_F(E)$ is isomorphic to a subgroup of $S_n$. □

**E.g.** Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and $E/\mathbb{Q} = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ its splitting field. $[E:F] = 6$, so $|\mathrm{Aut}_F(E)| = 6$ since $f(x)$ is separable. $f(x)$ has three distinct roots, so $\mathrm{Aut}_F(E) \leq S_3$, and since $|S_3| = 6$, $\mathrm{Aut}_F(E) \cong S_3$

## Fixed Fields

**Def** Let $E/F$ and $\psi \in \mathrm{Aut}_F(E)$. Define $E^\psi = \{a \in E \mid \psi(a) = a\}$ the fixed field of $\psi$. Note that $F \subseteq E^\psi \subseteq E$. If $G \leq \mathrm{Aut}_F(E)$, we can also discuss the fixed field of $G$,

$$E^G = \bigcap_{\psi \in G} E^\psi = \{a \in E \mid \psi(a) = a \text{ for all } \psi \in G\}.$$

**Thm 47.** Let $f(x) \in F(x)$ be separable and $E/F$ its splitting field. Then $E^{\mathrm{Aut}_F(E)} = F$.

*Pf.* Write $G = \mathrm{Aut}_F(E)$ and $L = E^G$. $F \subseteq L$ and so $\mathrm{Aut}_L(E) \leq G$. On the other hand, if $\psi \in G$, by the definition of $L$, $\psi(a) = a$ for all $a \in L$, so $\psi \in \mathrm{Aut}_L(E) = G$. Since $f(x)$ is separable, * * * TO BE CONTINUED * * *

PMATH 348 The Galois and the Groups: Tokyo Drift

12 Feb 2016

Recall Thm 47. Let $f(x) \in F[x]$ be separable with splitting field $E/F$. Then if $G = Aut_F(E)$, $E^G = F$.

Pf. (cont) Let $L = E^G$. We have seen that $Aut_F(E) = Aut_L(E)$. Since $f(x)$ is separable over $F$ and splits over $E$, $f(x)$ is also separable over $L$ and has $E$ as its splitting field over $L$. By Thm 45, we have

$$[E:L][L:F] = [E:F] = |Aut_F(E)| = |Aut_L(E)| = [E:L]$$

and hence $[L:F] = 1$, that is, $L = F$. □

## §8. Galois Extensions

**Def.** Let $E/F$ be an algebraic field extension. Let $p(x) \in F[x]$ be the minimal polynomial of $\alpha \in E$. $\alpha$ is *separable* over $F$ if $p(x)$ is separable. If all $\alpha \in E$ are separable, $E/F$ is a *separable extension*.

**Thm 48** Let $E/F$ be the splitting field of $f(x) \in F[x]$. If $f(x)$ is separable, then $E/F$ is separable.

**Pf** Let $p(x) \in F[x]$ be the minimal polynomial of $\alpha \in E$, and let $\{\alpha = \alpha_1, \alpha_2, \dots, \alpha_n\} \subseteq E$ be the distinct roots of $p(x)$. Define $\tilde{p}(x) = (x-\alpha_1)\cdots(x-\alpha_n) \in E[x]$. Let $G = Aut_F(E)$ and $\psi \in G$. By Lem 42, $\psi$ permutes $\alpha_1, \dots, \alpha_n$, the roots of $\tilde{p}(x)$. Thus,

$$\psi(\tilde{p}(x)) = (x-\psi(\alpha_1))\cdots(x-\psi(\alpha_n)) = (x-\alpha_1)\cdots(x-\alpha_n) = \tilde{p}(x)$$

and so $\tilde{p}(x) \in E^\psi[x]$. $\psi \in G$ was arbitrary, so $\tilde{p}(x) \in \left(\bigcap_{\psi\in G} E^\psi\right)[x] = E^G[x]$. $f(x) \in F[x]$ is separable and $E$ is the splitting field of $f(x)$, so by Thm 47, $E^G = F$.

By construction, $\tilde{p}(\alpha) = 0$, so $p(x) \mid \tilde{p}(x)$, but since the roots of $\tilde{p}(x)$ are the distinct roots of $p(x)$, $p(x) \mid \tilde{p}(x)$. $\tilde{p}(x)$ is monic, so $p(x) = \tilde{p}(x)$, which by the construction of $\tilde{p}(x)$ is a separable polynomial. Hence $\alpha$ is separable, and since $\alpha \in E$ was ~~arbitrary~~, $E/F$ is also separable. □

**Rem.** By Thm 28, if $F$ has characteristic 0, it is perfect, so all polynomials in $F[x]$ are separable and thus every algebraic extension of $F$ is separable.

**Cor 49.** Let $E/F$ be a finite extension, where $E = F(\alpha_1, \dots, \alpha_n)$. If each $\alpha_i$ is separable, then $E/F$ is separable.

**Pf.** Let $p_i(x) \in F[x]$ be the minimal polynomial of $\alpha_i$. $f(x) = p_1(x)\cdots p_n(x)$ is separable since each $\alpha_i$ was separable, so by Thm 48, the splitting field $L/F$ of $f(x)$ is separable. $L \ni \alpha_1, \dots, \alpha_n$, so $E \subseteq L$, and thus $E/F$ is also separable. □

**Cor 50.** Let $E/F$ be an algebraic extension and $L = \{\alpha \in E \mid \alpha \text{ is separable}\}$. Then $L$ is a field.

**Pf.** Let $\alpha, \beta \in L$. $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in F(\alpha,\beta)$ (when $\beta \neq 0$), which is a separable extension by Cor 49, so $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in L$, and thus $L$ is a field. □

**Def.** Let $E = F(\alpha)$ be a simple extension. Then $\alpha$ is a *primitive element* of $E/F$.

**Thm 51.** (Primitive Element Theorem) If $E/F$ is a finite separable extension, then $E/F$ is simple. In particular, every finite extension in characteristic zero is simple.

PMATH 348 # Primitive Element Theorem

22 Feb 2016 Recall that an algebraic extension $E/F$ is separable if the minimal poly of each $\alpha \in E$ is separable.

**Thm 51.** (Artin) If $E/F$ is a finite separable extension, $E/F$ is simple.

**Pf** Note that finite extensions of finite fields are finite and hence simple, so WLOG $F$ is an infinite field. By induction, it suffices to consider the case $E = F(\alpha, \beta)$. Let $\gamma = \alpha + \lambda\beta$ for $\lambda \in F$. If $\beta \in F(\gamma)$, then $\alpha = \gamma - \lambda\beta \in F(\gamma)$ so $E = F(\gamma)$ and we are done. Let $a(x)$ and $b(x)$ be the minimal polynomials of $\alpha$ and $\beta$ over $F$. $\beta \notin F$ so $\deg b > 1$ and so there exists a root $\tilde{\beta} \neq \beta$ of $b(x)$. Then choose $\lambda \in F$ such that

$$\lambda \neq \frac{\tilde{\alpha} - \alpha}{\beta - \tilde{\beta}}$$

for all roots $\tilde{\alpha}$ of $a(x)$ and roots $\tilde{\beta} \neq \beta$ of $b(x)$ in the splitting field of $a(x)b(x)$ over $F$. This choice is possible since $F$ is infinite and $\deg a, \deg \beta < \infty$. Consider

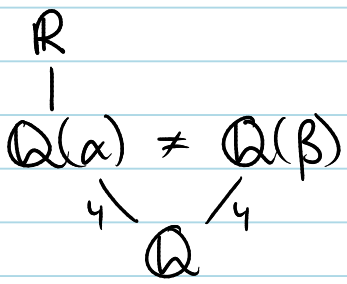
$$f(x) = a(\gamma - \lambda x) \in F(\gamma)[x].$$

$f(\beta) = a(\gamma - \lambda\beta) = a(\alpha) = 0$, but for $\tilde{\beta} \neq \beta$, $\gamma - \lambda\tilde{\beta} = \alpha + \lambda(\beta - \tilde{\beta}) \neq \tilde{\alpha}$ for any $\tilde{\alpha}$, so $f(\tilde{\beta}) = a(\gamma - \lambda\tilde{\beta}) \neq a(\tilde{\alpha}) = 0$. Thus, the minimal polynomial $c(x) \in F(\gamma)[x]$ of $\beta$ divides both $f(x)$ and $b(x)$. $E/F$ is separable, so $b(x) \in F[x]$ has distinct roots, $c(x)$ does as well. $c(x) \mid \gcd(b(x), f(x)) = x - \beta$ so $c(x) = x - \beta$ and $\beta \in F(\gamma)$. This completes the proof. $\square$

## Normal Extensions

**Def** Let $E/F$ be algebraic. $E/F$ is a <u>normal extension</u> if for any irreducible $f(x) \in F[x]$, either $f(x)$ has no roots in $E$ or it splits in $E$.

**E.g.** Let $\alpha \in \mathbb{R}$ satisfy $\alpha^4 = 5$, and let $\beta = (1+i)\alpha$. $\pm\alpha \in \mathbb{Q}(\alpha)$ but $\pm i\alpha \notin \mathbb{Q}(\alpha)$, and $\pm\alpha$ and $\pm i\alpha$ are the roots of $x^4 - 5 \in \mathbb{Q}[x]$, so $\mathbb{Q}(\alpha)$ is not normal / $\mathbb{Q}$. $\mathbb{Q}(\beta)$ is also not normal — note that $\beta^4 = (2i\alpha^2)^2 = -4\alpha^4 = -20$, so $\pm\beta, \pm i\beta$ are the roots of $x^4 + 20$, so it would suffice to show $i \notin \mathbb{Q}(\beta)$, which reduces to $\alpha \notin \mathbb{Q}(\beta)$, which follows because $\mathbb{Q}(\alpha)$ is a real field and so cannot equal $\mathbb{Q}(\beta)$.



