Advanced Algebraic Structures

Lenie (H.M.) Goossens
S4349113

1B 2023-2024

Contents

Lecture 1 **3**
Introduction . . . 3
Basic definition . . . 3

Lecture 2 **6**
Normal Extensions . . . 6
Separable extensions . . . 7

Lecture 3 **9**
Properties of separability . . . 9

Lecture 4 **12**
Properties Galois extensions . . . 12

Lecture 5 **15**
Galois correspondence . . . 15

Lecture 5 **18**
Cyclotomic fields . . . 18

Lecture 7 **21**
Extensions of $\mathbb{F}_q$ . . . 21
Cyclic extensions . . . 21
Symmetric polynomials . . . 23

Lecture 8 **24**
Computing Galois group of polynomials 25
Algebraic closure of a field 25
Extra curriculum: Infinite Galois theory 26

Lecture 9 **27**
Homomorphism theorem 27
Submodules 29
Quotient modules 29

Lecture 10 **30**

Lecture 11 **34**
Universal property (UP) of direct sums 35
Modules over PID's 36

Lecture 12 **37**
Linear algebra over fields (normal forms of matrices) 38

Lecture 13 **41**
Exactness 41
Homomorphisms 42

Lecture 14 **45**
Split exact sequences 45
Projective modules 47

Lecture 15 **50**

Catch-up session 04-04-2024 **53**

NEED TO REMEMBER **54**

Lecture 1

Introduction

$f = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Q}[X]$ polynomial.
Q: "What are its roots?

$n = 1$ then $x - a \leftrightarrow x = a$

$n = 2$ then $x^2 + px + q \Leftrightarrow x = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$

$n = 3$ then x^3+px^2+qx+r. We see that if we replace x by $x-\frac{p}{3}$. Then we get x^3+px+q.
Discriminant $\Delta = \left(\frac{q}{2}\right) + \left(\frac{p}{3}\right)^3$. Then one root is $\sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}}$
This is called CARDANO FORMULA

$n = 4$ "solvable by radicals",i.e. there is a formula only involving $+, -, /, \sqrt[n]{\ldots}$

$n \geq 5$ then is not solvable by radicals in general. This is Abel Raffini Theorem
Galois explained this in a conceptial way, also over general ground fields. Made shift from polynomials to field extensions.

Basic definition

K FIELD
$K[x] = \{a_0 + a_1 x + \ldots + a_n x^n | n \geq 0, a_i \in K\}$
$K(x) = \mathrm{Quot}(K[x]) = \left\{\frac{f(x)}{g(x)} | f, g \in K[X], g \neq 0\right\}$
PRIME FIELD OF A FIELD smallest subfield of $K = \begin{cases} \mathbb{Q} \ \mathrm{char}(K) = 0 \\ \mathbb{F}_p \ \mathrm{char}(K) = p > 0 \end{cases}$
L/K FIELD EXTENSION $L \supseteq K$.
$[L : K] = \dim_K L$ which is DEGREE OF L OVER K
L/K finite iff $[L : K] < \infty$. Note that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 < \infty$ and $[\mathbb{R} : \mathbb{Q}] = \infty$.
TOWER LAW: $L/M/K$ then $[L : K] = [L : M] \cdot [M : K]$.
$A \subseteq L$ SUBSET then

- $K[A]$ = smallest subring of L containing the field K and the set A.
- $K(A)$ = smallest subfield of L containing the field KK and the set A.

$a \in L$ ALGEBRAIC OVER K if $\exists 0 \neq f \in K[X]$ s.t. $f(a) = 0$.
If $a \in L$ TRANSCEDENTAL OVER K if $a \in L$ not algebraic over K.
Note that $\mathbb{Q}(\sqrt{\pi})/\mathbb{Q}$ is transcedental and $\mathbb{Q}(\pi)/\mathbb{Q}$ is transcedental but $\mathbb{Q}(\sqrt{\pi})/\mathbb{Q}(\pi)$ is algebraic.
$0 \neq f \in K[X]$ MINIMAL POLYNOMIAL OF $a \in L$ over K if f is monic and has minimal degree. (irreducible and unique).

From Algebraic structures $K[X] \to K[a]$ with $x \mapsto a$ where a algebraic.
Then $K[X]/(f) \xrightarrow{\sim} K[a] = K(a)$ where f minimal polynomial.
Then $[K[a] : K] = \deg(f)$, $K-$ basis of $k[a] : 1, a, a^2, \ldots, a^{\deg(f)-1}$.

L/K ALGEBRAIC $\Leftrightarrow \forall a \in L$ are algebraic over K.
L/K TRANSCENDENTAL if L/K is not algebraic.

Proposition:
L/K is finite $\Rightarrow L/K$ algebraic.$L \xrightarrow{f} L'$ -homomorphism iff $f|_K = \mathrm{id}_K$.
Proof:
Arbitrary $x \in L$. Take $x^0, x^1, \ldots, x^{[L:K]}$ are $K-$ lin. dep. Here we use that $[L : K] < \infty$. Therefore we see that $\sum\limits_{i=0} a_i x^i = 0$ so there exists a minimal polynomial. So L/K is algebraic.

The converse is false: $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots]/\mathbb{Q}$ is infinite and algebraic.

$a \in L$ where L/K transcendental then $K[a] \cong K[X]$ polynomial ring and $K(a) \cong K(X)$ field of rational functions over K.

L, L' field extensions of field K then a K HOMOMORPHISM $L \to L'$ is field homomorphism $\phi : L \to L'$ s.t. $\phi|_K = \mathrm{id}_K$.
K ISOMORPHISM bijective K- homomorphism. L, L' are $K-$ isomorphic $(L \cong_K L')$ if $-$ isomorphism $L \to L'$ exists. $K-$ automorphism if K- isomorphism with $L = L'$.
Example:
$\tau : \mathbb{C} \to \mathbb{C}$ with $z \mapsto \overline{z}$. $\mathbb{R}-$ automorphism is $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}_{\mathbb{C}}, \tau\}$ but $\mathrm{Aut}(\mathbb{C})$ is uncountable.

K field and $0 \neq f \in K[X]$ then L/K SPLITTING FIELD OF f OVER k iff

i $f = \prod_{i=1}^{n} (x - \alpha_i) \in L[x]$ splits completly into linear factors

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

Proposition 1.1 (I.3.2)

1) $\exists$ splitting field $L/K \& [L:K] \leq \deg(f)!$
2) A splitting field L/K is unique up to $K-$ isomorphism (Prop 6.5/AS Top III.5.4)

Proof:

1. Induction on degree of f. If $\deg(f)=1$, then $L=K$ is splitting field. Otherwise take irreducible fact $f_1|f$ then $K[X]/(f_1)$ is a field extension of K of degree $\deg(f_1) \leq \deg(f)$ and $f_1(\overline{x})=0$.
   Now do induction with $\frac{f}{(x-\overline{x})} \in L[X]$.

2. For induction prove slightly more general statement. $\phi_0 \to \phi_0 : K_1[X] \tilde{\to} K_2[X]$ with $\sum a_i x^i \mapsto \sum \phi_0(a_i)x^i$.
   $K_1 \tilde{\to} K_2$ by ϕ_0 s.t. $0 \neq f_1 \in K_1[X] \to f_2 = \phi_0(f_1) \in K_2[X]$. Then L_i/K_i splitting fields of f_i for $i=1,2$. Then there exists ϕ s.t. $L_1 \tilde{\to} L_2$ by ϕ,Which implies uniqueness by taking $K_1=K_2=K, \phi_0=\mathrm{id}_K$.

   We proof this by induction.
   If f_1 constant, take $L_i = K_i$.
   Otherwise take $\phi_1|f_1$ irreducible. Since isomorphic with ϕ_0 we see that $\phi_2=\phi_0(\phi_1) \in K_2[X]$.
   L_i/K_i splitting field: $\exists \alpha \in L_1$ s.t. $\phi_1(\alpha)=0$,and $\exists \beta \in L_2$ s.t. $\phi_2(\beta)=0$. So we see that $K_1[\alpha] \tilde{\to} K_2[\beta] : \sum a_i x^i \mapsto \sum \phi_0(a_i)\beta^i$.
   By induction can extend ϕ_1 to $\phi : L_1 \tilde{\to} L_2$.

Example:
$K=\mathbb{Q}, f=x^3-2$, splitting field $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Then $f=(X-\sqrt[3]{2})\cdot f_2 \in \mathbb{Q}(\sqrt[3]{2})[X]$. Note that f_2 has roots in $\mathbb{C} \setminus \mathbb{R}$ while $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.
Now note that the other roots of x^3-2 are $\zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}$. So then $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2})/\mathbb{Q}$ is a splitting field of degree $3\cdot 2 = 3!$.

Lecture 2

Normal extensions

L/K NORMAL iff $\forall f \in K[x]$ that has root in $L : f$ splits over L iff $\forall \alpha \in L : \text{minpol}_K(\alpha)$ splits over L.

$H \leq G$ subgroup and $[G : H] = 2 \Rightarrow H \trianglelefteq G$ i.e. $H = gHg^{-1}$ for all $g \in G$.
$\text{Spl}_M(\alpha)$ is splitting field of α over M.

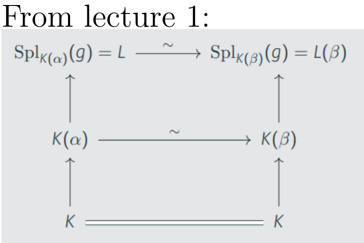
Theorem 2.1 (Bianchi 3.6):

$$\begin{aligned} &L/K \text{ finite then following equivalent :} \\ &1) L/K \text{ normal} \\ &2) L = \text{spl}_K(g) \text{ for some } g \in K[x] \end{aligned} \tag{Thm 2.1/Bianchi 3.6}$$

Proof:

$1 \Rightarrow 2$ $L = K(\alpha_1, \ldots, \alpha_n)$ since L/K finite. Def. $f_i := \text{minpol}_K(\alpha_i)$ which splits over L, since normal. Define $g := \prod_{i=1}^{n} f_i$. Therefore $L = K(\alpha_1, \ldots, \alpha_n) \subseteq \text{Spl}_K(g) \subseteq L$. For this we must have equality throughout

$2 \Rightarrow 1$ $\alpha \in L, f := \text{minpol}_K(\alpha), M := \text{Spl}_L(f) \supseteq L$. Want $M = L$. Let $\beta \in M : f(\beta) = 0$. From lecture 1:



Hence $[L : K] = [L(\beta) : K]$, hence $\beta \in L$. Therefore $M \subseteq L$. Since we defined M in such a way that $M \supseteq L$, we see that we get $L = M$.

Example:
$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \text{Spl}_{\mathbb{Q}}((X^2 - 2)(X^2 - 3))/\mathbb{Q}$ normal
$\text{Spl}_{\mathbb{Q}}(X^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ normal
$\mathbb{F}_p(t^{1/p}) = \text{Spl}_{\mathbb{F}_p(t)}(X^p - t)/\mathbb{F}_p(t)$ normal.
Warning: normality is not transitive, i.e. if we have L/M normal, M/K normal then it does not imply that L/K is normal.
Warning: Distinguish $\text{Aut}_K(L)$ as field extensions or as vector space.

Separable extensions

1. $0 \neq f \in K[x]$ separable iff f hs no multiple roots in $\mathrm{Spl}_K(f)$
2. $\alpha \in L$ separable over K iff $\mathrm{minpol}_K(\alpha)$ separable.
3. L/K separable iff all $\alpha \in L$ separable over K

Non-example:

- $\mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)$ not separable since $X^P - t = (X - t^{1/p})^p$
- $[L : K] = 2$ not separable iff $\mathrm{char}(K) = 2$ and $L = K(\sqrt{d})$ with $d \in K \setminus K^{\square}$ where $K^{\square} = \{k \in K | \exists z \in \mathbb{Z}; z^2 = k\}$

  This is because $\alpha \in L$ then $\mathrm{minpol}_K(\alpha) = (X - \alpha)(X - \overline{\alpha}) = X^2 - pX + q$ where $p = \alpha + \overline{\alpha}, q = \alpha\overline{\alpha}$. Since α not separable over K iff $\alpha = \overline{\alpha}$ therefore $p = 2\alpha \in L$.

Example:
$X^2 + X + 1 \in \mathbb{F}_2[X]$ irreducible and separable.

K field, then

$$(-)' : K[X] \to K[X] \text{ s.t. } f = \sum_{i \geq 0} a_i x^i \mapsto f' := \sum_{i \geq 1} i a_i x^{i-1}$$

Proposition 2.2

$$\begin{aligned} &f, g \in K[X] \text{ then:} \\ &1)\text{formal derivative is } K-\text{ linear (as vector space)} \\ &2)\text{LEIBNIZ RULE: } (fg)' = f'g + fg' \\ &3) \text{ root } \alpha \text{ of } f \text{ is SIMPLE: } (\#\text{roots}(\alpha) = 1 \text{ iff } f'(\alpha) \neq 0 \end{aligned} \tag{Prop 2.2}$$

Example:
$(X^p - t)' = pX^{p-1} = 0$ if $\mathrm{char}(K) = p > 0$.

K is PERFECT iff $K = K^p := \{x^p : x \in K\}$ iff frobenius norm is surjective.

Theorem 2.3 (Bianchi 4.4)

$$\begin{aligned} &L/K \text{ finite is SEPARABLE if} \\ &1)\mathrm{char}(K) = 0, \text{or} \\ &2)\mathrm{char}(K) = p > 0 \text{ and } p \nmid [L : K] \text{ or} \\ &3)\mathrm{char}(K) = p > 0 \text{ and } K = K^p \end{aligned} \tag{Thm 2.3/Bianchi 4.4}$$

Proof:
$\alpha \in L, f = \text{minpol}_K(\alpha)$. $\beta \in M : f(\beta) = 0, f = \text{minpol}_K(\beta)$.
If β not simple root $\Rightarrow f'(\beta) = 0$ hence $f' = 0$ so f irreducible.
If $\text{char}(K) = p \Rightarrow f \equiv a_0$ contradiction.
$\text{char}(K) = p \Rightarrow f = g(x^p)$ hence $p|[K(\alpha) : K]|[L : K]$.
$K = K^p, f = g(x^p) = h(x)^p$ reducible, contradiction.

Therefore the following **Corollary:**

$$L/K \text{ finite only INSEPARABLE if } \text{char}(K) = p > 0 \text{ is not perfect } \& p|[L : K] \quad \text{(Cor 2.4)}$$

Proposition 2.5 (transitivity of separability)

$$\begin{aligned} &L/M/K \text{ then following equivalent} \\ &1)\ L/K \text{ separable} \\ &2)\ L/M \,\&\, M/K \text{ separable} \end{aligned} \quad \text{(Prop 2.5)}$$

Lecture 3

$K \subseteq L, M$ then $\mathrm{Hom}_K(L, M) = \{\phi : L \to M$ field hom. s.t. $\phi|_K = \mathrm{id}_K\}$

Properties of separability

L/K is normal field extension iff $\forall \alpha \in L$ the $\mathrm{minpol}_K(\alpha)$ splits completly over L
L/K is SEPARABLE FIELD EXTENSION iff $\forall \alpha \in L$, the $\mathrm{minpol}_K(\alpha)$ does not have multiple roots in a splitting field of f.

Example L/K is separable if $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p > 0$ and K is perfect,i.e. $K = K^p = \{a^p | a \in K\}$

Note that this is not an iff statement. As in $\mathbb{F}_{p^n}(t)/\mathbb{F}_p(t)$ of degree n, is separable, while $\mathbb{F}_p(t)$ is not perfect.

Lemma 3.1:

$K(\alpha)/K$ finite simple (gen. by 1 element) field extension, M/K some extension
1natural bijection $\mathrm{Hom}_K(L(\alpha), M) \tilde{\to} \{$roots of f in $M\}$ with $f = \mathrm{minpol}_K(\alpha)$
$\tilde{\to}$ is canonical hom. with $\mathrm{Hom}_K(K(\alpha), M) \ni \varphi \mapsto \varphi(a)$
2$\#\mathrm{Hom}_K(K(\alpha), M) \leq \deg(f) = [K(\alpha) : K] < \infty$
3 f separable, splits over $M \Rightarrow \#\mathrm{Hom}_K(K(\alpha), M) = [K(\alpha) : K]$ (Lem 3.1)

Proof of 1:

$$\begin{array}{ccccc} \mathrm{Hom}_K(K(\alpha), M) & \tilde{\to} & \mathrm{Hom}_K(K[x]/f, M) & \tilde{\to} & \{g : \mathrm{Hom}_K(K[x], M) | g(f) = 0\} \\ \downarrow\sim & & & & \\ K[x]/(f) & & & & \end{array}$$

Therefore $\beta \in M | f(\beta) = 0$, so $f \subseteq \ker(g) \Leftrightarrow x \mapsto$ root of f in M.
2,3 direct consequence of 1.

Proposition 3.2:

$$
\begin{aligned}
&L/K \text{ finite}, M/K \text{ some field extension.}\\
&1)\ \#\mathrm{Hom}_K(L,M) \leq [L:K] < \infty\\
&2)\ L/K \text{ inseparable then } \#\mathrm{Hom}_K(L,M) < [L:K]\\
&3)\ L/K \text{ separable } \Rightarrow \exists M \text{ s.t. } \#\mathrm{Hom}_K(L,M) = [L:K]\\
&\text{so } M \text{ separates roots of minpols of } \alpha \in L
\end{aligned} \quad \text{(Prop 3.2)}
$$

Proof:

1. Induction on $[L:K]$. Base case: $L = K$ then okay. Let $\alpha \in L \setminus K$. By Lemma $\#\mathrm{Hom}_K(K(\alpha), M) \leq [K(\alpha):K]$. By induction every $\sigma : K(\alpha) \hookrightarrow M$ has at most $[L:K(\alpha)]$ extensions to $L \hookrightarrow K$.
   Therefore $\#\mathrm{Hon}_K(L,M) \leq [L:K(\alpha)][K(\alpha):K] = [L:K]$.

