Trace & Norm

E/F finite field extension.

Let $u \in E$. Def. $m_u : E \longrightarrow E$, $m_u(\sigma) = u \cdot \sigma$. F-linear map!

Def $T_{E/F}(u) = \mathrm{Tr}(m_u) \in F$ and $N_{E/F}(u) = \det(m_u) \in F$.

> Example $u = a + ib \in \mathbb{C}$, $a, b \in \mathbb{R}$. $T_{\mathbb{C}/\mathbb{R}}(u) = 2a$
> $\mathbb{C}$ has basis $\{1, i\}$. $m_u = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ $N_{\mathbb{C}/\mathbb{R}}(u) = a^2 + b^2$

Properties Let $u, v \in E$, $a \in F$.

- $T_{E/F}(u+v) = T_{E/F}(u) + T_{E/F}(v)$
- $T_{E/F}(au) = a\, T_{E/F}(u)$

$\Big\}$ $T_{E/F} : E \longrightarrow F$ is F-linear.

- $N_{E/F}(uv) = N_{E/F}(u)\, N_{E/F}(v)$
- $N_{E/F}(au) = a^n N_{E/F}(u)$, $n = [E:F]$.
- $T_{E/F}(1) = n = [E:F]$
- $N_{E/F}(1) = 1$.

Note: $N_{E/F} : E^* \longrightarrow F^*$ group hom.

Prop Assume E/F finite Galois, $\mathrm{Gal}(E/F) = \{\sigma_1, \dots, \sigma_n\}$, $u \in E$.

Then $T_{E/F}(u) = \sum_{i=1}^{n} \sigma_i(u)$ and $N_{E/F}(u) = \prod_{i=1}^{n} \sigma_i(u)$.

~~Proof~~

~~Assume first $E = F(u)$.~~

~~Min. poly $f(x) = x^n + b_{n-1}x^{n-1} + \dots + b_0 \in F[x]$ for u.~~

~~$f(x) = \prod_{i=1}^{n} (x - \sigma_i(u))$.~~

~~E has basis $\{1, u, u^2, \dots, u^{n-1}\}$.~~

$$m_u = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & -b_0 \\ 1 & 0 & 0 & 0 & 0 & -b_1 \\ 0 & 1 & 0 & 0 & 0 & -b_2 \\ 0 & 0 & 1 & 0 & 0 & \vdots \\ 0 & 0 & 0 & 1 & 0 & \\ 0 & 0 & 0 & 0 & 1 & -b_{n-1} \end{bmatrix}$$

$$\mathrm{Tr}(m_u) = -b_{n-1} = \sum_{i=1}^{n} \sigma_i(u)$$

$$\det(m_u) = (-1)^n b_0 = \prod_{i=1}^{n} \sigma_i(u)$$

Proof: $K = F(u)$. $d = [K:F]$, $m = [E:K]$, $dm = n$.

Min. poly for u /F: $f(x) = x^d + b_{d-1}x^{d-1} + \cdots + b_0 \in F[x]$.

Basis for K/F: $\{1, u, \ldots, u^{d-1}\}$

Basis for E/K: $\{w_1, w_2, \ldots, w_m\}$.

Set $K_j = K \cdot w_j = \mathrm{span}_F\{w_j, uw_j, \ldots, u^{d-1}w_j\}$.

$m_u : K_j \longrightarrow K_j$, Matrix:

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & -b_0 \\ 1 & 0 & 0 & 0 & -b_1 \\ 0 & 1 & 0 & 0 & \vdots \\ 0 & 0 & 1 & 0 & \\ 0 & 0 & 0 & 1 & -b_{d-1} \end{bmatrix}$$

Matrix for $m_u : E \longrightarrow E$: $E = K_1 \oplus \cdots \oplus K_m$

$$m_u = \begin{bmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{bmatrix}$$

$$N_{E/F}(u) = \det(m_u) = \det(A)^m = ((-1)^d b_0)^m = (-1)^n b_0^m$$

$$T_{E/F}(u) = \mathrm{Tr}(m_u) = m\,\mathrm{Tr}(A) = -m\,b_{d-1}$$

Consider $\eta_1(u), \eta_2(u), \ldots, \eta_n(u)$.

Each $\eta_i(u)$ is a root of $f(x)$, each root appears m times.

$$\Rightarrow \prod_{i=1}^{n} (x - \eta_i(u)) = f(x)^m.$$

$$(-1)^n \prod_{i=1}^{n} \eta_i(u) = \text{const. term} = b_0^m$$

$$-\sum_{i=1}^{n} \eta_i(u) = \text{coef. of } x^{n-1} = m\,b_{d-1}.$$

$\square$

Example $E = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$ square free, $m \neq 0, 1$.

$E = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$. $\mathrm{Gal}(E/\mathbb{Q}) = \{1, \eta\}$, $\eta(a + b\sqrt{m}) = a - b\sqrt{m}$.

$$N_{E/\mathbb{Q}}(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2$$

$$T_{E/\mathbb{Q}}(a + b\sqrt{m}) = 2a.$$

<u>Thm</u> E/F finite Galois, $G = Gal(E/F)$.

Let $\varphi : G \longrightarrow E^*$ be any map satisfying

$$\varphi(\xi\eta) = \varphi(\xi) \cdot \xi(\varphi(\eta)) \quad \forall\ \xi, \eta \in G.$$

Then $\exists\ 0 \neq v \in E$ s.t. $\varphi(\eta) = v \cdot \eta(v)^{-1} \quad \forall\ \eta \in G.$

<u>Note:</u> converse is clear!

<u>Proof</u> Linear indep. of characters $\Rightarrow \sum_{\eta \in G} \varphi(\eta) \cdot \eta \neq 0 \in Hom_F(E, E)$.

Choose $w \in E$ s.t. $\sum_{\eta \in G} \varphi(\eta) \cdot \eta(w) \neq 0 \in E$. Def. $v = \sum_{\eta \in G} \varphi(\eta) \cdot \eta(w) \neq 0$.

Let $\xi \in G$.

$$\xi(v) = \sum_{\eta \in G} \xi(\varphi(\eta)) \cdot \xi\eta(w) = \sum_{\eta \in G} \varphi(\xi\eta)\, \varphi(\xi)^{-1} (\xi\eta(w))$$

$$= \left(\sum_{\eta \in G} \varphi(\xi\eta) \cdot (\xi\eta)(w) \right) \cdot \varphi(\xi)^{-1} = \left(\sum_{\eta \in G} \varphi(\eta) \cdot \eta(w) \right) \cdot \varphi(\xi)^{-1}$$

$$= v \cdot \varphi(\xi)^{-1}$$

$\Rightarrow \varphi(\xi) = v \cdot \xi(v)^{-1}$!

