Algebra 2 - 521 Lecture Notes
Prof Janet Vassilev

Galen Novello

March 13, 2020

Contents

1 Jan 22 2020

1.1 logistics

- 1st Homework 10.1 5,7,13, 10.2 1,4,6,7, 10.3 7
- See syllabus online

1.2 Modules

- def: An abelian group M (under $+$) is a (left) R-module if we have an action $R \times M \to M$, such that for all $r, s \in R, m, n \in M$

  1. $(r+s)m = rm + sm$
  2. $r(m+n) = rm + rn$
  3. $(rs)m = r(sm)$
  4. If R has unity then $1m = m$.

  Reverse properties define a right module, but we will consider modules to be left unless otherwise stated. If R is commutative we can define $mr = rm$ to give both a left and right module that are the same (although it is possible to defined different left and right structures even when R is commutative).

- an R- submodule is a subset $\emptyset \neq N \subset M$ which satisfies the module axioms. can simply check that if $x, y \in N$ then $rx - y \in N$ for all $r \in R$.

- Def: R-module homomorphism. If M, N are R modules then $\phi : M \to N$ is an R module homomorphism if $\phi(rm + n) = r\phi(m) + \phi(n)$

- Def: R-algebra. A ring S is an R-algebra if there is ring homomorphism $\phi : R \to S$ satisfying $r\phi(r') = \phi(rr')$. If R and S have unity we require

$$(*)\phi(1_R) = 1_S$$

  $(*) \Rightarrow r\phi(1) = \phi(r)$.

- $Hom_R(M, N)$ is the set of R-module homomorphisms for M to N. If we define $(\phi+\psi)(m) = \phi(m)+\psi(m)$ then $Hom_R(M, N)$ is an abelian group. If we define $(r\phi)(m) = r(\phi(m))$ then $Hom_R(M, N)$ is an R-module. $Hom_R(M, M)$ then with the addition defined above $Hom_R(M, M)$ is an abelian group. since $\phi \circ \psi \in Hom_R(M, M)$, its is a ring.

- Let M be an R-module and $\{N_i\}_{i \in I}$ with $N_i \subseteq M$ are R-submodules of M then $\sum_{i \in I} N_i = \{n_{i_1} + ... + n_{i_t} : n_{i_j} \in N_{i_j}\}$ the set of all finite sums is an R-submodule of M with

$$(n_{i_1} + ... + n_{i_t}) + (n_{j_1} + ... + n_{j_s}) = n_{i_1} + ... + n_{i_t} + n_{j_1} + ... + n_{j_s}$$

  and

$$r(n_{i_1} + ... + n_{i_t}) = rn_{i_1} + ... + rn_{i_t}.$$

- If $A \subset M$ then $RA = \{r_1a_1 + ...r_na_n : a_i \in A\}$ the set of all finite sums is the R-module generated by A. If $A = \{a\}$ then Ra is called a cyclic R-module. If $|A| = n < \infty$ and $N = RA$ we say that N is a finitely generated R-module. Not necessarily R.

2 Jan 24

2.1 Review of Direct Products

2.1.1 External Viewpoint for direct products

- Let $N_1, ..., N_s$ be R-modules. can construct $N_1 \times ... \times N_s = \{(n_1, ..., n_s) | n_i \in N_i\}$. Called the direct product of N_i's. With addition and scalar multiplication component-wise this is an R-module.

2.1.2 internal viewpoint for direct products

- M an R-module $N_1, ..., N_s \subset M$. with $N_1 + ... + N_s = M$. If $N_i \cap (N_1 + ... + \hat{N_i} + ... + N_s) = 0$ for all i then M is a direct sum of $N_1, ..., N_s$. if sum on N_i is not all of M then the sum is a direct sum if $N_i \cap (N_1 + ... + \hat{N_i} + ... + N_s) = 0$ (just not equal to M).

2.1.3 note about direct products and sums

If $N_1, ..., N_s$ are R-modules then $N_1 \oplus ... \oplus N_s = \{(n_1, ..., n_s : n_i \in N_i\} = N_1 \times ... \times N_s$ are the same thing as R-modules.

In the infinite case we have $\{N_i\}_{i \in I}$ then $\oplus_{i \in I} N_i = \{r_1\phi_{i_1} + ... + r_n\phi_{i_n} : r_i \in R\}$ where $\phi_j : \oplus_{i \in I} N_i \to N_j$ (ϕ_j picks the jth component). In direct sum can only have finite linear combinations of the ϕ_j. In infinite direct product can have infinite linear combinations.

2.2 Free modules

- Let A be a set then $F(A)$ is the free R-module on the set A if every element of $F(A)$ can be expressed uniquely in the form $r_1 a_{i_1} + ... r_n a_{i_n}$ for $r_j \in R$ and $a_{i_j} \in A$ (only finitely many terms can be involved in sum).

  This is equivalent to

  1. A is linearly independent
  2. A spans $F(A)$.

- The universal property for free modules. Let A be a set, M an R-module. Given any set map $\phi : A \to M$ as below there is a unique Φ such that the diagram commutes:

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[dr, "\phi"'] & F(A) \arrow[d, "\Phi"] \\ & M \end{tikzcd}$$

  Note i is an inclusion map, $i(a) = a$, M is an R-module and Φ is an R-module homomorphism.

  Main part of proof is showing the uniqueness of Φ.

2.3 Tensor Products

- Let $R \subseteq S$ be rings with unity. M is an S module. Then M is an R-module as well.

  If M is R module then M does not have to be an S module.

  Tensor product $S \otimes_R M$ can be thought of as a way of extending the scalars of R to make M an S module.

- Consider $F(S \times M)$ Note that $(s_1 + s_2, m), (s_1, m), (s_2, m)$ are all generators of $F(S \times M)$ so we need to mod out by certain relations.

  Let $R_1 : (s_1 + s_2, m) - (s_1, m) - (s_2, m)$ for all $s_1, s_2 \in S$, $m \in M$.

  $R_2 : (s, m_1 + m_2) - (s, m_1) - (s, m_2)$ for all $s \in S$, for all $m_1, m_2 \in M$.

  To get the needed associative like property let $R_3 : (s, rm) - (sr, m)$ for all $s \in S$, $m \in M$, $r \in R$.

  Then let $H =$ R-module generate by R_1, R_2, R_3 and we can define $S \otimes_R M := \dfrac{F(S \times M)}{H}$.

  To make sense of all this use universal property

$$\begin{tikzcd}
M \arrow[r] \arrow[rr, bend left, "i"] \arrow[dr, "\phi"'] & S \times M \arrow[r] & F(S \times M) \arrow[dl, "\Phi"] \\
& N &
\end{tikzcd}$$

3 Jan 27. Guest Lecturer Alex Buium

3.1 Tensor Products

- Let R be a commutative ring, $M, N, P, \ldots.$ R-Modules
- Def: A map from $M \times N \to P$ is bilinear if it is R-linear in each argument.
- Def: $M \otimes N = \dfrac{E}{F}$

  $E =$ free abelian group with basis $M \times N = \{\sum r_i(x_i, y_i) : r_i \in \mathbb{Z}, (x_i, y_i) \in M \times N\}$.

  $F =$ subgroup generated by

  $$\{(x+y,z)-(x,z)-(y,z), (x, \tilde{y}+z)-(x,\tilde{y})-(x,z), (rx,\tilde{y})-(x,r\tilde{y}) : x,y \in M, \tilde{y}, z \in N, r \in R\}.$$

  Remark there is a bilinear map $f_{can} : M \times N \to M \otimes N$ defined by $f_{can}(x,y) = x \oplus y = (\widehat{x,y})$. Note relations above given $(x+y) \oplus z - x \oplus z - y \oplus z = 0$ etc...

  Define an R-module structure on $M \otimes N$ by $r(x \otimes y) = rx \otimes y = x \otimes ry$.