2. Take $\alpha \in L$ inseparable over K. By Lemma, we see then
   $\#\mathrm{Hom}_K(K(\alpha), M) < [K(\alpha):K]$.Hence from 1, we see that
   $\#\mathrm{Hom}_K(L,M) < [K(\alpha):K][L:K(\alpha)] = [L:K]$.

3. $L = K(\alpha_1, \ldots, \alpha_n)$ and let $f_i := \mathrm{minpol}_K(\alpha_i)$, separable over K.
   Let M' split all f_i. Claim this M works (i.e. $M = M'$).
   Proof by induction. By Lemma we see for $n = 1$, we have f_1 which splits over M, so $\#\mathrm{Hom}_K(K(\alpha_1), M) = [K(\alpha_1):K]$.
   $\forall \sigma : K(\alpha_1) \hookrightarrow M$ count number of extensions. $\tilde{\sigma} : L \hookrightarrow M$. Claim: Exactly $[L : K(\alpha_1)]$ extensions. Extension means commutative diagram. So if $iota$: $K(\alpha_1) \to L, \sigma : K(\alpha_1) \to M$ and $\tilde{\sigma} : L \to M$ then $\sigma = \tilde{\sigma} \circ \iota$.
   Need to verify htat $g_i := \mathrm{minpol}_{K(\alpha_1)}(\alpha_i)_{i \geq 2}$ splits under σ in M in order to apply the induction hypothesis. $g_i | f_i \in K[X]$ then $\sigma(g_i) | \sigma(f_i) = f_i \in K[X]$.
   f_i splits over M hence also $\sigma(g_i)$. I.e.., the induction hypothesis is satisfied, so $M = M'$. Therefore $\#\mathrm{hom}_K(L,M) \geq [L:K(\alpha)] \cdot [K(\alpha):K] = [L:K]$. Since we already had $\#\mathrm{Hom}_K(L,M) \leq [L:K]$ we see that $\#\mathrm{Hom}_K(L,M) = [L:K]$.

Theorem 3.3:

$$L/K \text{ finite so } L = K(\alpha_1, \ldots, \alpha_n) \text{ if } \alpha_i \text{ separable over } K \Rightarrow L/K \text{ separable} \quad \text{(Thm 3.3)}$$

Proof:
From (Prop 3.2).3 we see that $\exists M/K$ s.t. $\#\mathrm{Hom}_K(L,M) = [L:K]$
,therefore by (Prop 3.2).2 L/K is separable.

Corollary:
A splitting field of a separable polynomial f is separable.
Proof:
α_i root of f, and $f_i := \text{minpol}_K(\alpha_i)|f$. Then since f sep., we see that f_i sep.
So by (Thm 3.3) L/K sep.

L/K finite is GALOIS iff $/K$ is normal and sep. (Note that this is also Bianchi 5.10)
We can define it for alg. field extensions.

Proposition 3.4 (Bianchi 5.4):

$$L/K \text{ finite then following equivalent}$$
$$1) L/K \text{ Galois}$$
$$2) L \text{ splitting field of sep polynomial over } K \qquad \text{(Prop 3.4/Bianchi 5.4)}$$

Proof:

$1 \Rightarrow 2$ Normality criterion $\Rightarrow L = \text{Spl}_K(f), f \in K[x]$. Now assume $f = \prod_{i=1}^{n} f_i$ where f_i irreducible and square free factorization. $L = \text{spl}_K(f)$ so split over l,, so f_i have root in L. Since sep. we see f_i have only simple roots, we see that since $f = \prod_{i=1}^{n} f_i$ is sep.

$2 \Rightarrow 1$ $L = \text{Spl}_k(f) \Rightarrow L/K$ is normal by normal criterion.
By Corollary above, we see that since $L = \text{spl}_K(f)$ we have sep.

Lemma 3.5:

$$L/K \text{ algebraic field extension} \Rightarrow \text{Hom}_K(L,L) = \text{Aut}_K(L) \qquad \text{(Lem 3.5)}$$

Proof:
Every field hom. is injective. So only have to show that $\text{Hom}_K(L,L)$ is surjective.
$[L:K] < \infty$ we see that it is already clear since tehn surjective automatically follows.
So we just need to reduce to finite extensions.
Let $\phi \in \text{Hom}_K(L,L)$. Let $\alpha \in L$. Then since L/K is algebraic, $\exists 0 \neq f \in L[x] : f(\alpha) = 0$.
Then $V_L(f) = \{\beta \in L | f(\beta) = 0\}$ which is the vanishing set of f in L. We see that this set is finite.
Claim:$\phi(V_L(f)) \subseteq V_L(f)$.
$\phi : V_L(f) \to V_L(f)$ is injective because ϕ is $VL(f)$ finite, so therefore $\phi : V_L(f) \xrightarrow{\sim} V_L(f)$. Therefore $\forall \alpha : \phi : L \to L$ surjective so automorphism.
Let $f = \sum_{i=0}^{n} a_i x^i$ then $\phi(f(\beta)) = g\left(\sum_{i=0}^{n} \alpha_i \beta^i\right) = \sum_{i=0}^{n} \phi(\alpha_i)\phi(\beta)^i$. Since $\phi|_K = \text{id}_K$ we see that $\phi(f(\beta)) = \sum_{i=0}^{n} \alpha_i \phi(\beta)^i$ so $\phi(\beta_\epsilon V_L(f)$.

Lecture 4

$V_L(f) = \{\beta \in L | f(\beta) = 0\}$.
Note:
Any M/K s.t. $\forall \alpha \in L : \text{minpol}_K(\alpha)$ splits without multiple factors, satisfies $\#\text{Hom}_K(L, M) = [L : K]$.
We see that in the lecture Lemma 4.1, is in fact (Lem 3.5)

Properties Galois extensions

Proposition 4.2 (Bianchi 5.8)

$$L/K \text{ finite then following equivalent}$$
$$1)\ L/K \text{ Galois}$$
$$2)\ \#\text{Gal}(L/K) = \#\text{Aut}_K(L) = [L : K] \qquad \text{(Prop 4.2/Bianchi 5.8)}$$

Proof:

$1 \Rightarrow 2$ note that $[L : K] \overset{\text{prop 1 L3}}{=} \#\text{Hom}_K(L, L) \overset{L4.1}{=} \#\text{Aut}_K(L)$.

$2 \Rightarrow 1$ TBS:$\forall \alpha \in L$ we must have $f = \text{minpol}_K(\alpha)$ splits without multiple factors over $L \Leftrightarrow \#V_L(f) = \deg(f) = [K(\alpha) : K]$. Note that $\#V_L(f) \cong \#\text{Hom}_L(K(\alpha), L)$. Take arbitrary $\sigma \in \text{Hom}_L(K(\alpha), L)$. Then σ extends to at most $[L : K(\alpha)]$ exntesions to L. $\#\text{Hom}_K(L, L) = \#\text{Aut}_K(L) = [L : K]$.
Note that $\#\text{Hom}_K(L, L) = \#V_L(f)[L : K(\alpha)] \leq \deg(f) \cdot [L : K(\alpha)] = [K(\alpha) : K][L : K(\alpha)] \leq [L : K]$.
Since $[L : K] = [L : K]$ we get that $\#V_L(f) = \deg(f) = [K(\alpha) : K]$ which implies that $\forall \alpha \in L, \text{minpol}_K(\alpha)$ splits into linear terms without multiplicity in L.

For L/K galois,Galois group $\text{Gal}(L, K) = \text{Aut}_K(L)$ with composition as group low. So $\text{Gal}(L, K) = \{\sigma : L \to L | \sigma|_K = \text{id}_K\}$ since extension is finite, we see that group is finite, and $\#\text{Gal}(L/K) = [L : K]$

Galois group of separable polynomial, is the galois group of a splitting field.
If 2 field extensions $L/L, L'/K$ with $\phi : L \to L'$ isomorphic, then $\phi_* \text{Gal}(L/K) \xrightarrow{\sim} \text{Gal}(L'/K)$
We see that $g_*(\sigma) : L' \xrightarrow{\phi^{-1},\sim} L \xrightarrow{\sigma,\sim} L \xrightarrow{\phi,\sim} L'$ so $L' \to L'$ is isomorphic.

Lemma 4.3 (Bianchi 5.5):

$$L/K \text{ finite Galois ext.}, K \subset F \subset L \text{ interm. field ext.} \Rightarrow L/F \text{ Galois} \qquad \text{(Lem 4.3/Bianchi 5.5)}$$

Do not really understand what happens in next section:
L/K arbitrary field extensions, then $\mathrm{Aut}_K(L) = \{\sigma : L \xrightarrow{\sim} L \text{ s.t. } \sigma|_K = \mathrm{id}_K\}$
If we have $L/M/K$ then $\mathrm{Aut}(L) = \sigma|_M = \mathrm{id}|_M \implies \sigma|_K = \mathrm{id}_K$.
$\mathrm{Aut}_M(L) \leq \mathrm{Aut}_K(L)$

- Therefore well-defined map $\{M | L \supseteq M \supseteq K\} \to \{\text{subgroups of } \mathrm{Aut}_K(L)\}$ s..t. $M \mapsto \mathrm{Aut}_M(L)$.
- If $M' \subseteq M$ then $\mathrm{Aut}_M(L) \leq \mathrm{Aut}_{M'}(L)$
  Note that this map is bijective if L/K finite Galois with inverse function:
  $H \leq \mathrm{Gal}(L/K) \mapsto L^H = \{\alpha \in L | \sigma(\alpha) = \alpha, \forall \sigma \in H\}$.
- $M = L$ then $\mathrm{Aut}_L(L) = \{\mathrm{id}_L\}$.
- $M = K$ then $\mathrm{Aut}_K(L)$ is full group.

We want that $L^{\mathrm{Aut}_K(L)} = K$. We need to use L/K Galois, because otherwise it is false.

If $L = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal, $\mathrm{Aut}_{\mathbb{Q}(L)} = \{\sigma : L \xrightarrow{\sim} L | \sigma|_L = \mathrm{id}_L\}$ therefore we see that $\sigma(\sqrt[3]{2}) = \zeta_3^i \sqrt[3]{2}$. Note that since $\sigma(\sqrt[3]{2}) \in L \subseteq \mathbb{R}$ we see that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Therefore σ fixes a generator $\sqrt[3]{2}$ of L therefore $\sigma = \mathrm{id}_L$ therefore $\mathrm{Aut}_{\mathbb{Q}}(L) = \{\mathrm{id}\}$ therefore $L^{\mathrm{Aut}_{\mathbb{Q}}(L)} = L^{\mathrm{id}} = L \supsetneq \ldots$
If $L = \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ then $\sigma(\sqrt{2}) = \sigma(\sqrt[4]{2}^2) = \sigma(\sqrt[4]{2})^2 = (\pm\sqrt[4]{2})^2 = \sqrt{2}$ therefore we see ...
L/K not separabe so $L = \mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t) = K$, where $L = \mathrm{Spl}_K(X^p - t)$ with $\sigma \in \mathrm{Aut}_K(L)$ maps roots of $X^p - t$ to roots. There is exactly one root $X^p - t = (X - t^{1/p})^p$. Therefore $\mathrm{Aut}_K(L) = \{\mathrm{id}_L\} \Rightarrow L^{\mathrm{Aut}_K(L)} = L \supsetneq K$. **Corollary 4.4 (Bianchi 5.9):**

$$\begin{aligned} &L/K \text{ finite then following equivalent:} \\ &1)\ L/K \text{ Galois} \\ &20\ L^{\mathrm{Aut}_K(L)} = K \end{aligned} \tag{Cor 4.4/Bianchi 5.9}$$

Proof:

$1 \Rightarrow 2$ $\forall \alpha \in L, \forall \sigma \in \mathrm{Aut}_K(L), \sigma(\alpha) = \alpha$ therefore $\alpha \in K$.
Let $\alpha \in L^{\mathrm{Aut}_K(L)} \Rightarrow \mathrm{Aut}_K(L) \leq \mathrm{Aut}_{K(\alpha)}(L)$.
Since $K \subseteq K(\alpha)$ by the inclusion rev. We have $\mathrm{Aut}_{K(\alpha)}(L) \leq \mathrm{Aut}_K(L)$
so $\mathrm{Aut}_{K(\alpha)}(L) = \mathrm{Aut}_K(L)$
Therefore $[L : K(\alpha)] = \#\mathrm{Aut}_{K(\alpha)}(L) = \#\mathrm{Aut}_K(L) = [L : K]$.
Therefore $[K(\alpha) : K] = 1$ by tower law so $\alpha \in K$. Which is what we wanted to show.

$2 \Rightarrow 1$ $G = \mathrm{Aut}_K(L)$. Show $\forall \alpha \in L$, we have $f = \mathrm{minpol}_K(\alpha)$ splits into multiple factors in L.
Define $g := \prod_{\sigma \in G} (X - \sigma(\alpha)) \in L[X]$.
Claim: $g \in K[X]$ where $K = L^g$.
$\forall \tau \in G$ we have $\tau g = \prod_{\sigma \in G} (X - \tau\sigma(\alpha)) = \prod_{\sigma \in \tau G} (X - \sigma(\alpha)) = \prod_{\sigma \in G} (X - \sigma(\alpha)) = g$.
i.e.,τ permutes the roots of g, hence it fixes the coefficients, hence $g \in L^G[x] \overset{2}{=} K[X]$. If,$\sigma = \mathrm{id}$ we get $g(\alpha) = 0$. This is because one of the terms in the definition of g is equal to zero, so the whole product is equal to zero, so $g(\alpha) = 0$. So $g \in K[X]$ implies that $\mathrm{minpol}_K(\alpha) | g$ so f splits into linear factors in L hence L/K is Galois.

Lecture 5

L/K finite is galois $\Leftrightarrow$ normal+separable $\Leftrightarrow L = \mathrm{Spl}_K(f), f \in K[x]$ separable $\Leftrightarrow \#\mathrm{Aut}_K(L) = [L:K] \Leftrightarrow L^{\mathrm{Aut}_K(L)} = k$.
In this case: $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$.

Lemma 5.1 (Top II.2.2)

L/K finite field extension s.t. $\#\{M : L/M/K\} < \infty \Rightarrow L$ simple,i.e. $\exists \alpha \in L$ s.t. $L = K(\alpha)$ (Lem 5.1/Top II.2.2)

Proof:

Case 1 K finite $\overset{L/K}{\Rightarrow} L$ finite $\Rightarrow L^\times$ is cyclic (i.e. $L = \langle\alpha\rangle$)$\Rightarrow L = K(\alpha)$ simple.

Case 2 $L = K(\alpha_1, \dots, \alpha_n)$ since L/K finite.

Prove by induction that $K(\alpha, \alpha')$ simple.
If $n = 1$, we see that $L = K(\alpha_1)$ so already simple.
$\#\{K(\alpha + \lambda\alpha') | \lambda \in K\} < \infty$ since subfield of L/K. Where K infinite. So pigeon hole principle: $\exists \lambda \neq \lambda' \in K : K(\alpha + \lambda\alpha') = K(\alpha + \lambda'\alpha') =: M$. Therefore $\alpha + \lambda\alpha', \alpha + \lambda'\alpha' \in M \Rightarrow (\lambda - \lambda')\alpha \in M$. Since $\lambda \neq \lambda'$ we see that $\lambda - \lambda' \neq 0$ so $\alpha' \in M$. So then $\alpha = (\alpha + \lambda\alpha') - \lambda\alpha' \in M$.
Therefore $K(\alpha, \alpha') \supseteq M \ni \alpha, \alpha'$ hence $K(\alpha, \alpha') = M = K(\alpha + \lambda\alpha')$. Therefore base case holds).
For the induction step, assume that $K(\alpha_1, \dots, \alpha_{n-1}) = \hat{M}(\hat{\alpha})$. Therefore $K(\alpha_1, \dots, \alpha_n) = \hat{M}(\hat{\alpha}, \alpha_n) = M(\alpha)$. By using that we proved it for 2 elements.

Galois correspondence

Galois correspondence 5.2 (Bianchi 6.3):

L/K finite Galois has inclusion-reversion bijection:

$$\{M : L/M/K\} \underset{\beta: H \mapsto L^H}{\overset{\alpha: M \mapsto \mathrm{Gal}(L/M)}{\rightleftarrows}} \{H \leq \mathrm{Gal}(L/K)\}$$

α injective, βsurjective (Gal Cor 5.2/Bianchi 6.3)

Observation:
$\mathrm{Gal}(L/K)$ finite, therefore finitely many subgroups H, therefore $\{H \leq \mathrm{Gal}(L/K)\}$ finite.
SInce α injective, we see that $\{M : L/M/K\}$ is finite.

Proof:
We only have to prove that $\forall H \le \mathrm{Gal}(L/K)$ we have $\mathrm{Gal}(L/L^H) = H$.
By (Prop 4.2/Bianchi 5.8) $\#\mathrm{Gal}(L/K) = [L : K] < \infty$. Since α injective, L/K only fin. many subfields because the finite group $\mathrm{Gal}(L/K)$ has only finitely many subfields. Therefore by (Lem 5.1/Top II.2.2), $L = K(\alpha)$ is simple.
Trick $f := \prod_{\sigma\in H}(X - \sigma(\alpha)) \in L[X]$
$\forall \tau \in H : \tau f = f$ where $\tau f = \prod_{\sigma\in H}(X - \tau\sigma(\alpha)) = \prod_{\tilde{\sigma}\in\tau H}(X - \tilde{\sigma}(\alpha)) = f$ since H is a group.
Therefore coeffs of f are in L^H so $f \in L^H[X]$. Therefore $\#H = \deg(f) \ge [L : L^H]$ since $L = \mathrm{Spl}_{L^H}(f)$. Note that $[L : L^H] = \#\mathrm{Gal}(L/L^H)$ since L/L^H is Galois. So far therefore $\#H \ge \#\mathrm{Gal}(L/L^H)$.
But $H \le \mathrm{Gal}(L/L^H)$ because H fixes L^H by definition of L^H. SO $\#H \le \#\mathrm{Gal}(L/L^H)$. But we had $\#\mathrm{Gal}(L/L^H) \le \#H$ so $\#H = \#\mathrm{Gal}(L/L^H)$. We also have $H \le \mathrm{Gal}(L/L^H)$ but since cardinality of both groups are the same, we see that $H = \mathrm{Gal}(L/L^H)$.