$\square$

<u>Hilbert's Thm 90</u> E/F cyclic Galois, $Gal(E/F) = \langle \eta \rangle$. Let $u \in E$.

Then $N_{E/F}(u) = 1 \iff \exists\ v \in E : u = v \cdot \eta(v)^{-1}$.

<u>Proof</u>

$\Leftarrow$: $N_{E/F}(u) = N_{E/F}(v) \cdot N_{E/F}(\eta(v)^{-1}) = N(v) \cdot N(v)^{-1} = 1$.

$\Rightarrow$: Def. $\varphi : G \longrightarrow E^*$ by

$$\varphi(\eta^i) = u \cdot \eta(u) \cdot \eta^2(u) \cdots \eta^{i-1}(u), \quad \text{for } 1 \leq i \leq n = [E:F]$$

$\boxed{\text{Note: } \varphi(1) = \varphi(\eta^n) = N(u) = 1.}$ $\boxed{\varphi(\eta) = u.}$

If $i+j \leq n$ then $\varphi(\eta^i \cdot \eta^j) = u \cdot \eta(u) \cdot \eta^2(u) \cdots \eta^{i+j-1}(u) = \varphi(\eta^i) \cdot \eta^i(\varphi(\eta^j))$

If $i+j > n$ then $\varphi(\eta^i \cdot \eta^j) = \varphi(\eta^{i+j-n}) = \varphi(\eta^n) \cdot \eta^n(\varphi(\eta^{i+j-n}))$

$$= u \cdot \eta(u) \cdot \eta^2(u) \cdots \eta^{i+j-1}(u) = \varphi(\eta^i) \cdot \eta^i(\varphi(\eta^j)).$$

Thm $\Rightarrow \exists\ v \in E^*$ s.t. $u = \varphi(\eta) = v \cdot \eta(v)^{-1}$.

<u>Hilbert's Thm 90</u> E/F cyclic Galois, $Gal(E/F) = \langle \eta \rangle$, $u \in E$.

Then $N_{E/F}(u) = 1 \iff \exists\, v \in E : v \cdot \eta(v)^{-1}$.

<u>Cor</u> E/F cyclic Galois, $[E:F] = n$. Assume F contains n distinct n-th roots of 1.
Then $E = F(u)$ for some $u \in E$ with $u^n \in F$.

Note: Already proved this for $n = p$ prime.

<u>Proof</u> $z \in F$ primitive n-th root of 1.

$$N_{E/F}(z) = \prod_{i=0}^{n-1} \eta^i(z) = z^n = 1.$$

Hilbert $\Rightarrow$ $\exists\, u \in E$: $z = u \cdot \eta(u)^{-1}$.

$$1 = z^n = u^n \cdot \eta(u^n)^{-1} \Rightarrow \eta(u^n) = u^n \Rightarrow u^n \in F.$$

If $u^m \in F$ then $z^m = u^m \cdot \eta(u^m)^{-1} = 1 \Rightarrow m \geq n$.

Min poly for u/F : $x^n - u^n = \prod_{i=0}^{n-1}(x - z^i u)$.

(Any proper factor has const term $z^t u^m$, $m < n$, so $\notin F$.)

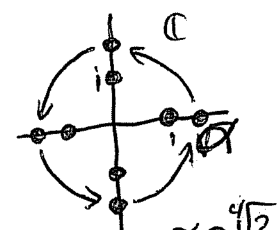
$\therefore [F(u):F] = n$, $E = F(u)$.

$\square$

<u>Example</u> $F = \mathbb{Q}(\sqrt{-1})$, [redacted] $E = F(\sqrt[4]{2})$.

$Gal(E/F) = \langle \eta \rangle$, $\eta(\sqrt{-1}) = \sqrt{-1}$, $\eta(\sqrt[4]{2}) = i\sqrt[4]{2}$.

$z = -\sqrt{-1}$. $z = \alpha \cdot \eta(\alpha)^{-1}$.



$\alpha = \sqrt[4]{2}$

$\boxed{\text{Additive Analogues from last time.}}$

Commutative Rings

Will study ring R that is commutative ($ab=ba$ $\forall a,b\in R$) with $1\in R$.

Recall: R is Noetherian

$\Updownarrow$ Every chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ stabilizes: $\exists N: I_N = I_{N+1} = \cdots$

$\Updownarrow$ Every non-empty set of ideals in R has a maximal element.

k field $\Rightarrow$ $k[x_1,\dots,x_n]$ Noetherian.

Hilbert basis Thm R Noetherian $\Rightarrow$ $R[x_1,\dots,x_n]$ Noetherian.

Close relation: Com. algebra $\Leftrightarrow$ algebraic geometry.

k field. $\mathbb{A}^n = k^n$ affine space of dim. n.

$f\in k[x_1,\dots,x_n]$ defines $f: \mathbb{A}^n \to k$, $(a_1,\dots,a_n)\mapsto f(a_1,\dots,a_n)$.

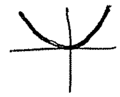
Exercise: k infinite: $f=0$ as a function $\Leftrightarrow$ $f=0$ as a polynomial.

Cor $f\neq g \in k[x_1,\dots,x_n]$ $\Rightarrow$ $f\neq g: \mathbb{A}^n \to k$.

$\therefore$ $k[x_1,\dots,x_n]$ = ring of polynomial functions $\mathbb{A}^n \to k$. (still $|k|=\infty$)

Def $I\subseteq k[x_1,\dots,x_n]$ subset.

$Z(I) = \{a\in\mathbb{A}^n \mid f(a)=0 \ \ \forall f\in I\}$. algebraic set

Example $Z(y-x^2) =$  $\subseteq \mathbb{R}^2$.

Note: 1) If $J=\langle I\rangle \subseteq k[x_1,\dots,x_n]$ then $Z(J)=Z(I)$.

2) $\bigcap_\alpha Z(I_\alpha) = Z(\bigcup I_\alpha)$

$Z(I_1)\cup\cdots\cup Z(I_m) = Z(I_1\cdot I_2\cdot\dots\cdot I_m)$, $I_1\cdot I_2\cdots I_m = \{a_1a_2\cdots a_m \mid a_i\in I_i$

$Z(0)=\mathbb{A}^n$, $Z(1)=\emptyset$.

$\therefore$ Algebraic sets give closed sets of topology on $\mathbb{A}^n$. Zariski topology.

Q: What is a Zariski-open subset of $\mathbb{R}$?

Def Given $X\subseteq\mathbb{A}^n$, set $I(X)=\{f\in k[x_1,\dots,x_n] \mid f(a)=0 \ \ \forall a\in X\}$

Examples: 1) $I(\mathbb{A}^n)=\{0\}$.

2) $|k|=\infty$: $I(Z(y-x^2)) = \langle y-x^2\rangle \subseteq k[x,y]$.

