Modern Algebra

MATH 505, University of Washington, Autumn 2021

These lecture notes are for MATH 505, "Modern Algebra," taught by Julia Pevtsova at The University of Washington during Winter 2022. These notes are written by Tony Zeng using Jackson Petty's `coursework-latex` repository. These notes are not official and have not been proofread by the instructor for the course. Please report any mistakes to me at `txz@uw.edu`.

Contents

1 January 3, 2022

1.1 *Last Quarter Final Solutions*

Problem 1.1. Given $(a, n) = 1$, prove that $a^{\phi(n)} \equiv 1 \pmod{n}$.

Solution. Could take for granted that $(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} | (a, n) = 1\}$. If you wanted to show, easier to show a is invertible iff $(a, n) = 1$, which follows from Bezout's lemma:

$$b = a^{-1} \in \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \exists b, c \text{ s.t. } ba + ca = 1 \Leftrightarrow (a, n) = 1$$

As a result, $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$, so by Lagrange's theorem, $a^{\phi(n)} \equiv 1 \pmod{n}$. ■

Problem 1.2. Let $S \subset R$ be a multiplicative subset, and $\mathcal{P}$ is a maximal element in the set of ideals not intersecting S, then $\mathcal{P}$ is prime.

Solution. Let $\mathcal{P}$ be such an element, and suppose it is not prime. Then there exists $a, b \notin \mathcal{P}$ such that $ab \in \mathcal{P}$. Then $(a) + \mathcal{P}$ and $(b) + \mathcal{P}$ intersect S. Therefore, there exits $x, y \in R$ and $p, q \in \mathcal{P}$, but $xa + p, yb + q \in S$. Their product is

$$xyab + xaq + ybp + pq \in S \cap \mathcal{P}$$

which is a contradiction. ■

Problem 1.3. G is solvable implies G/N and N are solvable.

Solution. G is solvable gives existence of the series

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$$

with abelian quotients. Notice that $\{e\} \triangleleft N \triangleleft G$ is also a normal series. Then by Schreier's theorem, there exists

$$\{e\} = H_0 \triangleleft H_1 \triangleleft \ldots \triangleleft H_k = N \triangleleft \ldots \triangleleft H_m = G$$

So N is solvable by taking the first half of the series, and G/N is solvable by taking second half and using the third isomorphism theorem (or correspondence). That is, for $i \geq k$,

$$\frac{H_{i+1}/N}{H_i/N} \simeq \frac{H_{i+1}}{H_i}$$

is abelian. ■

Solution. Start with a series for G, and look at its image under the projection $G \to G/N$, and look at the intersection of each element in the series with N. ■

Problem 1.4. G a p-group, $G/[G,G]$ cyclic implies that G is cyclic.

Solution. Since $\Phi(G) = G^p[G,G]$, we get a well-defined surjective homomorphism $G/[G,G] \to G/\Phi(G)$ ($[G,G] < \Phi(G)$). $g[G,G] \subset g\Phi(G)$ implies that $G/\Phi(G) = \langle \overline{g} \rangle$ since the image of a cyclic group is cyclic. Then by Burnside's basis theorem, $G = \langle g \rangle$ is cyclic. ■

Solution. Can also be shown using induction on n, where $|G| = p^n$, and the fact that $Z(G)$ is non-trivial. ■

Problem 1.5. $G = \langle a, b | a^4 = b^6 = 1, bab^{-1} = a^3 \rangle$ has order 24.

Solution. $|G| \leq 24$ since the last relation tells us that every element of G can be written in the form $a^i b^j$ for $0 \leq i \leq 3$, $0 \leq j \leq 5$. For the other direction, consider the semi-direct product $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/6\mathbb{Z}$ where $\varphi : \mathbb{Z}/6\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ such that $\varphi(1)(a) = a^{-1}$. This will be well-defined, as the relations will be preserved. Then by the universal property of the free group, we get a well-defined surjective homomorphism from

$$F(\{a,b\}) \to \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/6\mathbb{Z}$$

which sends $a \mapsto (1,0)$ and $b \mapsto (0,1)$. Also, note that $a^4 \mapsto 4 \cdot (1,0) = 0$, $b^6 \mapsto 6 \cdot (0,1) = 0$, and $bab^{-1}a \mapsto (0,1)(1,0)(0,5)(1,0) = 0$ by construction of φ. So we get a well-defined surjective homomorphism from $G \to \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/6\mathbb{Z}$, so $|G| \geq 24$. ■

Problem 1.6. Let $R = \mathbb{Z}[x]$ and $M \subset R$ be a maximal ideal. Show that R/M is a finite field.

Solution. We showed in class that a ring modded out by a maximal ideal is a field. We need only show finiteness. First note that $M \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$.

1. $M \cap \mathbb{Z} \neq (0)$. Then $M \cap \mathbb{Z} = (p)$. Let $M' = M/(p) \subset \mathbb{Z}/p[x]$. Note that

$$\frac{\mathbb{Z}/p[x]}{M'} = \frac{\mathbb{Z}[x]/(p)}{M/(p)} = \frac{Z[x]}{M}.$$

Therefore, $M' = (f_0)$ for some irreducible $f_0 \in \mathbb{Z}/p[x]$. Let f be a polynomial representative of the equivalence class f_0. Then $M \subset (f) + (p) = (p, f)$ so $M = (p, f)$. Then

$$\frac{\mathbb{Z}[x]}{M} = \frac{\mathbb{Z}/p[x]}{(f_0)} = \mathbb{Z}/p[\alpha]$$

where α

2. $M \cap \mathbb{Z} = (0)$. Let $M'' = \mathbb{Q}[x]M$ (the ideal in $\mathbb{Q}[x]$ generated by M). $M'' = (f_1)$ and by multiplying by a fraction, we can assume f_1 has integer coefficients and content 1. Then $M = (f_1)$, for if $h \in M$, then $h \in M''$ and has integer coefficients, so $h = gf_1$ and is reducible in $\mathbb{Q}[x]$. Therefore, by Gauss's lemma, $g \in \mathbb{Z}[x]$ so $M = (f_1)$. But then $\mathbb{Z}[x]/M$ will not be a field. This is because $\mathbb{Z} \hookrightarrow \mathbb{Z}[x]/M$ and so this quotient is infinite. If $\deg f_1 > 0$, then there exists $n \in \mathbb{Z}$ such that $f_1(n) \neq 0, 1, -1$ and thus has a prime divisor p. Then the map $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[p]$ by $\varphi(x) = n \pmod p$ satisfies

$$\varphi(f_1(x)) = f_1(\varphi(x)) = f_1(n) = 0 \pmod p.$$

Thus we have a well-defined $\tilde{\varphi} : \mathbb{Z}[x]/(f_1) \to \mathbb{Z}[p]$. Domain is infinite, codomain is finite, so if $\tilde{\varphi}$ is not the zero map, it will have a non-trivial proper kernel. Observe that if $\tilde{\varphi}(1) = 0 \pmod p$, then there exists $g, h \in \mathbb{Z}[x]$ such that $gf_1 + hp = 1$. But if we evaluate at n, we get $g(n)f_1(n) + h(n)p = 1$ is a contradiction since the LHS is divisible by p. $\tilde{\varphi}$ cannot be the zero map, so $\mathbb{Z}[x]/(f_1)$ is not a field, so case 2 is not possible.

■

2 January 5, 2022

2.1 *Normal and separable extensions, Splitting fields*

Recall (last thing from 2021)

Proposition 2.1. *L algebraically closed, and $\sigma : F \to L$ a non-trivial field homomorphism. If E/F is an algebraic extension, then there exists $\tilde{\sigma}$ such that*

$$\begin{array}{ccc} E & \xrightarrow{\tilde{\sigma}} & L \\ \cup & \nearrow_{\sigma} & \\ F & & \end{array}$$

such that $\tilde{\sigma}|_F = \sigma$.

Note: $\tilde{\sigma}$ not unique.

Separable

Definition (Separable). E/F is any algebraic extension.

1. $\alpha \in E$ is **separable** (over F) if $\mathrm{Irr}_F(\alpha)$ has all distinct roots.
2. E/F is separable if every element is separable.
3. $p(x) \in F[x]$ is separable if all its roots are distinct.

Remark 2.1 — Condition (2) is not very practical. We'll work around it. We'll show $F(\alpha)/F$ is separable iff α is separable.

Disclaimer: not easy to be a non-separable extension.

L/F a finite extension. Consider

$$\Sigma_{\mathrm{id}}(L/F) = \left\{ \tilde{\sigma} : L \to F^{\mathrm{alg}} \middle| \tilde{\sigma}|_F = \mathrm{id} \right\}$$

where $\tilde{\sigma}$ are field homomorphisms.

Example 2.1. $F = \mathbb{Q}$ and $L = \mathbb{Q}\left(\sqrt[3]{2}\right)$. What is the size of $\Sigma_{\mathrm{id}}(L/F)$. Answer is 3.

Claim 2.1 — $x^3 - 2$ is fixed by any $\tilde{\sigma}$, so for all $\tilde{\sigma}$, $\tilde{\sigma}\left(\sqrt[3]{2}\right)$ is a root of $x^3 - 2$ again, and there are 3 distinct roots. $\omega = e^{2\pi i/3}$, $\omega^3 = 1$. The roots of $x^3 - 2$ are $\sqrt[3]{2}\omega^k$, $k \in \{0, 1, 2\}$.

$$\#\Sigma_{\mathrm{id}}(L/F) = 3 = \#\text{ distinct roots of } x^3 - 2$$

$\tilde{\sigma}$ makes one of the following mappings: $\sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$, or $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2$.

Definition. For L/F a finite extension,

$$|L : F|_{\text{sep}} = \#\Sigma_{\text{id}}(L/F)$$

Remark 2.2 — L/F separable iff $|L : F|_{\text{sep}} = |L : F|$. This follows from the following proposition.

Proposition 2.2. *L/F a finite extension.*

1. $\alpha \in L$, $|F(\alpha) : F|_{sep} =$ *# distinct roots of* $Irr_f(\alpha)$.
2. $|L : F|_{sep} \leq |L : F|$
3. $|L : F|_{sep}$ *is multiplicative. ($E/L/F$ implies that)*

$$|E : L|_{sep} \cdot |L : F|_{sep} = |E : F|_{sep}$$

Proof. HW problem. Hint: L/F, $\sigma : F \to F^{\text{alg}}$.

$$\Sigma_\sigma(L/F) = \left\{ \tilde{\sigma} : L \to F^{\text{alg}} \middle| \tilde{\sigma}|_F = \sigma \right\}$$

Then $\#\Sigma_\sigma$ is the same for σ and id. ∎

Corollary 2.3. *L/F finite, $\alpha \in L$. TFAE.*

1. *α separable.*
2. *$Irr_F(\alpha)$ has distinct roots.*
3. $|F(\alpha) : F|_{sep} = |F(\alpha) : F|$.
4. *$F(\alpha)/F$ separable.*

Corollary 2.4. *L/F separable iff $|L : F| = |L : F|_{sep}$.*

Proof. HW. ∎

Are there non-separable extensions?

Claim 2.2 — $p(x)$ is an irreducible polynomial over F. Then $p(x)$ is separable.

Proof. Suppose $p(x)$ has a double root α. Then

$$p(x) = (x - \alpha)^2 q(x) \in F(\alpha).$$

Differentiate.

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

is divisible by $(x-\alpha)$. In other words, $p'(x) = (x-\alpha)g(x) \in F(\alpha)$. But $p'(x) \in F[x]$. Conclusion: $(p(x), p'(x)) \neq 1$. We are in an ED ($F[x]$), so $1 \leq d(x) = (p(x), p'(x))$. $d(x)|p(x) \Rightarrow p(x)$ is not irreducible. Contradiction. ■

This proof is wrong. Where is the problem? It might happen that $p'(x) = 0$. How can it happen? What can we say about F?

Recall:

$$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \Rightarrow p'(x) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots.$$

We must have $nx^{n-1} = 0$, which can only happen if char $F = p$ and $p \mid n$.

x^2, x^2+1 are both reducible, so they don't work. $\mathbb{F}_p$ is not good enough. All extensions of $\mathbb{F}_p$ (a perfect field) are separable.

3 January 7, 2022

Question 3.1 — Non-separable polynomial $f(x) \in F[x]$. Need characteristic of F to be some prime p. Take $\mathbb{F}_p(t)$. Then consider

$$f(x) = x^p - t \in \mathbb{F}_p(t)[x] \quad \text{and} \quad f'(x) = px^{p-1} = 0.$$

$f(x)$ is irreducible over F (exercise). $f(x)$ has a root $\sqrt[p]{t} \in F\left(\sqrt[p]{t}\right)$.

$$f(x) = x^p - t = \left(x - \sqrt[p]{t}\right)^p$$

MISSING STUFF FIRE ALARM FIX THIS

Definition. E/F is a **splitting field** for $f(x)$ if

- $f(x)$ splits into linear factors in E, and
- E is minimal with respect to this property (that is, f does not not split in any subextension of E).

Example 3.1. $f(x) = x - a$, $a \in F$. F is the splitting field.

Remark 3.1 — Let $\alpha_1, \ldots, \alpha_n$ be all the roots of f. $E = F(\alpha_1, \ldots, \alpha_n)$.

Example 3.2. $f(x) = x^3 - 2$. What is $E/\mathbb{Q}$ the splitting field? What is $|E : \mathbb{Q}|$. f has roots $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$, i.e.

$$f(x) = \left(x - \sqrt[3]{2}\right)\left(x - \sqrt[3]{2}\omega\right)\left(x - \sqrt[3]{2}\omega\right)$$

$$E = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\right) = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$$

$$\mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$$

$$\mathbb{Q}\left(\sqrt[3]{2}\right) \qquad\qquad \mathbb{Q}(\omega)$$

$$\mathbb{Q}$$

Proposition 3.1. *For all $f(x) \in F[x]$, there exists a splitting field E/F.*

Proof. Use algebraic closure, intersect things. ■

> **Definition.** E/F is **normal** if for all irreducible $f(x) \in F[x]$, if f has a root in E, then it splits in E (all roots in E).

Example 3.3.

1. $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ is not normal.
2. $\mathbb{Q}(i)$ is normal.
3. Base field is normal.
4. Any E/F with $[E:F] = 2$.
5. $\mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$ is normal with degree 6.

Observation: for irreducible $f \in F[x]$ with $\deg f = n$, and E/F a splitting field, then $n \leq |E:F| \leq n!$. Inequality is tight for all n.

4 January 10, 2022

Proposition 4.1. *$f(x) \in F[x]$, splitting field for f exists.*

Proof. Exercise. ■

Proposition 4.2. *Field isom $\sigma F \to \tilde{F}$, $f(x) \in F[x]$ irreducible. $\sigma(f) \in \tilde{F}[x]$ is defined to be the polynomial obtained by applying σ to the coefficients of f. In this way, we can always extend maps b/w fields to maps b/w polynomial rings. Let α be a root of f, and $\tilde{\alpha}$ be a root of $\sigma(f)$. Then there exists unique isomorphism $\tilde{\sigma}$ such that $\tilde{\sigma}(\alpha) = \tilde{\alpha}$ and the following diagram commutes.*

$$\begin{array}{ccc} F(\alpha) & \longrightarrow & \tilde{F}(\tilde{\alpha}) \\ \Big| & & \Big| \\ F & \xrightarrow{\sigma} & \tilde{F} \end{array}$$

Proof. Let $f(x) = \mathrm{Irr}_F(\alpha)$. Then $\sigma(f)(x) = \mathrm{Irr}_F(\tilde{\alpha})$. For any $\beta \in F(\alpha)$, we can write

$$\beta = \sum_{i=0}^{m} b_i \alpha^i \Rightarrow \tilde{\sigma}(\beta) = \sum \tilde{\sigma}(b_i \alpha^i) = \sum \sigma(b_i)\sigma(\alpha)^i = \sum \sigma(b_i)\tilde{\alpha}^i$$

We can write

$$F(\alpha) \simeq \frac{F[x]}{(f(x))} \quad \text{and} \quad \tilde{F}(\tilde{\alpha}) = \frac{\tilde{F}[x]}{(\sigma(f)(x))}.$$

We have isomorphim $\tilde{\sigma} : F \to \tilde{F}$ which can be extended to isomorphism $\tilde{\sigma} : F[x] \to \tilde{F}[x]$ (just sending $x \mapsto x$).

$$\tilde{\sigma}(f(x)) = \sigma(f)(x) \Rightarrow \tilde{\sigma} : (f(x)) \simeq (\sigma(f)(x))$$

which implies that we still have an ismorphism when we mod out.

$$\tilde{\sigma} : \frac{F[x]}{(f(x))} \simeq \frac{\tilde{F}[x]}{(\sigma(f)(x))}$$

$\tilde{\sigma} : F(\alpha) \simeq \tilde{F}(\tilde{\alpha})$. ■

Example 4.1.

$$\begin{array}{ccc} \mathbb{Q}\left(\sqrt[3]{2}\right) & \xrightarrow{\sqrt{2}} & \mathbb{Q}\left(\sqrt[3]{2}\omega\right) \\ \Big| & & \Big| \\ \mathbb{Q} & \longrightarrow & \mathbb{Q} \end{array}$$

Corollary 4.3. *(existence of "extensions of hom") The diagram commutes.*

$$\begin{array}{ccc} E & \overset{\exists\tilde{\sigma}}{\dashrightarrow} & \tilde{F}^{\alpha} \\ \big| & & \big| \\ F & \xrightarrow{\sigma} & \tilde{F} \end{array}$$

Proof. Induction. ∎

Equivalent conditions for normality.