Lemma 5.3 (Bianchi 6.4)

$$\sigma \in \mathrm{Gal}(L/K) \rightsquigarrow \sigma(M) := \{\sigma(\alpha) | \alpha \in M\} \subseteq L \text{ field}$$
$$\Rightarrow \mathrm{Gal}(L/\sigma(M)) = \sigma\mathrm{Gal}(L/M)\sigma^{-1} := \{\sigma\tau\sigma^{-1} | \tau \in \mathrm{Gal}(L/M)\} \quad \text{(Lem 5.3/Bianchi 6.4)}$$

Proof:
Let $\tau \in \mathrm{Gal}(L/K)$ then $\tau \in \mathrm{Gal}(L/\sigma(M))$
iff $\tau(\sigma(\alpha)) = \sigma(\alpha)$ for all $\sigma(\alpha) \in \sigma(M)$ so $\forall \alpha \in M$.
Iff $\sigma^{-1}\tau\sigma)(\alpha) = \alpha, \forall \alpha \in M$.
Iff $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/M)$ iff $\tau \in \sigma\mathrm{Gal}(L/M)\sigma^{-1}$.

Proposition 5.4

L/K finite Galois with $L/M/K$ then M/K is normal (so Galois) iff
$N := \mathrm{Gal}(L/M) \trianglelefteq \mathcal{G} := \mathrm{Gal}(L/K)$
then $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \xrightarrow{\sim} \mathrm{Gal}(M/K)$ s.t. $\sigma N \mapsto \sigma(M)$ well def. group isom.
(Prop 5.4)

Proof:
$N \trianglelefteq \mathcal{G}$ normal $\overset{\text{def}}{\Leftrightarrow} \sigma N\sigma^{-1} = N, \forall \sigma \in \mathcal{G}$. Iff, $\mathrm{Gal}(L/\sigma(M)) = \mathrm{Gal}(L/M), \forall \sigma \in \mathcal{G}$.
Iff $\sigma(M) = M$ by Gall. correspondence, iff $\sigma(M) \subseteq M$ since we have a homomorphism from $\sigma(M) \to M$ which is an automorphism (since finite field extension), therefore $\sigma(M) \subseteq M \Rightarrow M \subseteq \sigma(M)$, so $M = \sigma(M)$.

To show $\sigma(M) \subseteq M, \forall \sigma \in \mathcal{G}$ iff M/K normal:
$\Leftarrow$. Assume M/K normal. Let $\alpha \in M, \sigma \in \mathcal{G}, f := \text{minpol}_K(\alpha)$, then $f(\sigma(\alpha)) \overset{\sigma|_K = \text{id}_K}{=} \sigma(f(\alpha)) = \sigma(0) = 0$
Since M/K normal, f splits over M, so $\sigma(\alpha) \in M$.
$\Rightarrow$ Assume $\sigma(M) \subseteq M, \forall \sigma \in \mathcal{G}$. Let $\alpha \in M, g := \prod_{\sigma \in \mathcal{G}} (X - \sigma(\alpha))$. Since $\sigma(\alpha) \in M$, we see that $g \in M[X]$. Since $\tau g = g, \forall \tau \in \mathcal{G}$, we see that $g \in K[X]$ therefore $\text{minpol}_K(\alpha)|g$.
Since g splits over M, we see that $\text{minpol}_K(\alpha)$ splits over M. Hence M/K is normal.
So we only need to check the isomorphism. Define $\phi : \text{Gal}(L/K) \to \text{Gal}(M/K)$ with $\sigma \mapsto \sigma|_M$. Since M/K normal, we see well-defined homomorphism, becuase $\sigma(M) = M$. We see that $\ker(\phi) = \{\sigma \in \text{Gal}(L/K) | \sigma|_M = \text{id}_M\} = \text{Gal}(L/M)$. By using homomorphism theorem of groups, we see that $\text{Gal}(L/K)/\ker(\phi) \to \text{Gal}(M/K)$ is injective, so $\psi : \text{Gal}(L/K)/\text{Gal}(L/M) \to \text{Gal}(M/K)$ is injective.
To prove ψ is isomorphism, it is enough to prove that $\#(\text{Gal}(L/K)/\text{Gal}(L/M)) = \#\text{Gal}(M/K)$. Note that $[L : K][L : M] = [M : K]$ by tower law. so ψ indeed isomorphism. By Tower law, we see surjective, so therefore $\text{Gal}(L/K)/\text{Gal}(L/M) \to \text{Gal}(M/K)$ is indeed isomorphism.

Lemma 5.5:

$$L/K \text{ finite sep.} \Rightarrow \exists \tilde{L}/L \text{ s.t. } \tilde{L}/K \text{ finite Galois} \qquad \text{(Lem. 5.5)}$$

Proof:
L/K finite then $L(\alpha_1, \dots, \alpha_n 9$. $fi = \text{minpol}_K(\alpha_i)$ separable. WLOG, pairwise coprime. (otherwise delete multiple ones, since either equal or coprime (Note irreducibility since minimal polynomial).). $\tau = \text{Spl}_K(\prod f_i) \supseteq L$ separable, normal and finite.

Theorem 5.6 (Bianchi 6.5):

$$L/K \text{ fin. separable} \Rightarrow \exists \alpha \in L \text{ s.t. } L = K(\alpha) \text{ so simple} \qquad \text{(Thm 5.6/Bianchi 6.5)}$$

Proof:
By (Gal Cor 5.2/Bianchi 6.3) we see that it is sufficient to show that L/K has only finitely many subfields. By (Lem. 5.5) $\tilde{L}/L/K$ finite and Galois, therefore $\tilde{L}/L$ has finitely many subfields, so L/K has only finitely many subfields.

Example:
$\text{Char}(K) \neq 2$ therefore L/K quadratic has the form $L = K(\sqrt{a})$ with $a \in K \setminus K^{\square} = K \setminus \{b^2 | b \in K\}$. Note that $L = \text{Spl}_K(X^2 - a)$ normal and separable, since if $f = X^2 - a$, then $(f, f') = (X^2 - a, 2X) = 1$ for $X \neq 0$. Therefore $\#\text{Gal}(K(\sqrt{a})/K) = [K(\sqrt{a} : K] = 2$. Denote the zeros of a polynomial f over L by $V_L(f)$. Therefore we see that $\sigma(V_L(X^2 - a)) = V_L(X^2 - a) = \{\pm\sqrt{a}\}$.

Lecture 6

Lemma 6.1
Missing

Example 6.2 (6.6 Bainchi)
$L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Claim:$\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$.
Consider $L_1 := \mathbb{Q}(\sqrt{2}), L_2 := \mathbb{Q}(\sqrt{3})$.
Claim: $L_1 \neq L_2$. Otherwise $\text{Gal}(L_1/\mathbb{Q}) = \text{Gal}(L_2/\mathbb{Q}) = \{\text{id}_{L_2}, \sigma\}$.
So then $\sigma : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}$. Which would imply that $\sigma(\sqrt{2}\sqrt{3}) = \sqrt{2}\sqrt{3}$. So then $\sqrt{6} \in \mathbb{Q}$ whic h is a contradiction, so $L_1 \neq L_2$.
WE see that we have $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. If $\mathbb{Q}(\sqrt{2}, \sqrt{3}) := L = L_1 \cdot L_2$ then $[L : \mathbb{Q}] = 2 \cdot 2 = 4$. Therefore $\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ or $\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Note that $\mathbb{Z}/4\mathbb{Z}$ has exactly 1 subgroup, while $\text{Gal}(L/\mathbb{Q})$ has more then 1 so contradiction. Therefore $\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Note that $(\mathbb{Z}/2\mathbb{Z})^2$ has 3 proper subgroups: $\left\langle\begin{pmatrix}1\\0\end{pmatrix}\right\rangle, \left\langle\begin{pmatrix}0\\1\end{pmatrix}\right\rangle, \left\langle\begin{pmatrix}1\\1\end{pmatrix}\right\rangle$.
What is τ, σ If $L_3 = L^{\langle\sigma\tau\rangle}$ then $(\sigma\tau)(\sqrt{6}) = \sigma(\sqrt{3}(-\sqrt{3})) = \sqrt{6}$ so then $\sqrt{6} \in L_3$ so therefore $[L_3 : \mathbb{Q}] = 2$.

Example 6.3
$L := \text{Spl}_{\mathbb{Q}}(X^3 - 2)$. We see that $2 = [\mathbb{Q}(\zeta_3) : \mathbb{Q}]$ and $3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})]$. Both divide $[L : \mathbb{Q}]$. Note that $\text{Gal}(L/Q) \hookrightarrow S_3$ by Lemma 6.1, therefore $\#\text{Gal}(L/\mathbb{Q})|3! = 6$
Proper subgroups of S_3 are $\langle(1,2,3)\rangle = \{1, (1,2,3), (1,3,2)\}$ and $\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle$.
Those subgroups are not normal. Therefore $(\mathbb{Q}(\sqrt[3]{2}))/\mathbb{Q}, (\mathbb{Q}(\sqrt[3]{2})\zeta_3^2)/\mathbb{Q}, (\mathbb{Q}(\sqrt[3]{2})\zeta_3^2)/\mathbb{Q}$ are not normal.

Cyclotomic fields

Proposition 6.4/Bianchi 7.3

$$\text{Char}(K) \nmid n \Rightarrow X^n - 1 \in K[X] \text{ separable} \qquad \text{(Prop 6.4/Bianchi 7.3)}$$

Proof: $(X^n - 1)' = nX^{n-1} \neq 0$, where $(X^n - 1) \neq 0$ and $nX^{n-1} \neq 0$. Therefore $(X^n - 1, nX^{n-1}) = 1$ so $X^n - 1$ separable.

Assume $\text{char}(K) \nmid n$.
Definition 6.5
L field, $\mu_n(L) := \{\zeta_n L^\times | \zeta^n = 1\}$ group of $n-$ th roots of unity in L.
proposition 6.6/Top III.5.4

$$\mu_n(L) \text{ is finite cyclic} \qquad \text{(Prop 6.5/AS Top III.5.4)}$$

Example:
$L = \mathbb{C}$ then $\mu_n(\mathbb{C}) = \left\{ e^{\frac{2\pi i k}{n}} | 0 \leq k < n \right\}$.

Definition 6.6

$\zeta_n \in \mu_n(L)$ PRIMITIVE iff $\mathrm{ord}(\zeta_n) = n$ iff $\langle \zeta_n \rangle = \mu_n(L)$.
$K(\mu_n) := \mathrm{Spl}_K(X^n - 1)$. Note that $K(\mu_n) = K(\zeta_n)$ iff ζ_n is primitive.
Example:
$\zeta_n \in \mathbb{F}_q \Leftrightarrow \mathrm{ord}(\zeta_n) | (q-1) = \#\mathbb{F}_q^\times$

Property:
(ζ_n primitive then ζ_n^a primitive) iff $(a, n) = 1$.
Example:
$\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ since $\zeta_3^3 - 1 = 0$ but $\zeta_3 - 1 \neq 0$, therefore root of $\frac{x^3-1}{x-1} = x^2 + x + 1$. Roots are $\frac{-1 \pm \sqrt{1^2 - 4 \cdot 1}}{2} = \frac{-1 \pm \sqrt{-3}}{2}$.

Lemma 6.7/Bianchi 7.8

$$\zeta_n \text{ primitive n-th root of unity} L := K(\zeta_n), G := \mathrm{Gal}(L/K)$$
$$\Rightarrow \begin{cases} (1) & \sigma \in G \to \sigma(\zeta_n) = \zeta_n^a \text{ with } (a, n) = 1 \\ (2) & \forall \zeta \in \mu_n(L), \sigma(\zeta) = \zeta^a \end{cases} \quad \text{(Lemma 6.7/Bianchi 7.8)}$$

Proof: $\zeta \in G$ maps roots of $x^n - 1$ to roots, so $\sigma(\zeta_n) = \zeta_n^a$ for some $a \in \mathbb{Z}$ since $\langle \zeta_n \rangle = \mu_n(L)$.
$\sigma \in \mathrm{Aut}_K(L)$ therefore $\sigma|_{\mu_n(L)} \in \mathrm{Aut}(\mu_n(L))$ therefore σ maps generators of $\mu_n(L)$ to genarators of $\mu_n(L)$. Note that therefore $(a, n) = 1$.
Take $\zeta \in \mu_n(L)$ therefore $\zeta = \zeta_n^b$ with $b \in \mathbb{Z}$ so then $\sigma(\zeta) = \sigma(\zeta_n^b) = \sigma(\zeta_n)^b = (\zeta_n^a)^b = \zeta_n^{ab} = (\zeta_n^b)^a = \zeta^a$

THE MOD-N CYCLIOTOMIC CHARACTER OF K
$\chi_{K,n} : \mathrm{Gal}(K(\zeta_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ s.t. $\sigma \mapsto \chi_{K,n}(\sigma) := a_0 \cdot \sigma(\zeta_n) = \zeta_n^{a_0}$
N-TH CYCLOTOMIC POLYNOMIAL:
$\Phi_n := \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^a) \in K[X]$.

Proposition 6.8/Bianchi 7.9

$$\begin{cases} 1) \ \chi_{K,n} \text{ injective group homo. independent of choice of primitive nth root } \zeta_n \\ 2) \ \Phi_n \text{ is irreducible } \Leftrightarrow \chi_{K,n} \text{ surjective} \end{cases} \quad \text{(Prop 6.8/Bianchi 7.9)}$$

Proof:

1) (Lemma 6.7/Bianchi 7.8) implies $\chi_{K,n}$ well defined and independent of ζ_n. $\chi_{K,n}$ homomorphism with $\sigma, \tau \in \mathrm{Gal}(K(\zeta_n), K)$ s.t.$(\sigma\tau)(\zeta_n) = \zeta_n^{\chi_{K,n}(\sigma\tau)}$
Note that $(\sigma\tau)(\zeta_n) = \sigma(\zeta_n^{\chi_{K,n}(\tau)}) = \sigma(\zeta_n)^{\chi_{K,n}(\tau)} = (\zeta_n^{\chi_{K,n}(\sigma)})^{\chi_{K,n}(\tau)} = \zeta_n^{\chi_{K,n}(\sigma)\cdot\chi_{K,n}(\tau)}$. So in $(\mathbb{Z}/n\mathbb{Z})^\times$ we see that $\zeta_n^{\chi_{K,n}(\sigma\tau)} = \zeta_n^{\chi_{K,n}(\sigma)\chi_{K,n}(\tau)}$.
$\chi_{K,n}$ injective, so $\zeta_{K,n}(\sigma)1$ implies $\zeta_n^{\chi_{K,n}(\sigma)} = \sigma(\zeta_n)$. Therefore σ fixes ζ_n. Now use that $\langle\zeta_n\rangle = \mu_n(L)$ so σ fixes L hence $\sigma = \mathrm{id}_L$.
2) $\mathrm{minpol}_K(\zeta_n)|\Phi_n$ because $\Phi_n(\zeta_n) = 0$. Therefore $\#(\mathbb{Z}/n\mathbb{Z})^\times = \deg(\Phi_n) \geq \deg(\mathrm{minpol}_K(\zeta_n)) = [K(\zeta_n) : K] = \#\mathrm{Gal}(K(\zeta_n)/K)$.
Therefore equality iff Φ_n irreducible, so $\#\mathrm{Gal}(K(\zeta_n)/K) = \#(\mathbb{Z}/n\mathbb{Z})^\times$. Since $\chi_{K,n}$ is injective, this implies surjectiveness.