3) $k=\mathbb{C}$. $X=\mathbb{Z}^n\subseteq\mathbb{A}^n$. Then $I(\mathbb{Z}^n)=\{0\}\subseteq\mathbb{C}[x_1,\dots,x_n]$.

Note: $I(X)\subseteq k[x_1,\dots,x_n]$ always ideal.

Pf (2): $f(x,y)\in I(X)\subseteq k[x,y]$.
Poly div. by $y-x^2$ in $k[x][y]$:
$f(x,y)=q(x,y)\cdot(y-x^2)+r(x)$.
$a\in k \Rightarrow$ $f(a,a^2) = q(a,a^2)(a^2-a^2)+r(a)$

$r=0$ $\Uparrow$

Note: Let $f, g \in k[x_1, \dots, x_n]$. $X \subseteq \mathbb{A}^n$ subset.
If f, g define same function $X \to k$, then $f - g \in I(X)$
$\Rightarrow \bar{f} = \bar{g} \in k[x_1, \dots, x_n]/I(X)$.

Def $A(X) = k[x_1, \dots, x_n]/I(X)$ coordinate ring of X = ring of poly fcns on X.

Exercise 1) $I \subseteq I(Z(I))$
2) $X \subseteq Z(I(X))$. = Zariski closure of X.

Q: Which ideals have form $I = I(X)$?

Def R com. ring, $I \subseteq R$ ideal.
I is radical if $f^n \in I, n \geq 1 \Rightarrow f \in I$.

Note: $X \subseteq \mathbb{A}^n \Rightarrow I(X) \subseteq k[x_1, \dots, x_n]$ radical ideal.

Example $\langle x^2+1 \rangle \subseteq \mathbb{R}[x]$ is radical but not equal to $I(X)$, $X \subseteq \mathbb{R}$.
Why?

Def $I \subseteq R$ ideal. $\sqrt{I} = \mathrm{rad}(I) = \{f \in R \mid \exists n \geq 1 : f^n \in I\}$.

Exercise 1) $\sqrt{I} \subseteq R$ radical ideal.
2) I radical ideal $\Leftrightarrow I = \sqrt{I}$.
3) Prime ideals are radical.

Def k field. k is alg. closed if every poly $f(x) \in k[x]$ has a root.
Equivalent: If $k \subseteq E$ finite/alg. extension then $E = k$.

Fact: Any field k has an algebraic closure $\bar{k}$. ($\bar{k}$ alg. closed, $k \subseteq \bar{k}$ alg.)
All alg. closures of k are isomorphic. (not canonically.)

Exercise k alg. closed $\Rightarrow |k| = \infty$.

Hilbert's Nullstellensatz

$k = \bar{k}$ alg. closed, $I \subseteq k[x_1, \dots, x_n]$ ideal.
Then $I(Z(I)) = \sqrt{I}$.

Examples 1) $\bar{\mathbb{R}} = \mathbb{C}$.
$\bar{\mathbb{Q}} = \{a \in \mathbb{C} \mid a \text{ alg. over } \mathbb{Q}\}$
$= \{a \in \mathbb{C} \mid \mathbb{Q} \subseteq \mathbb{Q}(a) \text{ finite ext.}\}$

$\overline{\mathbb{Z}/p\mathbb{Z}} = \bigcup_{q = p^m} \mathbb{F}_q$ union of all finite fields of char p.

<u>Def</u> k field. Any ring of the form $R \cong k[x_1, \dots, x_n]/I$ is called an <u>affine ring</u> over k

<u>Thm</u> (Noether's Normalization Theorem)

Let R be any affine ring over k. Then $\exists\, y_1, \dots, y_r \in R$ s.t. $y_1, \dots, y_r$ alg. indep. over k and R is a finitely generated module over the subring $S = k[y_1, \dots, y_n] \subseteq R$.

<u>Proof</u> Induction over # generators for R. (n).

$n = 0 \Rightarrow R = k$. $S = k$, ok!

Assume R generated by n elts, $R = k[x_1, \dots, x_n]/I$.

WLOG: $I \neq 0$.

Let $0 \neq f \in I$.

<u>Assume f monic in x_n</u>: $f = x_n^d + f_{d-1} x_n^{d-1} + \dots + f_0$, $f_i \in k[x_1, \dots, x_{n-1}]$

Then $k[x_1, \dots, x_n]$ is a finite module over $T = k[x_1, \dots, x_{n-1}, f] \subseteq k[x_1, \dots, x_n]$

In fact, $k[x_1, \dots, x_n]$ free T-module with basis $1, x_n, \dots, x_n^{d-1}$.

$\Rightarrow R = k[x_1, \dots, x_n]/I$ finite module over $T/I \cap T$.

$T/I \cap T$ generated by $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_{n-1}$. since $f \in I$.

Induction: $\exists\, y_1, \dots, y_r \in T$ s.t. $y_1, \dots, y_r$ alg. indep. $/k$ and $T/_{I \cap T}$ finite module over $S = k[y_1, \dots, y_r]$.

$S \subseteq T/_{I \cap T} \subseteq R$. $T/_{I \cap T}$ f.g. S-module + R f.g. $T/_{I \cap T}$-mod.
$\Rightarrow R$ f.g. S-module.

Strategy: Find non-zero poly in I that is monic in x_n.

Write $f = \sum c_{\underline{a}} x^{\underline{a}}$, $x^{\underline{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, $c_{\underline{a}} \in k$.

Choose $e \in \mathbb{N}$ s.t.
$\forall \underline{a}\ \forall i$: $c_{\underline{a}} \neq 0 \Rightarrow a_i < e$.

Set $x_i' = x_i - x_n^{e^i}$ for $1 \le i \le n-1$.

Then $k[x_1, \dots, x_n] = k[x_1', \dots, x_{n-1}', x_n]$.

<u>Claim:</u> f monic in x_n as polynomial in $k[x_1', \ldots, x_{n-1}', x_n]$.

$$x_1^{a_1} \cdots x_n^{a_n} = (x_1' + x_n^{e})^{a_1} (x_2' + x_n^{e^2})^{a_2} \cdots (x_{n-1}' + x_n^{e^{n-1}})^{a_{n-1}} x_n^{a_n}$$

is monic in x_n, highest term is:

$$x_n^{a_n + a_1 e + \cdots + a_{n-1} e^{n-1}}$$

Choice of e $\Rightarrow$ all monomials in f have distinct highest terms.

$\therefore$ $f \in k[x_1', \ldots, x_{n-1}', x_n]$ monic in x_n.

$\Rightarrow$ $k[x_1, \ldots, x_n]$ finite module over $k[x_1', \ldots, x_{n-1}', f]$, etc.

$\square$

Def R commutative ring, S commutative R-algebra.
I.e. have ring hom. $R \longrightarrow S$.