Theorem 4.4. *E/F a finite extension. TFAE.*

1. *For all $\sigma : \sigma : E \to F^{\alpha}$ such that $\sigma|_F = id$, $\sigma(E) = E$.*
2. *E is a splitting field for some $f(x) \in F[x]$ (not irreducible).*
3. *E/F normal.*

Proof. (1) to (3) to (2) to (1).
(1) to (3): $f(x) \in F[x]$ irreducible. Let $\alpha \in E$ be a root of f, and $\beta \in E$ another root of f. We want to show that $\beta \in E$.

$$\begin{array}{ccc} E & \xrightarrow{\exists\tilde{\sigma}} & F^{\text{alg}} \\ \big| & & \big| \\ F(\alpha) & \xrightarrow{\exists\sigma} & F(\beta) \\ \big| & & \big| \\ F & \xrightarrow{\text{id}} & F \end{array}$$

There exists $\sigma : F(\alpha) \to F(\beta)$ where $\sigma(\alpha) = \beta$ and $\sigma|_F = \text{id}$. There exists $\tilde{\sigma} : E \to F^{\text{alg}}$ such that $\tilde{\sigma}|_{F(\alpha)} = \sigma$. But by (1), $\tilde{\sigma}(E) = E$ so $\beta = \sigma(\alpha) = \tilde{\sigma}(\alpha) \in E$.
(3) to (2): Let $\alpha \in E$. Let $f(x) = \text{Irr}_F(\alpha)$. Since E is normal, $f(x)$ splits in E. If $F(\alpha) = E$, we are done. If not, let $f(x) = f_1(x)$, and pick $\alpha_2 \in E \setminus F(\alpha)$ and repeat the process. Since E/F, this will terminate.
(2) to (1): Indeed, let $\alpha_1, \ldots, \alpha_n$ be all the roots of $f(x)$. Then $F(\alpha_1, \ldots, \alpha_n) = E$. But σ permutes the roots.

$$\{\alpha_1, \ldots, \alpha_n\} \to^{\sigma} \{\alpha_1, \ldots, \alpha_n\}$$

E is generated by these roots, so σ must leave E invariant.

$$\sigma(E) = \sigma(F(\alpha_1, \ldots, \alpha_n)) = E$$

∎

Definition (Galois group)**.** For extension E/F, the **Galois group** of E/F is *Galois group*

$$\text{Gal}(E/F) = \text{Aut}_F(E) = \{\sigma : E \to E : \sigma|_F = \text{Id}\}.$$

Remark 4.1 — If E/F is finite normal, then $\mathrm{Gal}(E/F) = \Sigma_{\mathrm{id}}(E/F) = \left\{\sigma : E \to F^{\mathrm{alg}} : \sigma|_F = \mathrm{id}\right\}$.

Definition (Galois extension)**.** E/F is Galois if E/F is normal separable. *Galois extension*

Looking ahead, if E/F is a finite Galois extension, then $|\mathrm{Gal}(E/F)| = |E : F|$.

Galois theory studies correspondence between Galois extensions (E/F) and Galois groups ($\mathrm{Galois}(E/F)$).

5 January 12, 2022

5.1 *Normal extensions and Galois groups*

Proposition 5.1.

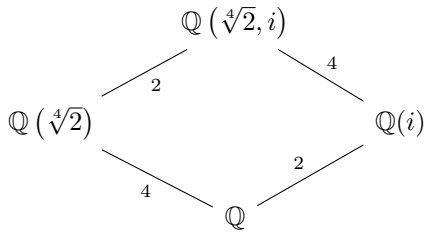
1. *If we have $L/E/F$, where L/F is normal, then L/E is also normal.*
2. *If we have $E_1/F, E_2/F$ normal with $E_1, E_2 \subset F^{alg}$, then composites and intersections are normal, i.e. $E_1E_2/F, E_1 \cap E_2/F$ are normal.*

Proof. HW. ■

Example 5.1.

1. $|E : F| = 2 \Rightarrow E/F$ is normal. Indeed, $\alpha \in E$, $E = F(\alpha)$; take $f(x) = \mathrm{Irr}_F(\alpha)$, so $\deg f = 2$. $f(x) = (x-\alpha)(x-\beta)$ $f(x) \in F[x]$ and $x - \beta \in E[x]$ together imply that $x - \beta \in E[x]$. Alternatively, $f(x) = x^2 + ax + b$, α, β roots of $f(x)$ implies that $\alpha + \beta = -a$ and $\alpha\beta = b$., so $\beta = -a - \alpha \in E$.
2. $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{Q}\left(\sqrt[4]{2}\right)$. Each intermediate extension is degree 2, and so is normal. The large extension $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$ is not normal. $\mathrm{Irr}_{\mathbb{Q}}\left(\sqrt[4]{2}\right) = x^4 - 2$, which is irreducible by Eisenstein $(p = 2)$. Roots of $x^4 - 2$ are $\sqrt[4]{2}i^k$, where $i^2 = -1$ and $k \in [4]$.

What is the "normal closure" of $\mathbb{Q}\left(\sqrt[4]{2}\right)\mathbb{Q}$? In other words, what is the splitting field of $x^4 - 2$. It is precisely $\mathbb{Q}\left(\sqrt[4]{2}, i\right) = \mathbb{Q}\left(\sqrt[4]{2}, \sqrt[4]{2}i\right)$. Its degree is 8.



Recall that we defined $\mathrm{Gal}(E/F) = \mathrm{Aut}_F(E)$. If E/F is normal then it is just $\Sigma_{\mathrm{id}}(E/F)$ that we have seen before.

Example 5.2. Take $E = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$, where ω is third primitive root of unity. E is the splitting field of $x^3 - 2$. $|E : \mathbb{Q}| = 6$. Normal and separable implies Galois. Expectation $|\mathrm{Gal}(E/\mathbb{Q})| = |E : \mathbb{Q}| = 6$. So is it $\mathbb{Z}/6\mathbb{Z}$ or

S_3? $G = \mathrm{Gal}(E/\mathbb{Q})$ permutes the roots of $x^3 - 2$. This means $G < S_3$. It has order 6, so it must be S_3.

Let's also compute G explicitly. $\varphi : E \to E$ automorphism which fixes $\mathbb{Q}$. Just need to specify $\varphi\left(\sqrt[3]{2}\right)$ and $\varphi(\omega)$ since E is generated by $\sqrt[3]{2}, \omega$. Our options are that $\sqrt[3]{2} \to \{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ and $\omega \to \{\omega, \omega^2\}$. Let $\sigma : E \to E$ be defined by fixing ω and sending $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$. Let $\tau : E \to E$ be defined by fixing $\sqrt[3]{2}$ and sending $\omega \mapsto \omega^2$. Notice that $\sigma^3 = \tau^2 = \mathrm{id}$. We can also check that $\tau\sigma\tau = \sigma^2$. Therefore, we have an explicit isomorphism $G \simeq S_3$.

Claim 5.1 — For E/F (finite) Galois, $|E : F| = |\mathrm{Gal}(E/F)|$.

Example 5.3. (bad cases)

1. $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ is not normal.

$$\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right) = \left\{\sigma : \mathbb{Q}\left(\sqrt[3]{2}\right) \to \mathbb{Q}\left(\sqrt[3]{2}\right) : \sigma|_{\mathbb{Q}} = \mathrm{id}\right\}$$

   Any such $\sigma \neq \mathrm{id}$ takes $\sqrt[3]{2}$ to $\sqrt[3]{2}\omega$ or $\sqrt[3]{2}\omega^2 \notin \mathbb{Q}\left(\sqrt[3]{2}\right)$, so the Galois group is trivial.
2. $\mathbb{F}_p(t) = F$, $E = F\left(\sqrt[p]{t}\right)$. $\mathrm{Irr}_F\left(\sqrt[p]{t}\right) = x^p - t$ has only one root, so since automorphisms permute roots, there is only one automorphism, the identity. The Galois group is trivial.

6 January 14, 2022

6.1 Galois theory

We need 2 fundamental theorems about algebraic extensions.

Theorem 6.1 (Primitive element theorem)**.** *Suppose K/k is a finite separable extension. Then there exists $\alpha \in K$ such that $K = k(\alpha)$.*

Theorem 6.2 (Normal basis theorem)**.** *K/k a finite Galois extension, then there exists irreducible $f(x) \in k[x]$ such that*

1. *$f(x) = \prod(x - \alpha_i)$ in $K[x]$ and*
2. *$\{\alpha_i\}$ form a basis of K/k (as a vector space over k).*

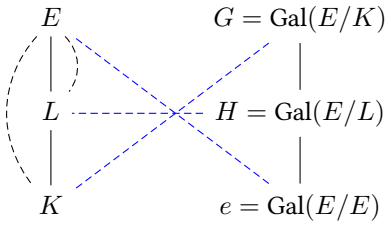
Proof of both in homework.

Example 6.1. $E = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$, our favorite example. This is the splitting field of $x^3 - 2$.

1. Primitive element theorem tells us there exists $\alpha \in E$ such that $E = \mathbb{Q}(\alpha)$. Note that $\sqrt[3]{2}\omega$ does not work, since its minimal polynomial is also $x^3 - 2$, but the extension has degree 6. Instead we can check $\sqrt[3]{2} + \omega$ (consider all the conjugates of this, and multiply all linear factors). To compute the conjugates (other groups), let $G = \text{Gal}(E/\mathbb{Q}) = S_3$, whose generators we computed last time. Then we can just compute $\varphi(\alpha)$ for each $\varphi \in G$. The roots will be $\left\{\sigma_i\left(\sqrt[3]{2} + \omega\right)\right\}$, where σ_i are the elements of G. They will all be distinct.
2. What is a normal basis $E/\mathbb{Q}$. All conjugates of $\alpha = \sqrt[3]{2} + \omega$ form a basis. In other words, all roots of $\text{Irr}_F\left(\sqrt[3]{2} + \omega\right)$.

Galois Theory provides a kind of dictionary between extensions and groups. Allows us to transform questions about extensions into questions about groups.

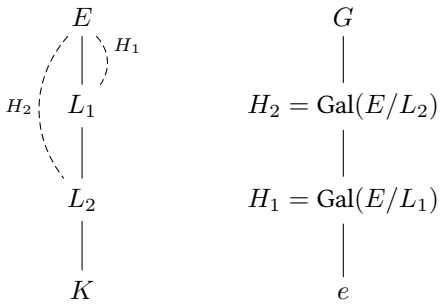
Take $E/L/K$, where E/K is Galois, and $G = \text{Gal}(E/K)$. Then we have one-to-one order reversing correspondence between subextensions and subgroups. $K \subset L \subset E \sim e < H < G$. Below, blue dashed lines indicate correspondence, and dashed lines indicate Galois extensions. Solid lines on the right indicate subgroup/subfield inclusion.



Subextensions $E/L/K \leftrightarrow$ subgroups $H = \text{Gal}(E/L) < G$.

This correspondence satisfies various nice properties.

1. L/K Galois (normal) $\Leftrightarrow H = \text{Gal}(E/L) \triangleleft G$. In that case, $\text{Gal}(L/K) \simeq G/H$.
2. In the diagram above, $G/H = \text{Gal}(L/K)$.
3. $L_2 \subset L_1 \Leftrightarrow H_1 < H_2$.



Remark 6.1 — The bigger L/K is, the smaller $H = \text{Gal}(E/L)$ gets.

The original application of solvability: E/K is solvable in radicals

Theorem 6.3 (Abel-Ruffini)**.** *There exists $f(x) \in \mathbb{Q}[x]$ with degree 5 not solvable in radicals.*

Proof. Need to construct $E/\mathbb{Q}$ such that $\text{Gal}(E/\mathbb{Q}) \simeq A_5, S_5$. ■

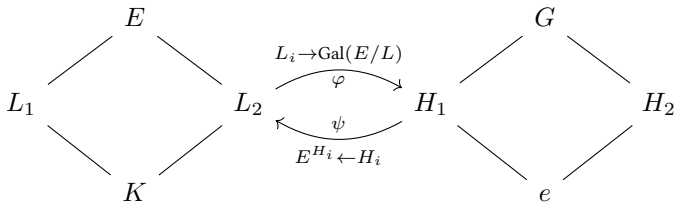
Fixed field

Definition (Fixed field)**.** E/K, algebraic extension. $H < G$, $G < \text{Aut}_k(E)$.

$$E^H = \{\alpha \in E \mid \forall \sigma \in H, \sigma(\alpha) = \alpha\}$$

the H-invariants in E. This is the **fixed field** of H.

$E \to E^H$ and $L \to \text{Gal}(E/L)$ are how we go back and forth between fields and groups.



The following properties hold.

L subextension of E corresponds to H subgroups of G (is a bijection).

Theorem 6.4. *The correspondence we have been talking about holds.*

Theorem 6.5. *Under the bijection from the previous theorem,*

$$L_1 \cap L_2 \leftrightarrow H_1 H_2$$

$$L_1 L_2 \leftrightarrow H_1 \cap H_2$$

$$L_1 \subset L_2 \leftrightarrow H_1 > H_2$$

Theorem 6.6. *L/K is Galois iff $H \triangleleft G$. In that case, Gal$(L/K) = G/H$.*

7 January 19, 2022

Remark 7.1 — E^G is indeed a field.

Lemma 7.1. *If E/K is Galois, let $G = Gal(E/K)$. Then $E^G = K$. In other words, the invariant under the Galois action is the ground field.*

Proof. First $K \subset E^G$, since for all $\sigma \in G$, $\sigma|_K = \mathrm{id}$. We need o show that $E^G \subset K$. Let $\alpha \in E^G$ with $f(x) = \mathrm{Irr}_K(\alpha)$. If f has degree 1, then $f(x) = x - \alpha$ and $\alpha \in K$. Suppose $\deg f \geq 2$, and let β be another root. E/K is Galois, so f is separable (and normal), so $\beta \neq \alpha$ and $\beta \in E$. Then by the "extension property,"

$$\begin{array}{ccc} E & \xrightarrow{\exists \tilde{\sigma}} & E \\ | & & | \\ K(\alpha) & \xrightarrow{\exists \sigma} & K(\beta) \\ | & & | \\ K & \xrightarrow{\mathrm{id}} & K \end{array}$$

with $\tilde{\sigma}|_{K(\alpha)} = \sigma$, $\sigma(\alpha) = \beta$, and $\sigma_K = \mathrm{id}$. But $\tilde{\sigma}(\alpha) = \alpha$ ($\tilde{\sigma} \in \mathrm{Gal}(E/K) = G$). $\alpha \in E^G \Rightarrow \alpha = \beta$. Contradiction. f has degree 1, so $\alpha \in K$. Hence, $E^G \subset G$. ∎

Corollary 7.2. *The*

$$\begin{array}{ccc} E & & G \\ & \overset{L \to Gal(E/F)}{\underset{E^H \leftarrow H}{\overset{\varphi}{\underset{\psi}{\rightleftarrows}}}} & \\ L & & H \\ K & & E \end{array}$$

Proof. $L \to \mathrm{Gal}(E/L) = H$. Take $E = E, K = L, G = H$, so by the previous lemma, $E^H = L$. ∎

Remark 7.2 — It implies that φ is injective.