Theorem 6.9/Bianchi 7.12

$$\Phi_n \in \mathbb{Z}[X] \text{ monic and irreducible} \qquad \text{(thm 6.9/Bianchi 7.12)}$$

Proof:
$\Phi_n|X^n - 1 \in \mathbb{Z}[X]$,by Gauss lemma, we see that Φ_n monic in $\mathbb{Z}[X]$.
$f := \mathrm{minpol}_{\mathbb{Q}}(\zeta_n)$. Since ζ_n primitive,n th root of unity, we see that $X^n - 1 = f \cdot h$ where $h \in \mathbb{Z}[X]$ monic.
If for $p \not| n$ prime, we see that $f(\zeta_n^p) \neq 9$. Note that $0 = (\zeta_n^p)^n - 1 = f(\zeta_n^p)\cdot h(\zeta_n^p)$. So ζ_n is a root of $h(x^p)$. Therefore $f|h(x^p)$ so $h(x^p) = f \cdot g$.
$f, g \in \mathbb{Z}[x]$ monic by gauss. Can reduce coefficients mod p to get $\overline{h(x^p)} = \overline{fg} = \overline{f}\overline{g}$. So $(\overline{h})^p = \overline{h(x^p)}$, by Frobini. Therefore $(\overline{h}, \overline{f}) \neq 1$. So $\overline{X^n - 1}$ has multiple roots so $(\overline{X^n - 1}', X^n - 1) \neq 1$. But we see that this is equal to $(nX^{n-1}, X^n - 1)$ which is nonzero, since $p \not| n$ so therefore $(nX^{n-1}, X^n - 1) = 1$. So contradiction.
$\forall p \not| n, f(\zeta_n^p) = 0$ any root of Φ_n is ζ_n^a. Since $(a, n) = 1$. Write $a = \prod_{i=1}^{k} p_i^{k_i}$. By repeating $f(\zeta_n^p) = 0$, we get for those p_i that $f(\zeta_n^a) = 0$.
Note:
$\mathrm{Frob}_p : (\mathbb{Z}/p\mathbb{Z})[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$ is a ring hom. So Frob_p acts trivially on the coefficients in $\mathbb{Z}/p\mathbb{Z}$

Lecture 7

If $\text{char}(K) \not| \, n$, then

$$\chi_{K,n} : \text{Gal}(K(\zeta_n)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \,\text{s.t.}\, \sigma \mapsto (a_\sigma : \sigma(\zeta_n) = \zeta_n^{a_\sigma})$$

Is abelian extension.
χ surjective iff $\Phi_n = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \xi_n^a)$ is irreducible in $K[X]$.
Holds if $K = \mathbb{Q}$ so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Kronecker-Weber Theorem:
$K/\mathbb{Q}$ abelian $\Rightarrow \exists n \geq 1 : \mathbb{Q}(\zeta_n) \supseteq K \supseteq \mathbb{Q}$.(arithmetic statement)

Extensions of $\mathbb{F}_q$

Theorem 7.1/AS IX

$$\forall n \geq 1, \exists!\, \text{extension}\, \mathbb{F}_{q^n}/\mathbb{F}_q \,\text{of degree}\, n \,\text{up to isomorphisms,}\, \mathbb{F}_{q^n} = \text{Spl}_{\mathbb{F}_q}(X^{q^n} - X) \quad \text{(thm 7.1.1./AS IX.1.1)}$$

And

$$\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \langle \text{Frob}_q \rangle \cong \mathbb{Z}/n\mathbb{Z} \,\text{with}\, \text{Frob}_q : x \mapsto x^q \,\text{is cyclic} \quad \text{(thm 7.1.2/AS IX.1.1)}$$

Proof:
1) [AS IX.1.1]
2) $\text{Frob}_q \in \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ because $x^{q^n} = x$ for all $x \in \mathbb{F}_{q^n}$ with $\text{ord}(\text{Frob})|n$.
$1 \leq k < n \Rightarrow \text{Frob}_q^k$ s.t. $x \mapsto x^{q^k}$. If $\text{frob}_q^k = \text{id}_{\mathbb{F}_{q^n}}$ so $x^{q^k} - x = 0$ for all $q \in \mathbb{F}_{q^n}$ and we see we have $<$ for degrees, there we use $k < n$.

Cyclic extensions

Lemma 7.2 (lin. independence of characters)

$$L \,\text{field}, G \,\text{group}, \sigma_i : G \to L \,\text{pairwise dist. homo.}$$
$$\Rightarrow \sigma_i \,\text{lin. independent} \left(\text{i.e.} \sum_{i=1}^n \lambda_i \sigma_i = 0 \Rightarrow L \ni \lambda_i = 0\right) \quad \text{(Lemma 7.2)}$$

Ass. minimal relation, i.e.,$\lambda_i \neq 0, \forall i$. Then since σ_i pairwise distinct, exisets $g \in G$: $\sigma_1(g) \neq \sigma_2(g)$. Then $\forall h \in G$ we get

$$\sum_i \sigma_i(gh) = \sum_i \lambda_i \sigma_i(g)\sigma_i(h) = 0$$
$$\sigma_1(g)\sum_{i=1}^{n} \lambda_i\sigma_i - \sum_{i=1}^{n} \lambda_i\sigma_i(g)\sigma_i(h) = 0$$
$$\sum_i \lambda_i(\sigma_1(g) - \sigma_i(g))\sigma_i(h) = 0, \forall h \in G$$

Note that $\sigma_1(g) - \sigma_i(g) = 0$ if $i = 1$ and $\sigma_1(g) - \sigma_i(g) \neq 0$ if $i \neq$. This means that $\sum_{i=1}^{n} \lambda_i\sigma_i$ is not minimal, which is a contradiction. So there is not a minimal relation

Theorem 7.3/ (Bianchi 7.18)(classification of cyclic extensions)

$$\begin{aligned} &\mathrm{char}(K) \not| \, n, \zeta_n \in K^\times \\ &1)\, c \in K^\times/(K^\times)^n \Rightarrow K(\sqrt[n]{c})/K \text{ is cyclic of order } n \\ &2)\, \mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z} \Rightarrow \exists c \in K^\times \text{ s.t. } L = K(\sqrt[n]{c}) \end{aligned} \qquad \text{(Thm 7.3,Bianchi 7.18)}$$

Proof:

1) $x^n - c = \prod_{i=1}^{n}(X - \zeta_n^{i-1}\sqrt[n]{c}) \in K(\sqrt[n]{c})$. Splits over $K(\sqrt[n]{c})$ since $\zeta_n \in K$.
Hence $K(\sqrt[n]{c})/K = \mathrm{Spl}_K(X^n - c)$ is normal. Since $\zeta_n^{i-1}\sqrt[n]{c})$ are not roots for $(X^n - c)'$ we see that the roots $\zeta_n^{i-1}\sqrt[n]{c}$ are distinct (for $i = 1, \dots, n$). Therefore we see that $K(\sqrt[n]{c})/K$ is separable, so Galois.
$\sigma \in G := \mathrm{Gal}(K(\sqrt[n]{\zeta})/K)$, we see that sigma maps roots to roots. So $\sigma(\sqrt[n]{c}) = \zeta_n^{a_\sigma}\sqrt[n]{c} = \kappa(\sigma)\sqrt[n]{c}$, so we see that we get $\kappa : G \to \mu_n(K) \cong (\mathbb{Z}/n\mathbb{Z})/\sigma(\sqrt[n]{c})$.
First prove κ is a homomorphism.

- $(\sigma\tau)(\sqrt[n]{c}) = \sigma(\tau(\sqrt[n]{\sigma})) = \sigma(\zeta_n^{a_\tau}\sqrt[n]{c}) = \zeta_n^{a_{[}\tau}\sigma(\sqrt[n]{c}) = \zeta_n^{a_\tau}\zeta_n^{a_\sigma}\sqrt[n]{c} = \zeta_n^{a_\sigma + a_\tau}(\sqrt[n]{c})$
  κ injective, then $\kappa(\sigma) = 1$,so σ fixes $\sqrt[n]{c}$ generates $\kappa(\sqrt[n]{c})$ so $\sigma = \mathrm{id}$
  κ is surjective if $\kappa^d(\sigma) = 1, \forall \sigma \in G$, then $(\zeta_n^{a_\sigma})^d\sqrt[n]{c}^d = \sigma(\sqrt[n]{c})^d = \sqrt[n]{c}^d$. Since $\mathrm{ord}(\sqrt[n]{c}) = n$ we get $n|d$.

2) $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z} \cong \langle\sigma\rangle = \{1, \sigma, \dots, \sigma^{n-1}\} \overset{\text{(Lemma 7.2)}}{\Rightarrow} \exists \alpha : \sum_{i=0}^{n-1} \sigma_n^{-i} \cdot \sigma^i(\alpha) \neq 0$ plays the role of $\sqrt[n]{c}$.
$\sigma(b) = \sum_{i=0}^{n-1} \zeta - n^{-i}\sigma^{i+1}(\alpha) \overset{\text{ind. shift}}{=} \zeta_n \sum_{i=0}^{n-1} \zeta^{-(i+1)}\sigma^{i+1}(\alpha) = \zeta_n \cdot b$.
Therefore $\sigma(b^n) = \sigma(b)^n = (\zeta_n b)^n = b^n$. Here $b := \sum_{i=0}^{n-1} \zeta^{-(i+1)}\sigma^{i+1}(\alpha)$.

So $\sigma(b) = \zeta_n b \neq b$ therefore $\sigma^i(b) = b$ iff $n|$ so $\text{Gal}(L/K(b)) = \{\text{id}\}$ so $L = K(b)/K$ cyclic of order n.

Symmetric polynomials

K field, $n \geq 1, K(X_1, \ldots, X_n)$ function field in n variables, which is $\text{Frac}(K[X_1, \ldots, X_n])$.
$K(\underline{x}) \ni f_n(z) = (z - x_1)(z - x_2)\ldots(z - x_n)$ with,$\deg(f_n) = n$. Here $(\underline{x}) = (x_1, \ldots, x_n)$.
And $f_n(z) = z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} \pm \ldots + (-1)^n \sigma_n$.
$\sigma_i(x_1, \ldots, x_n)$ are i th elementary SYMMETRIC POLYNOMIALS in n variables. Are invariant under permuting x_i i.e. $x_i \mapsto x_{\tau(i)}$ where $\tau \in S_n$.
$\sigma_1 = x_1 + x_2 + \ldots + x_n, \sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n$ and $\sigma_n = x_1 \cdot x_n$ where σ_i has $\binom{n}{i}$ summands
$M := K(\sigma_1, \ldots, \sigma_n) \leq K(\underline{x})^{S_n} \subseteq K(\underline{x})$.
We show now that we have $K(\underline{x})^{S_n} = K(\underline{x})$
Note that $K(\underline{x}) = \text{Spl}_M(f_n)$ therefore we get $[K(\underline{x}) : M] \leq \deg(f_n)! = n!$ we see that $\text{Gal}(K(\underline{x})/M) \hookrightarrow S_n$.
We want to show also surjective.
$\forall \tau \in S_n, (x_i \mapsto x_{\tau(i)}) \in \text{Gal}(K(\underline{x}/M)$ because it fixes σ_j. Therefore $\#\text{Gal}(K(\underline{x})/M) \geq \#S_n = n!$. So $\text{Gal}(K(\underline{x})/M) = n!$, therefore $\text{Gal}(K(\underline{x})/M) \xrightarrow{\sim} S_n$.

Example:
$n = 2, f_2 = (Z - x_1)(Z - x_2) = Z^2 - (X_1 + X_2)Z + X_1X_2 = z^2 - \sigma_1 Z + \sigma_2$.
We see that $\zeta_2 = -1$ which is not equal to 1 if $\text{Char}(K) \not| 2$.
$[K(X_1, X_2) : K(\sigma_1, \sigma_2)] = \#S_2 = 2! = 2$. Let $b := \sum \zeta_2^{-i} X_i = X_1 - X_2$, so—,$b^2 = (X_1 - X_2)^2$. So $\sigma : X_1 \mapsto X_2, X_2 \mapsto X - 1$, then $\sigma(b^2) = (X_2 - X_1)^2 = (X_1 - X_2)^2 = b$.
Note that $b^2 = X_1^2 - 2X_1X_2 + X_2^2$. So $b \in K(X_1, X_2)^{S_2} = K(\sigma_1, \sigma_2)$.
Note that $b^2 - (X_1 + X_2)^2 = b^2 - \sigma_1^2 = -4X_1X_2 = -4\sigma_2$. Therefore $b^2 = \sigma_1^2 - 4\sigma_2$.
So $K(X_1, X_2) = K(\sigma_1, \sigma_2)[\sqrt{\sigma_1^2 - 4\sigma_2}]$, note that $\sigma_1^2 - 4\sigma_2$ is the discriminant of f_2, so $K(x_1, x_2) = K(\sigma_1, \sigma_2)[\sqrt{D(f_2)}]$.
$b = X_1 - X_2, \sigma_1 = X_1 + X_2$ so $X_1 = \frac{1}{2}(b + \sigma_1) = \frac{1}{2}\left(\sqrt{\sigma_1^2 - 4\sigma_2} + 1\right)$ and
$X_2 = \frac{1}{2}(\sigma_1 - b) = \frac{1}{2}\left(\sigma_1 - \sqrt{\sigma_1^2 - 4\sigma_2}\right)$

Lecture 8

Missed first part, first page on brightspace not readable.

L/K finite separable field extension is SOLVABLE iff $\text{Gal}(\tilde{L}/K)$ is solvable with $\tilde{L}/K$ Galois closure of L/K.

Solvable in radicals iff $\exists L = L_n \supseteq L_{n-1} \supseteq \ldots \supseteq L_0 = K$, where $L_{i+1} = L_i(\alpha_i)$ where α_i root of $x^{n_i} - c_i \in L_i[x]$.
(So it is just a field extension by adjoining an extra root for some polynomial in the field before.

For $\text{char}(K) = p?0$ of $x^p - x - c_i \in L_i[x]$ if $[L_{i+1} : L_i] = p = \text{char}(K) > 0$.

Lemma (perminance properties):
If M_1/K is solvable, so is $(M_1M_2)/M_2$.

Transitivity $L/M/K$: L/K is solvable iff L/M and M/K is solvable.
Therefore if M_1/K solvable and M_2/K solvable, then M_1M_2/K solvable.

Main theorem:
L/K finite separable, then equivalent:

1. L/K solvable
2. L/K solvable in radicals.

Proof:
Assume for simplicity $\text{char}(K) \nmid [\tilde{L} : K]$.

$2 \Rightarrow 1$ $L = L_n \supseteq \ldots \supseteq L_0 = K$.
$L_{i+1} = L_i(\alpha_i)$ where α_i root of $x^{n_i} - c_i \subseteq L_i[X]$.
$\tilde{L}_i$ galois closure of L_i/K. By induction assume $\tilde{L}_i/K$ is solvable.
Show $\tilde{L}_{i+1}/K$ is solvable, by permanance it sufficies $\tilde{L}_{i+1}/\tilde{L}_i$ solvable.
$\tilde{L}_{i+1} = \tilde{L}_i(\sqrt[n]{c_i}, \zeta_n) = \text{Spl}_{\tilde{L}_i}(x^{n_i} - c_i)$
$\tilde{L}_i(\zeta_{n_i})$ is cyclic, therefore abelian in $(\mathbb{Z}/n_i\mathbb{Z})^\times$. By permanance properties for solvable groups we get $\text{Gal}(\tilde{L}_{i+1}/\tilde{L}_i)$ is abelian in $(\mathbb{Z}/n\mathbb{Z})^\times$, therefore solvable. Also that for any subfield.

$1 \Rightarrow 2$ $G = \text{Gal}(\tilde{L}/K)$ solvable, where $G = G_n$, and $G_i \rhd G_{i-1}$ cyclic for $i \in \{2, \ldots, n\}$.
By permanence properties: transitivity of being solvable in radicles, implies that it is sufficient to prove L/K cyclic where $p \nmid [L : K] =: n$. Therefore L/K solvable

in radicals.
L/K cyclic, then $L(\mu_n)/(K(\mu_n)/K)$ is cyclic. We see that $K(\mu_n)/L$ is solvable.
We see that $L(\mu_n) = L(\mu_n, \sqrt[d]{c})$ for some $d|n$, by lecture 7.
We see that $L(\mu_n)/K$ solvable in radicals by transitivity, but we see that $K \subseteq L \subseteq L(\mu_n)$ hence K/L is also solvable in radicals (permanence)

Corollary:
$n \geq 4$, the general equation $f_n \in K(x_1, \ldots, x_n)[z]$ is not solvable in radicals.
Proof:
$\text{Gal}(f_n) \cong S_n$ is solvable iff $n \leq 4$. So f_n only solvable if $n \leq 4$.

Only for general equations, specific fields are solvable.

Galois group of polynomials

Lemma:
$f \in K[X]$ irreducible, then $G : \text{Gal}(f) \leq S_n$ is transitive.
(So $\forall 1 \leq i, j \leq n, \exists \sigma \in G$ s.t. $\sigma(i) = j$)

Lemma:
p prime, $G \leq S_p$ is transitive $\Rightarrow \exists$ p-cycle in G.
If furthermore, G contains transposition (so $\sigma(i) = j, \sigma(j) = i) \Rightarrow G = S_p$.

Theorem Dedekind:
$f \in \mathbb{Z}pX]$ monic and irreducible,p prime s.t. the reduction $\overline{f} \in (\mathbb{Z}/p\mathbb{Z})[X]$ has no multiple factors, say $\overline{f} = \overline{f}_1 \cdot \overline{f}_n$ then $G_f := \text{Gal}(f)$ contains permutation of type
$(\deg(\overline{f}_1), \deg(\overline{f}_2), \ldots, \deg(\overline{f}_n))$
So first permutation is of length $\deg(\overline{f}_1)$ the second permutation of length $\deg(\overline{f}_2)$ and so on.

Example:
$X^5 - X - 1 \in \mathbb{Z}[X]$ is monic. We see that $\overline{f} \mod 5$ is irreducible. Therefore irreducible in $\mathbb{Z}[X] \Rightarrow \mathbb{Q}[X]$,$G_f := \text{Gal}(f)$ contains a 5-cycle (where $5 = \deg(\overline{f})$). We see that $\overline{f} = \overline{f}_1 \cdot \overline{f}_2 \in (\mathbb{Z}/2\mathbb{Z})[X]$. Where $\overline{f} = (X^2 + X + 1)(X^4 + X^2 + 1)$ so G_f contains $\sigma = (12)(345)$. We see that $\sigma^3 = (12)^3(345)^3 = (12)$, which is a transposition. Therefore by first lemma of this section, we see that $Gf \cong S_5$.

Algebraic closure of a field

K is ALGEBRAICALLY CLOSED iff $f \in K[X] \setminus K$ (so non-constant) has a root in K iff it splits completly over K iff $\forall L/K$ algebraic (therefore $L = K$, so does not have proper algebraic extensions).

Theorem:

> $\forall$field K, $\exists$ALGEBRAIC CLOSURE $K^{\text{alg}} := \overline{K}/K$
> that is an ALGEBRAIC EXTENSION OF K that is algebraically closed
> it is unique up to non-unique isomorphisms.

$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is absolute Galois group of $\mathbb{Q}$ which is infinite.