PMATH 348 **Hundo Hype**

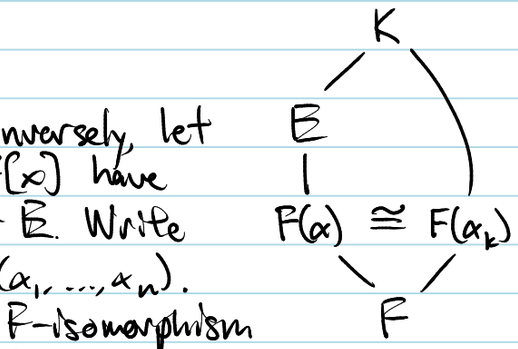
26 Feb 2016 Recall $E/F$ is normal if every irreducible $p(x) \in F[x]$ has either no roots in $E$ or splits.

**Thm 52** A finite extension $E/F$ is normal iff it is the splitting field of some $f(x) \in F[x]$.

**Pf.** Suppose $E/F$ is normal. $E = F(\alpha_1, \dots, \alpha_n)$ is finite, so take $p_k(x) \in F[x]$ the minimal polynomial of $\alpha_k$. Since $E$ is normal and $p_k(\alpha_k) = 0$, each $p_k$ splits and so

$$E = F(\text{all roots of } p_k \mid 1 \le k \le n),$$

i.e. $E$ is the splitting field of the product $p_1(x) \cdots p_n(x)$. Conversely, let $E/F$ be the splitting field of some $f(x) \in F[x]$. Let $p(x) \in F[x]$ have a root $\alpha \in E$, and let $K/E$ be the splitting field of $p(x)$ over $E$. Write $p(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ for $c \in F^*$, $\alpha = \alpha_1 \in E$, $\alpha_2, \dots, \alpha_n \in K = E(\alpha_1, \dots, \alpha_n)$. Since $F(\alpha) \cong F[x]/(p(x)) \cong F(\alpha_k)$ for $1 \le k \le n$, we have the $F$-isomorphism $\phi : F(\alpha) \to F(\alpha_k)$. Note that $p(x) f(x) \in F[x] \subseteq F(\alpha_i)[x]$ for all $i$, so we can view $K$ as the splitting field of $p(x)f(x)$ over $F(\alpha_i)$ for each $i$. By Thm 16, there exists an $F$-isomorphism $\psi : K \to K$ extending $\phi$. In particular, $\psi \in \mathrm{Aut}_F(K)$, so it permutes the roots of $f(x)$. $E$ is the splitting field of $f(x)$, so $\psi(E) = E$ and it follows $\alpha_k = \psi(\alpha) \in E$, so $K = E$ and $p(x)$ splits over $E$. Hence, $E/F$ is normal. □




**E.g.** We will show every quadratic extension — $E/F$ with $[E:F] = 2$ — is normal. Let $\alpha \in E \setminus F$, so $E = F(\alpha)$. Let $p(x) = x^2 + ax + b$ be the minimal polynomial of $\alpha$ over $F$. If $\beta$ is another root of $p(x)$, $p(x) = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$, i.e. $\beta = b/\alpha \in E$. Hence $E$ is the splitting field of $p(x)$ over $F$, and it follows that $E/F$ is normal by Thm 52.

**E.g.** $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not a normal extension, because $x^4 - 2$ has a root in $\mathbb{Q}(\sqrt[4]{2})$, but does not split since $i\sqrt[4]{2} \notin \mathbb{R} \supseteq \mathbb{Q}(\sqrt[4]{2})$. Note, however, that both $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ are quadratic extensions, and hence normal, so we observe that the composition of normal extensions is not necessarily itself normal.

**Prop 53.** If $E/F$ is a normal extension and $F \subseteq K \subseteq E$, then $E/K$ is normal.

**Pf.** *** TO BE CONTINUED ***

PMATH 348 **Things**

29 Feb 2016 Recall Thm 52. A finite extension $E/F$ is normal iff it is the splitting field of some $f(x) \in F[x]$.

**Prop 53.** If $E/F$ is a normal extension and $K$ an intermediate field, $E/K$ is normal.

**Pf** Let $p(x) \in K[x]$ be irreducible with a root $\alpha \in E$. Let $f(x) \in F[x]$ be the minimal polynomial of $\alpha$ over $F$ — $p(x) \mid f(x)$, so if $f(x)$ splits, then so does $p(x)$. $E/F$ is normal, so every such $f(x)$ splits, and hence $E/K$ is normal. □

**Rem.** Note that $K/F$ need not be normal.

**Prop 54.** Let $E/F$ be a normal extension and $\alpha, \beta \in E$. The following are equivalent: (1) $\alpha$ and $\beta$ have the same minimal polynomial (2) there exists $\psi \in Aut_F(E)$ such that $\psi(\alpha) = \beta$.

**Pf.** (2) $\Rightarrow$ (1) Let $p(x)$ be the min poly of $\alpha$ over $F$ and $\psi \in Aut_F(E)$ with $\psi(\alpha) = \beta$. Write $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, so that

$$p(\beta) = a_0 + a_1\beta + \cdots + a_n\beta^n = \psi(a_0) + \psi(a_1)\psi(\alpha) + \cdots + \psi(a_n)\psi(\alpha^n) = \psi(p(\alpha)) = 0.$$

Hence $p(x)$ is the minimal polynomial of $\beta$ over $F$, the same as $\alpha$.

(1) $\Rightarrow$ (2). Suppose both $\alpha$ and $\beta$ have the same min poly $p(x)$ over $F$. We have that $F(\alpha) \cong F[x]/(p(x)) \cong F(\beta)$ so there exists an $F$-isomorphism $\phi: F(\alpha) \xrightarrow{\sim} F(\beta)$ with $\phi(\alpha) = \beta$. By Thm 52, $E$ is the splitting field of some poly $f(x) \in F[x]$ over $F$, so it is also the splitting field of $f(x)$ over $F(\alpha)$ and $F(\beta)$ respectively. Hence there exists an $F$-isomorphism $\psi: E \xrightarrow{\sim} E$ extending $\phi$, that is, with $\psi(\alpha) = \beta$. □

**Def** A **normal closure** $N/F$ of a finite extension $E/F$ satisfies $E \subseteq N$ and for all $L$ intermediate fields of $N/E$, if $L$ is normal, then $L = N$.

**Thm 55.** Every finite extension $E/F$ has a normal closure that is unique up to $E$-isomorphism.

**Pf.** $E = F(\alpha_1, \ldots, \alpha_n)$. Let $p_i(x) \in F[x]$ be the minimal polynomial of $\alpha_i$ over $F$, and let $N/E$ be the splitting field of the product $p_1(x) \cdots p_n(x)$ over $E$, or equivalently over $F$. By Thm 52, $N$ is normal over $F$. Letting $L$ be an intermediate field of $N/E$, $L$ contains each $\alpha_i$, so it must split $p_1(x) \cdots p_n(x)$ if it is normal, i.e. $L \supseteq N$. This proves existence. Now, let $N/E$ be as obtained above and $N'/E$ another normal closure. $N'$ is normal over $F$ and contains all the $\alpha_i$, so $N' \supseteq \tilde{N}$ the splitting field of $p_1(x) \cdots p_n(x)$ over $F$, and thus over $E$. By Cor 17, $N$ and $\tilde{N}$ are $E$-isomorphic. Being a splitting field, $\tilde{N}$ is normal over $F$, so $N' = \tilde{N} \cong N$. □

PMATH 348 # Galois Correspondence

2 & 4 Mar 2016 Recall that for a finite extension $E/F$, by Thm 52, $E$ is normal iff it is the splitting field of some $f(x) \in F[x]$. Also, by Thm 48, $E$ is separable if it is the splitting field of a separable polynomial $f(x) \in F[x]$.

**Def.** An algebraic extension $E/F$ is **Galois** if it is normal and separable. The **Galois group** $\mathrm{Gal}_F(E)$ of a Galois extension $E/F$ is the automorphism group $\mathrm{Aut}_F(E)$. A Galois extension is **abelian**, **cyclic**, or **solvable** if the Galois group has that property.

**Rem.** By Thm 48 and Thm 52, a finite Galois extension is the splitting field of a separable polynomial with coefficients in the base field. If $E/F$ is the Galois extension of $f(x) \in F[x]$ separable of degree $n$, then $\mathrm{Gal}_F(E) \hookrightarrow S_n$, by Thm 46. Also, by Thm 45,

$$|\mathrm{Gal}_F(E)| = [E:F].$$

**E.g.** Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ be the splitting field of $(x^2-2)(x^2-3)(x^2-5) \in \mathbb{Q}[x]$, which is a separable polynomial. Then $[E:\mathbb{Q}] = 8$. Since $\psi \in \mathrm{Gal}_{\mathbb{Q}}(E)$ must have $\psi(\sqrt{p}) \in \{\pm\sqrt{p}\}$ for $p = 2, 3$, and $5$, and $|\mathrm{Gal}_{\mathbb{Q}}(E)| = [E:\mathbb{Q}] = 8$, we see $\mathrm{Gal}_{\mathbb{Q}}(E) \cong \mathbb{Z}_2^3$.