Lemma 7.3. *E/K separable (not assume finite). Suppose for all $\alpha \in E$, $|K(\alpha) : K| \leq n$. Then $|E : K| \leq n$.*

Proof. Let $\gamma \in E$ such that $|K(\gamma) : K|$ is maximal possible. Then $|K(\gamma) : K| = \deg \mathrm{Irr}_K(\gamma)$. Claim: $E = K(\alpha)$. Why? Suppose not. Let $\beta \in E \setminus K(\gamma)$. Consider $K(\gamma, \beta) \supsetneq K(\gamma)$. By the primitive element theorem, $K(\gamma, \beta) = K(\alpha)$ for some

$\alpha \in E$. But then $|K(\alpha) : K| > |K(\gamma) : K|$ which contradicts choice of γ. This proves the claim.

$$E = K(\gamma) \Rightarrow |E : K| = |K(\gamma) : K| \leq n$$

■

Theorem 7.4 (Artin). *K a field. $G < Aut(K)$, $|G| = n$. Let $k = K^G$. Then*

1. *K/k is a Galois extension of degree n.*
2. *$Gal(K/k) = G$.*

Proof. $\alpha \in K$. Let $\{\sigma_1(\alpha), \ldots, \sigma_m(\alpha)\}_{\sigma_i \in G}$ be the largest set of distinct conjugates of α. G acts on this set by permutations (by construction). Consider

$$f(x) = \prod_{i=1}^{m} (x - \sigma_i(\alpha)).$$

Observations:

1. $f(x) \in k[x]$. This is because G leaves f invariant (by permuting the linear factors), and $k = K^G$. Alternatively, coefficients of f are symmetric polynomials (over α conjugates), so they remain invariant.
2. $\deg f = m \leq n$.
3. $f(x)$ is separable.
4. $\alpha = \sigma_1(\alpha)$ is a root ($\sigma_1 = e \in G$).

Then let L be the splitting field of f. $L < K$. We have $|L : k| \leq n$. L is normal as a splitting field, L is separable since f is separable. Hence by the second lemma, $|K : k| \leq n$. Also K/k is normal[1] and separable so we have Galois. We have $G < \text{Gal}(K/k) = \text{Aut}_k(K)$ by construction of k. So $|\text{Gal}(K/k)| = |K : k| \leq n$ and $|\text{Gal}(K/k)| \geq |G| = n$, so we have equality. G has order n as well, so $\text{Gal}(K/k) = G$. ■

[1] *Why?*

8 January 21, 2022

8.1 Proof of Galois correspondence theorems

Proof of correspondence.

Proof. First, $\psi \circ \varphi$ sends $L \to \varphi\text{Gal}(E/L) = H \to^{\psi} E^H$. This is just L by a previous lemma (2 lectures ago), so $\psi \circ \varphi = \text{id}$. On the other hand, $H \to^{\psi} E^H \to^{\varphi} \text{Gal}(E/E^H)$, and by Artin's theorem, E/E^H is Galois, and $\text{Gal}(E/E^H) = H$ (by taing $K = E$ and $G = H$ in Artin's theorem). Therefore, $\varphi \circ \psi = \text{id}$. ∎

Read Dummit and Foote for proof of second theorem.

Proof of third theorem.

Proof. Assume L/K is Galois. Want to show that H is a normal subgroup of G. Take $G \to^{f} \text{Gal}(L/K)$, which takes $\sigma \in G = \text{Gal}(E/K)$ where $\sigma : E \to E$ and sends it to its restriction $\sigma_L : L \to L$ (well-defined since L/K is normal). In other words, $f(\sigma) = \sigma|_L$. Claim: $H - \text{Ker } f$. Indeed, $f(\sigma) = \text{id} \Leftrightarrow \sigma_L = \text{id}$. This implies $\sigma \in \text{Gal}(E/L) = \text{Aut}_L(E)$. This proves the claim, so $H = \text{Ker } f$ is normal in G. We also claim that $f : G \to \text{Gal}(L/K)$ is surjective. This is because any automorphism of L can be extended to an automorphism of E (extension of homomorphisms property). For all $\tau : L \to L$, $\tau|_K = \text{id}$, there exists $\sigma : E \to E$ such that $\sigma_L = \tau$. So, $f : G \to \text{Gal}(L/K)$, $\text{Ker } f = H$. By the first isomorphism theorem, $\text{Gal}(L/K) = G/H$.

On the other hand, suppose $H \triangleleft G$. We would like tos how that L/K is Galois. L/K is Galois. L/K is separable since $/K$ is separable. Only need to show it is normal. Suppose otherwise. If L is not normal, then there exists $\sigma : L \to L'$ different from L such that $\sigma|_K = K$. Extend σ to E. $\tilde{\sigma} : E \to E$. Let $H' = \text{Gal}(E/L')$ which we can do since E/K is Galois.

$$\begin{array}{ccc} E & \longrightarrow & E \\ {\scriptstyle H}\big(\big| & & \big| \big){\scriptstyle H'} \\ L & \xrightarrow{\sigma} & L' \\ \big| & & \big| \\ K & \longrightarrow & K \end{array}$$

Claim: $H' = \tilde{\sigma} H \tilde{\sigma}^{-1}$. That is, if τ fixes L', then $\tilde{\sigma}\tau\tilde{\sigma}^{-1}$ fixes L'. Why? $\tilde{\sigma}H\tilde{\sigma}^{-1} < \text{Aut}_{L'}(E)$. Indeed, let $\tau \in H = \text{Gal}(E/L)$. Let $a \in L'$, and calculate

$$\tilde{\sigma}\tau\tilde{\sigma}^{-1}(a) = \tilde{\sigma}\tau\tilde{\sigma}^{-1}|_{L'}(a) = \tilde{\sigma}\tau\sigma^{-1}(a).$$

$\sigma^{-1}(a) \in L$, so $\tau(\sigma^{-1}(a)) = \sigma^{-1}(a)$ since $\tau|_L = \text{id}$ which means

$$= \sigma(\sigma^{-1}(a)),$$

so $\tilde{\sigma}\tau\tilde{\sigma}^{-1}|_{L'} = L$. Hence $\tilde{\sigma}H\tilde{\sigma}^{-1} < H'$. But they have the same order: $|H| = |E : L| = |E : L'| = |H'|$, so $\tilde{\sigma}H\tilde{\sigma}^{-1} = H$. Since H is normal, $H = H'$. By the first

correspondence theorem, since H corresponds to L and H' corresponds to L', $L = L'$. Contradiction. L was normal. ■

Recall equivalent conditions for E/K normal (alg).

1. If $f \in K[x]$ has a root in E, it splits in E.
2. For all $\sigma : E \to K^{\text{alg}}$, $\sigma|_K = \text{id}$, $\sigma(E) = E$.
3. E is a splitting field of a family of polynomials.

9 January 24, 2022

Example 9.1. Suppose f has degree 3, f irreducible, $f \in k[x]$, and $\text{char}(k) \neq 2, 3$. Let K_f be the splitting field of f over k. $|K_f : k| = 3, 6$.

- Recall $f = x^3 - 2$. $K_f = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$. $|K_f : \mathbb{Q}| = 6$.
- What about 3? Consider the same f but over the field $k = \mathbb{Q}(\omega)$. $|\mathbb{Q}\left(\sqrt[3]{2}, \omega\right) : \mathbb{Q}(\omega)| = 3$.
- Consider also $k = \mathbb{F}_3(t)$.
- $x^3 - t$ over $\mathbb{C}(t)$.

What about $\mathbb{Q}$? We'll see later.

Proposition 9.1. *$f(x) \in k[x]$, $\deg f = 3$. Let α be a root of f. Then TFAE. char$(k) \neq 2, 3$ (to prevent separability trouble)*

1. *$k(\alpha)/k$ is not normal.*
2. *$[K_f : k] = 6$.*
3. *Gal$(K_f/k) = S_3$.*

Proof. Breakout rooms exercise. ∎

Definition. Take irreducible f of degree 3 with roots $\alpha_1, \alpha_2, \alpha_3$. We say that

$$\Delta = \delta^2$$

is the **discriminant** of f where

$$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1).$$

Note that Δ is well-defined by f.

Remark 9.1 — If $\text{char}(k) \neq 2, 3$,

1. distinct α_i means $\Delta \neq 0$, and
2. we can assume $f(x) = x^3 + px + q$ (linear substitution leaves everything we care about invariant).

Lemma 9.2. 1. *$\Delta \in k$.*

2. *$\Delta = -4p^3 - 27q^2$.*

Proposition 9.3. *Same assumptions as previous propositions. TFAE.*

1. *$\Delta \notin k^2$ (Δ is not the square of some element in k)*
2. *$k(\alpha)/k$ is not normal.*

3. $[K_f : k] = 6$.
4. $Gal(K_f/k) = S_3$.

10 January 26, 2022

We were discussing degree 3 polynomials $f \in k[x]$, where $\text{char}(k) \neq 2, 3$.

Remark 10.1 — Why should we expect a formula like $\Delta = -4p^3 - 27q^2$ (see Dummit and Foote for computation)? Δ is fixed by action of S_3 on $\{\alpha_i\}$ which means Δ can be expressed in terms of elementary symmetric functions.

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

$$\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = p$$

$$\alpha_1\alpha_2\alpha_3 = -q$$

Degree of $\Delta = 6$.

Proof of proposition from last time.

Proof. (1) is equivalent to sauing $\delta \notin k^2$. $\delta \in k$ is equivalent to saying $\text{Gal}(K_f/k)$ (which is S_3) fixes δ. $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$. By symmetry any permutation of the roots negates δ or leaves it fixed. $\text{Gal}(K_f/k)$ does not contain elements of degree 2 (transpositions), which is equivalent to saying $\text{Gal}(K_f/k) < A_3 \neq S_3$. This is true iff $|\text{Gal}(K_f/k)| = 3$. This gives us (1) iff (2), (3), and (4) (recall the previous proposition which shows equivalence among the last three conditions). ∎

Remark 10.2 — Condition (1) is practical. Use it for HW.

Note: if ever f reducible, Galois group (by correspondence) obtained by product of Galois groups of the irreducible components.

Proposition 10.1. $\deg f = p$ *(prime) with* $f \in \mathbb{Q}[x]$ *irreducible. If* f *has exactly 2 non-real roots, then Gal*$(\mathbb{Q}_f/\mathbb{Q}) = S_p$.

Proof. By a HW problem, we know that S_p is generated by a cycle of length p and any transposition. Take α any root of f, where we know $|\mathbb{Q}(\alpha) : \mathbb{Q}| = p = \deg f$, so p divides $|\mathbb{Q}_f : \mathbb{Q}| = |\text{Gal}(\mathbb{Q}_f/\mathbb{Q})|$ which we will call G. Note that we assume everything lies in some fixed algebraic closure of $\mathbb{Q}$. p divides $|G|$, $G < S_p$. G has an element of order p (which are precisely cycles of length p), so G contains a p-cycle. Let α_1, α_2 be the only 2 non-real roots. Then complex conjugation is an automorphism of $\mathbb{Q}_f$. It permutes α_1, α_2 and fixes all other (real) roots. We have a p-cycle and a transposition, so we are done.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{z \mapsto \overline{z}} & \mathbb{C} \\ | & & | \\ \mathbb{Q}_f & \xrightarrow{z \mapsto \overline{z}} & \mathbb{Q}_f \end{array}$$

■

The condition that we have exactly 2 non-real roots is essential. If we have 4 complex roots, conjugation is still an automorphism, but it is a product of 2 transpositions, not just a single transposition, so we don't know that we have all of S_p.

Example 10.1. Consider $f(x) = x^5 - x - 1$ in $\mathbb{Q}[x]$. What are $[\mathbb{Q}_f : \mathbb{Q}]$ and $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$? Can we use the previous proposition here? Namely, let's see how many non-real roots it has. We can compute that it has exactly 1 real root. We cannot use the previous proposition to prove anything about the Galois group.

Another method involes "reduction mod p."

10.1 Finite Fields

For prime p, we have $\mathbb{F}_p$, the field of p elements. If F has characteristic p, then $\mathbb{F}_p \subset F$ implies $F/\mathbb{F}_p$ is an extension. Assume f is finite. Then $F/\mathbb{F}_p$ is a finite (and therefore algebraic) extension. Let $|F : \mathbb{F}_p| = n = \dim_{\mathbb{F}_p} F$. Pick a basis $\{\alpha_i\}$ of F over $\mathbb{F}_p$. Then any $\alpha \in F$ can be written as $\alpha = \sum_{i=1}^{n} a_i \alpha_i$, with $\alpha_i \in \{0, \dots, p-1\}$. Therefore, we have $|F| = p^n$. Notice also that $|F^*| = p^n - 1$. Lagrange tells us for any $\alpha \neq 0$ in F, $\alpha^{p^n - 1} = 1$. Then for any $\alpha \in F$, we have $\alpha^{p^n} = \alpha$. Fix $\mathbb{F}_p \subset \mathbb{F}_p^{\mathrm{alg}}$

Theorem 10.2 (Structure of finite fields)**.** *p prime. For any $n \in \mathbb{Z}_{>0}$, there exists a unique finite field $F/\mathbb{F}_p$ such that*

1. $|F| = p^n$,
2. $|F : \mathbb{F}_p| = n$,
3. *F is a splitting field of $x^{p^n} - x = f(x)$, and is a Galois extension of degree n.*

Remark 10.3 — Addendum: $F = \mathbb{F}_{p^n}$.

Proof. $f(x) = x^{p^n} - x$ is separable. Indeed, $f'(x) = -1 \neq 0$. Let F be the set of all roots of $f(x)$ in $\mathbb{F}_p^{\mathrm{alg}}$. Since f is separable, it has p^n distinct roots, so $|F| = p^n$. It turns out F is actually a field. $\alpha, \beta \in F$ means $\alpha^{p^n} = \alpha$ and likewise for β. Compute

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$$

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$$

$$(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$$

F contains 0 and 1, so F is a field. F is an extension of $\mathbb{F}_p$, that is $\mathbb{F}_p \subset F$ (by Fermat's little theorem). For all $a \in \mathbb{F}_p$, $a^p = a$ implies $a^{p^n} = a$. Hence, $F = (\mathbb{F}_p)_{f(x)}$ which

means $F/\mathbb{F}_p$ is Galois (since f is separable and F is a splitting field). (We'll talk about uniqueness next time.) ■

11 January 28, 2022

Proof Continued. Let $F/\mathbb{F}_p$ be a finite field of size p^n. Then we established that F is a splitting field of $f(x) = x^{p^n} - x$, and splitting fields are unique up to isomorphism. ■

By the theorem, $F/\mathbb{F}_p$ is Galois of degree n ($|F| = p^n$). What is $\mathrm{Gal}(F/\mathbb{F}_p)$.

> **Definition.** We will denote $F = \mathbb{F}_q$ or $F = \mathbb{F}_{p^n}$ to denote the finite field of size p^n ($q = p^n$). The **Frobenius automorphism** $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ which maps $\alpha \mapsto \alpha^p$.

The Frobenius automorphism is a field homomorphism since $\mathrm{char}(\mathbb{F}_{p^n} = p$. $\varphi \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}) = \mathrm{Aut}_{\mathbb{F}_{p^n}}(\mathbb{F}_{p^n})$ since $\varphi|_{\mathbb{F}_p} = \mathrm{id}$. This holds by Fermat's little theorem ($a \in \mathbb{F}_p$, $a^p = a \Rightarrow \varphi(a) = a$).