- Theorem: Universal property of $\otimes$. Let $f : M \times N \to P$ be bilinear map then there is a unique R module homomorphism, ϕ, making the following diagram commutative:

$$\begin{tikzcd}
M \times N \arrow[r, "f_{can}"] \arrow[d, "f"'] & M \otimes N = \frac{E}{F} \arrow[dl, "\phi"] \\
P & E \arrow[u] \arrow[l, "\Phi"]
\end{tikzcd}$$

  Proof. Enough to show $\Phi : E \to P$ with $\Phi(F) = 0$. enough to find map of set Φ' such that Φ' such that induced map Φ (induced by Φ') vanishes on F.

  Let $\Phi'(x,y) = f(x,y)$. Then

  $$\Phi((x+y,z)-(x,z)-(y,z)) = \Phi'(x+y,z) - \Phi'(x,z) - \Phi'(y,z) = f(x+y,z) - f(x,z) - f(y,z).$$

  And similarly for the other relations above. $\square$

- Remark: $M \oplus N$ is generated as an R-module by $x \oplus y$ with $x \in M$, $y \in N$ (simple tensors). So any element of $M \oplus N$ can be written (non-uniquely) as a sum $\sum_{i=1}^{N} x_i \oplus y_i$. So if $x \oplus y$ for all x, y then $M \oplus N = 0$.

- Ex. $\mathbb{Z}_7 \oplus_Z \mathbb{Q} = 0$ enough to show that $x \oplus y = 0$ for all $x = \hat{k} \in \mathbb{Z}_y$ and all $y = \dfrac{a}{b} \in \mathbb{Q}$. Can compute $x \oplus \hat{k} \oplus \dfrac{a}{b} = \hat{k} \oplus \dfrac{7a}{7b} = \hat{k} \oplus 7\dfrac{a}{7b} = 7\hat{k} \oplus \dfrac{a}{7b} = 0 \oplus \dfrac{a}{7b} = 0$.

- Ex $\mathbb{Q} \oplus_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$. Let $f : \mathbb{Q} \to \mathbb{Q} \oplus_{\mathbb{Z}} \mathbb{Q}$ by $f(x) = 1 \otimes x$. Consider

$$\begin{tikzcd}
\mathbb{Q} \times \mathbb{Q} \arrow[r, "can"] \arrow[d, "b"'] & \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \arrow[dl, "g"] \\
\mathbb{Q} &
\end{tikzcd}$$

  with $b(x,y) = xy$ so $g(x \otimes y) = xy$.

  Note enough to show maps are inverse on simple tensors. $f(g(x \otimes y)) = f(xy) = 1 \otimes xy =?x \oplus y$.

  Proof of ?. say $x = \dfrac{a}{b}$, $y = \dfrac{c}{d}$ so

  $$\frac{a}{b} \otimes \frac{c}{d} = \frac{ac}{b} \otimes \frac{1}{d} =$$

  $$\frac{ac}{b} \otimes \frac{b}{bd} = \frac{acb}{b} \otimes \frac{1}{bd} = ac \otimes \frac{1}{bd} = 1 \otimes \frac{ac}{bd} = 1 \otimes xy$$

  So f and g are inverses and we have the desired isomorphism.

- Theorem (Properties of tensor products)

  1. $(M \otimes_R N) \otimes P \cong M \otimes_R (N \otimes_R P)$
  2. $M \otimes_R N \cong N \otimes_R M$
  3. $M \otimes_R R \cong M$
  4. $M \otimes (N \oplus P) = (M \otimes N) \oplus (M \otimes P)$

  Proof. of 4. Look at the diagrams. Take

$$\begin{tikzcd}
M \times (N \oplus P) \arrow[r, "can"] \arrow[d, "b"'] & M \otimes (N \oplus P) \arrow[dl, "\phi"'] \\
(M \otimes N) \oplus (M \otimes P) &
\end{tikzcd}$$

  where $b = (m, (m, p)) = (m \otimes m, m \otimes p)$ is bilinear. To defined $\Psi : (M \otimes N) \oplus (M \otimes P) \to M \otimes (N \oplus P)$. it is enough to find 2 maps $\Psi_1 : M \otimes N \to Q$ and $\Psi_2 : M \otimes P \to Q$. Then $\Psi(c, y) = \Psi_1(x) + \Psi_2(y)$ to get these use univesality property of tensors $b_1(m, n) = m \otimes (n, p)$. Then check $\phi \circ \Psi = 1$ and $\Psi \circ \phi = 1$.

  $\square$

4 Jan 29

4.1 more on tensor products

- $M \otimes (\oplus_i N_i) \cong \oplus_i (M \otimes N_i)$. If M, N free R modules with bases $(e_i), (f_j)$ then $M \otimes N$ is free with basis $(e_i \otimes f_j)$. This is becasue $M \cong R^m$, $N \cong R^n$ then

$$M \otimes N \cong (\underbrace{R \oplus .... \oplus R}_{m-times}) \otimes (\underbrace{R \oplus ... \oplus R}_{n-times}) \cong (R \otimes_R R) \oplus .... = \underbrace{R \oplus ... \oplus R}_{mntimes} = R^{mn}.$$

So $\underbrace{M \otimes ... \otimes M}_{ntimes}$ is free with basis $e_{i_1} \otimes ... \otimes e_{i_k}$ so any element has the form $suma_{i_1...i_n} e_{i_1} \otimes ... \otimes e_{i_n}$.

In $M \otimes M ... \otimes M \otimes M^* \otimes ... \otimes M^*$ with $M^* = Hom_R(M, R)$. then elements look like $\sum a^{j_1...j_n}_{i_1...i_n} e_{i_1} \otimes .... \otimes e_{i_m} \otimes e^*_{j_i} \otimes ... \otimes e^*_{j_n}$ where $e^*_j(e_i) = \delta_{ij}$.

4.2 Exact sequences

- Def: $M_1 \xrightarrow{f_1} M_2 ... \xrightarrow{f_2} M_n$ is exact if $Im(f_1) = ker(f_2)$, $Im(f_2) = ker(f_3)$, ... $Im(f_i) = ker(f_{i+1})$. This implies that $f_2 \circ f_1 = f_3 \circ f_2 = ... = 0$.

- Remark: $0 \longrightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} P \longrightarrow 0$. exact iff α injective, β surjective. and $ker(\beta) = im(\alpha)$. An exact sequence with 5 sets is called short exact.

- Ex Let $M \subset N$ be a submodule then $0 \longrightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} N/M \longrightarrow 0$ with α the inclusion map and β the cannonical map is a short exact sequence.

- Def: $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is isomorhic to $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ if there are isomorphisms α, β, γ making the following commute

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] \arrow[d, "\alpha"'] & M \arrow[r] \arrow[d, "\beta"'] & M'' \arrow[r] \arrow[d, "\gamma"'] & 0 \\
0 \arrow[r] & N' \arrow[r] & N \arrow[r] & N'' \arrow[r] & 0
\end{tikzcd}$$

- Prop: every short exact seq isomorphic to the one in the example above.

- Def: A short exact sequence

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

is split iff the following equivalent conditions are satisfied.

1. α has a left inverse $\pi : M \to M'$ such that $\pi \circ \alpha = 1_{M'}$
2. β has a right inverse $\sigma : M'' \to M$ such that $\beta \circ \sigma = 1_{M''}$.
3. The exact sequence is isomorphic to

$$0 \longrightarrow M' \xrightarrow{i} M' \oplus M'' \xrightarrow{p} M'' \longrightarrow 0$$

where $i : x \to (x, 0)$ and $p : (x, y) \to (y)$.

- Remark: $M \cong M' \oplus M''$ is implied by (3) but is not enough for the sequence to be split.

Proof. That the 3 condition are equivalent.

- $1 \Rightarrow 2$. Let $\sigma : M'' \to M$ since β is surjective given $m'' \in M''$ can pick m with $\beta(m) = m''$ then $\pi(m) \in M'$. Now apply α, and $\alpha(\pi(m)) \in M$. want to define $-\sigma(m'') = \alpha(\pi(m)) - m$.
  Need to see if this is invariant for different choice of $\tilde{m}$ such that $\beta(\tilde{m}) = m''$. Then

$$\alpha(\pi(\tilde{m})) - \tilde{m} - (\alpha(\pi(m)) - m) = \alpha(\pi(\tilde{m} - m)) - \tilde{m} + m \quad (*)$$

  now $\tilde{m} - m \in Ker\beta = Im\alpha$. so there is m' such that $\alpha(m') = \tilde{m} - m$. Then $(*) = \alpha(m') - \alpha(m') = 0$ so σ is well defined.
  Now $\beta(\sigma(m'')) = \beta(-\alpha(\pi(m)) + m) = \beta(m) = m''$. So σ has the desired composition property.
- other implications are similar.