**Thm 56.** (Artin) Let $E$ be a field and $G$ a finite subgroup of $\mathrm{Aut}(E)$. Recall that $E^G = \bigcap_{\psi \in G} E^\psi = \{\alpha \in E \mid \psi(\alpha) = \alpha \text{ for all } \psi \in G\}$. Then $E/E^G$ is a finite Galois extension and $\mathrm{Gal}_{E^G}(E) = G$.

**Pf.** Let $n = |G|$, $F = E^G$, and $\alpha \in E$. Consider the orbit of $\alpha$ under the obvious action of $G$, i.e. $\bar{\alpha} = \{\psi(\alpha) \mid \psi \in G\} = \{\alpha = \alpha_1, \dots, \alpha_m\}$, which is finite because $G$ is. Note $m \le n$. Let $f(x) = (x-\alpha_1)\cdots(x-\alpha_m)$. Each $\psi \in G$ permutes $\alpha_1, \dots, \alpha_m$, so since the coefficients of $f(x)$ are symmetric w.r.t. $\bar{\alpha}$, $f(x) \in E^G[x] = F[x]$. Let $g(x)$ be a factor of $f(x)$, WLOG $g(x) = (x-\alpha_1)\cdots(x-\alpha_\ell)$. If $\ell \neq m$, there exists $\psi \in G$ with $\{\alpha_1, \dots, \alpha_\ell\} \neq \{\psi(\alpha_1), \dots, \psi(\alpha_\ell)\}$, so $g(x) \notin F[x]$. Hence $f(x)$ is the minimal polynomial of $\alpha$ over $F$, and since it is separable by construction, $E$ is a Galois extension.

Now suppose for a contradiction that $[E:F] > n$. Then there exist $F$-linearly independent $\beta_1, \dots, \beta_{n+1} \in E$. Consider the system $\psi(\beta_1)v_1 + \cdots + \psi(\beta_{n+1})v_{n+1} = 0$ for all $\psi \in G$ of $n$ linear equations in $n+1$ variables $v_i$. It has a nonzero solution in $E$, so let $(\gamma_1, \dots, \gamma_{n+1})$ be such a solution, with the minimal number of nonzero coordinates. WLOG $\gamma_1, \dots, \gamma_r$ are the nonzero coordinates, and note that clearly $r > 1$. So $\psi(\beta_1)\gamma_1 + \cdots + \psi(\beta_r)\gamma_r = 0$ for all $\psi \in G$; call this system $(*)$. By rescaling, WLOG we may take $\gamma_r = 1$. Looking at $(*)$ for $\psi = \mathrm{id} \in G$, we see that $\beta_1\gamma_1 + \cdots + \beta_r\gamma_r = 0$ — but since $\beta_1, \dots, \beta_r$ are linearly independent over $F$, some $\gamma_i \notin F$, WLOG $i > 1$. Choose $\phi \in G$ with $\phi(\gamma_1) \neq \gamma_1$, and then $0 = \phi(0) = \phi(\psi(\beta_1)\gamma_1 + \cdots + \psi(\beta_r)\gamma_r) = \phi\psi(\beta_1)\phi(\gamma_1) + \cdots + \phi\psi(\beta_r)\phi(\gamma_r)$ for all $\psi \in G$. Rewriting $\psi \mapsto \phi^{-1}\psi$, since $G$ is a group, we obtain $\psi(\beta_1)\phi(\gamma_1) + \cdots + \psi(\beta_r)\phi(\gamma_r) = 0$ for all $\psi \in G$; call this system $(**)$. Subtracting $(**)$ from $(*)$, we see, for all $\psi \in G$,

$$\psi(\beta_1)(\gamma_1 - \phi(\gamma_1)) + \cdots + \psi(\beta_r)(\gamma_r - \phi(\gamma_r)) = 0,$$

so $(\gamma_1 - \phi(\gamma_1), \dots, \gamma_r - \phi(\gamma_r), 0, \dots, 0)$ is a solution to the original system. Because $\gamma_1 \neq \phi(\gamma_1)$, this solution is not trivial, but since $\gamma_r = 1$, $\phi(\gamma_r) = 1 = \gamma_r$, so this solution has one more zero coordinate than $(\gamma_1, \dots, \gamma_r, 0, \dots, 0)$, contradicting the minimality assumption. Hence, $[E:F] \le n$.

So $E/F$ is a finite Galois extension. Thus, it is the splitting field of some polynomial over $F$. Since $F = E^G = \{\alpha \in G \mid \psi(\alpha) = \alpha \text{ for all } \psi \in G\}$, $G$ is a subgroup of $\mathrm{Gal}_F(E)$ by Thm 45 $n = |G| \le |\mathrm{Gal}_F(E)| = [E:F] \le n$, so $G = \mathrm{Gal}_F(E)$. $\square$

**Rem.** Let $E/E^G$ be a finite Galois extension with Galois group $G$. For $\alpha \in E$, let $\bar{\alpha} = \{\alpha = \alpha_1, \dots, \alpha_n\}$ be the orbit of $\alpha$ under the natural action of $G \le \mathrm{Aut}(E)$. Then the minimal polynomial of $\alpha$ over $E^G$ is $(x-\alpha_1)\cdots(x-\alpha_n) \in E^G[x]$.

**E.g.** Let $E = F(t_1, \dots, t_n)$ be the field of rational functions in $n$ variables over $F$. Consider the symmetric group $S_n$ as a subgroup of $\mathrm{Aut}(E)$, consisting of $F$-isomorphisms that permute $\{t_1, \dots, t_n\}$ — call this subgroup $G$. We will find $E^G$. By the above remark, the minimal poly of $t_1$ over $E^G$ is $f(x) = (x-t_1)\cdots(x-t_n) \in E^G$. Define the **elementary symmetric functions** of $t_1, \dots, t_n$ as, for $1 \le k \le n$,

$$s_k = s_k(t_1, \dots, t_n) = \sum_{\substack{A \subseteq \{1, \dots, n\} \\ |A| = k}} \prod_{i \in A} t_i$$

so e.g. $s_1 = t_1 + \cdots + t_n$, $s_2 = t_1t_2 + t_1t_3 + t_2t_3 + \cdots + t_{n-1}t_n$, $\dots$, $s_n = t_1t_2\cdots t_n$. Observe (?) that $f(x) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n \in L[x]$ for $L = F(s_1, \dots, s_n) \le E^G$. $L$ is the splitting field of $f(x)$ over $L$. Since $\deg f = n$, Thm 18 gives us that $[E:L] \le n!$. Well, by Thm 56, $n! = |S_n| = |G| = [E:E^G] \le [E:L] \le n!$, so $E^G = L$.

PMATH 348 **The Fundamental Theorem of Galois Theory**

7 Mar 2016 **Thm 57.** Let $E/F$ be a finite Galois extension and $G = \mathrm{Gal}_F(E)$. There is an inclusion-reversing bijective correspondence between the intermediate fields of $E/F$ and the subgroups of $G$. More precisely, the correspondence

$$\left\{\begin{matrix}\text{intermediate}\\ \text{fields of } E/F\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{subgroups}\\ \text{of } G\end{matrix}\right\}$$

$$L \longmapsto \mathrm{Gal}_L(E)$$

$$E^H \longleftarrow H$$

satisfies $L \subseteq L' \Leftrightarrow \mathrm{Gal}_L(E) \supseteq \mathrm{Gal}_{L'}(E)$ and $H \subseteq H' \Leftrightarrow E^H \supseteq E^{H'}$. In fact, $[L' : L] = [\mathrm{Gal}_L(E) : \mathrm{Gal}_{L'}(E)]$ and $[H' : H] = [E^H : E^{H'}]$.

**Pf.** Let $L$ be an intermediate field of $E/F$ and $H$ be a subgroup of $\mathrm{Gal}_F(E)$. Then $E^{\mathrm{Gal}_L(E)} = L$ by Thm 47. Also, $\mathrm{Gal}_{E^H}(E) = H$ by Thm 56. Hence the correspondence is bijective. Let $L'$ be another intermediate field. By Prop 53, $E/L$ and $E/L'$ are Galois, so $L \subseteq L' \Leftrightarrow \mathrm{Gal}_L(E) \supseteq \mathrm{Gal}_{L'}(E)$. Also,

$$[L' : L] = \frac{[E : L]}{[E : L']} = \frac{|\mathrm{Gal}_L(E)|}{|\mathrm{Gal}_{L'}(E)|} = [\mathrm{Gal}_L(E) : \mathrm{Gal}_{L'}(E)].$$

Similarly, if $H, H' \leq G$ then $H \subseteq H' \Leftrightarrow E^H \supseteq E^{H'}$, and also

$$[H' : H] = \frac{|H'|}{|H|} = \frac{|\mathrm{Gal}_{E^{H'}}(E)|}{|\mathrm{Gal}_{E^H}(E)|} = \frac{[E : E^{H'}]}{[E : E^H]} = [E^H : E^{H'}]. \quad \square$$

We have seen an example before that if $E/F$ is Galois and $L$ is an intermediate field, then $L/F$ is not necessarily Galois. What we will see is that $L/F$ is Galois iff $\mathrm{Gal}_L(E) \trianglelefteq \mathrm{Gal}_F(E)$.

**Thm 58.** Let $E/F$ be a finite Galois extension with Galois group $G$. Let $L$ be an intermediate field of $E/F$. Then for $\psi \in G$, $\mathrm{Gal}_{\psi(L)}(E) = \psi \mathrm{Gal}_L(E) \psi^{-1}$.