Proposition 11.1. *$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$ and φ is a generator.*

Proof. $\varphi \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = G$ implies $\langle\varphi\rangle < G$, a cyclic subgroup. We want to show that the order of φ is n. Let $d \leq n$ be the order of φ. Then $\varphi^d = \mathrm{id}$, so $\varphi^d(\alpha) = \alpha^{p^d} = \alpha$, for all $\alpha \in \mathbb{F}_{p^n}$. If $d < n$, then we'd have at most p^d elements in $\mathbb{F}_{p^n}$ since there are only p^d solutions to $\alpha^{p^d} = \alpha$. Hence $d = n$, so $\langle\varphi\rangle = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. ■

Corollary 11.2. *Let $F = \mathbb{F}_q$, with $q = p^n$. For any $m \geq 0$, there exists unique extension E/F of degree $|E : F| = m$, where $E = \mathbb{F}_{p^{nm}}$.*

Proof. For any n, there exists unique $F = \mathbb{F}_{p^n}$. For all $N, m \in \mathbb{Z}_{\geq 0}$, $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \Leftrightarrow n \mid m$. In that case, $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ is (cyclic) Galois extension with $\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^n}) \simeq \mathbb{Z}/(m/n)\mathbb{Z}$. ■

Observation: $\mathbb{F}_{p^2}/\mathbb{F}_p$ is a degree 2 extension with $p > 2$. $2 \neq x^2 \mod p$. Then $\mathbb{F}_p\left(\sqrt{2}\right)/\mathbb{F}_p$ is an extension of degree 2. Therefore, $\mathbb{F}_p\left(\sqrt{2}\right) = \mathbb{F}_{p^2}$.

Back to "tools" to compute Galois groups.

Proposition 11.3. *$f \in \mathbb{Z}[x]$ monic and irreducible. For prime p, let $\overline{f}(x) = f(x) \mod p$. Then $\overline{f}(x) \in \mathbb{F}_p[x]$. Assume $\overline{f}(x)$ is separable over $\mathbb{F}_p$. Then, we have the following.*

1. *There is a bijection between roots of $f(x)$ (in $\mathbb{Q}^{alg}$) and roots of $\overline{f}(x)$ (in $\mathbb{F}_p^{alg}$).*
2. *$\mathrm{Gal}(\mathbb{F}_{p,\overline{f}}/\mathbb{F}_p) \hookrightarrow \mathrm{Gal}(\mathbb{Q}_f, \mathbb{Q})$ (injects).*

Proof in Dummit & Foote.

Usefulness: can gain info about $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ by reducing modulo p.

Example 11.1. $f(x) = x^5 - x - 1$. If $G = \text{Gal}(\mathbb{Q}_f/\mathbb{Q})$, we know $G < S_5$.

12 January 31, 2022

Last time, we were computing $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$, where $f(x) = x^5 - x - 1$. Modulo p, usually $\overline{f}$ is separable. Then $\mathrm{Gal}(\mathbb{F}_{p,\overline{f}}/\mathbb{F}_p) \hookrightarrow \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$.

Take $p = 5$, and notice that f has no roots mod 5. Then if it factors it must be as a quadratic and a cubic. There is a unique quadratic extension of $\mathbb{F}_5$, so consider $\mathbb{F}_5\left(\sqrt{2}\right)$. Compute $f(a + b\sqrt{2})$ and notice that it is non-zero. Therefore, there is no quadratic subextension of the splitting field of $\overline{f}$, so $\overline{f}$ has no irreducible quadratic factor. Hence $\overline{f}$ is irreducible. For α a root of $\overline{f}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, so we must have a 5-cycle.

Take $p = 2$, and notice that f factors as $(x^2 + x + 1)(x^3 + x^2 + 1)$. Take α a root of the quadratic and β a root of the cubic. $\mathbb{F}(\alpha)$ has degree 2 and $\mathbb{F}(\beta)$ has degree 3, so their intersection is just the base field. Therefore, the Galois group of the splitting field of $\overline{f}$ is just the direct product of the Galois groups of $\mathbb{F}(\alpha)$ and $\mathbb{F}(\beta)$. Thus, we have a transposition.

Conclusion: We have a 5-cycle and transposition in $G = \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$, so $G \simeq S_5$.

> Remark 12.1 — Reducible over $\mathbb{Z}$ implies reducible over $\mathbb{F}_p$, so irreducible over $\mathbb{F}_p$ implies irreducible over $\mathbb{Z}$.

12.1 Cyclotomic extensions

k field, $n \in \mathbb{Z}_{>0}$. $\mathrm{char}(k) = p$, with $(p, n) = 1$. Terminology:

1. $\mu_n \in \overline{k}^*$ will be the group of n^{th} roots of unity in k.
2. $\xi \in \mu_n$ is a primitive n^{th} root of unity if $\xi^n = 1$ but $\xi^m \neq 1$ for all $m < n$.

> Claim 12.1 — $k(\mu_n) = k(\xi)$, where ξ is primitive.

Lemma 12.1. *Let $\mu \subset k^*$ be a finite subgroup. Then μ is cyclic.*

Proof. μ is abelian and finite, so

$$\mu = \prod_{p \text{ prime}} \mu_{(p)}$$

where $\mu_{(p)}$ is Sylow p-subgroup. Need to show that for all p, $\mu_{(p)}$ is cyclic. This is enough b/c then the product is cyclic when we have only one subgroup for each p. So why is $\mu_{(p)}$ cyclic? Let $\xi \in \mu_{(p)}$ be of maximal order p^m. Let $|\mu_{(p)}| = p^M$. Suppose $m < M$. Then for all $\tau \in \mu_{(p)}$, $\tau^{p^m} = 1$ implies that all elements of $\mu_{(p)}$ satisfy $x^{p^m} = 1$. There are at most p^m elements in $\mu_{(p)}$, of order p^M. Contradiction. Hence ξ has order p^M, so $\mu_{(p)} = \langle \xi \rangle$, which is cyclic. ∎

Corollary 12.2. *There exists primitive root of unity for any n.*

Proof. Take a generator of μ_n. ■

In fact, ξ is primitive iff $\mu_n = \langle \xi \rangle$.

Proposition 12.3. $(p, n) = 1$ *and* $\mathrm{char}(k) = p$. *(*$p \geq 0$*, in which case* (p, n) *condition doesn't matter)*

1. $k(\mu_n)/k$ *is Galois.*
2. $|k(\mu_n) : k| \leq \varphi(n)$ *(Euler totient).*
3. $|\mathrm{Gal}(k(\mu_n)/k)| \leq \varphi(n)$.
4. $\mathrm{Gal}(k(\mu_n)/k) < (\mathbb{Z}/n\mathbb{Z})^* = \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.

13 February 2, 2022

Proof of proposition from end of last time.

Proof.

1. $(p, n) = 1$ implies separable, as $f(x) = x^n - 1$. $k(\mu_n)$ splitting field of f, so normal. Then it is Galois.
3. $G = \text{Gal}(k(\mu_n)/k)$ acts on the roots $x^n - 1 = 0$, which means it acts on μ_n, so $G < \text{Aut}(\mu_n) = (\mathbb{Z}/n\mathbb{Z})^*$.
2. $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$, and $|k(\mu_n) : k| = |G| \leq \varphi(n)$.

■

Assume $k = \mathbb{Q}$.

> **Definition.** We write $\phi_n(x) = \text{Irr}_{\mathbb{Q}}(\xi)$, where ξ is a primitive n^{th} root of 1.

Example 13.1. For $n = p$, we have

$$\phi_n(x) = x^p + \ldots + 1.$$

This is iff.

Lemma 13.1. *$k = \mathbb{Q}$, ξ the n^{th} primitive root. Take $q \in \mathbb{Z}_{>0}$ and assume $(q, n) = 1$. Then ξ^q is also a root of $\phi_n(x)$.*

Proof. We can assume q is prime (since otherwise, take its prime decomposition and apply each prime factor one by one). Write

$$x^n - 1 = \phi_n(x)g(x).$$

Suppose $\phi_n(\xi^q) \neq 0$. Then it must be that $g(\xi^q) = 0$. Reduce everything mod q. Then

$$\overline{g}(\xi^q) = \overline{g(\xi^q)} = \overline{g(\xi)^q} = \overline{g(\xi)}^q = 0$$

Over $\mathbb{F}_q$, $\overline{\phi_n(\xi)} = 0$ and $\overline{g(\xi)} = 0$. Then $x^n - 1$ has a double root over $\mathbb{F}_q$. Contradiction, since $(q, n) = 1$. Therefore, $\phi_n(\xi^q) = 0$. ■

Note: correspondence of roots of polynomial and roots of polynomial over $\mathbb{F}_q$.

Corollary 13.2. *$\phi_n(x)$ is well-defined, i.e. it does not depend on the choice of ξ.*

Proposition 13.3. $k = \mathbb{Q}$.

1. $|\phi_n(x)| = \varphi(n)$.
2. $|\mathbb{Q}(\xi) : \mathbb{Q}| = \varphi(n)$.
3. *Gal*$(\mathbb{Q}(\xi)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$

Proof. Follows from lemma. ■

Facts:

1. We can compute
$$\phi_n(x) = \frac{x^n - 1}{\prod_{d|n} \phi_d(x)}.$$
2. We then have
$$\deg(x^n - 1) = n = \sum_{d|n} \varphi(d) = \sum_{d|n} \deg \phi_d(x).$$

13.1 Cyclic extensions

Definition (Cyclic)**.** A Galois extension L/k is called **cyclic** if the Galois group $\mathrm{Gal}(L/k)$ is cyclic. *Cyclic*

Example 13.2. Consider $f(x) = x^3 - 2$ over $k = \mathbb{Q}(\omega)$. $f(x)$ is irreducible over k. $k\left(\sqrt[3]{2}\right)/k$ is Galois, and $\mathrm{Gal}\left(k\left(\sqrt[3]{2}\right)/k\right) \simeq \mathbb{Z}/3\mathbb{Z}$.

Proposition 13.4. *Let char*$(k) = p$*, and* $(p, n) = 1$ *or* $p = 0$. $\mu_n \subset k$.

1. *If* L/k *is a cyclic Galois extension with Gal*$(L/k) \simeq \mathbb{Z}/n\mathbb{Z}$*, there exists* $a \in k$ *such that* $L = k\left(\sqrt[n]{a}\right)$.
2. $L = k\left(\sqrt[n]{a}\right)$, L/k *is Galois, and Gal*$(L/k) \simeq \mathbb{Z}/d\mathbb{Z} < \mathbb{Z}/n\mathbb{Z}$.

DF. 14.7 propositions 36, 37.

Backward: $L = k\left(\sqrt[n]{a}\right)$. L is the splitting field of $x^n - a$ since $\sqrt[n]{a} \cdot \xi^d \in L$, where $\langle \xi \rangle = \mu_n$.

Forward: More interesting. Read. Lagrange resolvent? ■

13.2 Solvability in radicals, Abel-Ruffini theorem

Here we talk about finite extensions. We have also stopped assuming $k = \mathbb{Q}$, but all theorems will be about $\mathbb{Q}$.

Definition (Solvable)**.** Let L/k be a finite Galois extension. We say that L/k is solvable if $\mathrm{Gal}(L/k)$ is solvable. *Solvable*

Note that the next definition does not require Galois.

Solvable

Definition (Solvable)**.** L/k a finite extension is **solvable** if there exists $E/L/k$ such that E/k is solvable.

Radical

Definition (Radical)**.** L/k is a finite separable extension. L/k is **radical** if there exists a tower of extensions

$$k = L_0 \subset L_1 \subset \ldots \subset L_i \subset L_{i+1} \subset \ldots \subset L$$

1. L_{i+1}/L_i is cyclotomic or
2. $L_{i+1} = L_i\,(\sqrt[n]{a})$ for some $a \in L_i$.

Example 13.3. Cyclotomic extensions are radical. Our favorite extension is radical.

Solvable in radicals

Definition (Solvable in radicals)**.** $f(x) \in k[x]$ separable is **solvable in radicals** if k_f/k is radical.

14 February 4, 2022

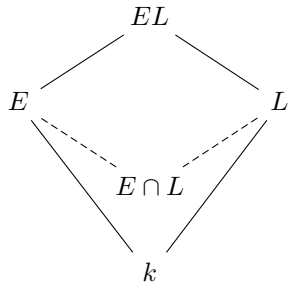
14.1 *Abel-Ruffini theorem*

Recall definitions of solvable and radical extensions.

All extensions finite.

Lemma 14.1. *(Solvable extension)*

1. *Suppose we know that E/k is solvable and L/k is Galois.*



   Then EL is solvable over L.

2. *For tower $E/L/k$, E/k is solvable iff E/L and L/k are solvable.*

Proof. HW. ■

> Remark 14.1 — A class of extensions satisfying 1 and 2 is called distinguished. Separable extensions are distinguished.

Lemma 14.2. *Radical extensions form a distinguished class (satisfying previous lemma). (In other words, take the word "solvable" in the previous lemma and replace it with "radical".)*

Proof. Partially HW. ■

> **Definition.** For k, fix some algebraic closure k^{alg}. For L/k a finite extension, we say that $\tilde{L}/L$ is the **normal closure** of L, the minimal normal extension of k which contains L.

> Remark 14.2 — $L = k(\alpha)$. $f = \text{Irr}_k(\alpha)$. $\tilde{L} = k_f$

Lemma 14.3. *L is radical iff $\tilde{L}$ is radical.*

Proof. Will be part of midterm practice. ■

Corollary 14.4. *$f \in k[x]$ and α a root of f. If α can be expressed in radicals, then any other root can.*

> Remark 14.3 — Quintics that are not solvable by radicals have no roots that can be expressed in radicals.

Take $\text{char}(k) = 0$ (separable?). In particular consider $k = \mathbb{Q}$.

Theorem 14.5 (Abel-Ruffini)**.** *L/k, a finite extension, is radical iff it is solvable.*

Proof. Replace L with $\tilde{L}$ so that we can assume L/k is Galois (previous lemma). So we assume L/k is Galois and radical. We have tower

$$k \subset L_1 \subset \ldots \subset L_i \subset L_{i+1} \subset \cdots \subset L$$

where $L_{i+1} = L_i\left(\sqrt[n_i]{a_i}\right)$ or L_{i+1}/L_i is a cyclotomic extension of degree m_i. Let m be the LCM of all m_i, n_i where L_{i+1}/L_i is cyclotomic and ξ be the primitive m^{th} root of unity.

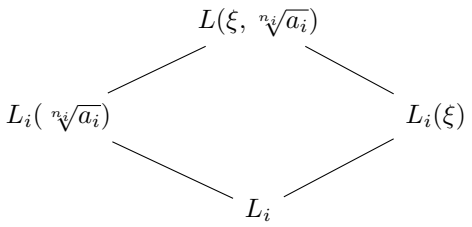
$$\begin{array}{ccc} k(\xi) & \text{——} & L(\xi) \\ | & & | \\ k & \text{————} & L \end{array}$$

$L(\xi)/k(\xi)$ is Galois.

$$k(\xi) \subset L_1(\xi) \subset \ldots \subset L_i(\xi) \subset \ldots \subset L(\xi)$$

Claim: it makes $L(\xi)/k(\xi)$ radical. Take $L_i(\xi) \subset L_{i+1}(\xi)$.

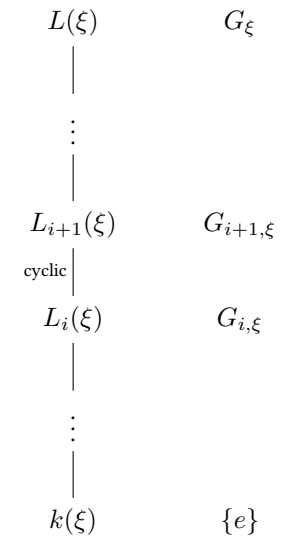
1. If L_{i+1}/L_i is cyclotomic, then $L_i(\xi) = L_{i+}(\xi)$.
2. If $L_{i+1} = L_i\left(\sqrt[n_i]{a_i}\right)$ then $L_{i+1}(\xi) = L_i(\xi)\left(\sqrt[n_i]{a_i}\right)$.