Extra curriculum: Infinite Galois theory

Extra curriculum: Not in exam.
L/K Galois (not necessarily finite), then there is a profinite group $\text{Gal}(L/K)$
Bijection $\{M : L/M/K\} \to \{H \leq \text{Gal}(L/K)\}$ s.t. $M \mapsto \text{Gal}(L/M)$ and $L^H \leftarrow H$.
M/K finite iff $\text{Gal}(L/M) \leq \text{Gal}(L/K)$ is open.
Exercise:
$\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \mathbb{Z} = \lim_{n} \mathbb{Z}/n\mathbb{Z}$
We see that $[\overline{K} : K] < \infty$ when

- $\overline{K} = K$, since then $[\overline{K} : K] = 1$, and when
- $K = \mathbb{R}$ so $\overline{K} = \mathbb{C} = \mathbb{R}(i)$ so $[\overline{K} : K] = 2$

Lecture 9

Definition VI.1.1.
R unitary ring,LEFT R MODULO M abelilan group $(M, +, 0)$ with ACTION on ring R, so

$$R \times M \to M, \quad (a, m) \mapsto am$$

s.t.$\forall a, b \in R, \forall m, n \in M$ it holds that:

RM1 $a(m + n) = am + an$

RM2 $(a + b)m = am + bm$

RM3 $a(bm) = (ab)m$

RM4 $1m = m$

Right R module defined analogously but with action $M \times R \to M$
Examples:

1. K ,field, then K modulos are same thing as K vector space.
2. $n > 0$, then R^n is an R mod. Note that $R^0 = \{0\}$ is also an R-mod.
3. $R \subset S$ subring, then S is an R mod If $S = R[t] = R[t_1, \dots, t_n]$ then also $R-$ modulo.
4. K field, $n > 0$ then K^n is R mod, where $R = K^{n \times n}$ and $R \times K^n \to K^n$ s.t. $(A, x) \mapsto Ax$
5. More generally, $G = (G, +, 0)$ abelian group, then $\text{End}_{\mathbb{Z}}(G) = \{\varphi : G \to G \text{ group hom.}\}$,in an ring via $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$ and $(\varphi\psi)(x) = \varphi(\psi(x))$. G is an $R-$ mod via $R \times G \to G$ s.t. $(\varphi, x) \mapsto \varphi(x)$.

Homomorphism theorem

If $\varphi : MM \to M'$ is an $R-$ mod homom. Then $R/\ker(\varphi) \cong \text{im}(\varphi) = \varphi(m)$ also $R-$ mod.

M, M' be R-mods. A map $\varphi : M \to M'$ is an R-MOD HOMOMORPHISM if φ is a group hom. and $\varphi(ax) = a\varphi(x), \forall a \in \mathbb{R}, x \in M$.
So $\text{Hom}_R(M, M') = \{\varphi : M \to M'$ which is R-mod-hom$\}$. Note that $\text{End}_R(M) = \text{Hom}_R(M, M)$.
$\varphi \in \text{Hom}_R(M, M')$ is isomorphism if φ is bijective.
Example:

1) M, M' abelian groups, then $\text{Hom}_{\mathbb{Z}}(M, M') = \{\varphi : M \to M'$ group homo.$\}$

2) K field, V, V' a K-vectorspace. $\varphi : V \to V'$ is $K-$ mod hom. iff φ is a K-linear map.

Remarks:

- $\varphi \in \text{Hom}_R(M, M')$ is injective iff $\ker(\varphi) = \{0\}$
- If $\varphi : M \to M', \psi : M' \to M$" are R-mod homo. then so is $\psi \circ \varphi$.

3) R commutative ring, $a \in R$mM R-mod, then $\varphi_a \in \text{End}_R(M)$ where
$\varphi_a : M \to M$ s.t. $x \mapsto ax$.

If $M = R$, then $\text{End}_R(R) = \{\varphi_a : a \in R\}$ since if,$\varphi \in \text{End}_R(R)$ then $\varphi = \varphi_a$ where $a = \varphi(1)$ so $\varphi(x) = \varphi(x \cdot 1) = x \cdot \varphi(1) = xa$

Remark:
If $\varphi : R \to R$ is a R-mod hom. then φ is not necessarily a ring hom.

4) E.g. we see that $R = K[t]$, then $\varphi(f(t)) = tf(t)$ is not a ring homomorphism, since $\varphi(1) = t \neq 1$, and it is a R-mod hom. We see that $\psi(f(t)) = f(t^2)$ which is a ring hom. but not an R-mod-hom.

5) $\mathbb{Z}[i] \to \mathbb{Z}^2$ s.t. $(a + bi) \mapsto (a, b)$ is a $\mathbb{Z}$ mod is. Similarly $\mathbb{Z}[\sqrt{2}] \cong \mathbb{Z}^2$ as $\mathbb{Z}$ mod isom. But $\mathbb{Z}[i] \ncong \mathbb{Z}[\sqrt{2}]$ as rings, since $(\mathbb{Z}[i])^\times = \{\pm1, \pm i\}$ and $\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1 + \sqrt{2})^n : n \in \mathbb{Z}\}$ so we see that the unit groups are of different size, so they can not be isomorphic (as rings).

Submodules

Let M be an $R-$ mod. Then a R-SUBMODULO of M is a subgroup N of M s.t. if,$x \in N$ and $a \in R$ then $ax \in N$.
Example

1) $\varphi : M \to M'$ is a R-mod-hom., then $\ker(\varphi) \subset M$ is a submod, $\text{im}(\varphi) \subset M'$ is a submod. We see $\forall S \subset M'$, that $\varphi^{-1}(S)$ is submod of M.

2) VMK vector spaces, then $N \subset V$ is a K-submod iff V is a lin. subspace.

3) $M_1, M_2 \subset M$ submod $\Rightarrow M_1 \cap M_2$ is a submod.
   More generally if I is a set and $M_i \subset M$ is a submod for all $i \in I$ then $\bigcap_{i \in I} M_i$ is a submod of M.

4) An left $R-$ submod of R is the same thing as an ideal of R.

5) $M-$ R- mod, $I \subset R$ ideal, if $S \subset M$ then $IS = \{\sum_{j=1}^{n} a_i j x_j : a_j \in I; x_j \in S, \forall j, n \geq 0\}$ is an $R-$ submod.
   I ideal, $\forall a \in I, \forall a_j \in I, aa_j \in I$.

Quotient modules

Lemma/definition M is R mod, $N \subset M$ is submod then

1. The factor group M/N is an $R-$ mod via $R \times M/N \to M/N$ s.t. $(a, x+N) \mapsto ax+N$
2. $\pi : M \to MN$ s.t. $x \mapsto x + N$ is a surjective $R-$ mod hom.

noet that if $x, x' \in N$ then $x + N = x' + N$ so $ax' + N = ax + a(x' - x) + N \subseteq ax + N$ similarly $ax + N \subseteq ax' + N$. Therefore we see that the function in 1) is well-defined. The proof now follows using the modulo axioms of both M and N. We know that it is already a group.
For the second one, we see that it is indeed already a surjective homomorphism from group theory so we only have to proof that it is a n R-mod-hom.

Lecture 10

Let R be a unitary ring.
Theorem 10.1 (Top VII.1.4):

$$\begin{aligned}&\varphi : M \to M' \text{ R-mod-hom } \exists! R-\text{ mod-hom } \tilde{\varphi} : M/\ker(\varphi) \to M' \text{ s.t. } \varphi = \tilde{\varphi} \circ \pi \\ &\text{i.e. } \tilde{\varphi} : M/\ker(\varphi) \to M' \text{ s.t. } x + \ker(\varphi) \mapsto \varphi(x) \\ &\text{is well-defined R-mod-hom and if } \varphi \text{ surjecitve } M/\ker(\varphi) \cong M'\end{aligned} \tag{Thm 10.1/Top VII.1.4}$$

Here π is canonical surjection
Theorem 10.2:

$$M \text{ R-mod}, N, P \subset M \text{ R-submods, then } (N+P)/P \cong N/(N \cap P) \tag{Thm 10.2}$$

Proof:
Need to show that $N \cap P$ is a submod of N, and P is a submod of $N+P$, then have to find explicit isomorphism.
Theorem 10.3:

$$\begin{aligned}&P \subset N \subset M \text{ R-submods} \\ \Rightarrow &N/P \subset M/P \text{ submod} \\ \Rightarrow &(M/P)/(N/P) \cong M/N\end{aligned} \tag{Thm 10.3}$$

Example:
$V = \mathbb{R}^2, U = \mathbb{R}\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), V_U = \{v + U : v \in V\}$ therefore $\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right) + U = \left(\begin{smallmatrix}y\\y'\end{smallmatrix}\right)$ iff $y = y'$.
So $V/U \to \mathbb{R}$ s.t. $\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right) + U \mapsto y$ is an R mod isom. induced by $V \to \mathbb{R}$ s.t. $\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right) \mapsto y$.
Lemma 10.4:

$$\begin{aligned}&V \text{ K-vector space}, U \subset V \text{ lin. subspace then} \\ &\dim_K(V) = n \Rightarrow V \cong K^n \text{ and } V \ncong K^m, \forall m \neq n\end{aligned} \tag{Lem. 10.4}$$

Proof:
Fix basis $B = (b_1, \ldots, b_n)$ of V then $\varphi : V \to K^n$ s.t. $\sum \lambda_i b_i \mapsto (\lambda_i)$. Is a K vector space.
But $\#B$ is uniquely determined by V.
Lemma 10.5

$$\begin{aligned}&\dim_K(V) = n, \dim_K(U) = m, (b_1, \ldots, b_m) \text{ basis of } U, (b_1, \ldots, b_m, b_{m+1}, \ldots, b_n) \text{ basis of } V, W = \langle b_{m+1}, \ldots, \\ &\pi|_W : V \to V/U \text{ s.t. } x \mapsto x + U \text{ is isomorphism}\end{aligned} \tag{Lem. 10.5}$$

Proof:
1) Hom. clear.

2) surjective: Let $v + U \in V/U$ so then $v = \sum_{i=1}^{n} \lambda_i b_i$. Let $u = \sum_{i=1}^{m} \lambda_i b_i \in U, w = \sum_{i=m+1}^{n} \lambda_i b_i \in W$
So then $v = u + w$ so $\pi|_W(v) = (v - u) + U = v + U$.
3) $\pi|_W$ is injective follows from $U \cap V = \{0\}$ since,$w + U = w' + U \Rightarrow w - w' \in U \cap W$.
Proposition 10.6

$$\dim_K(V) = n, \dim_K(U) = m \Rightarrow \dim_K(V/U) = n - m \quad \text{(Prop 10.6)}$$

Proof:
By taking same basis of above, then use (Lem. 10.5), which immediately shows this proposition.
Corollary
$\forall v \in V, \exists! u \in U, w \in W$ s.t. $v = u + w$

M be R-mod, $N, P \subset M$ submods, then M is (INNER) DIRECT SUM of P and N written $M = N \bigoplus P$ if

1. $M = N + P$ i.e.,$\forall x \in P, \exists y \in N, z \in P$ s.t. $x = y + z$.
2. $N \cap P = \{0\}$

This means $M = N \uplus P$ s.t. $\forall x \in M, \exists! y \in N, z \in P$ s.t. $x = y + z$.

I set,M_i R-mod, $\forall i \in I, \prod_{i \in I} M_i = \{(x_i)_{i \in I}$ .s.t $x_i \in M_i, \forall i \in I\}$. This is n $R-$ mod via componentwise addition and scaler multiplication, called the DIRECT PRODUCT of M_i.
Example:
$R^n = \prod_{i=1}^{n} R$ then $R^i = \{f : I \to R$ functions$\}$
Take $\mathbb{R}^{\mathbb{Z}_{\geq 0}} = \{$real sequences$\}$

(OUTER) DIRECT SUM of M_i is the $R-$ submod
$\bigoplus_{i \in I} M_i = \{(x_i)_{i \in I} \in \prod_{i \in I} M_i : x_i = 0, \forall$ but finitely many $i \in I\} \subseteq \prod_{i \in I} M_i$

R mod M is free, if $\exists I$ and R mod isomorphism s.t. $M \cong \bigoplus_{i \in I} R$REALLY IMPORTANT
Example:

- I finite then $\prod_{i \in I} M_i = \bigoplus_{i \in I} M_i$
- $R^n = \bigoplus_{i=1}^{n} R$ is free.
- $\bigoplus_{n \in \mathbb{Z}_{\geq 0}} \mathbb{R} = \{$sequences $(a_n)_{n \geq 0}$ s.t. $\exists N > 0 : a_n = 0, \forall n > N\}$

- $R[t]$ is free, since we can map $\sum a_n t^n \mapsto (a_n)$ so then we have $[t] \to \bigoplus_{n\in\mathbb{Z}_{\geq 0}} R$ which is isomorphic, hence free.
- V a K-vector space, $U \subset V$ linear subspace, then $V \cong U \bigoplus V/U$.
- M an R, mod, all $M_i \subset M$ submods, s.t. M is the inner direct sum of all M_i then M is isom. to the outer sum of the M_i.
- All K vector spaces are free.
- $\mathbb{Z}/2\mathbb{Z}$ is a free $\mathbb{Z}/2\mathbb{Z}$ mod. But not free as $\mathbb{Z}-$ mod. This is because M is a free $\mathbb{Z}-$ mod, then $\#M = 1$, if $M = \{0\}$ or $\#M = \infty$
- $M = \mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z}$ is not free as $\mathbb{Z}-$ mod, since $2(0,1) = (0,0)$ but $(0,1) \neq (0,0)$ but $\nexists x \in \mathbb{Z}^n$ of order 2.
- $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ as $\mathbb{Z}-$ mod, but also as $\mathbb{Z}/6\mathbb{Z}-$ mods.

REMARK:
If $d|N$ then $\mathbb{Z}/d\mathbb{Z}$ is $\mathbb{Z}/N\mathbb{Z}$-modulo. This is because $\mathbb{Z}/d\mathbb{Z} \cong (\mathbb{Z}/N\mathbb{Z})/d(\mathbb{Z}/n\mathbb{Z})$.

So Chinese remainder theorem: If $N = \prod p_i e^i$ where p_i prime, $e_i > 0$ then $\mathbb{Z}/n\mathbb{Z} \cong \bigoplus_i \mathbb{Z}/(p_i^{e_i})\mathbb{Z}$ as $\mathbb{Z}-$ mods and as $\mathbb{Z}/n\mathbb{Z}$-mods.

Theorem 10.6

$$R \text{ comm. ring}, m, n \geq 0. \text{then } \mathbb{R}^n \cong \mathbb{R}^m \Rightarrow n = m \qquad \text{(Thm. 10.6)}$$

Proof:
Recall $R = \mathbb{Z}$ then $\mathbb{Z}^m \cong \mathbb{Z}^n \Rightarrow (\mathbb{Z}/2\mathbb{Z})^m \cong (\mathbb{Z}/2\mathbb{Z})^m \Rightarrow m = n$
In general. Choose maximal idea $J \subset R$. Then $R/J = K$ is a field. Suppose exists isom. $\varphi : R^m \to R^n$ then $\varphi(J^m) \subset R^n$ is a submod so there exitss a K-vectorspace isomorphism $R^n/\varphi(J^m) \cong R^m/R^n \cong (R/J)^m = K$. We get $\dim_K = m$. This is because $R^n/\varphi(J^m) = \langle S \rangle$ where $S = \{e_i + \varphi(J^m) : i \in \{1, \dots, n\}\}$. We see that $\#S = n$ so $n \geq m$. Similarly we get $m \geq n$ so $m = n$.

For M free say $M \cong \mathbb{R}^n$ we call n the RANK of M (so $\text{rk}(M) = n$)
M is an R mod,$S \subset M$ subset. Then S is LINEAR INDEP/ of $\forall(\lambda_s)_{s\in S}$ where $\lambda_s \in R$ s.t. $\forall \lambda_s \neq 0$ we have $\sum_{s\in S} \lambda_s s = 0$ then all $\lambda_s = 0$.
S is GENERATING SET of M if $M = \langle S \rangle = \{\sum_{s\in S} \lambda_s s \text{ finite sums}\}$.
S is an R-BASIS if S is lin. indep, and a generating set.

M is FINITELY GENERATED if $M = \langle S \rangle$ for some $S \subset M$ finite.
M is CYCLIC if $M = \langle S \rangle$ where $\# S = 1$.

Lemma 10.7

$$\begin{gathered} M \text{ R-mod} \\ 1) S \subset M \text{ basis} \Leftrightarrow \forall x \in M, \exists! (\lambda_s)_{s \in S} : x = \sum_{s \in S} \lambda_s s \\ 2) M \text{ has basis} \Leftrightarrow M \text{ free} \end{gathered}$$

Proof:
Part 1: Sim. as LA
Part 2: If M is free, so $\varphi : M \cong \bigoplus_{i \in I} R \ni (e_i)_{i \in I}$ then $(\varphi^{-1}(e_i))$ is a basis.
If $(s_i)_{i \in I} = S \subset M$ basis, then $\varphi : M \to \bigoplus_{i \in I} R$ s.t. $s_i \mapsto e_i$. Still have to show isomorphism.

Example:
$M = R = \mathbb{Z} = \langle 1 \rangle$ where $\{1\}$ is basis, but we see that $M = \langle 2, 3 \rangle$ since $1 \in \langle 2, 3 \rangle$. If $S = \{2, 3\}$ we see that $(-3) \cdot 2 + 2 \cdot 3 = 0$ so not lin. indep. so S is not a basis and no subset of S is since $2 \notin \langle 3 \rangle, 3 \notin \langle 2 \rangle$.