(1) Let $s \in S$. Then s is <u>integral</u> over R if s is a root of a monic poly with coeffs. in R

(2) S is <u>integral</u> over R if all elts. of S are integral $/R$.

(3) S is a <u>finitely generated</u> R-algebra if $\exists\ R[x_1, \dots, x_n] \twoheadrightarrow S$. ring hom.

(4) S is <u>finite</u> over R if S is a finitely generated R-module.
($\exists\ R^N = R \oplus \cdots \oplus R \twoheadrightarrow S$ module hom.)

Thm (Cayley-Hamilton)

Def R com ring, M R-module, $J \subseteq R$ ideal. $J \cdot M \subseteq M$ submodule gen. by $\{a \cdot m \mid a \in J, m \in M\}$	$End(M)$ is a ring.

R ring, $J \subseteq R$ ideal, M R-module generated by n elts.
$\varphi : M \longrightarrow M$ R-homomorphism. If $\varphi(M) \subseteq J \cdot M$ then $\exists$
$p(x) = x^n + a_1 x^{n-1} + \dots + a_n \in R[x]$ such that $p(\varphi) = 0 \in End(M)$ and $a_i \in J^i$.

<u>Note</u>: If $M = R^n$ then φ given by $A \in Mat_n(R)$.
C.H. $\Rightarrow$ $p(\varphi) = 0$ where $p(x) = \chi_A(x) = \det(xI - A)$
$\varphi(M) \subseteq J \cdot M \Rightarrow A \in Mat_n(J) \Rightarrow a_i \in J$.

Proof M gen. by $m_1, \dots, m_n \in M$.
Write: $\varphi(m_i) = \sum_j a_{ij} m_j$, $a_{ij} \in J$.
Set $A = (a_{ij}) \in Mat_n(R)$.
M module over $R[x]$: $x \cdot m = \varphi(m)$, $p(x) \cdot m = p(\varphi)(m)$.

$$(xI - A)\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \Rightarrow \det(xI - A) \cdot m_i = 0 \quad \forall i$$

$\therefore$ $p(\varphi) = 0$ for $p(x) = \chi_A(x) = \det(xI - A)$.

$\square$

Def M R-module, $m_1, \dots, m_n \in M$. Then $m_1, \dots, m_n$ is a <u>basis</u> for M if
$R^n \xrightarrow{\cong} M$, $(a_1, \dots, a_n) \longmapsto \sum a_i m_i$.
In this case we say M is a <u>free R-module of rank n</u>.

$\boxed{\text{Exercise Rank of } M \text{ well def.!}}$

Cor R com ring, M f.g. R-module.
(a) Every surjective R-hom. $\alpha : M \to M$ is an isomorphism.
(b) If $M \cong R^n$ and $m_1, \dots, m_n$ generate M, then $\{m_1, \dots, m_n\}$ is a basis for M.

Proof (a) M is an $R[t]$-module, $p(t)\cdot m = p(\alpha)(m)$.

$\varphi = id : M \longrightarrow M$.

α surjective $\Rightarrow$ $\varphi(M) \subseteq (t).M$.

CH $\Rightarrow$ $\exists\ p(x) = x^n + a_1 x^{n-1} + \dots + a_n \in R[t][x]$ s.t. $p(id) = 0$ and $a_i \in (t)^i$.

Note: $p(1) = 1 - q(t)\cdot t$, $q(t) \in R[t]$.

$(1 - q(t)\cdot t)\cdot M = p(id)\cdot M \Rightarrow q(\alpha)\alpha = id : M \longrightarrow M. \Rightarrow \alpha$ iso.

(b) Assume $\gamma : M \xrightarrow{\cong} R^n$ iso and $m_1, \dots, m_n \in M$ generators R.

$\beta : R^n \twoheadrightarrow M$, $\beta(e_i) = m_i$.

$\beta\gamma : M \longrightarrow M$ surjective $\Rightarrow$ $\beta\gamma$ iso $\Rightarrow$ $\beta = (\beta\gamma)\gamma^{-1}$ iso.

$\Rightarrow m_1, \dots, m_n$ basis.

□

$\boxed{\text{LATER!}}$

Prop R com. ring, $J \subseteq R[x]$ ideal, $S = R[x]/J$.

Then S is finite over R $\Leftrightarrow$ J contains a monic poly.

Proof $\Leftarrow$: Assume $p(x) = x^n + a_1 x^{n-1} + \dots + a_n \in J$.

Then $R[x]/(p(x))$ free R-module with basis $1, x, \dots, x^{n-1}$.

And $R[x]/(p(x)) \twoheadrightarrow R[x]/J = S$.

$\Rightarrow$: Def. $\varphi : S \longrightarrow S$, $\varphi(m) = \bar{x}\cdot m$ (mult. in S.)

Then $\varphi(S) \subseteq R\cdot S$

CH $\Rightarrow$ $\varphi^n + a_1\varphi^{n-1} + \dots + a_n = 0 \in End_R(S)$, $a_i \in R$.

$\Rightarrow$ $\bar{x}^n + a_1 \bar{x}^{n-1} + \dots + a_n = 0 \in S$

$\Rightarrow$ $x^n + a_1 x^{n-1} + \dots + a_n \in J$.

follows from lemma

□

Lemma R com ring, S com R-alg. Then S finite $/R$ $\Rightarrow$ S integral $/R$.

Proof Let $s \in S$. Def. $\varphi : S \to S$, $\varphi(m) = s\cdot m$

Then $\varphi(S) \subseteq R\cdot S$.

CH $\Rightarrow$ $p(\varphi) = 0 \in End_R(S)$ for some monic $p(x) \in R[x]$.

$\Rightarrow$ $p(s) = p(\varphi)(1) = 0 \in S$.

□

Prop

Cor S finite over R $\Leftrightarrow$
S generated by finitely many integral elts. as R-algebra.

Proof
$\Rightarrow$: clear from lemma.
$\Leftarrow$: Assume $S = R[a_1, \dots, a_n]$, a_i integral over R.
Induction $\Rightarrow$ $S' = R[a_1, \dots, a_{n-1}]$ finite over R.
$S = S'[a_n]$ finite S'-module by prop.
$\therefore$ S finite over R.
□

Thm R com ring, S R-algebra. Then $\bar{R} = \{s \in S \mid s \text{ integral } /R\}$ is a subring of S.

Proof Assume $s, t \in S$ both integral over R.
Then $R[s,t]$ f.g. R-module. $\Rightarrow$ $R[s,t]$ integral $/R$
$\Rightarrow$ $s+t$, $s-t$, st integral $/R$.
□

Def $\bar{R} = \{s \in S \mid s \text{ integral } /R\}$ is the <u>integral closure</u> of R in S.