$\square$

- Example

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

with $\alpha(x) = 2x$, $\beta(y) = y + 2\mathbb{Z}$. This is not split since there is no non-zero homomorphism from $\mathbb{Z}/2/Z \to \mathbb{Z}$.

5 Jan 31

- Hw 10.4 3,4,6, 16.

5.1 Short 5 Lemma

- Given 2 short exact sequences and maps as below

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\psi"] \arrow[d, "\alpha"'] & M \arrow[r, "\phi"] \arrow[d, "\beta"'] & N \arrow[r] \arrow[d, "\gamma"'] & 0 \\ 0 \arrow[r] & L' \arrow[r, "\psi'"] & M' \arrow[r, "\phi'"] & N' \arrow[r] & 0 \end{tikzcd}$$

Then

1. If α, γ are 1-1 then so is β
2. If α and γ are onto so is β.
3. If α and γ are bijections then so is β

Proof. 1. See book

2. let $m' \in M'$ with $\phi'(m') \in N'$ Since γ is onto there is $n \in N$ with $\gamma(n) = \phi'(m')$. Since ϕ is onto there is $m \in M$ with $\phi(m) = n$. by commutativity of diagram we have $\gamma(\phi(m)) = \phi'(\beta(m)$ so $\gamma(n) = \phi'(m')$ then subtraction gives $\phi'(m' - \beta(m)) = 0$. so $m' - \beta(m) \in Im(\psi')$ so there is $l' \in L'$ with $\psi'(l') = m' - \beta(m)$. Now since α is surjective there is $l \in L$ with $\alpha(l) = l'$. From commutativity it then follows that $\beta(\psi(l)) = \psi'(\alpha(l)) = \psi'(l') = m' - \beta(m)$ adding $\beta(m)$ and using the homomorphism property of β then gives $\beta(\psi(l) + m) = m'$ and so β is surjective.
3. follows from 1 and 2.

□

5.2 projective modules

- Let

$$\begin{tikzcd} D \arrow[d, "f"'] \arrow[dr, "f'"] & \\ L \arrow[r, "\psi"'] & M \end{tikzcd}$$

Then $f \in Hom_R(D, L)$, $f' = \psi \circ f \in Hom_R(D, M)$.

But if

$$\begin{tikzcd} & D \arrow[d, "f"] \arrow[dl, "?"'] \\ L \arrow[r, "\psi"'] & M \end{tikzcd}$$

Then the map ? does not always exits. For example if $L = \mathbb{Z}$, $M = \mathbb{Z}_2$, $D = \mathbb{Z}_2$. if $f = id_{\mathbb{Z}_2}$ then $? : \mathbb{Z}_2 \to \mathbb{Z}$ must be the 0 map and then $\psi \circ ?$ must also be the zero map and therefore can not be the identity.

- Prop: Let $\psi : L \to M$ be an R- module homomorphism. Then the map $\psi' : hom_R(D, L) \to Hom_R(D, M)$ defined by $\psi'(f) = f' = \psi \circ f$ is a homomorphism of abelian groups. If ψ is one to one then so is ψ'.

Proof. East to check the homomorphism property. Suppose that $\psi'(f) = 0$ (the zero map). We want to show that $f = 0$. Compute $\psi'(f) = f' = \psi \circ f$ so $\psi \circ f(l) = 0$ for all $l \in L$. Since ψ is one to one we then have that $f(l) = 0$ for all l so f was actually the zero map. □

- Prop: Let

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\phi} N$$

be a left exact sequence then

$$0 \longrightarrow Hom_R(D, L) \xrightarrow{\psi'} Hom_R(D, M) \xrightarrow{\phi'} Hom_R(D, N)$$

is also a left exact sequence.

Proof. We have proved exactness at $Hom_R(D, L)$. Need to show at $Hom_R(D, M)$ i.e. $im\psi' = ker\phi'$. We will show that $im\psi' \subseteq ker\phi'$. If $f \in Hom_R(D, M)$ such that $\psi'(g) = f$, $f = \psi \circ g$. So $\phi(f) = \phi(\psi \circ g) = \phi \circ \psi(g)$. By (left) exactness we have that $\phi \circ \psi = 0$ (f had to be in ker ϕ'.)

Now assume that $f \in ker\phi'$ then $\phi'(f) = 0$ but by def $\phi \circ f = \phi'(f)$ so $\phi \circ f = 0$. So for all $d \in D$, $\phi(f(d)) = 0$ so (by exactness) there is $l \in L$ such that $\psi(l) = f(d)$ and since ψ is one to one l is unique. So there is a map $F : D \to L$ such that $F(d) = l$ and $\psi(F(d)) = f(d)$. $F \in Hom_R(D, L)$ and $\psi(F(d_1)) + \psi(rF(d_2) = f(d_1) + rf(d_2) = f(d_1 + rd_2) = \psi(F(d_1 + rd_2))$ so we have $F(d_1) + rF(d_2) = F(d_1 + rd_2)$ and it follows that $im\psi' \subset ker\phi'$. □

- returning to the example above consider

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\alpha} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_2 \longrightarrow 0$$

is full exact. So

$$0 \longrightarrow Hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}) \longrightarrow Hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}) \longrightarrow Hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_{2)}$$

has to be left exact, but it can not be fully exact since $Hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_{2)}) \cong \mathbb{Z}_2$.

If we have a module such that short exact sequence of modules implies short exactness of the Hom sequence that modules is called projective.

- Def/Prop: Let P be an R-module. The following are equivalent.

  1. If

  $$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

  is short exact then

  $$0 \longrightarrow Hom_R(P, L) \longrightarrow Hom_R(P, M) \longrightarrow Hom_R(P, N) \longrightarrow 0$$

  is short exact

  2. if

  $$\begin{tikzcd} & P \arrow[dl, "\exists f'"'] \arrow[d, "f"] \\ M \arrow[r, "\psi"'] & N \end{tikzcd}$$

  with $\psi \circ f' = f$.

  3. If

  $$0 \longrightarrow L \longrightarrow M \longrightarrow P \longrightarrow 0$$

  is short exact then P is direct summand of M

  4. P is a direct summand of a free module

if P satisfies any/all of the above equivalent propertied we call P projective.

6 Feb 3

6.1 Projective modules continued

- Proof of equivalent statements

Proof. – 1 $\iff$ 2 clear.

- 2 $\Rightarrow$ 3. Given

$$\begin{tikzcd} & & & P \arrow[dl, "f"'] \arrow[d, "id"] & \\ 0 \arrow[r] & L \arrow[r, "psi"] & M \arrow[r, "\phi"] & P \arrow[r] & 0 \end{tikzcd}$$

with $\phi \circ f = id$. Then

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r] & M \arrow[r] & P \arrow[r] & 0 \end{tikzcd}$$

is short exact so P is a direct summand of M.

- 3 $\Rightarrow$ 4. If A is a genereating set of P.
- 4 $\Rightarrow$ 2.

$$\begin{tikzcd} & F(A) \arrow[dl, "F"'] \arrow[d, leftrightarrow, "j"] & \\ & P \arrow[dl] & \\ M \arrow[r, "\phi"] & n \arrow[r] & 0 \end{tikzcd}$$

j the inclusion of P into $F(a)$ as a direct summand. id $a \in A$ then $f \circ \pi(a) = F(a)$ and bu universal property F is a homomorphism and $\phi \circ F \circ j = f$.

□

Any free R module is projective. R^n is a free R module on n-generators is projective.

- Ex if $R = \mathbb{Z}_6$ then by fundamental thm of finitely generated abelian groups. $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. Now $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are projective $\mathbb{Z}$ modules so

$$\oplus_{i \in I} \mathbb{Z}_2 \oplus_{j \in J} \mathbb{Z}_3 \oplus_{k \in K} \mathbb{Z}_6$$

is still a projective $\mathbb{Z}_6$ modules. But $\mathbb{Z}_8$, $\mathbb{Z}_4$ are not projective $\mathbb{Z}_6$ modules.