**Pf** For $\alpha \in \psi(L)$, $\psi^{-1}(\alpha) \in L$. If $\phi \in \mathrm{Gal}_L(E)$, then $\phi\psi^{-1}(\alpha) = \psi^{-1}(\alpha)$, so $\psi\phi\psi^{-1}(\alpha) = \alpha$, i.e. $\psi\phi\psi^{-1} \in \mathrm{Gal}_{\psi(L)}(E)$ for all $\phi \in \mathrm{Gal}_L(E)$. Hence $\psi \mathrm{Gal}_L(E) \psi^{-1} \subseteq \mathrm{Gal}_{\psi(L)}(E)$. Since the two groups have the same order, they are equal. $\square$

**Thm 59.** Let $E/F$ be a finite Galois extension with Galois group $G$ and an intermediate field $L$. Then $L/F$ is Galois iff $\mathrm{Gal}_L(E) \trianglelefteq G$, and then $\mathrm{Gal}_F(L) \cong G/\mathrm{Gal}_L(E)$.

PMATH 348 **Consequences of the Fundamental Theorem**

9 Mar 2016 Recall the inclusion-reversing correspondence between the intermediate fields of a finite Galois extension $E/F$ and the subgroups of its Galois group $G = \mathrm{Gal}_F(E)$: we have field $L \mapsto L^* = \mathrm{Gal}_L(E)$ and subgroup $H \mapsto H^* = E^H$.

**Thm 59.** Let $E/F$ be a finite Galois extension with Galois group $G$ and an intermediate field $L$. Then $L/F$ is Galois iff $L^* \trianglelefteq G$, and then $\mathrm{Gal}_F(L) \cong G/L^*$.

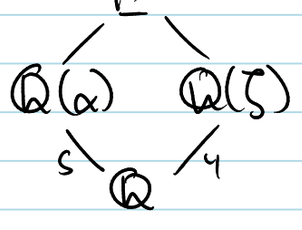
**Pf** $L/F$ is normal iff $\psi(L) = L$ for all $\psi \in G$ iff $L^* = \mathrm{Gal}_L(E) \cong \mathrm{Gal}_{\psi(L)}(E) = \psi\,\mathrm{Gal}_L(E)\,\psi^{-1}$ for all $\psi \in G$, by Thm 58. This condition is exactly that $L^* \trianglelefteq G$. Now, if $L/F$ is Galois, the restriction maps $G \to \mathrm{Gal}_F(L)$ given by $\psi \mapsto \psi|_L$ is well-defined. Moreover, it is surjective with kernel $L^*$, so by First Iso, $\mathrm{Gal}_F(L) \cong G/L^*$.

**Eg** Let $q = p^n$ for prime $p$ and consider the finite field $\mathbb{F}_q$ of order $q$ as an extension of $\mathbb{F}_p$ of degree $n$. The Frobenius map $\sigma_p : \mathbb{F}_q \to \mathbb{F}_q$ given by $\sigma_p(\alpha) = \alpha^p$ is an automorphism of $\mathbb{F}_q$. Since $\mathbb{F}_q$ is the splitting field of $x^q - x \in \mathbb{F}_p[x]$, $\sigma_p^n(\alpha) = \alpha^{p^n} = \alpha^q = \alpha$ for all $\alpha \in \mathbb{F}_q$, so $\sigma_p^n = \mathrm{id}$. In fact, for $1 \le m < n$, $\sigma_p^m \neq \mathrm{id}$, or else $\mathbb{F}_q$ would be the splitting field of $x^{p^m} - x$. So $\sigma_p$ has order $n$ in the Galois group $\mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)$, which has order $n$ by the degree of the extension. Thus $\mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)$ is cyclic, with generator $\sigma_p$.

Now consider $H \le G = \mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)$ of order $d$. Then $d \mid n$ and $[G:H] = \frac{n}{d}$. By Thm 57,

$$\frac{n}{d} = [G:H] = [H^* : G^*] = [\mathbb{F}_q^H : \mathbb{F}_p], \text{ so } H^* = \mathbb{F}_q^H = \mathbb{F}_{p^{n/d}}.$$

**Eg** Let $E$ be the splitting field of $x^5 - 7 \in \mathbb{Q}[x]$. $E = \mathbb{Q}(\alpha, \zeta)$ for $\alpha = \sqrt[5]{7}$ and $\zeta = e^{2\pi i/5}$, which have minimal polynomials $x^5 - 7$ and $\Phi_5(x) = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$, respectively, over $\mathbb{Q}$. $[\mathbb{Q}(\alpha):\mathbb{Q}] = 5$ and $[\mathbb{Q}(\zeta):\mathbb{Q}] = 4$ are divisors of $[E:\mathbb{Q}]$, so $20 \mid [E:\mathbb{Q}]$ and $[E:\mathbb{Q}(\zeta)] \ge 5$. But also, $[E:\mathbb{Q}(\zeta)] \le [\mathbb{Q}(\alpha):\mathbb{Q}] = 5$, so it is precisely 5. Thus, $[E:\mathbb{Q}] = [E:\mathbb{Q}(\zeta)][\mathbb{Q}(\zeta):\mathbb{Q}] = 20$, and so $G = \mathrm{Gal}_{\mathbb{Q}}(E)$ has order 20. Also, $G \hookrightarrow S_5$ since $x^5 - 7$ has degree 5.



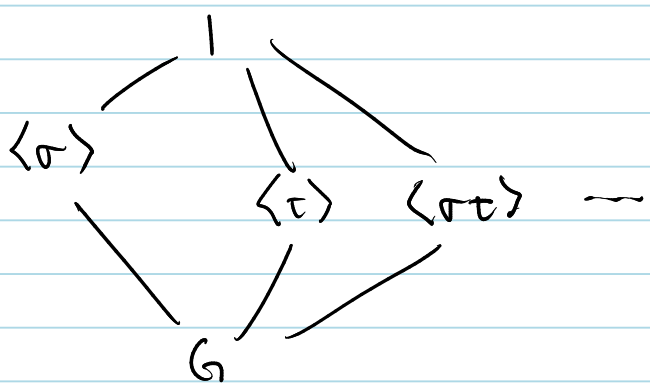

Define $\psi_{k,s} \in G$ to satisfy $\psi_{k,s}(\alpha) = \alpha\zeta^k$ for $k \in \mathbb{Z}_5$ and $\psi_{k,s}(\zeta) = \zeta^s$ for $s \in \mathbb{Z}_5^*$. Let $\sigma = \psi_{1,1}$ and $\tau = \psi_{0,2}$. We verify $\tau\sigma = \sigma^2\tau$, so that

$$G = \langle \sigma, \tau \mid \sigma^5 = \tau^4 = \sigma^2\tau\sigma^{-1}\tau^{-1} = 1 \rangle = \{\sigma^a\tau^b \mid 0 \le a < 5,\ 0 \le b < 4\}.$$