This Prop shows that $\bar{\bar{R}} = \bar{R} \subseteq S$:

Prop Assume $R \subseteq S \subseteq T$ are (sub)rings. If S integral$/R$ and T integral $/S$ then T is integral over R.

Proof Let $t \in T$. Write $t^n + a_1 t^{n-1} + \dots + a_n = 0$, $a_i \in S$.
$R' = R[a_1, \dots, a_n]$ finite over R.
$R'[t]$ finite over R' $\Rightarrow$ finite over R $\Rightarrow$ t integral $/R$.
□

Cor M f.g. R-module, $I \subseteq R$ ideal, R com ring.
$M = IM$ $\Rightarrow$ $\exists r \in I$: $rm = m$ $\forall m \in M$.

Proof
$\varphi = id : M \to M$. sat. $\varphi(M) \subseteq IM$.
$CH \Rightarrow$ $\varphi^n + a_1 \varphi^{n-1} + \dots + a_n = 0 \in End(M)$, $a_i \in I$.
$\Rightarrow$ $r := (-a_1 - a_2 - \dots - a_n) = 1 \in End(M)$.
□

Def R com. ring. The <u>Jacobson radical</u> of R is the intersection of all max ideals of R.

Nakayamas Lemma (NAK)

R com. ring, M f.g. R-module. $I \subseteq$ Jacobson radical.

(a) $IM = M \Rightarrow M = 0$.

(b) Let $m_1, \dots, m_n \in M$. If $\overline{m_1}, \dots, \overline{m_n}$ generate M/IM then $m_1, \dots, m_n$ generate M.

Proof (a) $\exists r \in I : rm = m \quad \forall m \in M$.

$\Rightarrow (r-1) \cdot M = 0$

$r \in$ all max ideals $\Rightarrow$ $r-1 \in R$ unit (Why?)

$\Rightarrow M = 0$.

(b) Set $N = M/\langle m_1, \dots, m_n \rangle$.

M/IM gen. by $\overline{m_1}, \dots, \overline{m_n} \Rightarrow M = IM + \langle m_1, \dots, m_n \rangle$

$\Rightarrow N = IN \Rightarrow N = 0$.

$\square$

Note: Often applied when (R, m) local ring (an only max. ideal.) M f.g. R-module and $M/mM = 0 \Rightarrow M = 0$.

Example $R = \mathbb{Z}_{(p)} = \{ \frac{a}{b} \in \mathbb{Q} \mid (p, b) = 1 \}$. $\quad M = \mathbb{Q}$.

$\mathbb{Q}/(p) \cdot \mathbb{Q} = 0$ but $\mathbb{Q} \neq 0$.

Thm (Noether's Normalization Theorem)

R affine ring over k. Then $\exists\, y_1, \dots, y_r \in R$ s.t. $y_1, \dots, y_r$ are alg. indep. over k and R is a f.g. module over the subring $S = k[y_1, \dots, y_r] \subseteq R$.

Proof

Induction on number of generators.

$R = k[x_1, \dots, x_n]/I$. If $n=0$ then $S = R = k$ works.

Assume $n \geq 1$. WLOG $I \neq 0$. Choose $0 \neq f \in I$.

$\boxed{\text{Last time: Easy if } f \text{ monic in } x_n}$

Write $f = \sum c_{\underline{a}} x^{\underline{a}}$, $x^{\underline{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, $c_{\underline{a}} \in k$.

Choose $e \in \mathbb{N}$ s.t. $\forall \underline{a}\ \forall i$: $c_{\underline{a}} \neq 0 \Rightarrow a_i < e$.

Set $x_i' = x_i - x_n^{e^i}$ for $1 \leq i \leq n-1$.

Then $k[x_1, \dots, x_n] = k[x_1', \dots, x_{n-1}', x_n]$.

<u>Claim</u>: f is monic in x_n as polynomial in $k[x_1', \dots, x_{n-1}', x_n]$

$$x_1^{a_1} \cdots x_n^{a_n} = (x_1' + x_n^{e})^{a_1} (x_2' + x_n^{e^2})^{a_2} \cdots (x_{n-1}' + x_n^{e^{n-1}})^{a_{n-1}} \cdot x_n^{a_n}$$

is monic in x_n, highest term is:

$$x_n^{a_n + a_1 e + \dots + a_{n-1} e^{n-1}}$$

Choice of $e \Rightarrow$ all monomials in f have distinct highest terms.

This proves claim.

$T = k[x_1', \dots, x_{n-1}', f]$. $\quad T \subseteq k[x_1', \dots, x_{n-1}', x_n]$ finite.

$T/I \cap T$ affine ring gen. by $\overline{x_1'}, \dots, \overline{x_{n-1}'}$ $\Rightarrow$

$$\exists\ S = k[y_1, \dots, y_r] \underset{\text{finite}}{\subseteq} T/I \cap T \underset{\text{finite.}}{\subseteq} R$$

$\square$

<u>Normalization</u>

R integral domain with field of fractions K.

The <u>normalization</u> of R is $\overline{R} = \{ s \in K \mid s \text{ integral over } R \}$

R is <u>normal</u> if $\overline{R} = R \subseteq K$.

<u>Example</u> k field $\Rightarrow$ $k[x_1, \dots, x_n]$ is normal.

<u>Exercise</u> R UFD $\Rightarrow$ $R[X]$ UFD.

Prop R UFD $\Rightarrow$ R normal.

Proof Assume r/s integral over R. WLOG: r, s relatively prime.

$\exists \; \left(\frac{r}{s}\right)^n + a_1 \left(\frac{r}{s}\right)^{n-1} + \dots + a_n = 0 \quad , \quad a_i \in R.$

$\Rightarrow r^n + s a_1 r^{n-1} + \dots + s^n a_n = 0$

$\Rightarrow s \mid r^n \Rightarrow s \in R$ unit $\Rightarrow \frac{r}{s} \in R.$

$\square$

Prop $R \subseteq S$ com. rings. $f(x) \in R[x]$ monic polynomial. Assume that $f(x) = g(x) \cdot h(x)$ where $g(x), h(x) \in S[x]$ are both monic. Then the coefs. of $g(x)$ and $h(x)$ are integral over R.

Proof Induction on $\deg(g) + \deg(h)$.

If $g(x) = x - a$ and $h(x) = x - b$ then $f(a) = f(b) = 0 \Rightarrow a, b$ integral$/R$.

Assume $\deg(g(x)) \geq 2$.

Set $S' = S[t]/\langle g(t) \rangle$, $\alpha = \bar{t} \in S'$.

Write $g(x) = g_1(x) \cdot (x - \alpha) \quad \in S'[x]$.

$f(x) = f_1(x) \cdot (x - \alpha) \quad \in R'[x]$, $\quad R' = R[\alpha] \subseteq S'$.

$f_1 = g_1 \cdot h \Rightarrow$ coefs in $g_1(x)$ and $h(x)$ integral over R'.