- What quotients of $\mathbb{Z}_{100}$ are projective.

$$\mathbb{Z}_{100} \to M \to 0.$$

Would need $M = \mathbb{Z}_4, \mathbb{Z}_{25}$, or $\mathbb{Z}_{100}$ since these are only subgroups for which $\mathbb{Z}_{100}$ can be written as a direct summand.

- If $R = \mathbb{Z}$ the only direct summands of free $\mathbb{Z}$ modules will be free $\mathbb{Z}$ modules. (i.e $\mathbb{Z}^n$ or $\mathbb{Z}^A$ for some infinite set A.

- Only projective R-modules over a $R =$ a field are free.

- Projective submodules of $\mathbb{Z}_{100}$ which are ideals? $25\mathbb{Z}_{100} \cong \mathbb{Z}_4$, $4\mathbb{Z}_{100} \cong \mathbb{Z}_{25}$, $\mathbb{Z}_{100}$, 0.

-

$$\begin{tikzcd} M \arrow[r, "\phi"] \arrow[dr, "F"'] & N \arrow[d, "f"] \\ & D \end{tikzcd}$$

Given ϕ, f F always exists, but given ϕ, F f does not necessarily exists. (Note $f \in Hom_R(N, D)$, $F \in Hom_R(M, D)$ so induced map $\phi' : Hom_R(N, D) \to Hom_R(M, D)$

For example in the diagram

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "2"] \arrow[dr, "id_{\mathbb{Z}}"'] & \mathbb{Z} \arrow[d, "f"] \\ & \mathbb{Z} \end{tikzcd}$$

f can not be well defined.

- Prop: If

$$M \xrightarrow{\phi} N \longrightarrow 0$$

with ϕ surjective then

$$0 \longrightarrow Hom_R(N, D) \xrightarrow{\phi'} Hom_R(N, D)$$

with $\phi'(f) = f \circ \phi$.

Proof. Let $f \in Hom_R(N, D)$ with $\phi'(f) = 0$ then $f \circ \phi = 0$ so $f \circ \phi(m) = 0$ for all $m \in M$. Since ϕ onto we have $f(n) = 0$ for all $n \in N$ so f is the zero map i.e ϕ' is injective. □

- Prop: If

$$L \xrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0$$

is left exact then

$$0 \longrightarrow Hom_R(N, D) \xrightarrow{\phi'} Hom_R(N, D) \xrightarrow{\psi'} Hom_R(L, D)$$

is right exact.

Proof. have already showed that ϕ' is injective. Need to show exactness at $Hom_R(M, D)$ i.e. $im\phi' = ker\psi'$. Take $f \in im\phi'$ then there is $g \in HOm_R(N, D)$ with $\phi'(a) = f$ so $\psi'(f) = \psi'(g \circ \phi) = g \circ \phi \circ \psi = g \circ 0 = 0$. so $f \in ker\psi'$. so $im\phi' \subset ker\psi'$.

Now take $f \in Ker\psi'$ then $\psi'(f) = 0$. then $f \circ \psi(l) = 0$ for all $l \in L$. so $f(m) = 0$ foall $m \in im\psi = ker\phi$. Since ϕ is onto for all $n \in N$ there is $m \in M$ with $\phi(m) = n$. so define $g \in Hom_R(N, D)$ by $g(n) = g \circ \phi(m) = f(m)$. Then $\phi'(g) = g \circ \phi = f$. so $f \in im\phi'$. so $ker\psi' \subset im\phi'$. □

7 Feb 5

7.1 More on projective/injective modules

- Prop. If

$$L \xrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0$$

is left exact iff If

$$0 \longrightarrow Hom_R(N,D)' \xrightarrow{\phi} Hom_R(M,D) \xrightarrow{\psi'} Hom_R(L,D)$$

is right exact for all R modules D.

Proof. $\Rightarrow$ was the previous proposition.

$\Leftarrow$ First we will show that ϕ' one to one $\Rightarrow \phi$ onto. Let $D = N/\phi(M)$ and consider $\pi_1 : N \to N/\phi(M)$ then $\pi_1(\phi(M)) = 0$. Moreover $\pi_1 \circ \phi = \phi'(\pi_1) = 0$ map, so $N - \phi(M)$ so ϕ is onto.

First show that $\phi \circ \psi - 0$ (i.e $im\psi \subset ker\phi$). $id_N \in Hom_R(N,N)$ so $\phi'(id_n) = id_N \circ \phi \in Hom_R(M,N)$ then $\phi'(id_N) \in ker\psi'$ and it follows that $\psi' \circ \phi'(id_N) = 0 \Rightarrow id_N \circ \phi \circ \psi = \phi \circ \psi = 0$.

Now see $ker\phi \subset im\psi$. Let $D = M/\psi(L)$ and $\pi_2 : M \to M/\psi(L)$. then $\psi'(\pi_2) = \pi_2 \circ \psi$ so $\pi_2 \circ psi(L) = 0$ so $\pi_2 \in im\phi'$ so there is f such that $\phi'(f) = \pi_2$ and if $m \in ker(\phi)$ then $\pi_2(m) = f \circ \phi(m) = 0 \Rightarrow m \in \psi(L)$ and we have that $ker(\phi) \subset im\psi$.

□

- Prop/Def:

Let Q be an R-module then TFAE

1. If

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0$$

is short exact $\Rightarrow$

$$0 \longrightarrow Hom_R(N,D)' \xrightarrow{\phi} Hom_R(M,D) \xrightarrow{\psi'} Hom_R(L,D) \longrightarrow 0$$

is short exact.

2.

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\psi"] \arrow[d, "f"'] & M \arrow[dl, "F"] \\ & Q & \end{tikzcd}$$

$\exists\ F \circ \psi = f$.

3.

$$0 \longrightarrow Q \xrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0$$

then Q is a direct summand of M

If any of these conditions hold then we say that Q is injective.

Proof. 1. mostly follows from previous propositions.

2. $2 \Rightarrow 3$.

3.

$$\begin{tikzcd} 0 \arrow[r] & Q \arrow[r, "\psi"] \arrow[d, "id"'] & M \arrow[dl, "F"] \\ & Q & \end{tikzcd}$$

$F \circ \psi = id$ gives the splitting if i.e. Q is a direct summand.

4. $3 \Rightarrow 2$. If Q is a direct summand of M then given

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "f"] \arrow[d, "g"'] & M \\ & Q & \end{tikzcd}$$

(will finish next time)

$\square$

- Def: An abelian group G is divisible if for all $n \in \mathbb{Z}$, $nG = G$. i.e for all $g \in G$ there is $g' \in G$, with $ng' = g$.
- Ex: $\mathbb{Z}$ is not divisible, but $\mathbb{Q}$ is.

  Given any short exact seq of $\mathbb{Z}$ modules.

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \arrow[r, "g(m)=nm"] \arrow[d, "i"'] & \mathbb{Z} \arrow[dl, "f"] \\ & \mathbb{Q} & \end{tikzcd}$$

  f always exists $f(m) = \dfrac{m}{n}$ since $f \circ g(m) = m = i(m)$.

  $\mathbb{Z}_n$ is not divisible for any positive integer $n \geq 2$.

  $\mathbb{Q}/\mathbb{Z}$ is injective. for example

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}_2 \arrow[r, "\cdot 3"] \arrow[d, "f"'] & \mathbb{Z}_6 \arrow[dl, "F"] \\ & \mathbb{Q}/\mathbb{Z} & \end{tikzcd}$$

  with $f(1) = \dfrac{1}{2} + \mathbb{Z}$, $F(n) = \dfrac{n}{6}$.

- Baer's Criterion: An R module Q is injective iff for every $g : I \to Q$ where I is a left ideal extends to a map $G : R \to Q$.