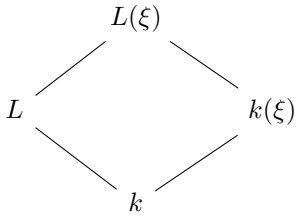
$L_{i+1}(\xi)/L_i(\xi)$ is Galois with cyclic Galois group. By Kummer's theorem (on characterization of cyclic extensions), we have that $L_{i+1}(\xi)/L_i(\xi)$ is cyclic (since we have the n_i^{th} primitive root of unity in $L_i(\xi)$ and $L_{i+1}(\xi) = L_i\left(\xi,\ \sqrt[n_i]{a_i}\right)$).

$$k(\xi) \subset L_1(\xi) \subset \ldots \subset L_i(\xi) \subset \ldots \subset L(\xi)$$

Let $G_\xi = \text{Gal}\left(L(\xi)/k(\xi)\right)$.



G_ξ is solvable, so $L(\xi)/k(\xi)$ is solvable.



Cyclotomic ($k(\xi)/k$) implies abelian implies solvable. $L(\xi)/k(\xi)$ and $k(\xi)/k$ are solvable so by the first lemma, $L(\xi)/k$ is solvable which implies L/k is solvable. ■

Corollary 14.6. *The quintic $f(x) = x^5 - x - 1$ over $\mathbb{Q}$ is not solvable in radicals.*

Proof. $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}) \simeq S_5$ is not solvable, so $\mathbb{Q}_f$ not radical. ■

15 February 7, 2022

Discussion: E/k "solvable in radicals" (sequence of towers of E) and "radical" (was a shorthand for the former).

We correct the following definition we saw previously.

> **Definition.** L/k is solvable in radicals if there exists $L \subset E$ such that E/k has a tower
> $$k \subset E_1, \subset, \ldots, \subset E$$
> where E_{i+1}/E_i is cyclotomic or $E_{i+1} = E_i\left(\sqrt[n_i]{a_i}\right)$.

Recall the lemma.

Lemma 15.1. *L/k is radical iff $\tilde{L}$, the normal closure, $\tilde{L}/k$ is radical.*

Lemma 15.2. *Let L/k be a finite separable extension and $\tilde{L}$ be its normal closure. L is radical (in the sense of the definition above) iff for $\tilde{L}/k$, there exists tower*

$$k = \tilde{L}_0 \subset \tilde{L}_1 \subset \ldots \subset \tilde{L}$$

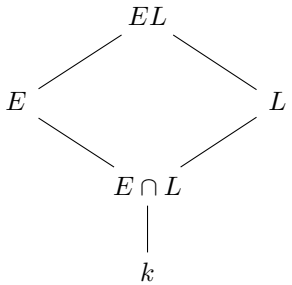
such that

1. *$\tilde{L}_{i+1}/\tilde{L}_i$ is cyclotomic or*
2. *$\tilde{K}_{i+1} = \tilde{L}_i\left(\sqrt[n_i]{a_i}\right)$.*

> Remark 15.1 — One can show that for L/k finite separable, $\alpha \in L$ such that $L = k(\alpha)$, we have $\tilde{L} = k_f$, $f = \mathrm{Irr}_k(\alpha)$, so $\tilde{L}$ is Galois. In other words, since L is separable, L can be written as $k(\alpha)$ by the primitive element theorem, and $\tilde{L}$ will be the splitting field of the minimal polynomial of α.

Following is usable for HW.

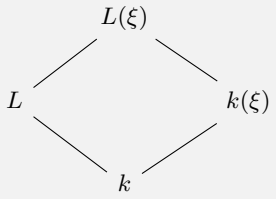
Lemma 15.3 (Another part of Galois correspondence)**.** *Suppose we have $E, L/k$ finite.*



If E/k is Galois (which implies $E/E\cap L$ is Galois), then EL/L is Galois and Gal$(EL/L) \simeq$ Gal$(E/E \cap L)$.

Proof. DF 14.4 Prop. 19. ∎

Remark 15.2 — We remark that for the forward direction, if ξ is a primitive root of unity of degree m, why is $L(\xi)/k(\xi)$ Galois? This is by Theorem 2 of Galois correspondence. $L(\xi) = Lk(\xi) \Rightarrow L(\xi)/k(\xi)$ is Galois.



Remark 15.3 — Going back to the very first claim of the proof, we can replace L with $\tilde{L}$. For radical, see lemma 3'[2]. For solvable, we need the following.

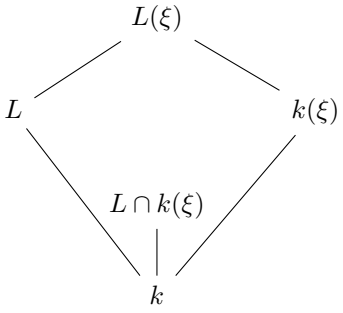
[2] *I think this means the corrected version of the lemma we talk about at the start of today.*

Lemma 15.4. *L/k a finite separable extension. $\tilde{L}$ is the normal closure. If there exists $E/L/k$ such that E/k is Galois, solvable, that is Gal(E/k) solvable, then Gal$(\tilde{L}/k)$ is solvable.*

Proof. By Galois correspondence, $\text{Gal}(E/k) \twoheadrightarrow \text{Gal}(\tilde{L}/k) \simeq \text{Gal}(E/k)/\text{Gal}(E/\tilde{L})$ (since $\tilde{L}/k$ is Galois). Kernels and quotients of solvable groups are solvable. [double arrow surjects] ∎

End of proof of Abel-Ruffini.

Proof. Backwards statement is L/k Galois solvable impllies L/k is radical. $|L : k| = n$. Let ξ be the n^{th} root of 1.



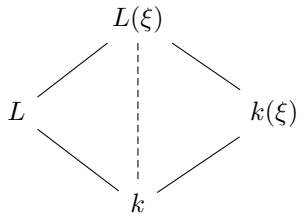
L/k solvable. Therefore, $L/L \cap k(\xi)$ is Galois solvable. By lemma, $\text{Gal}(L(\xi)/k(\xi)) \simeq \text{Gal}(L/L \cap k(\xi))$ so $L(\xi)/k$ is solvable. Let $G = \text{Gal}(L(\xi)/k(\xi))$. Then there exists a tower of subgroups with cyclic quotients. By Galois correspondence, there exists

tower

$$k(\xi) \subset \ldots \subset \tilde{L}_i \subset \tilde{L}_{i+1} \subset \ldots \subset L(\xi)$$

such that $\tilde{L}_{i+1}/\tilde{L}_i$ is cyclic. Kummer then gives $\tilde{L}_{i+1} = \tilde{L}\left(\sqrt[n_i]{a_i}\right)$ for some $a_i \in \tilde{L}_i$. Hence, $L(\xi)/k(\xi)$ is radical. ■

HW problem 2.



$k(\xi)/k$ radical implies $L(\xi)/k$ (Lemma 2), so L/k is radical (Lemma 2).

On the board (in diagram), $L(\xi)/k(\xi)$ radical and $k(\xi)$ radical implies $L(\xi)/k$ is radical, which in turn implies L/k is radical.

16 February 9, 2022

16.1 Applications of Galois theory

16.1.1 Inverse Galois problem

Theorem 16.1. *There exists L/K Galois with Galois group S_n for any $n \geq 1$. Moreover, for any finite group G, there exists E/L Galois with Gal$(E/L) = G$.*

Proof. For k, take $k[x_1, \dots, x_n]$, on which S_n acts on the left (by permuting variables). Let $L = \text{Frac } k[x_1, \dots, x_n] = k(x_1, \dots, x_n)$ (a transcendental extensions of k with transcendence degree n). Take K to be L^{S_n}. By Artin's, $\text{Gal}(L/L^{S_n}) = S_n$, and L/L^{S_n} is Galois.

Take any finite group G, and embed it into $G \hookrightarrow S_n$. Galois correspondence tells us that L^G/K is a subfield which corresponds to $G < S_n$. ■

> Remark 16.1 — Still true that for any n, there exists $L/\mathbb{Q}$ with $\text{Gal}(L/\mathbb{Q}) = S_n$ (DF section 14.9). Open question for arbitrary finite G. We do know the answer, however, if G is abelian.

Lemma 16.2. *Let G be a finite abelian group. Then there exists n such that $G \twoheadleftarrow^{\varphi} (\mathbb{Z}/n\mathbb{Z})^* = Aut_{gr}(\mathbb{Z}/n\mathbb{Z})$ (automorphism group).*

Proof. HW. ■

Theorem 16.3. *G finite abelian group. There exists $L/\mathbb{Q}$ Galois with Gal$(L/\mathbb{Q}) = G$.*

Proof. Let $G \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^* = \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$, where ξ is the primitive n^{th} root of 1.

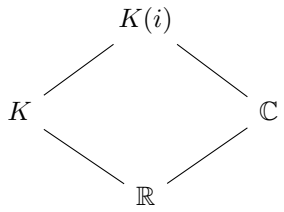
$$\begin{array}{ccc} \mathbb{Q}(\xi) & & (\mathbb{Z}/n\mathbb{Z})^* \\ & & | \\ L = \mathbb{Q}(\xi)^{\text{Ker}(\varphi)} & & \text{Ker}(\varphi) \\ | & & | \\ \mathbb{Q} & & \{e\} \end{array}$$

$\text{Ker}(\varphi) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^* \twoheadrightarrow^{\varphi} G$. $\text{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*/\text{Ker}(\varphi) = G$. ■

16.1.2 Fundamental theorem of algebra

Theorem 16.4. *$\mathbb{C}$ is algebraically closed.*

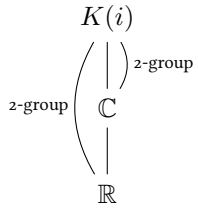
Proof. ($\deg f > 0$) Suffices to prove that any $f \in \mathbb{R}[x]$ has a root in $\mathbb{C}$. Indeed, let $f \in \mathbb{C}[x]$. If f does not have roots in $\mathbb{C}$, then $\overline{f}$ (conjugation), also doesn't have roots in $\mathbb{C}$. But then $f\overline{f} \in \mathbb{R}[x]$ and does not have roots. Hence, we can assume $f \in \mathbb{R}[x]$. Assume f is irreducible. Let $K = \mathbb{R}_f$ be the splitting field of f.



Either $K(i) = K$ (if $i \in K$) or $K(i) = K\mathbb{C}$. Then $K(i)/\mathbb{R}$ is Galois. Let $G = \mathrm{Gal}(K(i)/\mathbb{R})$. Let $P < G$ be a Sylow 2 subgroup.

$$\begin{array}{ll} K(i) & G \\ \deg{=}|P| \Big(& \\ L = K(i)^P & P \\ \deg{=}|G|/|P| \Big(& \\ \mathbb{R} & \{e\} \end{array}$$

$|L : \mathbb{R}|$ is odd. By the primitive element theorem, $L = \mathbb{R}(\alpha)$, and $g = \mathrm{Irr}_{\mathbb{R}}(\alpha)$ has odd degree. But there are no odd degree irreducible polynomials in $\mathbb{R}[x]$. Conclusion, $|G| = 2^m$, since $|G|/|P| = |L : \mathbb{R}| = 1$.



By Galois correspondence, $\mathrm{Gal}(K(i)/\mathbb{C}) = P'$ is a 2-group. P' is solvable, moreover, there exists filtration with $\mathbb{Z}/2\mathbb{Z}$ quotients. There exists $P'' \triangleleft P'$ such that $|P'/P''| = 2$.

$$\begin{array}{ll} K(i) & P' \\ P'' \Big(& \\ L = K(i)^{P''} & P'' \\ \mathbb{Z}/2\mathbb{Z} \Big(& \\ \mathbb{C} & \{e\} \end{array}$$

So $L/\mathbb{C}$ is a quadratic extension. $L = \mathbb{C}(\alpha)$, α is a root of a quadratic polynomial. But quadratic formula tells us any quadratic has its roots in $\mathbb{C}$. $\alpha \in \mathbb{C} \Rightarrow |K : \mathbb{C}| = 1$. Contradiction. ■

16.1.3 Abstract nonsense

Categories and functors (DF appendix, Maclane 'Categories for a working mathematician')

Definition. $\underline{\underline{C}}$ a **category** has

1. $ob\ \underline{\underline{C}}$ objects in $\underline{\underline{C}}$.
2. For all $A, B \in ob\ \underline{\underline{C}}$, we haev a set $\mathrm{Mor}_{\underline{\underline{C}}}(A, B)$.

such that

1. for all $A \in ob\ \underline{\underline{C}}$ here exists $\mathrm{id}_A \in \mathrm{Mor}(A, A)$,
2. $A, B, C \in ob\ \underline{\underline{C}}$, $f \in \mathrm{Mor}(A, B)$ and $g \in \mathrm{Mor}(B, C)$ implies there exists $g \circ f \in \mathrm{Mor}(A, C)$.

$$A \to^f B \to^g C$$

3. $A, B \in ob\ \underline{\underline{C}}$, $f \in \mathrm{Mor}(A, B)$, $\mathrm{id}_B \circ f = f$ and $f \circ \mathrm{id}_A = f$.

$$A \to^f B \to^{\mathrm{id}} B$$

4. Associativity of composition

$$f \circ (g \circ h) = (f \circ g) \circ h$$

Example 16.1.

1. Category of sets, $\underline{\underline{\mathrm{Sets}}}$. Objects are sets, and morphisms are maps between (of) sets.
2. Category of groups, $\underline{\underline{\mathrm{Gr}}}$. Objects are groups, and morphisms are homomorphisms.
3. $\underline{\underline{\mathrm{Ab}}} \subset \underline{\underline{\mathrm{Gr}}}$ the category of abelian groups is a (full) subcategory, full meaning it inherits all morphisms. (Abelian categories)

17 February 11, 2022

Example 17.1.

1. Posets. The poset category $\underline{\underline{\mathcal{P}}}$ has objects as vertices and morphisms are arrows/edges. The self-edge is the identity morphism.
2. For G a finite group, there is just one object A, and morphisms are elements of G. $g \in \mathrm{Mor}_{\underline{\underline{G}}}(A, A)$ is $\mathrm{End}_{\underline{\underline{G}}}(A)$. $h \circ g = hg$, $\mathrm{id}_A = e$.

Definition. $\underline{\underline{C}}$ a category, and $f \in \mathrm{Mor}_{\underline{\underline{C}}}(A, B)$ is an **isomorphism** if there exists $f^{-1} \in \mathrm{Mor}_{\underline{\underline{C}}}(B, A)$ such that $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$.

The example with a group $\underline{\underline{G}}$ is a groupoid.

Definition (Groupoid)**.** A **groupoid** is a category in which all morphisms are isomorphisms. *Groupoid*

Example 17.2.

1. Commutative rings.
2. Vector spaces over a field k (also an abelian category). Finite dimensional vector spaces over k.
3. Topological spaces $\underline{\underline{\mathrm{Top}}}$. Objects are topological spaces and morphisms are continuous maps.
4. $\underline{\underline{\mathrm{Top}_\cdot}}$ have objects as topological spaces with dist point, and morphisms as continuous maps preserving dist point.
5. Manifolds. $\underline{\underline{\underline{\mathrm{Man}}}}$.

17.1 Functors

Definition (Functor)**.** If we have categories $\underline{\underline{\mathcal{A}}}, \underline{\underline{\mathcal{B}}}$, $\mathcal{F} : \underline{\underline{\mathcal{A}}} \to \underline{\underline{\mathcal{B}}}$ is a **covariant functor** if *Functor*

1. for all $A \in \mathcal{A}$, $\mathcal{F}(A) \in \mathcal{B}$, and
2. for all $f : A \to A'$, there exists $\mathcal{F}(f) : \mathcal{F}(A) \to \mathcal{F}(A')$ such that

$$\mathcal{F}(\mathrm{id}_A) = \mathrm{id}_{\mathcal{F}(A)}$$

$$\mathcal{F}(gf) = \mathcal{F}(g) \circ \mathcal{F}(f)$$

$A \to^f A' \to^g A''$.