Lemma 10.8:

$$\begin{gathered} R \text{ comm. ring } I \subseteq R \text{ ideal} \\ a) I \text{ cyclic as } R-\text{mod} \Leftrightarrow I \text{ principal} \\ b) R \text{ domain then } I \text{ free} \Leftrightarrow I \text{ principal} \end{gathered} \tag{10.8}$$

Proof:
a) follows by definition of principal ideal and cyclic.
b) $\Leftarrow$ if, I is principal, then $I = Rx$ so $R \to I$ s.t. $a \mapsto ax$ is an isomorphism. So I is free.
$\Rightarrow$ suppose I is free, then if $\text{rk}(I) > 1, \exists x_1, x_2 \in I$ lin. indep. And $I \cong R^{\text{rk}(I)}$, but $x_2 x_1 - x_1 x_2 = 0$ which is a contradiction so $\text{rk}(I) = 1$, hence $I = Rx$ is principal.

Lecture 11

R ring, M_i an $R-$ mod for all $i \in I$ then

$$\bigoplus_{i\in I} M_i = \{(x_i)_{i\in I} : x_i \in M_i, \forall i \in I, x_i = 0, \text{for all but fin. many}\, i\}$$

$R-$ mod M is FREE if $\exists I$ s.t. $M =\cong \bigoplus_{i\in I} R$
M is free iff M has a basis (a lin independent generating set)
R domain, $I \subset R$ ideal, then I free iff I principal.

Theorem 11.1:

R principal ideal domain (PID), let M free R-mod then any $R-$ submod of M is free (Thm 11.1)

Proof:
See conrad, all most the same for $R = \mathbb{Z}$ (group theory)

Example:

- $R = \mathbb{Z}[\sqrt{-5}]$ and $M = \langle 2, -1 + \sqrt{-5}\rangle \subset R$ which is non-principal ideal, so not free as $R-$ mod. But $M \bigoplus M \cong R^2$ is free.
- $R = \{f \in C^\infty(\mathbb{R}) : f(x + 2\pi) = f(x)\}$ is a ring.
  $M = \{m \in C^\infty(\mathbb{R}) : m(x + 2\pi) = -m(x)\}$ is a module over R via $R \times M \to M, (f, m) \mapsto fm$ where $(fm)(x) = f(x)m(x)$.
  Claim:

  1. $M \bigoplus M \cong R^2$.
     Let $c_0(x) = \cos\left(\frac{x}{2}\right), s_0(x) = \sin\left(\frac{x}{2}\right)$. Then $s_0, c_0 \in M$. Let $\psi : R^2 \to M \bigoplus M$, s.t. $(f, g) \mapsto A\begin{pmatrix} f \\ g \end{pmatrix}$, where $A = \begin{pmatrix} c_0 & s_0 \\ -s_0 & c_0 \end{pmatrix}$
     We see that ψ is an $R-$ mod hom.
     $A^{-1} = \begin{pmatrix} c_0 & -s_0 \\ s_0 & c_0 \end{pmatrix}$ and $m, n \in M \Rightarrow mn \in R$.
     $\psi^{-1} : M \bigoplus M \to R^2$ s.t. $(m, n) \mapsto A^{-1}\begin{pmatrix} m \\ n \end{pmatrix}$ so ψ has an inverse, so ψ is an isomorphism.
  2. M is not free.
     Exercise VI.7.3. This says $M \cong I \subset R$ ideal, and

$I = \ker(\text{ev}_0) = \{f \in R : f(0) = 0\}$, It suffices to show that $\nexists R-$ mod isomorphism $\varphi : R \to M$. Suppose therefore there exists such a φ. Let $g := \varphi(1) \in M$. Let $a \in [0, 2\pi]$ s.t. $g(a) = 0$. Since φ surj, $\exists f \in R$ s.t. $\varphi(f) = c_a$ where $c_a(x) := \cos\left(\frac{x-a}{2}\right)$. We see hterfore that $\varphi(f) = f\varphi(1) = fg$. So then $0 = f(a)g(a) = c_a(a) = \cos(0) = 1$. But we see that $0 \neq 1$ so φ is not surjective, so φ is not a R-mod isomorphism. Therefore there does not exists an R-mod isomorphism, hence we are done?

Universal property (UP) of direct sums

Theorem 11.2 (UP):

R ring, M_i R-mod $\forall i \in I : \iota_i : M_i \to \bigoplus_{i\in I} M_i = N$ s.t. $x_i \mapsto (x_i, \delta_{ij})_{j\in I}$

This is an R-mod-hom, then following properties:

$a)$The pair $(N_i, (c_i)_{i\in I})$ satisfies UP:$\forall (M, (\varphi_i)_{i\in I}$ s.t. M R-mod, $\varphi_i : M_i \to M$ R-mod hom
$\Rightarrow \exists! \varphi \in \text{Hom}_R(N, M) : \varphi \circ \iota_i = \varphi_i, \forall i \in I$

$b)$ Let $(D, (j_i)_{i\in I}), D$ R-mod, $j_i : M_i \to D$ be R-mod hom.& satisfy a),
i.e. $\forall (M, (\varphi_i)_{i\in I}), \exists! \psi : \text{Hom}_R(D, M)$ s.t. $\psi \circ j_i = \varphi_i, \forall i \in I \Rightarrow D \cong N$

(Thm 11.2/UP)

Proof:

Part a Note that $x = (x_i)_{i\in I} \in N$ we have $x = \sum_{i\in I} \iota_i(x_i) \Leftarrow (*)$.
Consider $(M, (\varphi_i)_{i\in I})$ and supp $\exists \varphi \in \text{Hom}_R(N, M)$ s.t. $\varphi \circ \iota_i = \varphi_i, \forall i \in I$. Then for $x = (x_i)_{i\in I} \in N$,we have $\varphi(x) \overset{*}{=} \sum_{i\in I} \varphi(\iota_i(x_i)) = \sum_{i\in I} \varphi_i(x_i)$. so φ is already uniquely determined by $(M, (\varphi_i)_{i\in I})$
So this proofs both uniqueness, and $\varphi : N \to M$ s.t. $x = (x_i)_{i\in I} \mapsto \sum_{i\in I} \varphi_i(x_i)$ shows existence. Since φ is an $R-$ mod hom, and $\varphi \circ \iota_i = \varphi_i$.

Part b UP for D, with $M = N, \varphi_i = \iota_i$. So $\exists! \psi \in \text{Hom}_R(D, N)$ s.t. $\iota_i = \psi \circ j_i \Leftarrow \dagger$.
UP for N with $M = D$,$\phi_i = j_i$,so $\exists! \phi \in \text{Hom}_R(N, D)$ s.t. $j_i = \varphi \circ \iota_i$.
We show that ψ, φ are both isomorphisms, and to be more explicit, they are eachothers inverses.$\iota_i \overset{\dagger}{=} \psi \circ j_i = (\psi \circ \varphi) \circ \iota_i$. So we show that $\psi \circ \varphi = \text{id}$.
UP for N with $M - N$,and $\varphi_i = \iota_i$, then $\exists! \tilde{\phi} \in \text{Hom}_R(N, N)$ s.t. $\tilde{\varphi} \circ \iota_i = \iota_i$ for all $i \in I$. This holds for $\tilde{\varphi} = \text{id}_N$, and only for this one due to uniqueness. But we saw that it also hold for $(\psi \circ \varphi)$. Therefore we see that $\tilde{\varphi} = \psi \circ \varphi = \text{id}_N$. By similair reasoning,$\varphi \circ \psi = \text{id}_D$. Therefore φ, ψ are isom.

Modules over PID's

R comm. ring, M – R-mod. Then:
$x \in M$ TORSION iff $\exists a \in R \setminus \{0\}$ s.t. $ax = 0$.

For $R = \mathbb{Z}$ we see x torsion iff $\operatorname{ord}(x) < \infty$.
$\operatorname{Tor}(M) := \operatorname{Tor}_R(M) = \{x \in M \text{ torsion}\}$

Example:

1. V a K – vector space, therefore $\operatorname{Tor}(V) = \{0\}$
2. $M = \mathbb{Z}^n, R = \mathbb{Z}$, then $\operatorname{Tor}(\mathbb{Z}^n) = \{0\}$
3. $R = \mathbb{Z}, M = \mathbb{Z}/6\mathbb{Z}$ then $\operatorname{Tor}(M) = M$ since $6x = 0, \forall x \in M$.
4. $R = M = \mathbb{Z}/6\mathbb{Z}$ then $\operatorname{Tor}(M) = \{0, 2, 3, 4\}$
5. M fin. abel. group, then $M \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$ s.t., $d_1 | d_2 | \ldots | d_n \Rightarrow \operatorname{Tor}_{\mathbb{Z}} M = M$. If M is finitely generated, then we see $M \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$ for $r \geq 0$. Then $\operatorname{Tor}(M) \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$

$\operatorname{Ann}(M) = \operatorname{Ann}_R(M) = \{a \in R : ax = 0, \forall x \in M\}$ this is called ANNIHILATOR of M (Note that $\operatorname{Tor}(M) \subseteq M, \operatorname{Ann}(M) \subseteq R$.)

Lemma 11.3

$$\begin{aligned} &1)\ R \text{ integral domain, then } \operatorname{Tor}_R(M) \text{ is submodule of } M \\ &2)\ \operatorname{Ann}(M) \text{ is an ideal of } R \end{aligned} \tag{Lem 11.3}$$

Proof:
Tutorial

Go back to example 5, so T finite $\mathbb{Z}$– mod, then $T =\cong \bigoplus \mathbb{Z}/d_i\mathbb{Z}$. But $T =\cong \bigoplus_{i=1}^{t} A_i$ where A_i is the p_i Sylow subgroup. S.t. $\#T = \prod_{i=1}^{t} p_i^{e_i}$ where p_i prime and $e_i > 0$.

Lecture 12

If $\operatorname{Ann}(M) \neq \{0\}$ then $\operatorname{Tor}(M) = M$.

Let R be PID
Theorem 12.1:

T R-mod s.t. $\operatorname{Ann}(M) \neq \{0\}$, write $h \in \operatorname{Ann}(M) \setminus \{0\}$ as $h = \prod_{i=1}^{t} p_i^{e_i}$ with $p_i \in R$ prime and non-associated, $e_i > 0$ set $T_{h,i} := \{x \in T : p_i^{e_i} x = 0\}$

1) $T_{h,i}$ submod of T, $\forall i$
2) $T_{h,i} = \{x \in T : p_i^e x = 0$ for some $e > 0\} = T(p_i)$
3) $T = T(p_1) \bigoplus \cdots \bigoplus T(p_t)$
4) $\operatorname{Ann}(M) = hR$ and $p \in R$ prime then $T(p) = \{0\} \Leftrightarrow p \not| h$ (Thm 12.1)

Proof:

1) follows from definition

2) $T_{h,i} \subset T(p_i)$ is logic. Now set $q_i = \frac{h}{p_i^{e_i}} \in R$. Therefore $(q_i, p_i) = 1$. Let $x \in T(p_i)$. We know $p_i^e x = 0$ for some $e > 0$. Since $(q_i, p_i) = 1$ we see that $(q_i, p_i^e) = 1$, so therefore by Beizout, $1 = rp_i^e + sq_i$ for $r, s \in R$. So we get $p_i^{e_i} x = p_i^{e_i}(rp_i^e x + sq_i x) = p_i^{e_i} q_i s x$. Use that $p_i^{e_i} q_i = h$ therefore we get $p_i^{e_i} x = hsx = 0$ so we have $T(p_i) \subset T_{h,i}$ so $T(p_i) = T_{h,i}$

3) Write $1 = s_i q_i + \ldots + s_t q_t$. Let $x \in T$. Want to show: $\exists! x_i \in T(p_i) \forall i$, s.t. $x = x_1 + \ldots + x_t$. Let $x_i = x s_i q_i$ then $x = x_1 + \ldots + x_t$. Since $p_i^{e_i} x_i = hxs_0 = 0$,so $x_i \in T(p_i)$.
Now we have to show it is unique. Suff. to show if $y_1 + \ldots + y_t = 0$ for $y_i \in T(p_i)$ then all $y_i = 0$.
As in 2) let $1 = r_1 p_i^e + sq_i$, where $p_1^e y_i = 0$, then $y_i = rp_i^e y_i + sq_i y_i = sq_i y_i$.
If $y_1 + \ldots + y_t = 0$, then $y_i = sq_i y_i = -s \sum_{j \neq i}^{1} q_i y_j = 0$. If $i \neq j$ then $q_i y_j = s y_j q_i q_j = 0$ because $h | q_i q_j$. So we get $y_i = 0$ for all i.

4) Let $\operatorname{Ann}(T) = hR$. Suppose $T(p) = \{0\}$. Assume $p|h$, let $h = h' p^e$ s.t. $p \not| h$. $\forall x \in T$ we have $0 = hx = h' p^e x$, so $h' x \in T(p) = \{0\}$. So $h' \in \operatorname{Ann}(T)$, which is a contradiction as $h' \notin hR$. So $T(p) = \{0\} \Rightarrow p \not| h$.

Suppose $p \not| h$ let $h = \prod_{i=1}^{t} p_i^{e_i}$. Therefore $T = T(p_1) \oplus \ldots \oplus T(p_t)$. Note $ph \in \operatorname{Ann}(T)$. Therefore $T = T(p_1) \oplus \ldots \oplus T(p_t) \oplus T(p)$, so $T(p) = \{0\}$

Theorem 12.2:

$R\,\text{PID}, M\,\text{Fin. Gen.}\ R-\text{mod. Let}\ T = \text{Tor}(M)$
1) $M = F \bigoplus T$ where $F \cong M/T$ free and $\text{rank}(F)$ uniq. determ. by M
2) $T \neq \{0\}$ then $T \cong N_1 \bigoplus \ldots \bigoplus N_s, N_i = R/d_iR$ with $d_1|d_2|\ldots|d_s$ and
N_i submodules, $d_i \in R \setminus R^\times$ uniq. determ up to integers by multiples of $R^\times$
3) If $T \neq \{0\}$, then $T = T(p_1) \bigoplus \ldots \bigoplus T(p_t)$ where $p_1, \ldots, p_t \in R$ primes, s.t.
$T(p_i) \neq \{0\}$, where p_i uniquely determ. by M up to mult. by $R^\times$ (12.2)

Theorem 12.2 is called the structure theorem for finitely generated modules over PID
Proof:

1) See Conrad/GT

2) See Conrad/GT

3) M finitely generated, then T finitely generated. Say $T = \langle s_1, \ldots, s_n \rangle$. Let $h_i \in R \setminus \{0\}$ s.t. $h_i s_i = 9$. Then $h = \prod h_i \in \text{Ann}(T)$ now apply (Thm 12.1)

Linear algebra over fields (normal forms of matrices)

K field, V finite dimensional K-vector sapce, Let $\varphi \in \text{End}_K(V) = \{f : V \to V \text{ linear}\}$ then $\text{ev}_\varphi : K[t] \to \text{End}_K(V)$ s.t. $\sum\limits_i a_i t \mapsto \sum a_i \varphi^i$. is a ring hom. and a K-vector space.

Lemma 12.3:

1) $K[\varphi] = \text{ev}_\varphi([K(t)])$ com. subring of $\text{End}_K(V)$
2) V is $K[\varphi]$ mod via $K[\varphi] \times V \to V$ s.t. $(\sum a_i\varphi^i, x) \mapsto \sum a_i \varphi^i(x)$
3) V is a $K[t]$ mod via $K[t] \times V \to V$ s.t. $(f, x) \mapsto \text{ev}_\varphi(f) \cdot x = (\text{ev}_\varphi(f)(x))$
4) $\exists!$ monic $m_\varphi \in K[t]$ s.t. $K[\varphi] \cong K[t]/(m_\varphi)$
5) $m_\varphi | \mathcal{K}_\varphi$, char pol of φ (Lem. 12.3)

Proof:

1),2),3) Tutorial

4) $K[t]$ PID, therefore $\text{Ker}(\text{ev}_\varphi)$ prime. Let m_φ unique monic gen. Then $K[t]/(m_\varphi) \cong K[\varphi]$

5) Cayley-Hamilton

Theorem 12.4

$$\begin{aligned}&\text{Write}\, m_\varphi = \prod_{i=1}^{t} h_i^{e_i}, e_i > 0 \,\text{and}\, h_i \,\text{irr., monic, not ass.}\\ &1)\, V_i = \{v \in V | h_i^{e_i}(\varphi)(v) = 0\} \,\text{is}\, K[\varphi] - \& K[t] - \text{ submond of}\, V\\ &2)\, V_i \neq \{0\}\, \forall i \,\text{and}\, V_i \,\text{Generalized eigenspaces}\\ &3)\, V = V_1 \bigoplus \dots \bigoplus V_t\end{aligned} \tag{12.4}$$

Proof:
$K[t]$ PID, we generate $\ker(\text{ev}_\varphi) = \text{Ann}_{K[t]} V \neq \{0\}$. Then apply (Thm 12.1) with $h = m_\varphi$ so $T_{m_{\varphi,i}} = V_i$

Remark: Since V_i is a $K[\varphi]$ mod have $\varphi(V_i) \subset V_i$. This and $V = V_1 \oplus \dots \oplus V_t$ implies that can deal with the V_i separable

Example:
$m_\varphi = \mathcal{K}_\varphi = \prod_{i=1}^{n}(t - \lambda_i)$ with λ_i distinct.
$V_i = \{v \in V : (t - \lambda_i)(\phi)(v) = 0\} = \{v \in V : (\varphi - \lambda_i \text{id}_v)(v) = 0\}$ which is the eigenspace of λ_i.
$\dim V_i = 1 \Rightarrow V_i = Kx_i$ for some $x_i \in V_i$ therefore $V = Kx_1 \oplus \dots \oplus Kx_n$ then the matrix of φ w.r.t. to the basis B denoted by $M_B(\varphi)$ satisfy $M_B(\varphi) = \text{diag}(\lambda_1, \dots, \lambda_n)$ where $B = (x_1, \dots, x_n)$.