α integral over $R \Rightarrow$ coefs of $g(x)$, $h(x)$ integral over R.

$\square$

Cor R normal domain with field of fractions K, $f(x) \in R[x]$ monic.

$f(x)$ irred in $R[x] \iff f(x)$ irred in $K[x]$.

$\boxed{\text{Do } R \text{ UFD} \Rightarrow R[x] \text{ UFD using this!}}$

Weak Nullstellensatz $k = \bar{k}$ alg. closed. $I \subsetneq k[x_1, \dots, x_n]$ proper ideal.

Then $Z(I) \neq \emptyset \subseteq \mathbb{A}^n$.

Proof WLOG I max. ideal. $L = k[x_1, \dots, x_n]/I$ is a field.

Noether $\Rightarrow \exists$ finite extension $k[y_1, \dots, y_m] \subseteq L$.

If $m \neq 0$ then $y_1^{-1} \in L$ is integral over $k[y_1, \dots, y_m]$. But $k[y_1, \dots, y_m]$ normal $\lightning$

$\therefore k \subseteq k[x_1, \dots, x_n]/I$ finite field extension.

$k = \bar{k} \Rightarrow k \xrightarrow{\simeq} k[x_1, \dots, x_n]/I$. Choose $a_i \in k$ s.t. $x_i \equiv a_i \pmod{I}$.

$(x_1 - a_1, \dots, x_n - a_n) \subseteq I \Rightarrow I = (x_1 - a_1, \dots, x_n - a_n) \Rightarrow Z(I) = \{(a_1, \dots, a_n)\} \neq \emptyset$

$\square$

<u>Nullstellensatz</u> $k = \bar{k}$. $I \subseteq k[x_1, \to x_n]$ ideal. Then $I(Z(I)) = \sqrt{I}$.

$\boxed{\sqrt{I} \subseteq I(Z(I)) \text{ clear}}$

<u>Proof</u> $I = (f_1, \to f_m)$. Let $g \in I(Z(I))$.

Set $J = \langle f_1, \to f_m, yg - 1 \rangle \subseteq k[x_1, \to x_n, y]$.

Then $Z(J) = \emptyset \subseteq \mathbb{A}^{n+1}$ (If $(a_1, \to a_n, b) \in Z(J)$ then $(a_1, \to a_n) \in Z(I)$ $\Rightarrow g(a_1, \to a_n) = 0$.)

Weak NSS $\Rightarrow$ $J = \langle 1 \rangle$.

$1 = p_1 f_1 + \dots + p_m f_m + p_{m+1}(yg - 1)$, $p_i \in k[x_1, \to x_n, y]$.

Set $y = g^{-1}$: $1 = p_1(x_1, \to x_n, g^{-1}) \cdot f_1 + \dots + p_m(x_1, -, x_n, g^{-1}) \cdot f_m$

Mult. by g^N: $g^N \in \langle f_1, \to f_m \rangle = I \Rightarrow g \in \sqrt{I}$.

□

<u>Tensor Products</u>

R (com) ring, M, N, P R-modules. $\varphi : M \times N \longrightarrow P$ is <u>bilinear</u> if

(i) $\varphi(rm, n) = r\varphi(m, n)$ (ii) $\varphi(m, rn) = r\varphi(m, n)$

(iii) $\varphi(m + m', n) = \varphi(m, n) + \varphi(m', n)$ (iv) $\varphi(m, n + n') = \varphi(m, n) + \varphi(m, n')$.

<u>Def</u> A <u>tensor product</u> of M and N over R is an R-module T with a bilinear map $\alpha : M \times N \longrightarrow T$ whic is <u>universal</u>:

If $\varphi : M \times N \longrightarrow P$ is any bilinear map then $\exists!$ R-hom. $\tilde{\varphi} : T \longrightarrow P$ such that $\varphi = \tilde{\varphi} \circ \alpha$.

$$\begin{tikzcd} M \times N \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & P \\ T \arrow[ur, dashed, "\exists! \tilde{\varphi}"'] & \end{tikzcd}$$

<u>Uniqueness</u>:

Assume $\alpha : M \times N \longrightarrow T$ and $\beta : M \times N \longrightarrow T'$ are tensor products.

β bilinear $\Rightarrow \exists!\ \tilde{\beta} : T \longrightarrow T'$ s.t. $\beta = \tilde{\beta} \circ \alpha$

α bilinear $\Rightarrow \exists!\ \tilde{\alpha} : T' \longrightarrow T$ s.t. $\alpha = \tilde{\alpha} \circ \beta$.

<u>Claim</u>: $\tilde{\alpha} \circ \tilde{\beta} = id : T \longrightarrow T$

$\alpha : M \times N \longrightarrow T$ bilinear $\Rightarrow \exists!\ \varphi : T \longrightarrow T$ s.t. $\alpha = \varphi \circ \alpha$.

$$\begin{tikzcd} M \times N \arrow[r, "\alpha"] \arrow[d, "\alpha"'] & T \\ T \arrow[ur, dashed, "\exists! \varphi"'] & \end{tikzcd}$$

$\varphi = id$ works.

$\varphi = \tilde{\alpha} \circ \tilde{\beta}$ works since $\tilde{\alpha}\tilde{\beta}\alpha = \tilde{\alpha}\beta = \alpha$. $\therefore \tilde{\alpha}\tilde{\beta} = id$.

□

<u>Notation</u> $M \otimes_R N = M \otimes N = T$, $\tau(m,n) = m \otimes n \in M \otimes N$.

<u>Construction</u>:

F = free R-module with basis $M \times N$

$= \left\{ \sum_{i=1}^{N} r_i \cdot [m_i, n_i] \;\middle|\; r_i \in R \text{ and } [m_i, n_i] \in M \times N \right\}$

Idea: $F' \subseteq F$ submodule. $\quad M \otimes_R N := F/F'$.

$\tau : M \times N \longrightarrow M \otimes N = F/F'$

$(m, n) \longmapsto m \otimes n := 1 \cdot [m,n] + F'$.

Def. $F' \subseteq F$ submodule generated by all elts of the form

$1 \cdot [rm, n] - r \cdot [m,n]$

$1 \cdot [m, rn] - r \cdot [m,n]$

$1 \cdot [m+m', n] - 1 \cdot [m,n] - 1 \cdot [m', n]$

$1 \cdot [m, n+n'] - 1 \cdot [m,n] - 1 \cdot [m, n']$.

<u>Exercise</u> $M \otimes_R N = F/F'$ satisfies universal property.

<u>Properties</u>:

(1) $M \otimes_R N$ generated by $\{m \otimes n\}$ as R-module.