  Proof. $\Rightarrow$ is a consequence of def of injective:

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r, "i"] \arrow[d, "g"'] & R \arrow[dl, "G"] \\ & Q & \end{tikzcd}$$

  where $G|_I = g$

  $\Leftarrow$ use Zorn's lemma. Consider

$$0 \longrightarrow L \xrightarrow{f} M$$

  . WLOG assume that $L \subset M$ i.e. $f(L) \cong L$.

  let $S = \{(f', L') : f' : L' \to Q \text{ with } L \subset L' \subset M, f'|_L = f\}$. Now $S \neq \emptyset$ since $(f, L) \in S$. then $(f', L') \leq (f'', L'')$ if $L' \leq L''$ and $f''|_{L'} = f'$ given chain

$$(f_1, L_1) \subset (f_2, L_2) \subset ...$$

  Let $\tilde{L} = \cup_{i=1} L_i$ and define $\tilde{f} : \tilde{L} \to Q$ by $\tilde{f}(l) = f_i(l)$ where $l \in L_i$.

  Not hard to show that $(\tilde{f}, \tilde{L}) \subset S$. Then Zorn's Lemma says that S has maximal elements. Suppose that (g, M') is a maximal element will show that $M' = M$ (next time). $\square$

8 Feb 7

8.1 Finish Baer's theorem

- Baer's Criterion: An R module Q is injective iff for every $g : I \to Q$ where I is a left ideal extends to a map $G : R \to Q$.

  Proof. $\Rightarrow$ is a consequence of def of injective:

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r, "i"] \arrow[d, "g"'] & R \arrow[dl, "G"] \\ & Q & \end{tikzcd}$$

  where $G|_I = g$

  $\Leftarrow$

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\psi"] \arrow[d, "f"'] & M \\ & Q & \end{tikzcd}$$

  Let $S = \{(f', L') : L \subset L' \subset M', f'|_L = f\}$ then S is non empty since $(f, L) \in S$ and S is partially ordered since $(f', L') \leq (f'', L'')$ iff $L' \subset L''$ and $f''|_{L'} = f'$. Now let $K = \cup_{i\geq 1} L_i$ and $h : K \to Q$ defined by $h(k) = f_i(k)$. $C = \{L_i, f_i | i \in \mathbb{N}\}$ with $(L_i, f_i) \leq (L_j, f_j)$ which holds if $i \leq j$. If $(h, k) \in S$ need to check that h is a homomorphism (DIY). Since there is an upper bound by Zorn's Lemma, S has maximal elements.

  Since (K, h) is a maximal element we need to show that $K = M$. Suppose not then there is $m \in M \setminus K$. then $K + Rm$ is a submodule of M. Define $I = \{r \in R : rm \in K\}$, then I is an abelian group. now take $r' \in R$ then $(r'r)m = r'(rm)$, but $rm \in K$ so $r'K$ in K so I is a left ideal. Now if $g : I \to Q$ then there is $G : R \to Q$ extending g.

  Then let $\tilde{h} : K + Rm \to Q$ defined by $\tilde{h}(k + rm) = h(k) + G(r)$. This makes sense since if $rm \in K$ then $r \in I$ so can use $g : I \to Q$. Now if $h(k + rm) = k + rm = k' + r'm'$ then $k - k' = r'm' - rm$ and $h(k - k') = h(k) - h(k') = h(r'm' - rm)$. so if G is the extension of g then $h(r'm' - rm) = G(r' - r') = G(r') - G(r) \Rightarrow h(k') + G(r') = h(k) + G(r)$ so $\tilde{h}$ is well defined. So $\tilde{h} : K + Rm \to Q$ extends h which is a contradiction.

  So $K = M$ and $\tilde{h} : M \to Q$ is an extension.

  $\square$

- Theorem: If R is a PID then Q is injective iff for all $r \neq 0$ in R, $rQ = Q$.

  Note: if $R = \mathbb{Z}$ then this says Q is divisible.

  Proof. Since R is a PID evey ideal of R is of the form $I = (r)$. Then $f : (r) \to Q$. by $f(r) = q$. Q is injective iff there is $F : R \to Q$ with $F|_{(r)} = f$. Suppose that $F(1) = q'$ then $q = f(r) = F(r) = rF(1) = rq'$ so forall $q \in Q$ there is q' such that $q = rq' \iff Q = rQ$. $\square$

- Thm: Every $\mathbb{Z}$-module is a submodule of an injective $\mathbb{Z}$-module.

  Proof. Let M be a $\mathbb{Z}$ module there is some subset $A \subset M$ such that $M = \mathbb{Z}A$. Consider $\mathcal{F} = F(a)$ then there is $\pi : \mathcal{F} \to M$ by $\pi(a) = a$ by the universal property. Let $K = ker\pi$ then

$$0 \longrightarrow K \longrightarrow \mathcal{F} \longrightarrow M \longrightarrow 0$$

  so $M \cong \mathcal{F}/K$ so there is a free $\mathbb{Q}$ module on A $\mathcal{Q} \supset \mathcal{F} \supset K$. Moreover $\mathcal{Q}/K \supset \mathcal{F}/K$. since $\mathcal{Q}$ is a divisible $\mathbb{Z}$ module and since $\mathcal{Q}$ is injective, $\mathcal{Q}/K$ is also divisible and injective since if $nq' = q$ then $(n + K)(q' + K) = nq' + K = q + L$.

  $\square$

- Show M an R-module is contained in an injective R-module if R has unity.

  1. Step 1: Notice $Hom_R(R, M) \subset Hom_{\mathbb{Z}}(R, M)$ (Since R contains a copy of $\mathbb{Z}$).
  2. Step 2: $Hom_{\mathbb{Z}}(R, M)$ can be made into an R-module via $\phi \in Hom_{\mathbb{Z}}(R, M)$ defined by $(r\phi) : R \to M$ by $(r\phi)(r') := \phi(r'r)$. This defines scalar multiplicaiton by r Need to show $(r\tilde{r})\phi = r(\tilde{r}\phi)$ so compute

     $$((r\tilde{r})\phi)(r') = \phi(r'(r\tilde{r})) = \phi((r'r)\tilde{r}) = \tilde{r}\phi(r'r) = (r(\tilde{r}\phi))(r')$$

     .
  3. Step 3: Prop: if R is a ring with unity and $0 \to L \to M$ is exact sequence of R-modules then $f : L \to D$ extends to $F : M \to D$, and $f' : L \to Hom_{\mathbb{Z}}(R, D)$ will extend to $F' : M \to Hom_{\mathbb{Z}}(R, D)$.

     Proof. Given $f' : L \to Hom_{\mathbb{Z}}(R, D)$ define $f(l) = f'(l)(1_R)$. Since f extends to $F : M \to D$ can define $F'(m)(l) = F(m)$ and this given the extension. □
  4. Cor: Q is an injective $\mathbb{Z}$-module iff $Hom_Z(R, Q)$ is an injective R-module.

     Proof. $M \cong Hom_R(R, M) \subset Hom_{\mathbb{Z}}(R, M) \subset Hom_{\mathbb{Z}}(R, Q)$ □

9 Feb 10

9.1 Flat modules, sequences of Tensors

- Consider $0 \to \mathbb{Z} \to \mathbb{Q}$ and $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong \mathbb{Z}_2$, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong 0$.

  Since $Z_2 \neq 0$, $1 \otimes 1 : \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \to \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_2$ is the trivial map which is not an injection. So tensor products don't always preserve injections.

- Prop: $L \xrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0$ is left exact iff for all $R-$modules D we have

$$L \otimes_R D \xrightarrow{\psi\otimes 1} M \otimes_R D \xrightarrow{\phi\otimes 1} N \otimes_R D \longrightarrow 0$$

is left exact.

Proof. $\Leftarrow$ Take $D = R$ $K \otimes R \cong K$ for al R-modiles K then

$$\begin{tikzcd}
L \otimes_R D \arrow[r, "\psi\otimes 1"] \arrow[d, "\cong"'] & M \otimes_R D \arrow[r, "\phi\otimes 1"] \arrow[d, "\cong"'] & N \otimes_R D \arrow[r] \arrow[d, "\cong"'] & 0 \\
L \arrow[r, "\psi"] & M \arrow[r, "\phi"] & N \arrow[r] & 0
\end{tikzcd}$$

$\Rightarrow$. First we show if ϕ is onto so is $\phi \otimes 1$. Take $n \otimes d \in N \otimes D$. Since ϕ is onto there is $m \in M$ with $\phi(m) = n$. so $n \otimes d = \phi(m) \otimes d = \phi \otimes 1(m \otimes d)$ so $\phi \otimes 1$ is onto.