To gen. this, find basis for V using bases of V_i s.t. matrix of $B_i\, \varphi|_{v_i}$ wrt B_i is simple. By remark above, if we set $B = (B_1, \dots, B_t)$, then $M_B(\varphi) = \begin{pmatrix} M_{B_1}(\varphi|_{v_1}) & & \\ & \ddots & \\ & & M_{B_t}(\varphi|_{v_t}) \end{pmatrix}$ which is a block matrix.

Example:
$V + \mathbb{R}^3$, $A = \begin{pmatrix} 1 & -4 & 0 \\ 1 & -3 & 0 \\ -1 & 2 & -1 \end{pmatrix}$, $\varphi(x) Ax$, then $\mathcal{K}_\varphi(t) = (t+1)^3$. So then $A + I_3 = \begin{pmatrix} 2 & -4 & 0 \\ 1 & -2 & 0 \\ -1 & 2 & 0 \end{pmatrix} =$ $N \neq 0$ by $N^2 = 0$. So $M_\varphi = (t+1)^2$ so $V_t = \text{Ker}()\varphi + \text{id}_V)^2)$

Theorem 12.5:

$$\begin{gathered}\text{supp.}\, m_\varphi = (t-\lambda)^2, \lambda \in K \\ 1)\varphi = \lambda \text{id} + \psi \,\text{s.t.}\, \psi^2 = 0 \\ 2)\exists \text{basis}\, B \,\text{of}\, V \,\text{s.t.}\, M_B(\varphi) \text{ upp triang. matrix with only } \lambda\text{'s on diagonal}\end{gathered} \tag{12.5}$$

Proof:

1) $0 = m_\varphi(\varphi) = (\varphi - \lambda \text{id}_V)^2$. Define $\psi = \varphi - \lambda \text{id}_V$

2) Look at ψ first, $W_i = \ker(\psi^i)$ therefore $W_1 \subset W_2 \subset \ldots \subset W_l = V$. Construct basis B of V, so choose basis B_1 of W_1,extend to basis B_2 of W_2 and so on. Use $\psi(W_j) \subset W_{j-1}$ to show $M_B(\psi)$ is upper triangular with zeros on diagonal, then use 1)

Example:
$A = \begin{pmatrix} 1 & -4 & 0 \\ 1 & -4 & 0 \\ -1 & 2 & -1 \end{pmatrix}$, and $N = A + I_3, N^2 = 0$. Let $\psi = N$. $W_1 \subsetneq W_n = V$ where $W_1 = \ker(N) = \left\langle \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$. Since $W_2 = V$, can take $B = \left\langle \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle$. Then $N \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix} = 1 \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} - 1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. Therefore $M_B(\psi) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix} \Rightarrow M_B(\varphi) = \begin{pmatrix} -1 & 0 & 1 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$

Lecture 13

Exactness

R ring
A sequence

$$\ldots \to M \xrightarrow{f} N \xrightarrow{g} P \to \ldots \text{ of } R-\text{ mod homomorphisms} \tag{13.1}$$

-) is exact in N if $\text{im}(f) = \ker(g)$
-) is exact if it's exact everywhere
Remark:
(13.1) exact in $N \Rightarrow g \circ f = 0$ but not necessarily other way around.
Example:

1. $\{0\} \to N \xrightarrow{g} P$ s.t. $0 \mapsto 0$ is exact iff g is injective.
2. $M \xrightarrow{f} N \to 0$ with $x \mapsto 0$ iff f is surjective.
3. For all $R-$ mods M, P
   $0 \to M \xrightarrow{\iota_1} M \bigoplus P \xrightarrow{\pi_2} P \to 0$ s.t. $\iota_1 : x \mapsto (x, 0), \pi_2 : (x, y) \mapsto y$ is always exact. Since π_1 is inj, π_2 is surj. Furthermore $\ker(\pi_2) = \{(x, y) \in M \bigoplus P : y = 0\} = \text{im}\iota_1$
4. For all $R-$ mod hom. $g : N \to P$ we get
   $0 \to \ker(g) \xrightarrow{\iota} N \xrightarrow{g} \text{Im}(g) \to 0$. Note that we can write $\text{im}(g) \cong N/\ker(g)$. So
   $0 \to \ker(g) \xrightarrow{\iota} N \xrightarrow{\pi} N/\ker(g) \to 0$ s.t. $\pi : x \mapsto g(x) + \ker(g)$.

Short exact sequence (SES) of $R-$ mods is an exact sequence $0 \to M \to N \to P \to 0$.
Remark:
1) is shorter then the definition of SES, but it is not an SES.

Lemma 13.2:

$$\begin{array}{l}\forall \text{SES}\, 0 \to M \to N \to P \to 0 \,\text{exists a comm. diagram}\\
\begin{array}{ccccccccc} 0 & \to & M & \xrightarrow{f} & N & \xrightarrow{g} & P & \to & 0 \\ & & \cong\downarrow f & & \|\text{id}_N & & \cong\downarrow h & & \\ 0 & \to & \ker(g) & \xrightarrow{\iota} & N & \xrightarrow{\pi} & N/\ker(g) & \to & 0 \end{array}\\
h \,\text{inverse of}\, N/\ker(g) \to \text{Im}(g), x + \ker(g) \mapsto g(x)\end{array} \tag{Lem 13.2}$$

Proof:
We need to show both squares are commutative. Commutative is trivial. Note that since $\text{im}(f) = \ker(g$ and f injective (follows from example 1), we have that $f : M \to \ker(g)$ is an isomorphism.
For the second square, $\forall x \in N$ we need that $\pi(x) = h(g(x))$.
Since h inverse of $N/\text{ker}(g) \to \text{im}(g)$ we see that $h(g(x)) = x + \ker(g) = \pi(x)$
h is surjective, since $N/\ker(G) \to \text{im}(g)$ is isomorphism, but we need $P \to N/\ker(g)$ to be a well-def. isomorphism, which follows from that g is surjective.

Homomorphisms

Recall: M, N are $R-$ mods, then $\text{Hom}_R(M, N) = \{f : M \to N, R\,\text{mod-hom}\}$
Lemma 13.3:

$$\begin{array}{ll} M, N \,\text{are}\, R- \,\text{mods} & \\ 1 & \text{Hom}_R(M, N) \,\text{subgroup of}\, \text{Hom}_{\mathbb{Z}}(M, N) \,\text{with group law addition} \\ 2 & \text{End}_R(M) := \text{Hom}_R(M, M) \,\text{is subring of}\, \text{End}_{\mathbb{Z}}(M) \,\text{with composition} \end{array} \tag{Lem 13.3}$$

Examples:

1. K field then $\text{Hom}_K(K^n, K^m) \cong K^{n\times M}$

2. $n \geq 2, f \in \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ for $x \in \mathbb{Z}$ let $\overline{x} := x \mod n$. Therefore $f(\overline{x}) = x \cdot f(\overline{1})$. SO $0 = f(\overline{0}) = f(\overline{n}) = nf(\overline{1})$. This last multiplication is multiplication in $\mathbb{Z}$ which has no zero divisors, so $f(\overline{x}) = 0$ for all $x \in \mathbb{Z}$ therefore $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = \{0\}$.

3. R comm ring, M R-mod. For $x \in M$ let $f_x : R \to M$ s.t. $a \mapsto ax$.
   Claim: $\varphi : M \to \text{Hom}_R(R, M)$ s.t. $x \mapsto fx$ is an $R-$ mod isom.
   Proof:

   - $f_x \in \text{Hom}_R(R, M)$ which is easy.
   - $\varphi(x + y) = \varphi(x) + \varphi(y)$ which is clear.

- To show φ is an R-mod hom, still need to show $\forall b \in R, x \in M : \varphi(bx) = b\varphi(x)$. Note that $\varphi(bx) = f_{bx}$ and $b\varphi(x) = bf_x$.
  Let $a \in R$ then $f_{bx}(a) = abx$ and $bf_x(a) = bax$ but since R commutative, we see that $abx = bax$ so therefore indeed $f_{bx} = bf_x$. So $\varphi(bx) = b\varphi(x)$.
- φ injective. Let $x \in M \setminus \{0\}$ then $\varphi(x)(1) = f_x(1) = x \neq 0$ therefore φ injective.
- φ surjective. Let $f \in \operatorname{Hom}_R(R, M), \forall a \in R, \varphi(f(1))(a) = f(1) \cdot a$ since f R-mod hom. wew see that this is equal to $f(a)$. So $f = \varphi(f(1))$ so φ surjective.

Remark:
In book $\varphi^{-1} = \mathrm{ev}_1 : \operatorname{Hom}_R(R, M) \to M, f \mapsto f(1)$.
Remark:
We haven't said that $\operatorname{Hom}_R(R, M)$ is an R-modulo.

Lemma 13.4:

$$\operatorname{Hom}_R(M, N) \text{ is an } R-\text{ mod if } R \text{ commutative} \tag{Lem 13.4}$$

Proof:
When is $\operatorname{Hom}_R(M, N)$ an $R-$ mod? via $R \times \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(M, N)$ s.t. $(a, f) \mapsto af$ where $(af)(x) = af(x)$. To be this enough, we need $g = af : M \to N$ is an $R-$ mod hom. Let $b \in R, x \in M$, then $g(bx) = (af)(bx) = af(bx) = abf(x)$ $bg(x) = baf(x)$. These are equal if R is commutative.

From now one, we assume that R is commutative ring.

For $R-$ mod A we define $\operatorname{Hom}_R(A, -)$ takes an $R-$ mod M to the $R-$—,mod $\operatorname{Hom}_R(A, M)$ and it takes $R-$ mod $f \in \operatorname{Hom}_R(M, N)$ to $f_* \in \operatorname{Hom}_R(\operatorname{Hom}_R(A, M), \operatorname{Hom}_R(A, N))$ the PUSH FORWARD of f.
If $\varphi : A \to M$ and $f : M \to N$ then $f_*\varphi = f \circ \varphi$.
if $\varphi \in \operatorname{Hom}_R(A, M)$ then $f_*\varphi \in \operatorname{Hom}_R(A, N)$

Claim:
$f_* : \operatorname{Hom}_R(A, M) \to \operatorname{Hom}_R(A, N)$ is an $R-$ mod hom. so $a \in R, x \in A$ then $\varphi \in \operatorname{Hom}_R(A, M)$.
$f_*(a\varphi)(x) = f \circ (a\varphi)(x) = f(\varphi(ax)) = f(a\varphi(x)) = f(\varphi(x)) = a(f_*\varphi)(x)$

Question:
Let $f \in \operatorname{Hom}_R(M, N)$ when is f_* injective/surjective?
Surjective: If f is not surjective, then f_* is not surjective.

Example:
$R = \mathbb{Z} = M, N = \mathbb{Z}/2\mathbb{Z} = A$ then $f = \pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ s.t. $x \mapsto x \mod 2$ is surjective.
Then f_* is not surjective. $f_* : \mathrm{Hom}_{\mathbb{Z}} : (\mathbb{Z}/2\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$.
But we see that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}) = 0$ and $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ an dwe seee that $0 \to \mathbb{Z}/2\mathbb{Z}$ is not surjective, since sets are different size.
Injective: Let $f \in \mathrm{Hom}_R(M, N)$ injective,suppose $\varphi \in \ker f_*$ so $f(\varphi(x)) = 0, \forall x \in M$ so $\varphi(x) = 0, \forall x \in M$, so f_* is injective.

Theorem 13.5:

$$\text{Let } 0 \to M \xrightarrow{f} N \xrightarrow{g} P \text{ to be exact sequence of R-mod-homs}$$
$$\Rightarrow 0 \to \mathrm{Hom}_R(A, M) \xrightarrow{f_*} \mathrm{Hom}_R(A, n) \xrightarrow{g^*} \mathrm{Hom}_R(A, P) \text{ is exact} \qquad \text{(Thm 13.5)}$$

Proof:
Already discussed maps well-defined.
Exactness in $\mathrm{Hom}_R(A, M)$ is exact, since f_* is injective. (since f is injective since first line exact). $\mathrm{Hom}_R(A, N)$ exact requires $\mathrm{Im}(f_*) = \ker(g_*)$
Let $\psi \in \mathrm{im}(f_*)$ so $\psi = f_*\varphi$ for some $\varphi \in \mathrm{Hom}_R(A, M)$. Therefore $g_*(\psi) = g \circ f \circ \varphi$. Note that $g \circ f = 0$ since the first line is exact, therefore $g_*\psi = 0$ so $\psi \in \ker(g_*)$.
Now let $\beta \in \ker(g_*)$. Then $g \circ \beta(x) = 0$ for all $x \in M$ so $\mathrm{Im}(\beta) \subset \ker(g)$. Take $h := f^{-1} : \mathrm{im} f \to M$. IF we draw the scheme, we see that $\alpha = h \circ \beta$ so therefore $\beta = f \circ \alpha = f_*\alpha \in \mathrm{im}(f_*)$

Lecture 14

Split exact sequences

Example:

1. $0 \to M \xrightarrow{\iota_1} M \oplus P \xrightarrow{\pi_2} P \to 0$ where $\iota_1 : x \mapsto (x, 0)$ and $\pi_2 : (x, y) \mapsto y$.

A SES IS SPLIT/SPLITS if $\exists$ an $R-$ mod iso $\theta N \xrightarrow{\cong} M \oplus P$. S.t.

$$\begin{array}{ccccccccc} 0 & \to & M & \xrightarrow{f} & N & \xrightarrow{g} & P & \to & 0 \\ & & \| & & \cong\downarrow\theta & & \| & & \\ 0 & \to & M & \xrightarrow{\iota_1} & M \oplus P & \xrightarrow{\pi_2} & P & \to & 0 \end{array} \tag{a.14}$$

commutes

Examples:

1. Every SES of $K-$ vector spaces splits.
2. Nonexample: $0 \to \mathbb{Z} \xrightarrow{[2]} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} to 0$ where $[2]$ means that $x \mapsto 2x$ and $\pi : x \mapsto x \text{mod} 2$ is a non-split. Since if it is a split, then must have that the middle term $\mathbb{Z}$ must be isomorphic to $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ since $2(0, \overline{1}) = (0, \overline{0})$, so the right group has an element of order 2, while the LHS does not have an element of order 2.

Remark:

SES splits then $N \cong M \oplus P$ but ... see conrad splitting of.. Example 1.4.

For splittness, it's important and necessary that the maps in

$$0 \to M \to M \bigoplus P \to P \to 0 \tag{Form 14.1}$$

are ι_1 and π_2

If we have (Form 14.1) we see that we can also notice that $\pi_2 \circ \iota_2 = \text{id}_P$ and $\pi_1 \circ \iota_1 = \text{id}_M$.

14.2 (Splitting) Lemma:

Let $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ and $P \xrightarrow{h} N, N \xrightarrow{j} M$ SES Of R-mods, then following equiv.
1) above line splits
2) $\exists h \in \text{Hom}_R(P, N)$ s.t. $g \circ h = \text{id}_P$
3) $\exists j \in \text{Hom}_R(N, M)$ s.t. $j \circ f = \text{id}_M$
call h,j splittings of the line (Lem 14.2)

Proof:

$2 \Rightarrow 1$ Suppose 2), Let $\varphi : M \oplus P \to N$ s.t. $(x, y) \mapsto f(x)+h(y)$ then $\varphi \in \text{Hom}_R(M \oplus P, N)$.
Claim:

$$\begin{array}{ccccccccc} 0 & \to & M & \xrightarrow{\iota_1} & M \oplus P & \xrightarrow{\pi_2} & P & \to & 0 \\ & & \| & & \downarrow \varphi & & \| & & \\ 0 & \to & M & \xrightarrow{f} & N & \xrightarrow{g} & P & \to & 0 \end{array}$$

Commutes, so $\varphi \circ \iota_1 = f$ and $\pi_2 = g \circ \varphi$ since then we have $g(f(x) + h(y)) = g(f(x))+g(h(y)) = 0+y$. where the 0 follows from that N is exact, and the y follows from the condition that $g \circ h = \text{id}_P$.
It follows that φ is an isomorphism by exercise 2 on HW sheet 4, therfore we get indeed 1) By using $\theta := \varphi^{-1}$

$1 \Rightarrow 2$ Suppose $\exists \theta : N \to M \oplus P$ isomorphism s.t. (a.14) commutes. define $h : P \to N$ s.t. $y \mapsto \theta^{-1}(\iota_2(y))$ therefore $g \circ h(y) = g(\theta^{-1}(0, y))$ by commutative of diagram, $\pi_2 \circ \theta = g$ therefore $g(\theta^{-1}(0, y)) = \pi_2(\theta(\theta^{-1}(\iota_2(y)))) - \pi_2(\iota_2(y)) = y$ so we get indeed $g \circ h = \text{id}_P$

Note that $1 \Rightarrow 3$ is similair to $1 \Rightarrow 2$ and $3 \Rightarrow 1$ is similair to $2 \Rightarrow 1$.

Lemma 14.3:

$$\begin{aligned} &\text{supp.}\, N \xrightarrow{g} P, P \xrightarrow{h} N \,\text{are R-mod-homs s..t.}\, g \circ h = \text{id}_P \,\text{Then} \\ &1)\, g\,\text{surjective} \\ &2)\, 0 \to \ker(g) \xrightarrow{\iota} N \xrightarrow{g} P \to 0\,\text{is exact} \\ &3)\, N \cong \ker(g) \bigoplus P = \ker(g) \bigoplus \text{im}(g) \end{aligned} \qquad \text{(Lem 14.3)}$$

We call h a section of g.
Proof:

1. $\forall y \in P, \exists z \in Y$ s.t. $g \circ h(z) = y$ we see that we can take $z = y$. So $\exists x \in N$ s.t. $g(x) = y$ so g is indeed surjective (Where $x = h(y)$)
2. By 1, and that there is always an SES by the image of g.
3. $\cong$ by (Lem 14.2) from $2 \Rightarrow 1$, $=$ by $N = \text{im}(g)$

Projective modules

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow h & & \\ M & \xrightarrow{f} & N & \to & 0 \end{array}, \text{with}\, h \in \text{Hom}_R(P, N) \&\text{row exact} \qquad \text{(cond 14.4)}$$

If all (cond 14.4) holds, then P is PROJECTIVE if there $\exists \tilde{h} \in \text{Hom}_R(P, M)$ s.t. $h = f \circ \tilde{h}$ (so $h = f_*(\tilde{h})$ so $h \in \text{im} f_*$), see last picture.