(2) $M \otimes_R R = M$

(3) $M \otimes N \cong N \otimes M$

(4) $(M \otimes N) \otimes P = M \otimes (N \otimes P)$

(5) $(M \oplus N) \otimes P = (M \otimes P) \oplus (N \otimes P)$.

(6) $M \to N \to P \to 0$ exact seq. of R-modules

$\Rightarrow M \otimes Q \to N \otimes Q \to P \otimes Q \to 0$ is exact.

(7) $\varphi : M' \to M$ and $\psi : N' \to N$ R-homomorphisms $\Rightarrow$

$\exists! \; \varphi \otimes \psi : M \otimes N \longrightarrow M' \otimes N'$, $(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n)$.

<u>Exercise</u> Prove as many as possible (all?) from universal property.

Examples

1) If $N = R^n$ free R-module, then
$$M \otimes_R N = (M \otimes_R R) \oplus \cdots \oplus (M \otimes_R R) = M^{\oplus n}.$$

2) M free R-module with basis $\{m_1, \dots, m_s\}$.
N free R-module with basis $\{n_1, \dots, n_t\}$
$\Rightarrow M \otimes_R N$ free R-module with basis $\{m_i \otimes n_j\}$.

Base change

Let $\pi : R \longrightarrow S$ be a ring hom.

N S-module $\Rightarrow$ N also R-module: $r \cdot n = \pi(r) \cdot n$.

M R-module: $M \otimes_R S$ is an S-module. $s \cdot (m \otimes s') = m \otimes (ss')$.

Exercises Let M be an R-module.

$\boxed{Q}$: $\mathbb{Z}/\langle 23 \rangle \otimes_{\mathbb{Z}} \mathbb{Z}/\langle 101 \rangle$

1) $I \subseteq R$ ideal $\Rightarrow M/I \cdot M = M \otimes_R R/I$

2) $U \subseteq R$ mult. closed subset $\Rightarrow U^{-1}M = M \otimes_R U^{-1}R$

$\boxed{Q}$: $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$

Application:

~~Lemma R normal domain with field of fractions K~~

$\boxed{Q}$: $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/\langle 23 \rangle$

Lemma R normal domain. Then every irreducible monic polynomial in $R[x]$ is a prime element.

Proof
$K = K(R) = (R - \{0\})^{-1}R$ field of fractions.

$f(x) \in R[x]$ irreducible $\Rightarrow \langle f(x) \rangle \subseteq K[x]$ prime ideal.

$R[x]/\langle f(x) \rangle$ free R-module $\Rightarrow$

$$R[x]/\langle f(x) \rangle \subseteq R[x]/\langle f(x) \rangle \otimes_R K = K[x]/\langle f(x) \rangle \quad \text{field.}$$

$\Rightarrow \langle f(x) \rangle \subseteq R[x]$ prime ideal.

$\square$

Property (6): $M \to N \xrightarrow{\beta} P \to 0$ exact $\Leftrightarrow$ $P = \operatorname{coker}(M \to N)$.

Show: $M \otimes Q \to N \otimes Q \to P \otimes Q \to 0$ exact.

Enough: Show that $C := \operatorname{coker}(M \otimes Q \to N \otimes Q)$ is a tensor product of P and Q.

Bilinear map:
$$\begin{aligned} P \times Q &\longrightarrow C \\ (p, q) &\longmapsto \overline{n \otimes q} \qquad \text{where } \beta(n) = p. \end{aligned}$$

Assume $P \times Q \to H$ any bilinear map.

$$\begin{tikzcd} N \times Q \arrow[r] \arrow[d] & P \times Q \arrow[r] & H \\ N \otimes Q \arrow[urr, dashed, "\exists!"] \arrow[d] & & \\ C \arrow[uurr, dashed, "\exists!"'] & & \end{tikzcd}$$

More examples R ring, $R \to A$, $R \to B$ R-algebras.

$A \otimes_R B$ is an R-algebra.

$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$.

$R[x_1, \dots, x_n] \otimes_R A = A[x_1, \dots, x_n]$

$R[x_1, \dots, x_n] \otimes_R R[y_1, \dots, y_m] = R[x_1, \dots, x_n, y_1, \dots, y_m]$.

$R/I \otimes_R R/J = R/I+J$

Geometry (1) $X \subseteq \mathbb{A}^n$, $Y \subseteq \mathbb{A}^m$ alg. sets. $k = \bar{k}$.

$A(X) = k[x_1, \dots, x_n]/I(X)$ $A(Y) = k[y_1, \dots, y_m]/I(Y)$

$X \times Y \subseteq \mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$.

$A(X \times Y) = A(X) \otimes_k A(Y)$

(2) $X, Y \subseteq \mathbb{A}^n$. $Z = X \cap Y$.

$Z = Z(I(X) + I(Y)) \Rightarrow I(Z) = \sqrt{I(X) + I(Y)}$

Def $X \cap Y$ is <u>reduced</u> if $I(X) + I(Y) \subseteq k[x_1, \dots, x_n]$ radical ideal.

$X \cap Y$ reduced $\Rightarrow$ $A(X \cap Y) = A(X) \otimes_{A(\mathbb{A}^n)} A(Y)$.

Categories

Def A category $\mathcal{C}$ consists of

1) $\operatorname{ob}\mathcal{C}$ — a collection of objects
2) For $A, B \in \operatorname{ob}\mathcal{C}$, a set $\operatorname{Hom}(A,B) = \operatorname{Hom}_{\mathcal{C}}(A,B)$ of morphisms
$\operatorname{Hom}(A,B) = \{f : A \to B\}$.
2) For $A, B, C \in \operatorname{ob}\mathcal{C}$, a map $\operatorname{Hom}(A,B) \times \operatorname{Hom}(B,C) \to \operatorname{Hom}(A,C)$
$(f, g) \mapsto gf = g \circ f$.

Axioms:

- $(A,B) \neq (C,D) \Rightarrow \operatorname{Hom}(A,B) \cap \operatorname{Hom}(C,D) = \emptyset$
- Let $f \in \operatorname{Hom}(A,B)$, $g \in \operatorname{Hom}(B,C)$, $h \in \operatorname{Hom}(C,D)$.
Then $h(gf) = (hg)f$.
- Each $A \in \operatorname{ob}(\mathcal{C})$ has identity $1_A \in \operatorname{Hom}(A,A)$.
We have $f 1_A = f$ for all $f \in \operatorname{Hom}(A,B)$, $1_A g = g$ $\forall g \in \operatorname{Hom}(B,A)$.

Examples

Set = category of all sets.
ob Set $= \{$ all sets $\}$.
$A, B \in \operatorname{ob}$ Set $\Rightarrow \operatorname{Hom}_{\text{Set}}(A,B) = \{$ functions $A \to B\}$.

Grp = category of all groups.
$\operatorname{Hom}(A,B) = \{$ group homs. $A \to B\}$.

Ab = category of abelian groups.