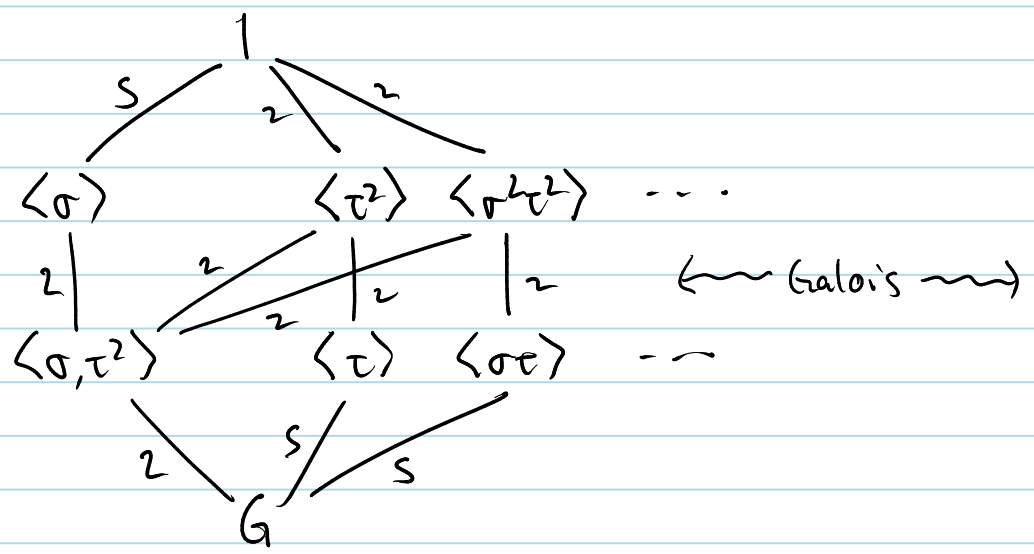
PMATH 348 **Groups of Order 20**

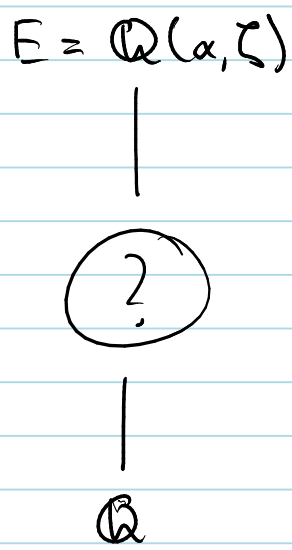
11 Mar 2016

Recall Eg. $E$ the splitting field of $x^5-7/\mathbb{Q}$. We saw $E=\mathbb{Q}(\alpha,\zeta)$ for $\alpha=\sqrt[5]{7}$ and $\zeta=e^{2\pi i/5}$. We have $[E:\mathbb{Q}]=20$ and $G=\mathrm{Gal}_{\mathbb{Q}}(E)$ having order 20. For $\psi\in G$, write $\psi=\psi_{k,s}$ if $\psi(\alpha)=\alpha\zeta^k$ and $\psi(\zeta)=\zeta^s$ for $k\in\mathbb{Z}_5$, $s\in\mathbb{Z}_5^\times$. Defining $\sigma=\psi_{1,1}$ and $\tau=\psi_{0,2}$ we see $G=\langle\sigma,\tau\mid\sigma^5=\tau^4=1,\tau\sigma=\sigma^2\tau\rangle$. By the first Sylow theorem, $G$ has Sylow 2- and 5-subgroups. By the third Sylow theorem, $n_5\equiv 1 \bmod 5$ and divides $|G|=20$, so $n_5=1$, and our Sylow 5-subgroup must be $\langle\sigma\rangle\cong\mathbb{Z}_5$. By the second Sylow theorem, $\langle\sigma\rangle\trianglelefteq G$. By the same argument, $n_2\in\{1,5\}$. If $n_2=1$, the Sylow 2-subgroup would be normal, and $G\cong\mathbb{Z}_5\times\mathbb{Z}_4\cong\mathbb{Z}_{20}$ would be abelian. But $\tau\sigma=\sigma^2\tau\neq\sigma\tau$, so this is not the case and $n_2=5$. We know $\langle\tau\rangle$ is one such group, so we may find the remaining Sylow 2-subgroups by conjugating $\sigma^a\tau^b\tau\tau^{-b}\sigma^{-a}=\sigma^a\tau\sigma^{-a}=\sigma^{a-2a}\tau=\sigma^{-a}\tau$ for $a\in\mathbb{Z}_5$, $b\in\mathbb{Z}_5^\times$, so the five 2-subgroups are $\langle\sigma^a\tau\rangle=\langle\psi_{a,2}\rangle$ for $a\in\mathbb{Z}_5$.

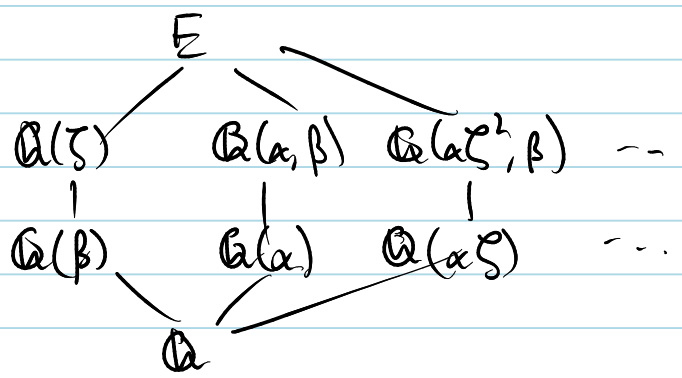



We have determined the subgroups of order 1, 4, 5, 20. This leaves subgroups of orders 2 and 10. The subgroups of order 2 must be contained in the Sylow 2-subgroups, and be cyclic, so they must be $\langle\sigma^{2a}\tau^2\rangle$ for $a\in\mathbb{Z}_5$. On the other hand, a subgroup of order 10 would have to contain the Sylow 5-subgroup $\langle\sigma\rangle$, so it must be $\langle\sigma,\tau^2\rangle$.




We now turn our attention to finding the intermediate fields. Recall the Galois correspondence $L\mapsto L^*=\mathrm{Gal}_L(E)$, $H\mapsto H^*=E^H$ for $L$ an intermediate field and $H$ a subgroup of $G$.




$\beta=\zeta+\zeta^{-1}$.

PMATH 348 # Solvability by Radicals

14 Mar 2016 For simplicity, suppose that $\operatorname{char} F \neq 2$ or 3. Recall the quadratic formula

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

giving solutions to the quadratic equation $x^2+bx+c=0$. An expression of such a form is called a radical. Instead of presenting the version of the cubic and quartic formulas given in class, consider the following.

First consider the solution of $x^2-2ax+b=0$. To solve this, we consider

$$(x-a)^2 = x^2-2ax+a^2 = x^2-2ax+b-b+a^2 = a^2-b$$

so that $x-a = \pm\sqrt{a^2-b}$, and thus the solutions are $x = a \pm \sqrt{a^2-b}$.

Now consider a general cubic equation $Ax^3+Bx^2+Cx+D=0$. WLOG $A=1$ by rescaling. Then apply the Tschirnhaus transformation, the substitution $x = t-\frac{B}{3}$.

$$\begin{aligned} 0 = x^3+Bx^2+Cx+D &= \left(t-\tfrac{B}{3}\right)^3 + B\left(t-\tfrac{B}{3}\right)^2 + C\left(t-\tfrac{B}{3}\right) + D \\ &= t^3 - 3\cdot\tfrac{B}{3}t^2 + 3\cdot\tfrac{B^2}{9}t - \tfrac{B^3}{27} + Bt^2 - 2B\cdot\tfrac{B}{3}t + B\cdot\tfrac{B^2}{9} + Ct - C\cdot\tfrac{B}{3} + D \\ &= t^3 + \left(C-\tfrac{1}{3}B^2\right)t + \left(\tfrac{2}{27}B^3 - \tfrac{1}{3}BC + D\right). \end{aligned}$$

So WLOG $B=0$. This substitution works to remove the $x^{n-1}$ term in a degree $n$ polynomial. Hence, consider the cubic $x^3-3ax-2b=0$. If we let $x = \sqrt[3]{p}+\sqrt[3]{q}$, then

$$x^3 = \left(p^{\frac{1}{3}}+q^{\frac{1}{3}}\right)^3 = p+q+3p^{\frac{2}{3}}q^{\frac{1}{3}}+3p^{\frac{1}{3}}q^{\frac{2}{3}} = (p+q)+3p^{\frac{1}{3}}q^{\frac{1}{3}}x$$

so then $x^3-3p^{\frac{1}{3}}q^{\frac{1}{3}}x-(p+q)=0=x^3-3ax-2b$, and comparing coefficients, $p^{\frac{1}{3}}q^{\frac{1}{3}}=a$, that is, $pq=a^3$ and $p+q=2b$. Then we consider the quadratic

$$0=(y-p)(y-q)=y^2-(p+q)y+pq=y^2-2by+a^3$$

which has solutions $p,q = y = b \pm \sqrt{b^2-a^3}$. Subject to a choice of third root of $p$ and the relation $p^{\frac{1}{3}}q^{\frac{1}{3}}=a$, $q$ is determined uniquely. Then the remaining solutions are given by $x = \zeta_3\sqrt[3]{p}+\zeta_3^2\sqrt[3]{q}$ and $x = \zeta_3^2\sqrt[3]{p}+\zeta_3\sqrt[3]{q}$, since these $x$ also satisfy the same cubic in $x$ as $\sqrt[3]{p}$ and $\sqrt[3]{q}$.

The solution of the cubic is due to Tartaglia, del Ferro, and Cardano.

Now consider the quartic $x^4+bx^2+cx+d=0$. *** TO BE FILLED IN ***

PMATH 348 **Cyclic Extensions**

16 Mar 2016

**Lem 62 (Dedekind's Lemma)** Let $K, L$ be fields and $\psi_i : L \to K$ distinct nonzero homomorphisms for $1 \le i \le n$. If $c_i \in K$ and

$$c_1\psi_1(\alpha) + \cdots + c_n\psi_n(\alpha) = 0 \quad \text{for all } \alpha \in L$$

then $c_1 = c_2 = \cdots = c_n = 0$.

Pf. Suppose for a contradiction there exists a minimal counterexample, i.e. $n \ge 2$ is minimal such that $c_1\psi_1(\alpha) + \cdots + c_n\psi_n(\alpha) = 0$ for all $\alpha \in L$ (call this (1)). Then all $c_i \neq 0$. Choose $\beta \in L$ such that $0 \neq \psi_1(\beta) \neq \psi_2(\beta)$. Then

$$c_1\psi_1(\alpha) + c_2\psi_2(\alpha)\frac{\psi_2(\beta)}{\psi_1(\beta)} + \cdots + c_n\psi_n(\alpha)\frac{\psi_n(\beta)}{\psi_1(\beta)} = 0 \quad \text{for all } \alpha \in L \qquad (2)$$

But then (1) − (2) gives

$$c_2\left(1 - \frac{\psi_2(\beta)}{\psi_1(\beta)}\right)\psi_2(\alpha) + \cdots + c_n\left(1 - \frac{\psi_n(\beta)}{\psi_1(\beta)}\right)\psi_n(\alpha) = 0 \quad \text{for all } \alpha \in L$$

which has one fewer term than (1), contradicting minimality of $n$. □

**Thm 63.** Let $F$ be a field and $n \in \mathbb{N}$ such that $\mathrm{ch}(F) \nmid n$. Suppose that $x^n - 1$ splits over $F$. (1) If $E/F$ is a cyclic Galois extension of degree $n$, then $E = F(\alpha)$ for some $\alpha \in E$ such that $\alpha^n \in F$. In particular, $x^n - \alpha^n$ is the minimal poly of $\alpha$ over $F$. (2) Conversely, if $E = F(\alpha)$ and $\alpha^n \in F$, then $E/F$ is cyclic of degree $d$ with $d \mid n$ and $\alpha^d \in F$. In particular, $x^d - \alpha^d$ is the minimal poly of $\alpha$ over $F$.

Pf Let $\zeta_n \in F$ be a primitive $n$-th root of unity. Note that since either $\mathrm{ch}(F) = 0$, or $\mathrm{ch}(F) = p$ and $p \nmid n$, $x^n - 1$ is separable, so $\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$ are all distinct.