14.5 Proposition:

$$F\,\text{free}\, R - \text{mod} \Rightarrow F\,\text{proj} \qquad \text{(Prop 14.5)}$$

Proof:
F free, so $F \cong \bigoplus_{i \in I} R$. Since F free, fix basis (b_i) of F. Consider diagram like (cond 14.4) , $\forall i \in I, \exists x_i \in M$ s.t. $h(b_i) = f(x_i)$. Define $\tilde{h}(b_i) = h(b_i)$. Now extend $\tilde{h}$ linearly to $\tilde{h} \in \text{Hom}_R(F, M)$ then $f \circ \tilde{h} = h$.

Extend linearly: $\forall z \in F, \exists!(\lambda_i)_{i \in I}$ for all $i \in R$ s.t. $z = \sum_{i \in I} \lambda_i b_i$. Define $\tilde{h}(z) = \sum \lambda_i \tilde{h}(b_i)$. Here we have finitely many λ_i nonzero. (So z is finite sum).

Lemma 14.6

$$\forall R - \text{mod}\, M, \exists \text{free}\, R - \text{mod F}\&\pi \in \text{Hom}_R(F, M)\, \text{surjective, so we have}\, F \xrightarrow{\pi} M \to 0 \tag{Lem 14.6}$$

Proof:

$F = \bigoplus_{x \in M} R$ is free with basis (e_x) s.t. $x \in M$. Where $(e_x)_y = \delta_{xy} = \begin{cases} 1 \text{ if } x = y \\ 0 \text{ otherwise} \end{cases}$

Then define $\pi(ex) = x$ and extend linearly, and we can observe that this π is indeed surjective.

Note that if $F = \bigoplus_{i \in I} R$ if $I = \{1, 2, 3\}$ then $F = R \oplus R \oplus R = R^3$.

Therefore $F = \bigoplus_{x \in M} R \begin{cases} = R^{|M|} \text{ if } |M| < \infty \\ \text{submod of } R^{\mathbb{N}} \text{ if } |M| = \#\mathbb{N} \end{cases}$

Theorem 14.7:

$$\begin{aligned} &\text{following equivalent} \\ &1)\, P\, \text{projective} \\ &2)\, \text{every SES with}\, P\, \text{at the end splits} \\ &3)\, \exists\, \text{free}\, R - \text{mod}\, F\&\text{an}\, R - \text{mod}\, Q\, \text{s.t.}F = P \bigoplus Q \end{aligned} \tag{Thm 14.7}$$

Proof:

1 ⇒ 2 By Lemma from L13, 2 follows from following claim: Every SES $0 \to \ker(g) \to N \xrightarrow{g} P \to 0$ splits.
Proof of claim:
Consider $\begin{array}{ccc} & P & \\ & \downarrow \text{id}_P & \\ N \xrightarrow{g} & P & \to 0 \end{array}$ then P projective, implies $\exists \tilde{h} : P \to N$ s.t. $g \circ \tilde{h} = \text{id}_p$. Then by splitting Lemma, we get 2.

2 ⇒ 3 Suppose 2, by (Lem 14.6), ∃ free F and SES $0 \to \ker(\pi) \xrightarrow{\iota} F \xrightarrow{\pi} P \to 0$. Then $F \cong \ker(\pi) \oplus P$, which is even more precies then part 3).

3 ⇒ 1 . Suppose 3), Let $F \cong P \oplus Q$, be free consider (cond 14.4), then since F projective, we can repace P by $P + Q$, so we see that $\exists \tilde{h}' : P \oplus Q \to M$. But we want $\tilde{h} : P \to M$. Therefore use that $\iota_1 : P \to P \oplus Q$ and $\tilde{h}' : P \oplus Q \to M$ then we can define $\tilde{h} := \tilde{h}' \circ \iota_1$.
Now observe $f \circ \tilde{h} = f \circ \tilde{h}' \circ \iota_1 = h \circ \pi_1 \circ \iota_1 = h \circ \text{id}_P$ so this implies 1)

Exercise:

1. Every $K-$ vector space is projective.

2. R PID $\Rightarrow$ every projective $R-$ mod is free, by 3 of (Thm 14.7), since every submod of a free $R-$ mod is free.

3. Claim: $\mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}/6\mathbb{Z}-$ mod. This is because a free modulo of $\mathbb{Z}/6\mathbb{Z}$ is of order infinity or a factor of 6.
   But it is proj $\mathbb{Z}/6\mathbb{Z}$ since $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Since $\mathbb{Z}/6\mathbb{Z}$ is a free $\mathbb{Z}/6\mathbb{Z}$ modulo, we can write this as $\mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/3\mathbb{Z}$.

4. If the modulo on the right is R, then the sequence must split.

Lecture 15

R commutative ring
Extra curriculum:

Fix $R-$ mod A. Then any $R-$ mod, M gives that $\text{Hom}_R(A,M)$ isan R ,mod.

S.t. $f: M \to N, \varphi: A \to M$ and $f_*\varphi = f \circ \varphi: A \to N$ is associative diagram.

A CATEGORY $\mathcal{C}$ consists of objects $(\text{ob}(\mathcal{C}))$, morphisms,$(\text{mor}(\mathcal{C})$ between objects $A \xrightarrow{f} B$ where $A, B \in \mathcal{C}$.
MORPHISM: or arrows, that has domains and codomains.
In this case, write $f \in \text{hom}(A,B)$ (This does not imply that f is a homomorphisms, only a morphism from A to B.)

$\exists$ map $\circ: \text{Hom}(A,B) \times \text{Hom}(B,C) \to \text{Hom}(A,C)$ with $(f,g) \mapsto g \circ f$
This is:

- $\circ$ is associative
- $\forall A \in \text{ob}(\mathcal{C}), \exists \text{id}_A \in \text{hom}(A,A)$ s.t. $\forall f \in \text{Hom}(A,B)$ we have $\text{id}_B \circ f = f = f \circ \text{id}_A$

Example:

$\mathcal{C}$	$\text{Ob}(\mathcal{C})$	$\text{mor}(\mathcal{C})$
set	sets	maps
R-mod	$R-$ mods	$R-$ mod-homs
Group	Groups	Group homomorphisms
Top	Topology spaces	cont. functions
Rel	Sets	Relations

Rel, stands for all sets with relations (For example $\text{Hom}(A,B) = \{R \subset A \times B\}$)
$R \subset A \times B, S \subset B \times S \Rightarrow S \circ R = \{(a,c) \in A \times C : \exists b \in B : (a,b) \in R \& (b,c) \in S\}$

FUNCTOR $F: \mathcal{C}_1 \to \mathcal{C}_2$ is a "morphism between categories", i.e.,

- $F(\text{ob}(\mathcal{C}_1)) \subset \text{ob}(\mathcal{C}_2)$
- $F(\text{mor}(\mathcal{C}_1)) \subset \text{mor}(\mathcal{C}_2)$
- $F(\text{id}_A) = \text{id}_F(A)$
- $F(f \circ g) = \begin{cases} F(f) \circ F(g) \text{ call F covariant or} \\ F(g) \circ F(f) \text{ call F contravariant} \end{cases}$

Example:

Forgetful functor R-mod $\to$set s.t.
,M R-mod $\mapsto M$ as a set and $f \in \mathrm{Hom}_R(A, B) \mapsto f : A \to B$ as map.
Also works for example for groups,Top
This function is Covariant.

Hom-functor Fix R mod A s.t. $\mathrm{Hom}_R(A, -)$: R-mod $\to$ R-mod s.t. $M \mapsto \mathrm{Hom}_R(A, M)$ and for $f \in \mathrm{Hom}_R(M, N)$ we have $f \mapsto f_*$ with $f_* \in \mathrm{Hom}_R(\mathrm{Hom}_R(A, M), \mathrm{Hom}_R(A, N))$

A function F R-mod $\to$ R-mod is LEFT EXACT if for all exact sequences
$0 \to M \xrightarrow{f} N \xrightarrow{g} P$ also the sequence $0 \to F(M) \xrightarrow{F(f)} F(N) \xrightarrow{F(g)} F(P)$ is exact.
A function F R-mod $\to$ R-mod is LEFT EXACT if for all exact sequences
$M \xrightarrow{f} N \xrightarrow{g} P \to 0$ also the sequence $F(M) \xrightarrow{F(f)} F(N) \xrightarrow{F(g)} F(P) \to 0$ is exact.
F isEXACT if it is left and right exact.

Recall:$\mathrm{Hom}_R(A, -)$ is left exact, but in general not right exact.

Theorem 15.1:

$$A \text{ R-mod, then } \mathrm{Hom}_R(A, -) \text{ is right exact iff } A \text{ projective} \tag{Thm 15.1}$$

Proof $\Leftarrow$
Suppose A projective, Let $M \xrightarrow{f} N \xrightarrow{g} P \to 0$. We want that
$\dagger : \mathrm{Hom}_R(A, M) \xrightarrow{f_*} \mathrm{Hom}_R(A, N) \xrightarrow{g_*} \mathrm{Hom}_R(A, P) \to 0$ is exact.

g_* is surjective: Let $\varphi \in \mathrm{Hom}_R(A, P)$. Consider $\begin{array}{ccccc} & & A & & \\ & \swarrow \exists h & \downarrow \varphi & & \\ N & \xrightarrow{g} & P & \to & 0 \end{array}$ so A projective
hence $\exists h \in \mathrm{Hom}_R(A, N)$ s.t. $\varphi = g \circ h = g_* h$ (so found pre-image namely h)

$\mathrm{im} f_* \subset \ker(g_*$ follows from $g \circ f = 0$

$\ker(g_* \subset \mathrm{im}(f_*)$ Let $\psi \in \ker(g_*)$ i.e. $g \circ \psi = 0$ so
,$\mathrm{im}\psi \subset \ker(g)$, but we saw that ,$\ker(g) = \mathrm{im} f$, since original sequence is exact.
Consider $\begin{array}{ccccc} & & A & & \\ & \swarrow \exists h & \downarrow \psi & & \\ M & \xrightarrow{f} & \mathrm{im}(f) & \to & 0 \end{array}$ since A projective, $\exists h \in \mathrm{Hom}_R(A, M)$ s.t. $\psi = f \circ h = f_* h$ so $\psi \in \mathrm{im} f_*$.

Therefore we see that $\dagger$ is exact.

Proof ⇒

Suppose A is not projective, ⇒ ∃ diagram
$$\begin{array}{ccccc} & & A & & \\ & & \downarrow \varphi & & \\ N & \xrightarrow{g} & P & \to & 0 \end{array}$$
s.t. $\nexists h \in \text{Hom}_R(A, N)$ with $\varphi = g \circ h$. i.e. $\varphi \in \text{Hom}_R(A, P) \setminus \text{im}(g_*)$ so $\ker(g) \xrightarrow{\iota} N \xrightarrow{N} \xrightarrow{g} P \to 0$ is exact but $\text{Hom}_R(A, \ker(g)) \xrightarrow{\iota_*} \text{Hom}_R(A, N) \xrightarrow{g_*} \text{Hom}_R(A, P) \to 0$ is not exact.

Snake Lemma:

For $\alpha \in \text{Hom}_R(A, A')$, def. $\text{coker}(\alpha) = A'/\text{im}(\alpha) = A'/\alpha(A)$

Consider comm. diagram of R-mod-homs, with exact rows (black), then ∃ exact sequence (blue)

$$\begin{array}{ccccccccc} & & \ker(\alpha) & \xrightarrow{f} & \ker(\beta) & \xrightarrow{g} & \ker(\gamma) & & \\ & & \downarrow \iota & & \downarrow \iota & & \downarrow \iota & & \\ 0 & \to & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \to & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \to & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \to & 0 \\ & & \downarrow \pi & & \downarrow \pi & & \downarrow \pi & & \\ & & \text{coker}(\alpha) & \xrightarrow{\tilde{f'}} & \text{coker}(\beta) & \xrightarrow{\tilde{g'}} & \text{coker}(\gamma) & & \end{array}$$

and $\delta : \ker(\gamma) \to \text{coker}(\alpha)$

Where $f : \ker(\alpha) \to \ker(\beta)$ is well defined, since $x \in \ker(\alpha) \Rightarrow \beta(f(x)) = f'(\alpha(x)) = 0$ since commutative, so $f(x) \in \ker(\beta)$

Similarly $g : \ker(\beta) \to \ker(\gamma)$ is well-defined.

$\tilde{f}(y + \alpha(A)) = f'(y) + \beta(B)$ is well-defined, since if $y \in \alpha(A)$ say $y = \alpha(x)$ for $x \in A$, then $f'(y) = \beta(f(x)) \in \beta(B)$.

Similarly $\tilde{g'}$ is well-defined.

δ is called connecting homomorphism, $\delta : \ker(\gamma) \to \text{coker}(\alpha)$ for $c \in \ker(\gamma)$, there exists $b \in B$ s.t. $g(b) = c$ since g is surjective (g is not necessarily surjective).

Since $c \in \ker(\gamma)$, we see that $g'(\beta(b)) = 0$, by commutative diagram, so $\beta(b) \in \ker(g')$.

Since exactness, we see that $\ker(g') = \text{im}(f')$ so $\exists a' \in A$ s.t. $\beta(b) = f'(a')$.

Define $\delta(c) = \pi(a') = a' + \alpha(A)$

δ is well-defined, since f' is injective, we see there exists unique $a' \in A'$ s.t. $f'(a') = \beta(b)$.

Furthermore we must have δ indep. of choice of b. Suppose $b_1 \in B$ s.t.] $g(b_1) = c$. Therefore $b - b_1 \in \ker(g)$, so, $b - b_1 \in \text{im}(f)$. Therefore exists unique $a \in A$ s.t. $f(a) = b - b_1$. So $\beta(b) - \beta(b_1) = f'(\alpha(a))$, so if $a'_1 \in A'$ s.t. $f'(a'_1) = \beta(b_1)$. Then $a' - a'_1 \in \alpha(A)$, so $\pi(a') = \pi(a'_1)$, so indep. of choices of b.

Complete Proof in Top's notes.

R commutative ring, M, N, S R-mods, then $b : M \times N \to S$ is BILINEAR, if $\forall m \in M, \forall n \in N$, we have that $M \to S$ s.t. $x \mapsto b(x, n)$ and $N \to S$ s.t. $y \mapsto b(m, y)$ are R-mod-homs.
Examples:

- Dot product
- Matrix multiplication
- Scalar products
- $R \times M \to M$ s.t. $(a, m) \mapsto a \cdot m$

A TENSOR PRODUCT of $M \& N$ (over R) is a pair (T, β), where T is an $R-$ and $\beta : M \times N \to T$ bilinear, s.t. $\forall$ pairs (S, b) where S is an $R-$ mod and $b : M \times N \to S$ bilinear, then $\exists! f \in \mathrm{Hom}_R(T, S)$ s.t. $\begin{matrix} M \times S & \xrightarrow{b} & S \\ \downarrow \beta & \nearrow f & \\ T & & \end{matrix}$ is a commutative diagram

Catch-up session 04-04-2024

Universal property Tensor products:
$\mathrm{Hom}_{R-\mathrm{mod}}(M \otimes_R N, L) \cong \mathrm{Bilin}(M \times N, L)$.

For example: $R \otimes_R M \cong M$
Note that Tensor product was extra curriculum.

$\mathrm{Tor}_R(M) = \{x \in M : \exists 0 \neq r \in R : rx = 0\}$
$\mathrm{Tor}_{\mathbb{Z}}(\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) = 0 \oplus \mathbb{Z}/2\mathbb{Z}$

NEED TO REMEMBER

L/K SEPERABLE iff $\forall \alpha \in L, \text{minpol}(\alpha)$ has no multiple roots in $\text{Spl}_K(\text{minpol}(\alpha))$

L/K NORMAL iff $\forall \alpha \in L, \text{minpol}(\alpha)$ splits completely into linear terms over L.

$\text{Tor}(M) \coloneqq \{x \in M : \exists a \in R \setminus \{0\} : ax = 0\}$
$\text{Ann}(M) \coloneqq \{a \in R : ax = 0, \forall x \in M\}$
$\text{Ann}(M) \neq \{0\} \Rightarrow \text{Tor}(M) = M$.

Equivalent:

1. P projective.

   P projective if we have $\begin{array}{ccccc} & & P & & \\ & & \downarrow h & & \\ m & \xrightarrow{f} & N & \to & 0 \end{array}$ there exists $\tilde{h} \in \text{Hom}_R(P, M) : h = f \circ \tilde{h}$.

2. Every SES with P at the end, splits:
   SES: $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ s.t. $\text{im}(f) = \ker(g)$
   SES Splits, if $\exists \theta \in \text{Hom}(N, M \oplus P)$ isomorphic s.t.

$$\begin{array}{ccccccccc} 0 & \to & M & \xrightarrow{f} & N & \xrightarrow{g} & P & \to & 0 \\ & & \| & & \downarrow \theta & & \| & & \\ 0 & \to & M & \xrightarrow{\pi_1} & M \oplus P & \xrightarrow{\pi_2} & P & \to & 0 \end{array}$$

3. Exists free R mod F, R mod Q s.t. $F = P \oplus Q$.
   F is free R mod s.t. $\exists I$ s.t. $F = \bigoplus_{i \in I} R$.

Note that F free $\Rightarrow$ F torsion free.