Now we must see we are exact at $M \otimes_R D$. $\sum_{i\in I} \psi(l_i) \otimes d_o = im(\psi \otimes 1)$. Then $\phi \otimes 1(\sum_{i\in I} \psi(l_i) \otimes d_i) = \sum_{i\in I} \phi \circ \psi(l_i) \otimes d_i = \sum_{i\in I} 0 \otimes d_i = 0$ so $im(\psi\otimes) \subset ker(\phi \otimes 1)$. To show equality we will consider a map. $\phi \otimes 1$ decomposes as

$$M \otimes_R D \longrightarrow (M \otimes D)/Im(\psi \otimes 1) \xrightarrow{\pi} (M \otimes D)/Ker(\phi \otimes 1) \xrightarrow{\cong} N \otimes D$$

need to show π is an isomorphism so consider $\pi' : N \otimes_R D \to (M \otimes_R D)/im(\psi \otimes 1)$. defined by $\pi'(n, d) = m \otimes d$ where $\phi(m) = n$. To see this is well defined take $m' \otimes d$, $m' = m + \psi(l)$ then $\phi(m') = \phi(m + \psi(l)) = \phi(m) + \phi \circ \psi(l) = \phi(m) = n$, so π' is well defined. Then by universal property there is $\tilde{\pi} : N \otimes_R D \to (M \otimes_R D)/im(\psi \otimes 1)$. Easy to see π' is R-balanced we have that $\tilde{\pi}$ is a (right) R-module homomorphism. Then $\tilde{\pi} \circ \pi(m \otimes d) = \tilde{\pi}(n \otimes d) = m \otimes d$ and $\pi \circ \tilde{\pi}(n \otimes d) = \pi(m \otimes d) = \phi(m) \otimes d = n \otimes d$. So π and $\tilde{\pi}$ are inverses so π is an isomorphism. So $Ker(\phi \otimes 1) = im(\psi \otimes 1)$.

□

- Def/Prop: Let A be a left R-module TFAE

  1. If $0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0$ is short exact then

     $L \otimes_R a \xrightarrow{\psi\otimes 1} M \otimes_R A \xrightarrow{\phi\otimes 1} N \otimes_R A \longrightarrow 0$ is exact

  2. If $0 \longrightarrow L \xrightarrow{\psi} M$ is short exact then

     $L \otimes_R a \xrightarrow{\psi\otimes 1} M \otimes_R A$ is exact.

- If 1 or 2 hold then A is flat. (if tensor sequence implies module sequence exact then A is called faithfully flat).

- Prop: (Hom tensor adjointness). Let R and S be rings with A a right R-module and B an (R, S) bimodule and C a right S-module. Then $Hom_S(A \otimes_R B, C) \cong Hom_R(a, Hom_S(B, C)$ as abelian groups.

Proof. take $\phi \in Hom_s(A \otimes_R B, C)$ for a fixed a define $\Phi(a) \in Hom_S(B, C)$ by $\Phi(a)(b) = \phi(a \otimes b)$. We can do this for each $a \in A$ so we get a homomorphism $\Phi : a \to \Phi(a)$. Now take $f : Hom_S(A \otimes_R B, C) \to Hom_R(A, Hom_S(B, C))$ defined by $f(\phi) = \Phi$.

Now take $\Phi \in Hom_R(A, Hom_S(B, C)$

$$
\begin{tikzcd}
A \times B \arrow[d] & (a, b) \arrow[d] \\
c & \Phi(a)(b)
\end{tikzcd}
$$

Not hard to show that such a map is R-balanced. This map induces a homomorphism $g : A \otimes_R B \to C$ by $\phi(a \otimes b) = \Phi(a)(b)$. THen $g : Hom_R(A, Hom_S(B, C)) \to Hom_s(A \otimes_R B, C)$ then $g(\phi) = \Phi$ then $f \circ g(\phi) = f(\Phi) = \phi$ and $g \circ f(\phi) = g(\phi) = \Phi$ so f and g are inverses giving that f an isomorphism.

□

9.2 dual vector spaces

- F a field and V is an F-vector space. The dual space of V is $V^* = Hom_F(V, F)$. If V is finite dimensional with basis $\{v_1, ..., v_n\} = B$ and defined $v_i^* \in V^*$ by $v_i^*(v_j) = \delta_{ij}$ then $v_i^*(\sum a_j v_j) = a_i$ so v_i^* is a basis of V^*. (note in the infinite dimensional case the v_i^* may not span the dual space)
- $V^{**} = Hom_F(V^*, F) = Hom_F(Hom_F(V, F), F)$.

10 Feb 12

10.1 Vector spaces

- Prop: let V be an F-vector space. Then there is an injective homomorphism (linear map) $\theta : V \to V^{**}$ defined by $\theta(v) = E_v$ where $E_v : V^* \to F$, $E_v(f) = f(v)$.

  Note $E_v \in V^{**}$ then $E_v(f + g) = (f + g)(v) = f(v) + g(v) = E_v(f) + E_v(g)$ and for $r \in F$ $E_v(rf) = (rf(v) = r(f(v)) = rE_v(f)$.

  Proof. We can start with v and extend to a basis of V which has $v \in B$. then $V^* : V \to F$ by $V^*(v) = 1$ and $V^*(w) = 0$ for all $w \neq v$, $w \in B$. Then $E_v(v^*) = V^*(v) = 1$. $\theta(v)$ is not the zero map since $\theta(v)V^* = E_v(V^*) = 1 \neq 0$. Since this can be done for all nonzero v we have $Ker\theta = 0 \Rightarrow \theta$ is 1-1. Then $\theta(v + \alpha w) = E_{v+\alpha w}$. Now just need to show $E_{v+\alpha w} = E_v + \alpha E_w$. so compute $E_{v+\alpha w}(f) = f(v + \alpha w) = f(v) + \alpha f(w) = E_v(f) + \alpha E_w(f)$, this holds for every $f \in V^*$ so we have $E_{v+\alpha w} = E_v + \alpha E_w$.

  □

10.2 graded rings

- We say a ring R is graded if $R = \oplus_{i=0}^{\infty}$ where R_i are R_0-modules and $R_iR_j \subset R_{i+j}$.

  R_i is the set of all homogeneous elements of R of degree u.

- Ex: $R = k[x]$ is graded ring with $deg(x) = 1$. $R_0 = k$, $R_i = kx^i$ then $kx^i \cdot kx^j = kx^{i+j}$ so $R_iR_j = R_{i+j}$.

  can put a different grading on $R = k[x]$ if $deg(x) = 2$ then $R_0 = k$, $R_1 = 0$ and $R_2 = kx$, $R_3 = 0$. and $R_{2n+1} = 0$ and $R_{2n} = kx^n$

  Non-homogeneous element of $k[x]$ with standard grading. i.e. $x + x^2$ non-homogeneous wheras x, x^2 are homogeneous.

  Take $k[x, y]$ with $R_0 = k$, $R_1 = 0$, $R_2 = kx$, $R_3 = ky$, $R_4 = kx^2$, $R_5 = kxy$, $R_6 = kx^3ky^2$.

- An ideal in a graded ring is graded is $I = \oplus_{i=0}^{\infty} I \cap R_i$ of $I = \oplus_{i=0}^{\infty} I_i$ with each I_i in the ith homogeneous piece and $R_iI_j \subset I_{i+j}$.

  if R graded and I a graded R-ideal then R/I is a graded ring

  with $R/I = \oplus_{i=0}^{\infty} R_i/I_i$.

- Suppose R is a commutative ring with unity, M is an R-module then left and right actions of R on M agree.

- define $T^k(M) = M \otimes_R M \otimes .... \otimes M$. Then the simple tensors in $T^k(M)$ are of the form $m_1 \otimes m_2 \otimes ... \otimes m_k$.