(1) Let $G = \mathrm{Gal}_F(E) = \langle \psi \mid \psi^n = 1 \rangle \cong \mathbb{Z}_n$, the cyclic group of order $n$. Apply Dedekind's Lemma to the elements $\psi^i : E \to E$ and coefficients $c_i = \zeta_n^{-i}$. Since $c_i \neq 0$, there exists $u \in E$ such that $\alpha = u + \zeta_n^{-1}\psi(u) + \cdots + \zeta_n^{1-n}\psi^{n-1}(u) \neq 0$. We see that $\psi^i(\alpha) = \alpha\zeta_n^i$ for $1 \le i \le n$. Thus, $\alpha\zeta_n^i$ are conjugate to each other and hence have the same minimal polynomial $p(x)$. Since $\alpha\zeta_n^i$ are also all distinct, $\deg p(x) = n$. $p(x) \in F[x]$, so it has the constant term $p(0) = \pm\alpha(\alpha\zeta_n)\cdots(\alpha\zeta_n^{n-1}) = \pm\alpha^n\zeta_n^{n(n-1)/2} \in F$. $\zeta_n \in F$, so $\alpha^n \in F$. $\alpha$ is a root of $x^n - \alpha^n$ and hence $p(x) = x^n - \alpha^n$. Since $F(\alpha) \subseteq E$ and $[F(\alpha) : F] = \deg p = n = [E : F]$, $E = F(\alpha)$. This proves (1).

* * * TO BE CONTINUED * * *

PMATH 348 **Laptop died...**

18 Mar 2016 Recall Thm 63. Let $F$ be a field and $n \in \mathbb{N}$ with $\mathrm{ch}(F) \nmid n$. Suppose that $x^n - 1$ splits over $F$. (2) If $E = F(\alpha)$ and $\alpha^n \in F$ then $E/F$ is a cyclic extension of degree $d$ with $d \mid n$ and $\alpha^d \in F$. In particular, $x^d - \alpha^d$ is the min poly of $\alpha/F$.

Pf. (2) Suppose $\alpha^n \in F$. Let $p(x) \in F[x]$ be the minimal polynomial of $\alpha$ over $F$. Since $\alpha$ is a root of $x^n - \alpha^n$, $p(x) \mid x^n - \alpha^n$, and so the roots of $p(x)$ are of the form $\alpha \zeta_n^k$. Then $p(x)$ has constant term $p(0) = \pm \alpha^d \zeta_n^k$ for $d$ the number of roots of $p(x)$ and some $k \in \mathbb{Z}$. Since $p(0), \zeta_n \in F$, we have $\alpha^d \in F$, and $\alpha$ is a root of $x^d - \alpha^d$. This is monic, so $p(x) = x^d - \alpha^d$. Now suppose for a contradiction that $d \nmid n$, so that $n = qd + r$ for $0 < r < d$ by the division algorithm. Then $\alpha^r = \alpha^{n-qd} = \alpha^n / (\alpha^d)^q \in F$, so $x^r - \alpha^r$ has $\alpha$ as a root, contradicting the minimality of $p(x)$. So $d \mid n$. Write $n = dm$. The roots of $p(x)$ are $\alpha \zeta_n^{km} = \alpha \zeta_d^k$ for $0 \le k < d$. $E/F$ is Galois, because it is the splitting field of $p(x)$ (which is separable) over $F$. The $\psi \in G = \mathrm{Gal}_F(E)$ for which $\psi(\alpha) = \alpha \zeta_d$ is a generator for $G$, since $\psi$ must fix $\zeta_n \in F$, so $G$ is cyclic of order $d$. $\square$

Now we will consider the case when $\mathrm{ch}(F) \mid n$ — that is, $\mathrm{ch}(F) = p > 0$ and $p \mid n$ — so $x^n - \alpha$ is no longer separable.

Thm 64. Let $F$ be a field with $\mathrm{ch}(F) = p > 0$. (1) If $x^p - x - a \in F[x]$ is irreducible, then its splitting field $E/F$ is a cyclic extension of degree $p$. (2) Conversely, if $E/F$ is a cyclic extension of degree $p$, then it is the splitting field of some irreducible $x^p - x - a \in F[x]$.

Pf. (1) Let $f(x) = x^p - x - a$ and let $\alpha$ be a root of $f(x)$. Then

$$f(\alpha+1) = (\alpha+1)^p - (\alpha+1) - a = \alpha^p + \underline{1} - \alpha - \underline{1} - a = f(\alpha) = 0,$$

(the $+1$ and $-1$ cancel)

Hence $\alpha + k$ is a root of $f(x)$ for all $k \in \mathbb{F}_p$. Since $f(x)$ has at most $p$ distinct roots, its roots are precisely $\{\alpha, \alpha+1, \dots, \alpha+p-1\}$. It follows that $E = F(\alpha + k \mid k \in \mathbb{F}_p) = F(\alpha)$ and $[E:F] = \deg f = p$. $\mathbb{Z}_p$ is the only group of order $p$, so $\mathbb{Z}_p \cong \mathrm{Gal}_F(E) = \langle \psi \rangle$ for the $\psi : E \xrightarrow{\sim} E$ given by $\psi|_F = \mathrm{id}$ and $\psi(\alpha) = \alpha + 1$.

(2) Let $G = \mathrm{Gal}_F(E) = \langle \psi \rangle \cong \mathbb{Z}_p$. Apply Dedekind's Lemma to $K = L = E$ and $\psi_i = \psi^i$ the elements of $G$ with $c_i = 1$ — there exists some $v \in E$ such that $\beta = v + \psi(v) + \cdots + \psi^{p-1}(v)$ is nonzero. $\psi^i(\beta) = \beta$ for all $\psi^i \in G$, so $\beta \in F$. Let $u = v/\beta$. Then

$$u + \psi(u) + \cdots + \psi^{p-1}(u) = \frac{v}{\beta} + \psi\left(\frac{v}{\beta}\right) + \cdots + \psi^{p-1}\left(\frac{v}{\beta}\right) = \frac{1}{\beta}\left(v + \psi(v) + \cdots + \psi^{p-1}(v)\right) = \frac{1}{\beta} \cdot \beta = 1.$$

Setting $\alpha = 0 \cdot u - 1 \cdot \psi(u) - 2 \cdot \psi^2(u) - \cdots - (p-1)\psi^{p-1}(u)$, we see $\psi(\alpha) = -\psi^2(u) - \cdots - (p-1)\psi^p(u)$, so

$$\psi(\alpha) - \alpha = \psi(u) + \psi^2(u) + \cdots + \psi^{p-1}(u) + \psi^p(u) = 1$$

since $\psi^p = \mathrm{id}$, and thus $\psi(\alpha) = \alpha + 1$ and $\psi(\alpha^p) = \psi(\alpha)^p = (\alpha+1)^p = \alpha^p + 1$.

* * * TO BE CONTINUED * * *

PMATH 348 # Cyclic Extensions, continued

21 Mar 2016 Recall Thm 64. Let $F$ be a field with $ch(F) = p > 0$. (2) If $E/F$ is a cyclic extension of degree $p$, then $E/F$ is the splitting field of some irreducible polynomial $x^p - x - a \in F[x]$.

Pf. (cont). Let $G = Gal_F(E) = \langle \psi \rangle \cong \mathbb{Z}_p$. We have seen there exists $\alpha \in E$ such that $\psi(\alpha) = \alpha + 1$ and then $\psi(\alpha^p) = \psi(\alpha)^p = (\alpha+1)^p = \alpha^p + 1$. It follows that

$$\psi(\alpha^p - \alpha) = \psi(\alpha^p) - \psi(\alpha) = \alpha^p + 1 - \alpha - 1 = \alpha^p - \alpha$$

so $\alpha^p - \alpha$ is fixed by $G$ and hence is an element of $F$. Then if $a = \alpha^p - \alpha$, $\alpha$ is a root of $x^p - x - a \in F[x]$. Since $[E:F] = p$, $[F(\alpha):F] \mid p$, and since $\alpha \notin F$, $F(\alpha) = E$, and also $x^p - x - a$ is the minimal polynomial of $\alpha$ over $F$. □

## Radical Extensions

Def. A finite extension $E/F$ is radical if there exists a tower of subfields

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E$$

such that $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$ for $d_i \in \mathbb{N}$.

Def Let $F$ be a field and $f(x) \in F[x]$. We say $f(x)$ is solvable by radicals if there exists a radical extension $E/F$ such that $f(x)$ splits over $E$.

Rem. It is possible that $f(x) \in F[x]$ is solvable by radicals, but its splitting field is not a radical extension (see Assignment 8). All we require is that $f(x)$ split in $E$.

Lem 65. If $E/F$ is a finite separable radical extension, then so is its normal closure $N/F$.