$\mathcal{F} : \underline{\underline{A}} \to \underline{\underline{B}}$ is contravariant if it "inverts the arrows". $f : A \to A'$.

$$\mathcal{F}(f) : \mathcal{F}(A') \to \mathcal{F}(A)$$

and composition

$$\mathcal{F}(gf) = \mathcal{F}(f) \circ \mathcal{F}(g)$$

Remark 17.1 — $\mathcal{A} \to \mathcal{A}^{\text{op}}$

Example 17.3. Forgetful functors. $\mathcal{F}$ from groups to sets (forgetting group structure).

Subcategory

Definition (Subcategory). $\underline{\underline{\mathcal{A}'}} \subset \mathcal{A}$ is a **subcategory** if ob $\underline{\underline{\mathcal{A}'}} \subset$ ob $\underline{\underline{\mathcal{A}}}$ and for all $A, B \in \mathcal{A}'$, $\text{Mor}_{\underline{\underline{\mathcal{A}'}}} \subset \text{Mor}_{\underline{\underline{\mathcal{A}}}}(A, B)$. $\underline{\underline{\mathcal{A}'}}$ is **full** if $\text{Mor}_{\underline{\underline{\mathcal{A}'}}} = \text{Mor}_{\underline{\underline{\mathcal{A}}}}(A, B)$.

Example 17.4. $\underline{\text{Ab}} \subset \underline{\text{Groups}}$ is full. Groups in sets is not full.
$\underline{\text{Man}} \subset \underline{\text{Top}}$.

Is $\underline{\text{Fields}} \to \underline{\underline{\text{Comm rings}}}$ full?

$\underline{\text{Fields}} \to \underline{\underline{\text{Comm rings}}} \to \underline{\underline{Ab}}$

∞-categories.

17.2 Natural transformations

If we have $\mathcal{F}, \mathcal{G} : \underline{\underline{\mathcal{A}}} \to \underline{\underline{\mathcal{B}}}$, a natural transformation $\eta : \mathcal{F} \to \mathcal{G}$ satisfies the following.

1. For all $A \in \underline{\underline{\mathcal{A}}}$, $\eta_A : \mathcal{F}(A) \to \mathcal{G}(A)$
2. For any $f : A \to B$, we have a commutative diagram

$$\begin{array}{ccc} \mathcal{F}(A) & \xrightarrow{\eta_A} & \mathcal{G}(A) \\ {\scriptstyle \mathcal{F}(f)}\downarrow & & \downarrow{\scriptstyle \mathcal{G}(f)} \\ \mathcal{F}(B) & \xrightarrow[\eta_B]{} & \mathcal{G}(B) \end{array}$$

Example 17.5. Top.

We have π_1 : Top. $\to$ Groups. H_1 : Top. $\to$ $\underline{\underline{Ab}}$ is a functor. h : $\pi_1(X,x) \to H_1(X,x)$ is a natural transformation. For $n=1$, $H_1(X,x) \simeq \pi_1(X,x)_{\text{ab}}$, where the 'ab' subscript is the abelianization, where $G_{\text{ab}} = G/[G,G]$.

Abelianization $(\cdot)_{\text{ab}}$: Groups $\to$ $\underline{\underline{Ab}}$ is a functor. $G \to H \to_{squiggle} G_{ab} \to H_{ab}$. id : Groups $\to$ Groups. id $\to (\cdot)_{ab}$ is a natural transformation $G \to G_{ab}$.

18 February 14, 2022

18.1 Rings and modules

For the following basic definitions and properties, R is an associative ring with 1.

R-module

Definition (R-module)**.** An abelian group M is a (left) **R-module** if $(M, +)$ is equipped with $R \times M \to M$ where $(a, m) \mapsto am$ such that

1. $a(m_1 + m_2) = am_1 + am_2$,
2. $(a_1 a_2)m = a_1(a_2 m)$ (left, right if you flip a_1, a_2),
3. $(a_1 + a_2)m = a_1 m + a_2 m$, and
4. $1m = m$.

Definition. For $M \in \underline{\underline{Ab}}$, we denote

$$\mathrm{End}_{\underline{\underline{Ab}}}(M) = \mathrm{Hom}_{\underline{\underline{Ab}}}(M, M).$$

Remark 18.1 — $\mathrm{End}_{\underline{\underline{Ab}}}(M)$ has a ring structure.

1. $f, g : M \to M \Rightarrow f + g : M \to M$.
2. Product: composition.

Warning: generally $\mathrm{End}(M)$ is not commutative.

We can give an equivalent definition of an R-module using $\mathrm{End}_{\underline{\underline{Ab}}}(R)$.

Proposition 18.1. *To define an R-module structure on M is equivalent to producing a ring homomorphism from $R \to End_{\underline{\underline{Ab}}}(M)$.*

Sketch. Remember that $\mathrm{End}(M) = \mathrm{Hom}(E, E)$. Suppose M is an R-module. Let $\rho_M : R \to \mathrm{End}(M)$ be the map which sends $a \mapsto \rho_M(a) : M \to N$, where $\rho_M(a)$ sends $m \mapsto am$. Then our four conditions will give us precisely that ρ_M is a ring hom. Suppose conversely that we are given $\rho_M : R \to \mathrm{End}(M) = \mathrm{Hom}(M, M)$. $R \times M \to M$, $(a, m) \mapsto \rho_M(a)(m) = am$. ∎

Definition. M, N are R-modules. $f : M \to N$ is an **R-module homomorphism** if

1. it is a homomorphism of abelian groups and
2. for all $a \in \mathbb{R}, m \in M$, $f(am) = af(m)$.

Claim 18.1 — We can now talk about the category $\underline{\underline{R\text{-mod}}}$. We always have a forgetful functor $\mathcal{F} : \underline{\underline{R\text{-mod}}} \to \underline{\underline{Ab}}$.

Example 18.1.
1. $\underline{\underline{\mathbb{Z}-\text{modules}}} = \underline{\underline{Ab}}$. $\mathbb{Z}\times M \to M$ with $(a,m) \mapsto am = m+\ldots+m$.
2. $\underline{\underline{\text{Vect}}}_k = \underline{\underline{k-\text{mod}}}$ for field k.

Remark 18.2 — R-mod is an abelian category.

18.1.1 Submodules, factor modules, and isomorphism theorems

Definition (R-submodule)**.** Let $M \in R-\text{mod}$ and $N \subset M$ be an abelian subgroup. N is an R-submodule if for all $a \in R$, $n \in N$, $an \in N$. *R-submodule*

Suppose $N \subset M$ submodule. Let M/N be the quotient (in $\underline{\underline{Ab}}$).

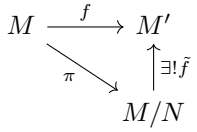
Proposition 18.2. *The map $R \times M/N \to M/N$ which sends $(a, \overline{m}) \mapsto \overline{am}$ is*

1. *well-defined,*
2. *defines an R-module structure on M/N, and*
3. *the map $M \to^{\pi} M/N$ which sends $m \mapsto \overline{m}$ is a map of R-modules.*

Proof. Exercise. ■

Definition (Factor/quotient module)**.** M/N with the R-module structure from the proposition is the **factor/quotient module**. *Factor/quotient module*

Proposition 18.3 (Universal property)**.** *Let $N \subset M$ be an R-submodule. Let $f : M \to M'$ be an R-module homomorphism such that $f(N) = 0$. Then there exists unique map $\tilde{f} : M/N \to M'$ such that the diagram commutes.*



Proof. Exercise. ■

From here objects are R-modules and maps are R-module homomorphisms unless explicitly stated otherwise.

Definition. $f : M \to M'$
1. $\text{Ker } f = \{m \in M \mid f(m) = 0\}$.
2. $\text{Im } f = \{m' \in M' \mid \exists m \in M, f(m) = m'\}$, subset of M'.
3. $\text{Coker } f = M'/\text{Im } f$.

Theorem 18.4. *$f : M \to M'$ an R-module homomorphism. Then $M/Ker\ f \simeq Im\ f$.*

Proof. Exercise. ■

Exact/short exact

Definition (Exact/short exact)**.** A sequence of R-modules and R-module homoprhisms

$$\ldots \to M_{i-1} \to^{f_{i-1}} M_i \to^{f_i} M_{i+1} \to \ldots$$

is **exact** if Ker $f_i =$ Im f_{i-1}. **Short exact sequence** of R-modules

$$0 \to M_1 \to^{f} M_2 \to^{g} M_3 \to 0$$

where the above is exact.

Remark 18.3 — The sequence

$$0 \to M_1 \to^{f} M_2 \to^{g} M_3 \to 0$$

is exact iff

1. f is injective,
2. Ker $g =$ Im f, and
3. g is surjective.

Remark 18.4 — $f : M \to M'$ is injective (monomorphism) if

1. f is injective as a map of abelian groups or equivalently,
2. Ker $f = 0$.

f is surjective (epimorphism) if

1. f is surjective in $\underline{\underline{Ab}}$ or equivalently,
2. Coker $f = 0$ (or Im $f = M'$).

Remark 18.5 —

1. $f : M \to M'$ gives short exact sequence
$$0 \to \text{Ker } f \to M \to^{f} \text{Im } f \to 0.$$
This encodes the first isomoprhism theorem, $M/\text{Ker } f \simeq \text{Im } f$.[3]
2. Also,
$$0 \to \text{Im } f \to M' \to^{f} \text{Coker } f \to 0.$$

We can splice (1) and (2) to get a long(er) exact sequence.

$$0 \to \text{Ker } f \to M \to^{f} M' \to \text{Coker } f \to 0,$$

intermediately, $M \to \text{Im } f \hookrightarrow M'$.

[3] *First non-trivial is injective, second non-trivial is surjective.*

19 February 16, 2022

Definition. $N, N' \subset M$ in R-mod.

$$N + N' = \{x + x' \in M \mid x \in N, x' \in N'\}$$

$S \subset M$, $\langle S \rangle$ is the submodule **generated** by S (a minimal submodule containing S). $N_i \subset N$, $i \in I$, $\cap_I N_i$ is a submodule.

Theorem 19.1. $N, N' \subset M$, $N'/N \cap N' \simeq (N + N')/N$.

Theorem 19.2. $M_1 \subset M_2 \subset M_3$. $M_2/M_1 \subset M_3/M_1$ *and*

$$\frac{M_3/M_1}{M_2/M_1} \simeq \frac{M_3}{M_2}.$$

Theorem 19.3. *Suppose we have surjective R-mod hom $f : M \twoheadrightarrow M'$. Let $N' \subset M'$ be a submodule. Then*

1. *$f^{-1}(N') \subset M$ is a submodule, and*
2. *$M/f^{-1}(N') \simeq M'/N'$.*

Theorem 19.4 (Correspondence)**.** *$N \subset M$ a submodule. There is 1 to 1 correspondence between submodules $N \subset L \subset M$ and submodules of M/N.*

Proof. Exercises. Reduce to first isomorphism theorem. ∎

Remark 19.1 — $N \subset R$ left submodule with respect to operation in R. N is a left ideal in R (equivalence). If R is commutative, then submodules in R are exactly the ideals of R.

19.1 Direct products and direct sums

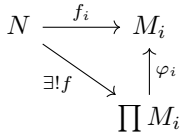
Definition. I an index set and M_i R-modules. The direct product of M_i is

$$\prod_{i \in I} M_i = \{(m_i)_{i \in I} | m_i \in M_i\}$$

with projections $\varphi_j : \prod_I M_i \to M_j$. $(m_i) + (n_i) = (m_i + n_i)$ and $a(m_i) = (am_i)$. φ_i are R-mod homs.

Remark 19.2 — $\prod_I M_i$ is a direct limit in the category R-mod.

Proposition 19.5. *$\{M_i\}_{i \in I}$, N in R-mod. $f_i : N \to M_i$ R-mod homs for all i. Then there exists unique map from $N \to M_i$ such that the following diagram commutes for any i.*



The product has a universal property with respect to maps into it (limit).

Example 19.1. $\underline{\underline{Vect_k}}$. Direct products exist. Can also think about finite dimensional vector spaces. Not all products exist there, as some direct products might be infinite.

Definition. I an index set and $\{M_i\}_{i\in I}$ R-modules. The direct sum is

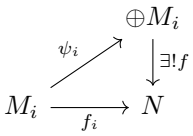
$$\oplus_I M_i = \{(m_i) \mid m_i \in M_i, \text{ where finitely many } m_i \text{ are non-zero}\}.$$

Maps $\psi_j : M_j \hookrightarrow \oplus_I M_i$ and R-mod structure is defined componentwise.

Remark 19.3 — $|I| < \infty$ then $\oplus_I = \prod_I$, but different for big sets.

Remark 19.4 — $\oplus M_i$ is a colimit (often called direct limit) in the category $\underline{\underline{\text{R-mod}}}$.

Proposition 19.6 (Universal property). *$\{M_i\}_{i\in I}$, N in $\underline{\underline{\text{R-mod}}}$. If we have $f_i : M_i \to N$, there exists unique $f : \oplus M_i \to N$ such that the following diagram commutes.*



Proof. Exercise. ■

20 February 18, 2022

20.1 Exact sequences of R-modules

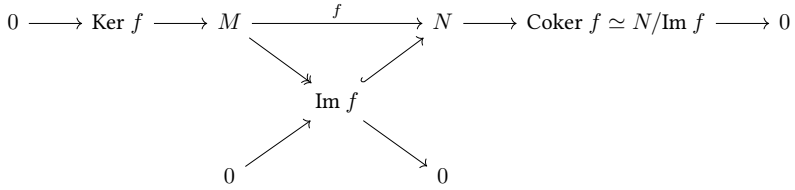
Recall what it means for a sequence to be exact.

Proposition 20.1. *Let*

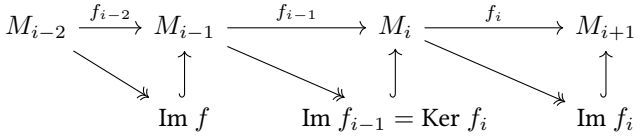
$$0 \to M \to^f M' \to^g M'' \to 0$$

be a short exact sequence of R-modules. Then f is injective, g is surjective, and $M'' \simeq M'/M$. Conversely, these all together imply that the sequence is exact.

Recall $M \to^f N$.



Remark 20.1 — Any long exact sequence can be decomposed into short exact sequences.



Split surjection/injection

Definition (Split surjection/injection)**.** $f : M \twoheadrightarrow N$ is a **split surjection** if

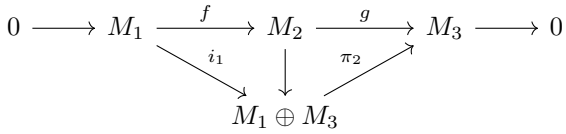
1. f is surjective, and
2. there exists $g : N \to M$ such that $f \circ g = \text{id}_N$.

$g : M \to N$ is a split injection is a **split injection** if

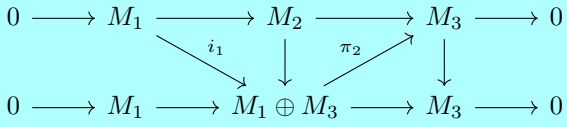
1. g is injective, and
2. there exists $f : N \to M$ such that $f \circ g = \text{id}_M$.

Proposition 20.2. *Let $0 \to M_1 \to^f M_2 \to^g M_3 \to 0$ be a short exact sequence of R-modules. TFAE.*

1. *f is a split injection.*
2. *g is a split surjection.*
3. *There exists $s : M_2 \to M_1 \oplus M_3$ an isomorphism.*



Example 20.1.



Definition (Split)**.** A short exact sequence satisfying conditions of the proposition is called **split**. *Split*

Example 20.2. In vector spaces over k, are there non-splict sequences? (No?) This is because we can complete a basis in V to a basis of W, that is, with $W = V \oplus V'$, $W \to V$ and $V \oplus V' \to V$ (basis of V' is a complement of the basis of V).

Example 20.3. $\mathbb{Z}$-modules.

$$0 \to \mathbb{Z}/3 \to \mathbb{Z}/6 \to \mathbb{Z}/2 \to 0$$

$\mathbb{Z}/6 \simeq \mathbb{Z}/3 \times \mathbb{Z}/2$, so it is split. What about

$$0 \to \mathbb{Z}/2 \to \mathbb{Z}/4 \to \mathbb{Z}/2 \to 0$$

No, as $\mathbb{Z}/4 \not\simeq \mathbb{Z}/2 \oplus \mathbb{Z}/2$.