  Note

$$r(m_1 \otimes m_2 \otimes ... \otimes m_k) =$$
$$rm_1 \otimes m_2 \otimes ... \otimes m_k =$$
$$m_1 \otimes rm_2 \otimes ... \otimes m_k = ...$$
$$= m_1 \otimes m_2 \otimes ... \otimes rm_k$$

- $f : M \times ... \times M_n \to N$ with M_i, N R-modules . then f is multilinear if

$$f(m_1, ..., m_i + m_i', ..., m_n) = f(m_1, .., m_i, .., m_n) + f(m_1, .., m_i', ..., m_n)$$

  and

$$f(m_1, ..., rm_i, ...m_n) = rf(m_1, .., m_i, ..., m_n)$$

  for all i.

- Define $T(M) = \oplus_{i=0}^{\infty} T^k(M)$ called the tensor algebra of M. defined multiplication for $m_1 \otimes m_2 \otimes ... \otimes m_i \in T^i(M)$ and $m_1' \otimes m_2' \otimes ... \otimes m_j' \in T^j(M)$ by

$$(m_1 \otimes m_2 \otimes ... \otimes m_i)(m_1' \otimes m_2' \otimes ... \otimes m_j') := m_1 \otimes m_2 \otimes ... \otimes m_i \otimes m_1' \otimes m_2' \otimes ... \otimes m_j' \in T^{i+j}(M)$$

  . This is a well defined multiplication justified through the universal property for tensors.

- universal property for tensor algebras: Let A be an R-algebra and $\phi : M \to A$ an R-module homomorphism. then there is a unique $\Phi : T(M) \to A$ such that $\phi_M = \Phi$. Proof by universal property of tensors.

- Ex: Let $M = \mathbb{Z}_n$ a $\mathbb{Z}$ module. Then since $\mathbb{Z}_n \otimes_n \mathbb{Z}_n \cong Z_n$ so $T^k(M) \cong \mathbb{Z}_n$ for all $k \geq 1$ ($T^0(M) = \mathbb{Z}$) and $T(M) \cong \mathbb{Z} \oplus Z_n \oplus \mathbb{Z}_n \oplus ... \cong \mathbb{Z}[x]/(nx)$

- Ex: Let $M = \mathbb{Q}$ then $T^0(M) = \mathbb{Z}$ and $T^k(M) = \mathbb{Q}$ for $k \geq 1$. So $T(M) \cong \mathbb{Z} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus ... \cong \mathbb{Z} + x\,\mathbb{Q}\,[x]$.

- Ex: Take $M = \mathbb{Q}/\mathbb{Z}$ then $T^0(M) = \mathbb{Z}$, $T^1(M) = \mathbb{Q}/\mathbb{Z}$ and $T^k = 0$ for $k \geq 2$. so $T(\mathbb{Q}/\mathbb{Z}) = \mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}$.

- Def: $\phi : M \times ... \times M \to N$ is symmetric multilinear if $\phi(m_1, ..., m_k) = \phi(\sigma(m_1), ..., \sigma(m_2))$ for all $\sigma \in S_k$ (the symmetric group).

11 Feb 14

11.1 Symmetric and Tensor Algebras

- Consider $M = k[x, y]$ as a k-module/k-Vector space. Then
$$T^0(M) = k,$$
$$T^1(M) = k[x, y],$$
$$T^2(M) =< f_{(x,y)} \otimes g_{(x,y)} >= k < x^i \otimes y^j, y^j \otimes x^i, x^i \otimes x^j, y^i \otimes x^j >$$
note since we're tensoring over k we have $x^i \otimes x^j \neq x^{i-1} \otimes x^{j+1}$, $x^i \otimes y^j \neq y^j \otimes x^i$, etc...

- consider an ideal $C(M)$ of $T(M)$ where $C(M)$ is the ideal generated by $m \otimes n - n \otimes m$. Then we can $C^0(M) = 0$, $C^1(M) = 0$,
$$C^2(M) =< m \otimes n - n \otimes m : m, n \in M > .$$
$$C^3(M) =< k \otimes m \otimes n - k \otimes n \otimes m, m \otimes n \otimes k - n \otimes m \otimes k : k, m, n \in M >$$
The symmetric algebra of M is $T(M)/C(M) = \oplus_{k \geq 0} T^k(M)/C^k(M) = S(M)$. we denote by $S^k(M) = T^k(M)/C^k(M)$.
We have $T^0(M) = S^0(M)$ and $T^1(M) = S^1(M)$ but they can be different at degree 2 and higher.

- Let k be a field and $M = k$. So 1 is my basis for k as a vector space. then $T(k) = \oplus_{i=0}^{\infty} k \cong k[x]$ which is commutative. Basis is $1_0, 1_1, 1_1 \otimes 1_1, ..., 1_1 \otimes ... \otimes 1_1, ...$ with $1_1 \to x$ and $\underbrace{1_1 \otimes ... \otimes 1_1}_{k-times} \to x^k$ so $T(k) = S(k)$.
But if we move to a 2-D vector space V we have $C^2(V) =< v_1 \otimes v_2 - v_2 \otimes v_1 : v_1, v_2 \in v > \neq 0$.
$$S^k(M) = \underbrace{M \otimes ... \otimes M}_{k-times} / < m_1 \otimes ... \otimes m_k - m_{\sigma(1)} \otimes .... \otimes m_{\sigma(m)} : \sigma \in S_m >$$

- Universal property for symmetric multilinear maps: Suppose $\phi(M \times ... \times M) \to N$ is symmetric multiplinear. Then there is a unique $\Phi : S^k(M) \to N$ such that $\phi = \Phi \circ i$ where $i : \underbrace{M \times ... \times M}_{k-times} \to S^k(M)$ with $i(m_1, ..., m_k) = m_1 \otimes ... \otimes m_k + C^k(M)$.

- Universal property for R-algebras.
If $\phi : M \to A$ with M an R-module and A an R-algebra then there is a unique $\Phi : S(M) \to A$ such that $\Phi|_M = \phi$.
$\phi^k : M \times ... \times M \to A$ defined by $\phi^k(m_1, ..., m_n) = \phi(m_1) \cdots \phi(m_k)$. Since A is commutative ϕ^k is symmetric and also not hard to show that it is multilinear.

- Alternating Maps: $\phi : \underbrace{M \times .... \times M}_{k-times} \to N$ is an alternating multilinear map if ϕ is multilinear and $\phi(m_1, ..., m_k) = 0$ if $m_i = m_j$ for some $i \neq j$.

- Exterior algebra: Let $A(M)$ be the ideal generated by $m \otimes m$ This is graded with $A^0(M) = A^1(M) = 0$ and $A^2(M) =< m \otimes m : minM >$, $A^3 =< n \otimes m \otimes n, m \otimes m \otimes n, m \otimes n \otimes m : m, n \in M >$. The the exterior algebra of M is $T(M)/A(M) =: \wedge M$.
$\wedge M$ can also be thought of as $\oplus_{i=0}^{\infty} T^i(M)/A^i(M) = \oplus_{i=0}^{\infty} \wedge^i(M)$. In this setting we have $(m \otimes n) + A(N) =: m \wedge n$.

- ex we have $m \wedge m$ for all m so, $(m + n) \wedge (m + n) = 0$ but by bilinearity we have
$$(m + n) \wedge (m + n) = m \wedge (m + n) + n \wedge (m + n) =$$
$$m \wedge m + m \wedge n + n \wedge m + n \wedge n \Rightarrow$$
$$m \wedge n + n \wedge m = 0 \Rightarrow m \wedge n = -n \wedge m$$
sometimes it is useful to think of
$$\wedge^k(M) = T^k(M)/ < m_1 \otimes ... \otimes m_n : \exists\ i, j\ s.t. m_i = m_j >$$

- Universal Prop for alternating multilinear maps: Given $\phi : M \times .... \times M \to N$ which is alternating multilinear then there is a unique $\Phi : \wedge^k(M) \to N$ with $\phi = \Phi \circ i$. where $i : M \times ... \times M \to \wedge^k(M)$ with $i(m_1, ..., m_k) = m_1 \wedge ... \wedge m_k$

12 Feb 17

12.1 More on exterior, alternating and symmetric algebra

- Suppose that V is an n-dimensional F-vector space (M a rank n free R-module), Then
$$dim \wedge^k V = \binom{n}{k}, \quad (rank \wedge^k M = \binom{n}{k}).$$
If $e_1, ..., e_n$ is a basis for V then $\{e_{i_1} \wedge ... \wedge e_{i_k} | i_1 < ... < i_k\}$ is a basis for $\wedge^k V$.
For the symmetric algebra $S^k(M)$ will have $n^2 - \binom{n}{k}$ basis elements.