Pf Since $E/F$ is finite and separable, by Thm 51, $E = F(\beta)$ for some $\beta \in E$. Since $E/F$ is also radical, there is a tower $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E$ such that $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$. Let $p(x) \in F[x]$ be the min. poly. of $\beta$ and $\beta = \beta_1, \beta_2, \ldots, \beta_n$ the roots of $p(x)$. By the definition of normal closure and Thm 52, $N = E(\beta_2, \ldots, \beta_n) = F(\beta_1, \ldots, \beta_n)$. Also, there is an $F$-isomorphism $\sigma_j : F(\beta) \xrightarrow{\sim} F(\beta_j)$ given by $\sigma_j(\beta) = \beta_j$ for $2 \le j \le n$. Since $N$ can be viewed as the splitting field of $p(x)$ over $F(\beta)$ and $F(\beta_j)$ respectively, by Thm 16, there is $\psi_j : N \xrightarrow{\sim} N$ extending $\sigma_j$. Thus $\psi_j \in Gal_F(E)$ and $\psi_j(\beta) = \beta_j$. We have the following towers of fields:

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m = E = F(\beta_1) = F(\beta_1)\psi_2(F_0) \subseteq F(\beta_1)\psi_2(F_1) \subseteq \cdots$$

$$\subseteq F(\beta_1)\psi_2(F_m) = F(\beta_1, \beta_2) = F(\beta_1, \beta_2)\psi_3(F_0) \subseteq F(\beta_1, \beta_2)\psi_3(F_1) \subseteq \cdots$$

$$\subseteq F(\beta_1, \beta_2)\psi_3(F_m) = F(\beta_1, \beta_2, \beta_3) \subseteq \cdots \subseteq F(\beta_1, \ldots, \beta_n).$$

We now verify this is a radical tower.

$$F(\beta_1, \ldots, \beta_{j-1})\psi_j(F_i) = F(\beta_1, \ldots, \beta_{j-1})\psi_j(F_{i-1}(\alpha_i)) = F(\beta_1, \ldots, \beta_{j-1})\psi_j(F_{i-1})(\psi_j(\alpha_i))$$

and $\psi_j(\alpha_i)^{d_i} = \psi_j(\alpha_i^{d_i}) \in \psi_j(F_{i-1})$. Thus $N/F$ is also radical. □

Rem. An irreducible $f(x) \in F[x]$ is solvable by radicals iff $f(x)$ has a root expressible by radicals.

PMATH 348 # Radical Extensions

23 Mar 2016 Recall a finite extension $E/F$ is radical if there exists $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E$ such that $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$ for $\alpha_i \in E$, $d_i \in \mathbb{N}$, and an $f(x) \in F[x]$ is solvable by radicals if it splits in some radical extension of $F$. Recall also Lem 65. If $E/F$ is finite, separable, and radical, then so is its normal closure.

Claim. Suppose $f(x) \in F[x]$ is irreducible and separable. $f(x)$ is solvable by radicals iff $f(x)$ has a root that is expressible by radicals. Pf. The forward direction is clear. So suppose $f(x)$ has a root in a radical extension $E/F$. By Lem 65, the normal closure $N/F$ is also radical. Since $f(x)$ splits over $N$, $f(x)$ is solvable by radicals. □

Def Let $F$ be a field and $f(x) \in F[x]$ be separable. Take $E$ to be the splitting field of $f(x)$ over $F$. The Galois group of $f(x)$ is $\mathrm{Gal}(f) = \mathrm{Gal}_F(E)$.

Thm 67 Let $F$ be a field of characteristic zero and $f(x) \in F[x]$ nonzero. Then $f(x)$ is solvable by radicals iff $\mathrm{Gal}(f)$ is a solvable group.

We will prove this result later.

Prop 68. Let $f(x) \in \mathbb{Q}[x]$ be irreducible and having degree $p$ some prime. If $f(x)$ has precisely two nonreal roots in $\mathbb{C}$, then $\mathrm{Gal}(f) \cong S_p$.

Pf Recall that $S_p$ can be generated by a 2-cycle and a $p$-cycle, so it suffices to show that $\mathrm{Gal}(f)$ has a 2-cycle and a $p$-cycle. Let $\alpha$ be a root of $f(x)$. Since $f(x)$ is irreducible of degree $p$, $[F(\alpha):F] = \deg f = p$ and so $p \mid |\mathrm{Gal}(f)|$. By Cauchy's Thm, there exists an element of order $p$, that is, a $p$-cycle. Furthermore, the conjugation map must interchange the two nonreal roots and fix the real roots, so it is an element of $\mathrm{Gal}(f)$. It follows that $\mathrm{Gal}(f) \cong S_p$. □

E.g. Consider $f(x) = x^5 + 2x^3 - 24x - 2 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, which is irreducible by Eisenstein's criterion. Since $\lim_{x \to -\infty} f(x) = -\infty$, $f(-1) = 19$, $f(1) = -23$, $\lim_{x \to \infty} f(x) = \infty$, $f(x)$ must have at least 3 real roots. Now, let $\alpha_1, \ldots, \alpha_5$ be the roots of $f(x)$. We see that $\sum_i \alpha_i = 0$ and $\sum_{i<j} \alpha_i \alpha_j = 2$, so $0 = (\sum_i \alpha_i)^2 = \sum_i \alpha_i^2 + 2\sum_{i<j} \alpha_i \alpha_j = \sum_i \alpha_i^2 + 4$ and since the sum of the squares of the $\alpha_i$ is negative, at least one of the roots is complex. So $f(x)$ has 3 real roots and 2 complex roots, and thus has $\mathrm{Gal}(f) \cong S_5$, which is not solvable.

PMATH 348 **Things of some sort or other**

28 Mar 2016 **Lem 66.** Let $E/F$ be a field extension and let $K, L$ be intermediate fields of $E/F$. Suppose $K/F$ is finite Galois. Then $KL/L$ is finite Galois and $\mathrm{Gal}_L(KL)$ is isomorphic to a subgroup of $\mathrm{Gal}_F(K)$.

*Pf.* (Sketch). Consider the restriction to $K$ map $\mathrm{Gal}_L(KL) \hookrightarrow \mathrm{Gal}_F(K)$. $\square$

Now recall **Thm 67** Let $F$ be a field with characteristic zero and $f(x) \in F[x]$ be nonzero. Then $f(x)$ is solvable by radicals iff $\mathrm{Gal}(f)$ is solvable.

*Pf* Suppose $f(x)$ is solvable by radicals, i.e $f(x)$ splits over some extension $E/F$ satisfying

$$F = F_0 \leq F_1 \leq \cdots \leq F_m = E$$

with $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$ for $d_i \in \mathbb{N}$. By Lem 65, we may assume $E/F$ is normal and thus Galois, i.e. $E$ is the splitting field of some $\tilde{f}(x) \in F[x]$. Let $n = \prod_{i=1}^m d_i$, let $L/E$ be the splitting field of $x^n - 1$ over $E$, and let $\zeta_n \in L$ be a primitive $n$-th root of unity. Set $K = F(\zeta_n)$ so that $L = E(\zeta_n) = EK$. Define $K_i = KF_i = F_i(\zeta_n)$. Then

$$F \leq F(\zeta_n) = K_0 \leq K_1 \leq \cdots \leq K_m = F_m(\zeta_n) = L,$$

and we have $K_i = K_{i-1}(\alpha_i)$ and $\alpha_i^{n} \in F_{i-1} \leq K_{i-1}$. Also, $\zeta_n \in K_{i-1}$, so $K_i$ is the splitting field of $x^{d_i} - \alpha^{d_i}$ over $K_{i-1}$, and is thus Galois. Moreover, by Thm 63, $K_i/K_{i-1}$ is cyclic. Note that $L$ is the splitting field of $\tilde{f}(x)(x^n - 1)$ over $F$ and also over $K_i$. Thus $L/F$ and $L/K_i$ is Galois. By the Galois correspondence,

$$G = \mathrm{Gal}_F(L) \supseteq \mathrm{Gal}_{K_0}(L) \supseteq \mathrm{Gal}_{K_1}(L) \supseteq \cdots \supseteq \mathrm{Gal}_{K_m}(L) = \mathbb{1}.$$

For each $\sigma \in \mathrm{Gal}_{K_{i-1}}(L)$ and $\psi \in \mathrm{Gal}_{K_i}(L)$, we claim $\sigma\psi\sigma^{-1}|_{K_i} = \mathrm{id}_{K_i}$. This holds because $\sigma(K_i) = K_i$ and $\psi$ fixes $K_i$. Thus, $\mathrm{Gal}_{K_i}(L) \trianglelefteq \mathrm{Gal}_{K_{i-1}}(L)$. Moreover, $\mathrm{Gal}_{K_{i-1}}(L)/\mathrm{Gal}_{K_i}(L) \cong \mathrm{Gal}_{K_{i-1}}(K_i)$ is cyclic. Finally, $\mathrm{Gal}_F(L)/\mathrm{Gal}_{K_0}(L) \cong \mathrm{Gal}_F(K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, so $\mathrm{Gal}_F(L)$ is solvable. Since $L = K\bar{E}$, $\mathrm{Gal}_E(\bar{E}) \cong \mathrm{Gal}_F(L)/\mathrm{Gal}_K(L)$ is a quotient of a solvable group and is thus solvable by Thm 40. Finally, $\mathrm{Gal}(f)$ is a quotient group of $\mathrm{Gal}_F(\bar{E})$, since $\bar{E}$ contains the splitting field of $f(x)$, so $\mathrm{Gal}(f)$ is solvable.

Conversely, suppose $\mathrm{Gal}(f)$ is solvable. * * * TO BE CONTINUED * * *.

W30

PMATH 348 # Cyclotomic Extensions Continued.

1 Apr 2016 Recall $\zeta_n = e^{2\pi i/n}$ and $\Phi_n(x) = \prod_{\substack{1\le k\le n \\ \gcd(k,n)=1}} (x-\zeta_n^k) \in \mathbb{Z}[x]$ is irreducible, and that $x^n - 1 = \prod_{d\mid n} \Phi_d(x)$ and $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \cong (\mathbb{Z}/(n))^*$.