Claim 20.1 — $0 \to \mathbb{Z}/m \to \mathbb{Z}/mn \to \mathbb{Z}/n \to 0$ splits iff $(n, m) = 1$.

20.1.1 Free modules

Definition. Finite sum is implied throughout.

1. An R-module M is **generated** by $\{x_i\} \subset M$ if for all $m \in M$, there exists $a_i \in R$ such that $m = \sum a_i x_i$.

2. For $\{x_i\} \subset M$, $\{x_i\}$ are R-linearly independent if whenever $\sum a_i x_i = 0$, $a_i = 0$ for all i.
3. $\{x_i\}$ is a **basis** of M if $\{x_i\}$ generate M and are linearly independent.

Question 20.1 — Does every module have a basis?

Example 20.4. $\mathbb{Z}/2$ a $\mathbb{Z}$-module. For all $n \in \mathbb{Z}/2$, $2n = 0$.

Definition (Free module)**.** An R-module which has a basis is called a **free module**. *Free module*

Example 20.5. $\mathbb{Z}/2$ is not a free $\mathbb{Z}$-module. A free $\mathbb{Z}$-module is isomorphic to $\oplus_I \mathbb{Z}$.

Proposition 20.3. *Let M be a free R-module with basis $\{x_i\}_{i\in I}$. Define a map $\lambda : \oplus_{i\in I} R_i \to M$ where $R_i = R$, given by mapping $1 \mapsto x_i$ (1 here meaning the unit in each corresponding copy of the ring R). Then λ is an isomorphism of R-modules.*

Proof. Exercise. ■

Proposition 20.4. *For all R-mod M, there exists epimorphism $\oplus_I R \to^f M$.*

Proof. Exercise. ■

Remark 20.2 — In abelian (and other) categories, free is usually replaced by projective. Think combing hedgehog/hairy ball.

Definition. M is **finitely generated** if there exists $\{x_i\}$ a finite generating set for M. M is **cyclic** if it is generated by a single element.

Example 20.6. $\mathbb{Z}/n = (\overline{1}) = (1 \mod n)$, cyclic $\mathbb{Z}$-module.

21 February 25, 2022

21.1 Modules over PID

Recall definition of free modules and finitely generated. $F \simeq \oplus_I R$, and M finitely generated means we have $F \twoheadrightarrow M$ epimorphism, where $F = \oplus_1^n R \simeq R^n$. If $F \simeq R^n$, then $n = \operatorname{rk} F$. M is cyclic if it can be generated by 1 element. If M is cyclic with generator m, then $R \to M$, with $1 \mapsto m$, $a \mapsto am$. This is an epimorphism. Let $I = \operatorname{Ker} \varphi$ be an ideal in R. By the 1st isomorphism theorem, $R/I \simeq M$. Vice versa, R/I (for all I ideals in R) is cyclic generated by $1 \mod I$.

From this point, we assume R is PID. It is commutative, a domain, and any ideal is principal. Two main examples: $\mathbb{Z}$ and $k[x]$, polynomials over a field.

Structure theorem for finitely generated modules over PID.

Theorem 21.1. *Let M be a finitely generated R-mod. There exists unique isomorphism*

$$M \simeq F \oplus \left(\bigoplus_P M_P \right)$$

where $F = \oplus R^{\operatorname{rk} M}$ and P prime ideals. M_p is the p primary part of M, and is given by

$$M_p \simeq \oplus R/p^{a_i},$$

$a_i \in \mathbb{Z}_{\geq 0}$.

Remark 21.1 — Since R is a PID, $P = (p)$, and $P^{a_i} = (p^{a_i})$, so $R/P^{a_i} = R/(p^{a_i})$.

Definition. The rank of M is $\operatorname{rk} M = \operatorname{rk} F$, the same as the rank of the free module in the decomposition of the previous theorem (this is well-defined).

Example 21.1. $R = \mathbb{Z}$. Any finitely generated abelian group

$$A \simeq Z^{\oplus n} \oplus \left(\bigoplus \text{cyclic groups} \simeq \mathbb{Z}/p^a \right),$$

where the first part is the torsion-free part, and the second is torsion (subgroup?).

Remark 21.2 — Another way to look at the structure theorem is that $M \simeq$ free $\oplus$ cyclics.

Example 21.2. Take $k = \mathbb{C}$ (but any algebraically closed field will do). $R = \mathbb{C}[x]$. Structure theorem is equivalent to Jordan canonical form. Cyclic modules over $\mathbb{C}[x]$. Let M be a cyclic $\mathbb{C}[x]$-mod of the form $\mathbb{C}[x]/(p^a)$. $p \in \mathbb{C}[x]$. $p = p(x) = x - a$ is irreducible. $M \simeq \mathbb{C}[x]/(x-a)^n$ is a finite dimensional vector space over $\mathbb{C}$, and $\dim M = n$. This has a basis $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$. Pick a different basis. $e_1 = \overline{1}$, $\overline{(x-a)}$, and $e_k = \overline{(x-a)^{k-1}}$. The action of x on this basis is given by an $n \times n$ (complex) matrix.

$$xe_1 = \overline{x} = \overline{(x-a)} + \overline{a} = e_1 + ae_1$$

$$xe_2 = x\overline{(x-a)} = \overline{(x-a)^2} + a\overline{(x-a)} = e_3 + ae_2$$

Similarly, for $i \leq n-1$, $xe_i = e_{i+1} + ae_i$.

$$xe_n = x\overline{(x-a)^{n-1}} = \overline{(x-a)^n} + a\overline{(x-a)^{n-1}} = ae_n$$

Let A be the matrix corresponding to the action of x with respect to this basis.

$$\begin{bmatrix} a & & & & \\ 1 & a & & & \\ & 1 & a & & \\ & & \ddots & \ddots & \\ & & & 1 & a \end{bmatrix}$$

Let $A \in M_l(\mathbb{C})$ (any matrix). Let V be an l-dimensional complex vector space. Define a $\mathbb{C}[x]$-module structure on V by letting x act via the matrix A. Apply the structure theorem o V (as $\mathbb{C}[x]$-module). V is finite dimensional, but $\mathbb{C}[x]^{\oplus n}$ is infinite, so it doesn't show up in the decomposition. Therefore, $V \simeq \oplus$cyclics, Jordan canonical form.

21.2 *Proof of structure theorem*

Lemma 21.2. *(R can be any ring here.) Let $0 \to M \to N \to F \to 0$ be a short exact sequence of R-modules, and assume F is free. Then the sequence splits.*

Remark 21.3 — The condition in the lemma "defines" projective modules.

22 February 28, 2022

22.1 Midterm solutions

Problem 22.1. Consider $\mathbb{Q}(\sqrt{17+\sqrt{17}})$.

Solution. Let $p = 17$, $\alpha = \sqrt{p+\sqrt{p}}$, and $\beta = \sqrt{p-\sqrt{p}}$. Conjugates of α are $\pm\alpha$ and $\pm\beta$. Let

$$f(x) = (x-\alpha)(x+\alpha)(x-\beta)(x+\beta) = (x^2-\alpha^2)(x^2-\beta^2)$$

$$= x^4 - 2px^2 + (p^2-p) = x^4 - 34x^2 + 272.$$

1. f is irreducible by Eisenstein with prime p. Alternatively, f has no linear factor, and any quadratic factor requires α^2, β^2, or $\alpha\beta$ to be rational. Again, alternatively, if not, α has to be quadratic, but then you conclude that $\sqrt{17}$ is rational.
2. $\mathbb{Q}(\alpha) = \mathbb{Q}_f$. Splitting field, separable (characteristic 0) implies Galois. Why splitting field? Certainly $\mathbb{Q}(\alpha) \subset \mathbb{Q}_f$.
   - $\sqrt{p} \in \mathbb{Q}(\alpha)$.
   - $\alpha\beta = \sqrt{p^2-p} = \sqrt{p-1}\sqrt{p}$. Since $17-1 = 4^2$, we get $\beta = \sqrt{p-1}\sqrt{p}/2 \in \mathbb{Q}(\alpha)$.

   This gives us normality. $\mathbb{Q}(\alpha)/\mathbb{Q}$ Galois of degree 4.
3. Take $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$. Take $\sigma(\alpha) = \beta$. Compute to check that $\sigma^2 \neq \mathrm{id}$. Conclude that our Galois group is $\mathbb{Z}/4$.

■

Problem 22.2. 3 part Galois question.

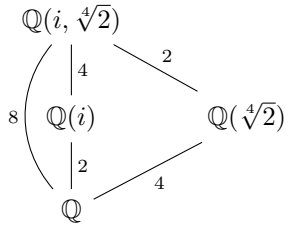
Solution. Claim: $\mathbb{Q}(\sqrt[4]{2}, i)$ splitting field of $f(x) = x^4 + 2$. Take $\omega^8 = 1$ primitive. Then roots of f are exactly $\omega^k \cdot \sqrt[4]{2}$. Note

$$\omega = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}} = \frac{1}{\sqrt{2}}(1+i).$$

Notice by dividing two roots of f that $i = \omega^2 \in \mathbb{Q}_f$. Also $\sqrt{2}\omega = (1+i) \in \mathbb{Q}_f$. Then

$$\frac{\omega\sqrt[4]{2}}{\omega\sqrt{2}} = \sqrt[4]{2} \in \mathbb{Q}_f.$$

$\omega\sqrt[4]{2}/\sqrt[4]{2} = \omega \in \mathbb{Q}_f$. Hence $\mathbb{Q}(i, \sqrt[4]{2}) \in \mathbb{Q}_f$. $\omega = (1+i)/\sqrt{2}$, so $\mathbb{Q}_f \subset \mathbb{Q}(i, \sqrt[4]{2})$. Tower



gives us $|\mathbb{Q}_f : \mathbb{Q}| = 8$ and $|\mathbb{Q}_f : \mathbb{Q}(i)| = 4$. Galois group of the first is a size 8 subgroup of S_4 implies D_4. For the second, note that $\mathbb{Q}_f$ is the splitting field of $x^4 - 2$, and invoke Kummer's theorem. Alternatively, $D_4 \simeq \mathbb{Z}/4 \rtimes \mathbb{Z}/2$, and this $\mathbb{Z}/2$ corresponds to $\mathbb{Q}(i)/\mathbb{Q}$. Factoring out leaves $\mathbb{Z}/4$.

For the second part, irreducible b/c no roots (rational root test). Galois b/c we adjoined one thing and irreducible. Discriminant to compute Galois group. ■

Problem 22.3. $f(x) = x^p - x - a$, $a \neq 0$ in $\mathbb{F}_p$.

Solution. 2 observations. Let α be a root. Then $\alpha + b \in \mathbb{F}_p$ is also a root (characteristic p and Fermat's little theorem). Take $L = \mathbb{F}_p(\alpha)$. Then L is the splitting field, as $\alpha, \alpha+1, \ldots, \alpha+p-1$ are all the roots. f is irreducible. Why? Suppose not. Then $f(x) = g(x)h(x)$, where g has roots $\alpha + b_i$, $b_i \in \mathbb{F}_p$. g has coefficients in $\mathbb{F}_p$, so $\sum \alpha + b_i \in \mathbb{F}_p$.

$$n\alpha + b \in \mathbb{F}_p \Rightarrow \alpha \in \mathbb{F}_p$$

is a contradiction. This tells us that the extension has degree p, so $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^p}$. Alternatively, let σ be the Frobenius automorphism. $\sigma(\beta) = \beta^p$. $\sigma(\alpha) = \alpha^p$. Note that $\sigma \in \mathrm{Aut}_{\mathbb{F}_p}(L)$ $f(x) = x^p - x - a$.

$$f(\alpha^p) = \alpha^{p^2} - \alpha^p - a = (\alpha^p - \alpha)^p - a = \alpha^p - a = 0$$

Let $\sigma(\alpha) = \alpha + b$, $b \neq 0$ since $\alpha \notin \mathbb{F}_p$. $\sigma^i(\alpha) = \alpha + ib$. All powers of σ are distinct, so $|\mathrm{Gal}(L/\mathbb{F}_p)| \geq p$, but $|L : \mathbb{F}_p| \leq p$, so $L/\mathbb{F}_p$ is Galois of degree p implies $L = \mathbb{F}_{p^p}$. ■

23 March 2, 2022

Problem 23.1. For positive integer D, parametrize solutions of $a^2 + Db^2$.

Solution. Consider $\mathbb{Q}(\sqrt{-D})$. Notice that $N(a + b\sqrt{-D}) = a^2 + Db^2$. Then by Hilbert's 90 theorem, there exists $\beta \in \mathbb{Q}(\sqrt{-D})$ such that

$$a + b\sqrt{-D} = \beta/\sigma(\beta) = \frac{r + s\sqrt{-D}}{r - s\sqrt{-D}},$$

where $r, s \in \mathbb{Q}$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{-D})/\mathbb{Q})$. We can of assume $r, s \in \mathbb{Z}$. Then we can compute that

$$a + b\sqrt{-D} = \frac{r^2 + 2rs\sqrt{-D} - Ds^2}{r^2 + Ds^2}$$

and therefore,

$$a = \frac{r^2 - Ds^2}{r^2 + Ds^2}, \quad \text{and} \quad b = \frac{2rs}{r^2 + Ds^2}.$$

For part (b), set $D = 1$, and consider

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1.$$

By part (a), we have that

$$\frac{x}{z} = \frac{u^2 - v^2}{,} \quad \text{and} \quad \frac{y}{z} = \frac{2uv}{u^2 + v^2}$$

which implies

$$(x, y, z) = \lambda(u^2 - v^2, 2uv, u^2 + v^2)$$

where $\lambda \in \mathbb{Q}$ takes the form $1/m$. Need to show $\lambda = 1$. Parity argument for odd λ. Assume x is odd. If u, v both odd, properties of squares mod 4, and x is even. Therefore, u, v not both odd, so 2 is not a factor. ■

Problem 23.2. Third isomorphism theorem.

Solution. $\varphi : M_3 \to M_3/M_1 \to (M_3/M_1)/(M_2/M_1)$. Check that Ker $\varphi = M_2$. ■

23.1 Proof structure theorem (cont.)

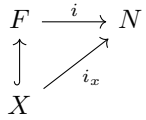
R a PID, everything happening in finitely generated R-mods.

All of this (for today) is general (not necessarily PID).

Proofs of omitted details in chapter 12 of DF.

Lemma 23.1. *Let $0 \to M \to_f N \to_g F \to 0$ be a short exact sequence with F free. Then it splits.*

Proof. Need to show that there exists $i : F \to N$ such that $g \circ i = \mathrm{id}_F$. Let X be a basis of F. Define a set map $i_x : X \to N$ by $x \mapsto g^{-1}(x)$. By the universal property of a free module, there exists unique i such that



extending i_x to an R-module homomorphism. ∎

Remark 23.1 — Free modules are "projective".

Remark 23.2 — F is free, so $F \simeq \oplus_I R = R^{\oplus I}$. The rank of F is the cardinality of I and is well-defined.

Torsion

Definition (Torsion)**.** Let M be an R-mod. Define $M_{\text{tor}} \subset M$ as

$$M_{\text{tor}} = \{m \in M \mid \exists a \in R : a \neq 0, am = 0\}$$

which we call the **torsion** part of M. If $m \in M_{\text{tor}}$, we say that m is a **torsion element**. If $M_{\text{tor}} = \{0\}$, we say M is **torsion free**. Otherwise, M has non-trivial torsion, we say it is **torsion**.

Example 23.1. $\mathbb{Z}, \mathbb{Q}$ is torsion-free. $\mathbb{Z}/n$ is torsion (multiply by $n \in \mathbb{Z}$)[4]. $\mathbb{Q}/\mathbb{Z}$ is torsion.

[4] *Think about definition of module, $\mathbb{Z}$ the ring acts on $\mathbb{Z}/n$.*

Remark 23.3 — M_{tor} is a submodule of M.