Top = category of top. spaces & continuous maps.

Rings = category of associative rings with 1.

R fixed ring.

R-mod = category of left R-modules & homomorphisms.
mod-R = category of right R-modules & homomorphisms.

Ab = $\mathbb{Z}$-mod.

Constructions

1) $\mathcal{C}$ category. Dual (or opposite) category $\mathcal{C}^{op}$ def. by

$\text{ob}\,\mathcal{C}^{op} = \text{ob}\,\mathcal{C}$

For $A, B \in \text{ob}\,\mathcal{C}^{op}$ set $\mathrm{Hom}_{\mathcal{C}^{op}}(A,B) = \mathrm{Hom}_{\mathcal{C}}(B,A)$.

2) $\mathcal{C}$ and $\mathcal{D}$ categories.

$\text{ob}(\mathcal{C}\times\mathcal{D}) = \{(A,B) : A \in \text{ob}\,\mathcal{C} \text{ and } B \in \text{ob}\,\mathcal{D}\}$.

If $(A,B) \in \text{ob}(\mathcal{C}\times\mathcal{D})$ and $(A',B') \in \text{ob}(\mathcal{C}\times\mathcal{D})$ then

$\mathrm{Hom}_{\mathcal{C}\times\mathcal{D}}((A,B),(A',B')) = \mathrm{Hom}_{\mathcal{C}}(A,A') \times \mathrm{Hom}_{\mathcal{D}}(B,B')$.

Concepts

$\mathcal{C}$ category, $A, B \in \text{ob}\,\mathcal{C}$, $f \in \mathrm{Hom}(A,B)$.

- f is an isomorphism if $\exists\, g \in \mathrm{Hom}(B,A)$ s.t. $gf = 1_A$ and $fg = 1_B$. g is called the inverse of f.

~~[illegible]~~

Let $f \in \mathrm{Hom}(A,B)$, $g \in \mathrm{Hom}(B,A)$.

If $fg = 1_B$ then g is a section of f

f is a retraction of g

Exercise If f has section g and retraction g', then $g = g'$ and f iso.

Def f is monic if ~~[illegible]~~ $fg_1 = fg_2 \Rightarrow g_1 = g_2 \quad \forall g_1, g_2 : C \to A$

f is epic if $g_1 f = g_2 f \Rightarrow g_1 = g_2 \quad \forall g_1, g_2 : B \to C$.

Exercise

f, g monic $\Rightarrow$ fg monic.

fg monic $\Rightarrow$ g monic.

g has retraction $\Rightarrow$ g monic.

Find similar statements about epic.

<u>R-mod</u>: $f: A \to B$ is injective $\Leftrightarrow$ monic
surjective $\Leftrightarrow$ epic.

$\Rightarrow$: clear.

$\Leftarrow$: Assume f NOT injective. $K = \ker(f) \subseteq A$. $\iota : K \xrightarrow{\subseteq} A$
$0 : K \xrightarrow{0} A$

Then $f\iota = f0$ but $\iota \neq 0$.

$\Leftarrow$: Assume f NOT surjective. $C = \mathrm{coker}(f) = B/f(A)$.

$p : B \to C$ proj. $0 : B \xrightarrow{0} C$.

$pf = 0f$ but $p \neq 0$.

<u>Prop</u> A morphism f in <u>Grp</u> is monic $\Leftrightarrow$ injective and
epic $\Leftrightarrow$ surjective.

<u>Proof</u> Tricky part: epic $\Rightarrow$ surjective.

Assume $f: A \to B$ group hom, f NOT surjective.

$C = f(A) \leq B$ subgroup.

If $C \lhd B$ normal then have $B \underset{0}{\overset{\text{proj.}}{\rightrightarrows}} B/C$ as above.

Assume $C \ntriangleleft B$ not normal.

Then $[B : C] \geq 3$.

Def. $\varphi : B \to \mathrm{Sym}(B)$, $\varphi(b)(x) = bx$. $\boxed{\varphi \text{ group hom.}}$

Want: $\psi : B \to \mathrm{Sym}(B)$ s.t. $\varphi f = \psi f$ but $\varphi \neq \psi$.

Choose $I \subseteq B$ set of reps. for right cosets in $C \backslash B$.

$$C \times I \xrightarrow{\text{bijective}} B$$
$$(c, u) \longmapsto cu$$

$\# I \geq 3$.

Choose $\pi \in \mathrm{Sym}(I)$ s.t. $\pi \neq \mathrm{id}$ and π has a fixed point.

Def. $\rho \in \mathrm{Sym}(B)$ by $\rho(cu) = c\,\pi(u)$ for $c \in C$ and $u \in I$.

Def. $\psi : B \to \mathrm{Sym}(B)$ by $\psi(b) = \rho \circ \varphi(b) \circ \rho^{-1} \in \mathrm{Sym}(B)$.

$\psi f = \varphi f$: $\psi(f(a))(cu) = \rho(\varphi(f(a))(\rho^{-1}(cu))) =$

$\boxed{x = cu}$

$$p\big(\varphi(f(a))\,(c\,\pi^{-1}(u))\big) = p\big(f(a)c \cdot \pi^{-1}(u)\big) = f(a)c \cdot \pi\pi^{-1}(u)$$ 5

$$= f(a)\,cu = \varphi(f(a))\,(cu).$$

$\psi \neq \varphi$: Choose $u_0, u_1 \in I$ s.t. $\pi(u_0) = u_0$, $\pi(u_1) \neq u_1$.

$$\varphi(u_1 u_0^{-1})(u_0) = u_1$$

$$\psi(u_1 u_0^{-1})(u_0) = p\big(\varphi(u_1 u_0^{-1})(p^{-1}(u_0))\big) = p\big(\varphi(u_1 u_0^{-1})(u_0)\big)$$

$$= p(u_1) \neq u_1.$$

$\square$

__Example__ In __Ring__, $\mathbb{Z} \longrightarrow \mathbb{Q}$ is epic. Not surjective.

__Prop__ In __Ring__ we have monic $\Leftrightarrow$ injective.

__Pf__ $\Leftarrow$ clear.

$\Rightarrow$: Assume ring hom. $f: A \longrightarrow B$ not injective.

$A \times A$ is a ring.

$K = \{(a_1, a_2) \in A \times A \mid f(a_1) = f(a_2)\} \subseteq A \times A$ subring.

$g_i: K \longrightarrow A$, $g_i(a_1, a_2) = a_i$ ring hom.

$f g_1 = f g_2$ by def. of K.

f not injective $\Rightarrow \exists\, a_1 \neq a_2 \in A$ s.t. $f(a_1) \neq f(a_2)$

$\Rightarrow (a_1, a_2) \in K$ and $g_1(a_1, a_2) \neq g_2(a_1, a_2)$.

$\square$