**Thm.** Any quadratic extension of $\mathbb{Q}$ in $\mathbb{C}$ is contained in some $\mathbb{Q}(\zeta_n)$.

**Pf.** A quadratic extension $E/\mathbb{Q}$ is the splitting field of $ax^2+bx+c \in \mathbb{Q}[x]$. $ax^2+bx+c$ has the roots $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$, so $E = \mathbb{Q}(\sqrt{b^2-4ac})$ for $b^2-4ac \in \mathbb{Q}$. Write $b^2-4ac = \frac{d}{q}$ for $d, q \in \mathbb{Z}$, $q>0$, and $(d,q)=1$.

So a quadratic extension of $\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{D})$ for $D$ squarefree. Note that $\mathbb{Q}(\sqrt{1}) = \mathbb{Q}$ and $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$. Also, for distinct primes $p, q$, if $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\sqrt{q}) \subseteq \mathbb{Q}(\zeta_m)$, then $\sqrt{pq} \in \mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{\mathrm{lcm}(n,m)})$. So it suffices to find cyclotomic extensions containing $\sqrt{D}$ for $D = p$ a prime.

If $p=2$, $(1+i)^2 = 2i$ and $1+i \in \mathbb{Q}(\zeta_4)$ so $\sqrt{2i} \in \mathbb{Q}(\zeta_4)$. Also, $i \in \mathbb{Q}(\zeta_4)$ so $\sqrt{i} \in \mathbb{Q}(\zeta_8)$, and then $\sqrt{2} = \sqrt{2i}\sqrt{i}^3 \in \mathbb{Q}(\zeta_8)$. So let $p$ be an odd prime. The min poly of $\zeta_p$ is $\Phi_p$. The discriminant of $\Phi_p(x)$ is defined $D(\Phi_p) = \prod_{1\le i<j<p} (\zeta_p^i - \zeta_p^j)^2 = (-1)^{\frac{p-1}{2}} p^{p-2} \in \mathbb{Z}$. So

$$\prod_{1\le i\ne j<p} (\zeta_p^i - \zeta_p^j) = \pm p^{\frac{p-3}{2}} \sqrt{(-1)^{\frac{p-1}{2}} p}.$$

$\frac{p-3}{2} \in \mathbb{Z}$ and $\prod_{1\le i\ne j<p} (\zeta_p^i - \zeta_p^j) \in \mathbb{Q}(\zeta_p)$. If $p \equiv 1 \bmod 4$, $\sqrt{p} \in \mathbb{Q}(\zeta_p)$. If $p \equiv 3 \bmod 4$, $\sqrt{-p} \in \mathbb{Q}(\zeta_p)$ so $\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$. Thus $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_{4p})$. $\square$

**Rem** Note that $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{D})) \cong 1$ or $\mathbb{Z}/(2)$, which is abelian.

**Thm** (Kronecker–Weber) Every finite abelian ext of $\mathbb{Q}$ is contained in a cyclotomic extension.

**Lem.** Let $p$ be a prime and $m \in \mathbb{N}$ with $p \nmid m$. Then for $a \in \mathbb{Z}$, $p \mid \Phi_m(a)$ iff $p \nmid a$ and $a \bmod p$ has order $m$ in $\mathbb{F}_p^*$, the multiplicative group of units of $\mathbb{F}_p$.

**Pf.** Let $p$ be prime and denote $\bar{a} = a \bmod p$. Let $k$ be the order of $\bar{a}$ in $\mathbb{F}_p^*$. Suppose $p \mid \Phi_m(a)$. Since $(m,p)=1$, $x^m - \bar{1} \in \mathbb{F}_p[x]$ has no repeated roots in any extension of $\mathbb{F}_p$. Write $x^m - \bar{1} = \overline{\Phi_m(x)}$, and notice $\prod_{d\mid m} \overline{\Phi_d(x)} \in \mathbb{F}_p[x]$. $p \mid \Phi_m(a)$ implies $\overline{\Phi_m(a)} = \bar{0}$, so $\bar{a}^m = \bar{1}$, i.e. $\bar{a} \ne \bar{0}$. Then if $k<m$, $x^k - \bar{1} = \prod_{d\mid k} \overline{\Phi_k(x)}^{d\mid m \ne d}$ gives $\overline{\Phi_d(\bar{a})} = \bar{0}$ for some $d \mid k$. But also $d \mid m$ since $\overline{\Phi_m(\bar{a})} = \bar{0}$, so then $\bar{a}$ is a repeated root of $x^m - \bar{1}$, which is a contradiction.

Conversely suppose $p \nmid a$ and $k = m$. If $d < m$, $\bar{a}^d \ne \bar{1}$, so $\overline{\Phi_d(\bar{a})} \ne \bar{0}$. Since $\bar{a}^m - \bar{1} = 0$ and $\bar{a}^m - \bar{1} = \overline{\Phi_m(\bar{a})} \prod_{d\mid m \ne d} \overline{\Phi_d(\bar{a})}$, we have $\overline{\Phi_m(\bar{a})} = 0$, i.e. $p \mid \Phi_m(a)$. $\square$

PMATH 348 **Infinitude of Primes $\equiv 1 \bmod n$**

4 Apr 2016 Recall Lem. Let $p$ be prime and $m \in \mathbb{N}$ with $p \nmid m$. Then for $a \in \mathbb{Z}$, $p \mid \Phi_m(a)$ iff $p \nmid a$ and $a \bmod p$ has order $m$ in $\mathbb{F}_p^*$.

**Lem.** If $f(x) \in \mathbb{Z}[x]$ is monic and nonconstant, the set of prime divisors of the nonzero integers in the sequence $f(1), f(2), f(3), \ldots$ is infinite.

**Pf** Suppose for a contradiction that only finitely many primes divide the elements of the sequence $f(1), f(2), \ldots$, say $p_1, \ldots, p_k$. Choose $s \in \mathbb{N}$ such that $m = f(s)$ is nonzero. Define $g(x) = \frac{1}{m} f(s + m p_1 p_2 \cdots p_k x)$. Observe that $g(0) = \frac{1}{m} f(s) = 1$, and that all other terms involving $x$ in $g(x)$ have a factor of $m$. Thus $g(x) \in \mathbb{Z}[x]$. Moreover, for all $n \in \mathbb{N}$,

$$g(n) = \tfrac{1}{m} f(s + m p_1 \cdots p_k n) \equiv \tfrac{1}{m} f(s) = 1 \bmod p_1 \cdots p_k.$$

Since $p_i \mid g(n) - 1$, we have $p_i \nmid g(n)$. Moreover, we can choose $n$ such that $|g(n)| > 1$. Thus $g(n)$ has a prime factor $p \notin \{p_1, \ldots, p_k\}$. Since $m g(n) = f(s + mnp_1 \cdots p_k)$, $p \mid f(s + mp_1 \cdots p_k)$, the desired contradiction. $\square$

**Weak Dirichlet's Thm.** For $m \in \mathbb{N}$ of least 2, there are infinitely many primes $p \equiv 1 \bmod m$.

**Pf.** By the previous lemma, there are infinitely many prime divisors of the nonzero elements of the sequence $\Phi_m(1), \Phi_m(2), \Phi_m(3), \ldots$. If prime $p \mid \Phi_m(a)$ for some $a \geq 2$, then by the other previous lemma, $\bar{a} = a \bmod p$ has order $m$ in $\mathbb{F}_p^*$. So $m \mid |\mathbb{F}_p^*| = p - 1$, i.e. $p$ must be congruent to 1 modulo $m$. $\square$

**Rem.** The stronger Dirichlet's Thm states that, for $(a, m) = 1$,

$$\pi(x, a, m) := \#\{p \leq x \text{ prime} \mid p \equiv a \bmod m\} \sim \frac{1}{\varphi(m)} \pi(x)$$

where $\pi(x) = \#\{p \leq x \text{ prime}\}$ is the prime-counting function.

## Inverse Galois Theory

**Thm.** Let $A$ be a finite abelian group. Then there exists a Galois extension $E/\mathbb{Q}$ with $E \leq \mathbb{Q}(\zeta_n)$ and $\mathrm{Gal}_{\mathbb{Q}}(E) \cong A$.

**Pf.** Write $A \cong \mathbb{Z}_{k_1} \times \cdots \times \mathbb{Z}_{k_s}$ and choose primes $p_1 < \cdots < p_s$ such that $p_i \equiv 1 \bmod k_i$, which is possible by the weak Dirichlet theorem. Then let $n = p_1 \cdots p_s$ and consider $E = \mathbb{Q}(\zeta_n)$.

$$G = \mathrm{Gal}_{\mathbb{Q}}(E) = (\mathbb{Z}/(n))^* \cong (\mathbb{Z}/(p_1))^* \times \cdots \times (\mathbb{Z}/(p_s))^* \cong \mathbb{Z}_{p_1 - 1} \times \cdots \times \mathbb{Z}_{p_s - 1},$$

so write $p_i - 1 = k_i d_i$, and note that there exists a subgroup $D_i \cong \mathbb{Z}_{d_i}$ of $C_{p_i - 1}$. Then $\mathbb{Z}_{p_i - 1}/D_i \cong \mathbb{Z}_{k_i}$. Define $H = D_1 \times \cdots \times D_s \leq G$ and see that $E^H/\mathbb{Q}$ is Galois and

$$\mathrm{Gal}_{\mathbb{Q}}(E^H) \cong G/H \cong \mathbb{Z}_{k_1} \times \cdots \times \mathbb{Z}_{k_s} \cong A. \quad \square$$