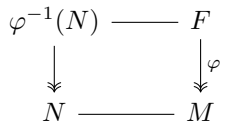
Theorem 23.2. *R a PID. A submodule of of a finitely generated free module is a finitely generated free module. Moreover, if $F' \subset F$, F free, rank of F is n, then F' is free, rank of F' is at most rank of F.*

DF. 12.1 ∎

Remark 23.4 — In homological algebra terminology, global dimension of R is 1.

Corollary 23.3. *R a PID. A submodule of a finitely generated module is finitely generated.*

Proof. Below, the lines denote subset (left subset of right).



■

24 March 4, 2022

Theorem 24.1. *R a PID, F a free module of rank n. $M \subset F$ is a non-zero submodule. Then M is free of rank at most n.*

Proof. Induction on n, the rank of F. Start with $n = 1$, in which case $F \simeq R$. $M \subset R$ implies it is a principal ideal, $M = (a)$, $a \in \mathbb{R}$ non-zero. a is a basis for M, that is, if $ra = 0$ for $r \in R$, $r = 0$. This is true since R is a domain.

Induction step $n - 1 \mapsto n$. Recall the lemma that if $0 \to M_1 \to M_2 \to F \to 0$ with F free, then it splits. $M \subset F$. Rank of F is n. Let $x_1, \ldots, x_n$ be a basis of F. Let F' be the submodule of F generated by $x_1, \ldots, x_{n-1}$.

$$F' = \bigoplus_i^{n-1} Rx_i$$

$\{x_1, \ldots, x_{n-1}\}$ is a basis of F', which means F' is free of rank $n - 1$. Define $M' = M \cap F'$.

$$\begin{array}{ccc} F' & \longrightarrow & F \\ \uparrow & & \uparrow \\ M' & \longrightarrow & M \end{array}$$

Consider the two following cases.

- $M \subset F'$, that is $M' = M$. Then M is free by induction hypothesis.
- $M \not\subset F' \Rightarrow M' \subsetneq M$.

Construct the sequence below (where line segments denote subset, bottom subset of top).

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F' & \longrightarrow & F & \longrightarrow & F/F' \simeq Rx_n & \longrightarrow & 0 \\ & & | & & | & & | & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M/M' & \longrightarrow & 0 \end{array}$$

But then M/M' is a submodule in a free module of rank 1, so M/M' is also free (by the base case) of rank 1. By the lemma, the second short exact sequence splits, therefore

$$M \simeq M' \oplus M/M'.$$

M' free by induction, M/M' free of rank 1. Sum of free modules is free, and this has rank at most $(n - 1) + 1 = n$. ∎

We use the following implicitly in discussing F/F' and M/M' in the proof above.

Lemma 24.2 (2nd isomorphism theorem)**.** *For $M, N' \subset N$ with $M' = M \cap N'$, we have that the inclusion $M \hookrightarrow N$ induces a map from $M/M' \to N/N'$ which is injective (isomorphism).*

Proof. Exercise. ■

Example 24.1. Main examples $\mathbb{Z}$, $k[x]$. Consider $k[x, y]$ and the ideal $I = (x^2, y)$. Can it be principal? If it is, $(x^2, y) = (f(x, y))$. In other words, there exist g, h such that

$$x^2 = f(x, y)g(x, y) \quad \text{and} \quad y = f(x, y)h(x, y).$$

Not possible. Most rings not PIDs.

Recall the last corollary from last time.

Proof. There exist a free finitely generated module $F \twoheadrightarrow^{\varphi} M$.

$$\begin{array}{ccc} F & \xrightarrow{\varphi} & M \\ \big| & & \big| \\ \varphi^{-1}(N) & \longrightarrow & N \end{array}$$

By the theorem, $\varphi^{-1}(N)$ is free of finite rank, so N is finitely generated. ■

Remark 24.1 — For any ring R, we have the following hierarchy of modules.

$$\{\text{free}\} \subset \{\text{projective}\} \subset \{\text{flat}\} \subset \{\text{torsion-free}\}$$

In a PID, these are all equal.

Theorem 24.3. *R a PID, M finitely generated module, then $M \simeq F \oplus M_{tor}$.*

$$0 \to M_{tor} \to M \to F \to 0$$

Proof. Ch. 12 (DF) ■

Remark 24.2 — Since $F \simeq M/M_{\text{tor}}$, it is well-defined up to isomorphism, which implies that $\text{rk}(M) = \text{rk}(F) = \text{rk}(M/M_{\text{tor}})$ is well-defined. Specific to PIDs.

p-primary component

Definition (p-primary component)**.** R a PID and (p) a prime ideal. Let M be an R-module. The p**-primary component** of M is

$$M_{(p)} = \{m \in M \mid p^i m = 0, i \in \mathbb{Z}_{>0}\}.$$

Definition. P, q irreducible in R are **associated primes** (denoted $p \sim q$) if there exists a unit $u \in R$ such that $p = uq$.

We hope then that $M_{(p)} = M_{(uq)}$.

Claim 24.1 — $P \sim q$ iff $(p) = (q)$.

a-torsion

Definition (a-torsion)**.** For non-zero $a \in R$, we can consider a**-torsion** of M,

$$M_a = \{m \in M \mid am = 0\}.$$

Remark 24.3 — Note the two following properties,

$$M_{\text{tor}} = \bigcup_{a \in R, a \neq 0} M_a$$

and

$$M_{(p)} = \bigcup_{i>0} M_{p^i},$$

noting that $M_p \neq M_{(p)}$.

Lemma 24.4. *$a = bc$ with $(b, c) = 1$. Then $M_a = M_b \oplus M_c$. (prototype: $\mathbb{Z}/pq \simeq \mathbb{Z}/p \times \mathbb{Z}/q$)*

Theorem 24.5. *Torsion splits as a direct sum of its p-primary components.*

$$M_{tor} \simeq \bigoplus_{\mathcal{P}} M_{(p)},$$

where $\mathcal{P}$ denotes the prime ideals in R.

25 March 7, 2022

Structure theorem for R a PID (part 3).

Recall our statement.

1. $M \simeq F \oplus M_{\text{tor}}$ with $\text{rk}(M) = \text{rk}(F)$.
2. $M_{\text{tor}} \simeq \bigoplus_{(p)\in\mathcal{P}} M_{(p)}$ ((p)-torsion, p-primary).

We will also have that if $M = M_{(p)}$, then

$$M_{(p)} \simeq \bigoplus_{i=1}^{N} R/(p^{n_i})$$

Definition. M an R-mod with $\{x_1, \dots, x_n\}$. $\{x_1, \dots, x_n\}$ are **independent** if for all $a_1, \dots, a_n \in R$, $\sum a_i x_i = 0$ implies that $a_j x_j = 0$ for all j.

Remark 25.1 — Weaker than linear independence.

Example 25.1. $M = \mathbb{Z}/p \oplus \mathbb{Z}/p^2$ as a $\mathbb{Z}$-module. Let a, b generate each piece. Then $pa + p^2 b = 0$ implies that $pa = p^2 b = 0$.

Theorem 25.1. *M finitely generated (p)-torsion R-module. Then there exists a set of independent generators for M.*

Proof. DF. ■

Theorem 25.2. *M a finitely generated R-module,*

$$M_{(p)} \simeq \bigoplus_{i=1}^{N} R/(p^{n_i})$$

Proof. Follows from previous theorem.

Let $x_1, \dots, x_N$ be independent generators of $M_{(p)}$.

$$M_{(p)} = Rx_1 + \ldots + Rx_N$$

This is a direct sum because $x_1, \dots, x_n\}$ are independent. $M_{(p)} \simeq \oplus Rx_i$.

Rx_i is cyclic. $I = \text{Ker}\, \varphi \hookrightarrow R \to^{\varphi} Rx_i$, with φ sending 1 to x_i. Since x_i is (p)-torsion, $I = (a) = (p^{n_i})$. Hence, $Rx_i \simeq R/I = R/(p^{n_i})$. ■

Claim 25.1 — This decomposition is unique.

25.1 Frobenius normal form

For R a PID, M finitely generated, there exist $d_1, \dots, d_n \in R$, such that $d_1 | d_2 | \dots | d_n$ (invariant factors) such that

$$M \simeq F \oplus \bigoplus_{i=1}^{n} R/(d_i),$$

(F free). $R = k[x]$, Frobenius normal form/rational canonical form.

Example 25.2. M a (p)-torsion module. Classical (Jordan) structure theorem says

$$M \simeq \bigoplus_{i=1}^{N} R/(p^{n_i}).$$

Then arranging our indices such that powers are increasing to get invariant factors,

$$p^{n_1} | \dots | p^{n_N}.$$

In general, "rearrangement" exercise.

25.2 (A snapshot of) Group representation theory

(J.P. Serre book, linear group representations)

G a group, k a field (or a commutative ring R like $\mathbb{Z}$).

Group ring

Definition (Group ring)**.** The **group ring** kG is a k-vector space (free module) with basis $\{e_g\}_{g \in G}$ and the following ring structure.

1. Addition of vectors as normal.
2. k-linear structure.
3. $e_g \cdot e_h = e_{gh}$, and extend k-linearly.
4. $1 = e_e$.
5. $e_n^{-1} = e_{n^{-1}}$.

Remark 25.2 — k-algebra is a ring with this k-vector space structure.

Example 25.3. Start with $G = \mathbb{Z}$. What is $k\mathbb{Z}$? Let $\mathbb{Z} = \langle x \rangle$. Then the basis of $\mathbb{Z}$ is the set of all powers of x, and we see that $k\mathbb{Z} \simeq k[x, x^{-1}]$ (power series), the localization of $k[x]$ at x.

Remark 25.3 — kG is commutative iff G is abelian.

Example 25.4. Take $G = \mathbb{Z}/n = \langle \sigma \rangle$. Then

$$k\frac{\mathbb{Z}}{n} \simeq \frac{k[x]}{\sigma^n - 1}.$$

Example 25.5. Take $S_3 \simeq D_3 = \{\sigma, \tau \mid \sigma^3 = \tau^2 = 1, \tau\sigma\tau = \sigma^2\}$. $kD_3 = k\langle \sigma, \tau \rangle / (\sigma^3 = \tau^2 = 1, \tau\sigma = \sigma^2\tau)$.

Note that $k[x, y] = k\langle x, y \rangle / (xy - yx)$.

Remark 25.4 — $|G| < \infty$ implies that $\dim_k kG = |G|$.

Definition. G a group. $V \in \mathrm{Vect}_k$. V is a linear representation of G if we have a map from $G \times V \to V$ sending $(g, v) \mapsto gv$ such that the following are true.

1. k-linear ($\alpha \in k, v_1, v_2 \in V$).

$$g(\alpha v) = \alpha(gv) \quad \text{and} \quad g(v_1 + v_2) = gv_1 + gv_2$$

2. $(g_1 g_2)v = g_1(g_2 v)$. $ev = v$.

26 March 9, 2022

Recall linear representations. $\mathrm{Rep}_k G$.

> **Definition.** φ is a map of G-morphisms if for all $g \in G, v \in V$, $\varphi(gv) = g\varphi(v)$.

Another point of view:

> Claim 26.1 — To give a representation of G on V is equivalent to defining a group homomorphism from $G \to^{\rho_V} GL(V)$ ($\simeq GL_n$), where
>
> $$GL(V) = \mathrm{Aut}_k(V) = \{f : V \to V \mid \text{ invertible } k\text{-linear maps}\}.$$
>
> If $\dim V = n$, we can identify $GL(V) \simeq GL_n$.

Why is this true? Any $g \in G$ yields a linear map $g : V \to V$ with $v \mapsto gv$, which is invertible by $g^{-1} : V \to V$, the inverse map. Define $\rho_V(g) = g : V \to V$ and notice it is a group homomorphism. $gh : V \to V$ sends $v \mapsto (gh)v$, whereas

$$h : V \to V \quad v \mapsto hv, \quad \text{and} \quad g : V \to V \quad hv \mapsto ghv,$$

so $\rho_V(gh) = \rho_V(g)\rho_V(h)$.

Yet another point of view:

> Claim 26.2 — Category isomorphism $\mathrm{Rep}_k G \simeq kG$-mod. On the left, $G \times V \to V$. On the right, $kG \times V \to V$, $a = \sum \alpha_g e_g$, $b = \sum \beta_h e_h$.

> **Example 26.1.** Take D_3 acting on $\mathbb{R}^2$. $D_3 = \langle \sigma, \tau \rangle$, rotation by 120 degrees and flip over x-axis. $D_3 \to GL_2(\mathbb{R})$. $e_1 = \binom{1}{0}, e_2 = \binom{0}{1}$.
>
> $$\sigma e_1 = \begin{pmatrix} -1/2 \\ \sqrt{3}/2 \end{pmatrix}, \quad \sigma e_2 = \begin{pmatrix} -\sqrt{3}/2 \\ -1/2 \end{pmatrix} \Rightarrow \sigma = \begin{bmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix}$$
>
> $$\tau \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$
>
> k-algebra:
>
> $$\mathbb{R}D_3 = \frac{\mathbb{R}\langle \sigma, \tau \rangle}{\langle \tau\sigma = \sigma^2\tau, \sigma^3 = \tau^2 = 1 \rangle}$$

Example 26.2. 1 dimensional representations. $G \to k^*$ ($\simeq GL_1$). In fact, $|G| = n$ implies $G \to \mu_n \subset k^*$. $g \in G \Rightarrow g^n = 1 \Rightarrow \rho(g)^n = 1$.

Example 26.3. X a set, $G \times X \to X$, G acts on X. For some field k, we can consider $\mathcal{F}(X)$ the functions $f : X \to k$, which is a k-vector space. $f_1, f_2 : X \to k$ yields $af_1 + bf_2 : X \to k$. $\mathcal{F}(X) \in \text{Rep } G$, $G \times \mathcal{F}(X) \to \mathcal{F}(X)$, $(gf)(x) = f(g^{-1}(x))$.

Example 26.4. $G \times kG \to kG$. Define $ge_h = e_{gh}$.

$$g\left(\sum \alpha_h e_h\right) = \sum \alpha_h e_{gh}$$

Regular representation of G. Contains all other representations over the complex numbers.

Claim 26.3 — $\text{Rep}_{\mathbb{C}} G$ is semisimple.

Theorem 26.1 (Mascke, 1897)**.** *Let G be a finite group, char k does not divide $|G|$. V be a finite dimensional representation, $W \subset V$ be G-invariant subspace (subrepresentation of V). Then there exists $W' \subset V$, subrepresentation such that $V = W \oplus W'$ (orthogonal complement). In other words,*

$$0 \to W \to V \to V/W \to 0$$

(Rep G) splits.

Proof. $W \to V$ splitting as vector spaces. $V = W \oplus W_1 \to^{\pi} W$. π is a map of vector spaces. Define $\tilde{\pi} : V \to V$ which sends

$$\tilde{\pi}(v) = \frac{1}{|G|} \sum_{s \in G} s\pi(s^{-1}v).$$

Claims:

1. $\tilde{\pi}$ is a G-map.

$$\tilde{\pi}(gv) = \frac{1}{|G|} \sum s\pi(s^{-1}gv) = \frac{1}{|G|} \sum s\pi\left((g^{-1}s)^{-1}v\right)$$

$$= \frac{1}{|G|} \sum g(g^{-1}s)\pi((g^{-1}s)^{-1}v) = g\left(\frac{1}{|G|}\sum_{s\in G} g^{-1}s\pi((g^{-1}s)^{-1}v)\right)$$
$$= g\tilde{\pi}(v)$$

2. $w \in W$, $\tilde{\pi}(w) = \pi(w) \in W$.
3. $w' \in W_1$, $\tilde{\pi}(w') = 0$.

■

Remark 26.1 — $GL_n, n = \dim V$. Can think about this as

$$\begin{bmatrix} A & B \\ 0 & C \end{bmatrix} \sim \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix},$$

always being able to convert block upper triangular (A invariant subspace) to block diagonal.

Example 26.5. In $\mathbb{F}_p$ ($\mathbb{Z}/p$??), take some matrix of size $p \times p$. Last Jordan block can't be split.