- Suppose that V is 2-dimensional with basis e_1 and e_2. Bases for $T^2(V), S^2(V), \wedge^2(V)$.
$T^2(V)$ basis is $e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2$.
$S^2(V)$ basis is $e_1 \otimes e_1$, $e_2 \otimes e_2$. $e_1 \otimes e_2$.
$\wedge^2(V)$ basis is $e_1 \wedge e_2$.

- $R = \mathbb{Z}[x, y]$, $I = (x, y)$ is not a free R-module. Consider $\phi : I \times I \to \mathbb{Z}$ by
$$\phi(a(x, y)x + b(x, y)y, c(x, y)x + d(x, y)y) = a_{0,0}d_{0,0} - b_{0,0}c_{0,0}$$
where subscript $0, 0$ denotes constant terms (in general subscript (n, m) indicates coef of $x^n y^m$. Lots of writing but not hard to show that this is bilinear. Also easy to check that it is alternating i.e. $\phi(a(x, y)x + b(x, y)y, a(x, y)x + b(x, y)y) = 0$.
So there is a unique $\Phi : \wedge^2 I \to \mathbb{Z}$ by
$$\Phi(ax + by, cx + dy) = a_{0,0}d_{0,0} - b_{0,0}c_{0,0}.$$
Note $\Phi(x \wedge y) = 1$. So we have $\wedge^2 \mathbb{Z}[x, y] = 0$ but $\wedge^2 I \neq 0$ so $\wedge^1 I \to \wedge^2 R$ is not an injection.

- Suppose that $\eta \in T^k(M)$. We say that η is symmetric if $\sigma(\eta) = \eta$ for all $\sigma \in S_k$. where σ is defined by action on simple tensor by $\sigma(m_1 \otimes ... \otimes m_k)$ by $m_{\sigma^{-1}(1)} \otimes ... \otimes m_{\sigma^{-1}(k)}$.
Define $\epsilon(\sigma) := sign(\sigma)$ (positive if σ is product of even number of transpositions and negative if product of odd number of transpositions.
We say that $n \in T^k(M)$ is alternating if $\sigma(\eta) = \epsilon(\sigma)\eta$ for all $\sigma \in S_k$.

- Ex $k = 3$.
$$e_1 \otimes e_2 \otimes e_3 + e_1 \otimes e_3 \otimes e_2 + e_2 \otimes e_1 \otimes e_3 + e_2 \otimes e_3 \otimes e_1 + e_3 \otimes e_1 \otimes e_2 + e_3 \otimes e_2 \otimes e_1$$
is a symmetric tensor in $T^3(V)$ where V is 3-dimensional.
$$e_1 \otimes e_2 \otimes e_3 - e_1 \otimes e_3 \otimes e_2 - e_2 \otimes e_1 \otimes e_3 + e_2 \otimes e_3 \otimes e_1 + e_3 \otimes e_1 \otimes e_2 - e_3 \otimes e_2 \otimes e_1$$
is an alternating tensor.

- Define: $Sym : T^k(M) \to T^k(M)$ by $Sym(\eta) = \sum_{\sigma \in S_k} \sigma(\eta)$. Notice that $Sym(\eta)$ is always a symmetric tensor.

- Define $Alt : T^k(M) \to T^k(M)$ by $Alt(\eta) = \sum_{\sigma \in S_k} \epsilon(\sigma)\sigma(\eta)$. Notice that $Alt(\eta)$ is always an alternating tensor.

- we have a 1-1 correspondence $\frac{1}{k!}Sym : S^k(M) \leftrightarrow \{$ symmetric tensors $\}$. Similarly $\frac{1}{k!}Alt : \wedge^k(M) \leftrightarrow \{$ alternating tensors $\}$

12.2 modules and vector spaces over PIDs

- Let F be a field and $F[x]$ a PID. Let V be an F-vector space. Can make V into an $F[x]$ module given a linear transformation $T : V \to V$ let $T^0 = I$, $T^1 = T$, $T^2 = T \circ T$, ...

  Then can define, for any polynomial $p = a_n x^n + ...a_0$, $p(x) \cdot v = p(T)(V) = a_n T^n + ...a_0 I$.

- Ex: If $T = 0$ then $T^i = 0$ for all i so $p(T) \cdot v = a_0 I v = a_0 v$.

- If $T = I$ then $p(T)(v) = (a_n + ... + a_0)v$.

- Let V be d dimensional define $T(x_1, ..., x_d) = (0, x_1, ..., x_{d-1})$. Then we have $T(e_i) = e_{i+1}$ for $i \neq d$ and $T(e_d) = 0$. and $T^k(e_i) = \begin{cases} e_{i+k} & 1 \leq i \leq d-k \\ 0 & otherwise \end{cases}$.

  Then for $d > n$, $P(T)(e_1) = a_0 e_1 + a_2 e_3 + ...a_n e_{n+1}$. and for $d \leq n$, $P(T)(e_1) = a_0 e_1 + a_2 e_3 + ...a_{d-1} e_d$.

  Similarly for $P(T)(e_2)$.

13 Feb 19

- Homework: 11.5 - 12,14. 12.1 5,6,13,14,15 Due Friday Feb 28

13.1 More on Modules over PID

- from last time define T: $V \to V$, $e_1, ..., e_n$ a basis of V, by $T(x_1, ..., x_n) = (0, x_1, ..., x_{n-1})$ then

$$T^k(e_i) = \begin{cases} e_{i+k} & 1 \le i \le n-k \\ 0 & otherwise \end{cases}.$$

If $m < n$ and $a_m x^m + ... + a_0$ then $(a_m x^m + ... + a_0)(e_i) = (0, 0, ..., \underbrace{a_0}_{ith}, a_1, ..., a_k$.

- Note: There is a 1-1 correspondence between

$$\{V : V \ an \ F[x] - module\}$$

and

$$\{F \text{ vector space } V \text{ paired with linear trans } T\}.$$

If V is an $F[x]$ module and T is the linear transformation that describes the action of x on a vector. Let W be an F-vector space of V. consider $T(W)$. Is W a submodule of V with respect to the $F[x]$ action on V. We have $p(x)(w) = p(T)(w) \in V$ when is this in W? Need $T(w) \in W$, i.e when W is T-invariant. So - W will be an $F[x]$ submodule of W iff $T(W) \le W$ i.e. W is T-invariant or T-stable.

for the example above with $T(e_i) = e_{i+1}$ then $W_i = \{(0, .., 0, x_i, .., x_n : x_i \in F\}$ are T-invariant. but $U_i = \{(x_1, ..., x_i, 0, 0, ..., 0\}$ is not T-invariant.

- A finitely generated R-module M has rank n if the largest number of linearly independent elements in M is n.

  Ex: $M = R^n$ has rank n. However if the module is not free then the rank is not necessarily equal to the number of generators.

  Ex: In $\mathbb{Z}[x.y]$, $I(x, y)$ then if we let $x = y$, $b = -x$ then $ax + by = 0$ with $a \neq 0$ and $b \neq 0$ so x, y are linearly dependent. Hence $rank I < 2$. Now $\{x\}$ is an R-linearly independent set so $Rank I = 1$.

- Def: An R-module M is Noetherian if $N_1 \subset N_2 \subset ... \subset N_i \subset ...$ is any chain of submodules in M there is n such that for all $i \ge n$, $N_i = N_n$. i.e. any ascending chain of submodules stabilizes (ascending chain condition).

  If all submodules of M are finitely generated then M is Noetherian.

  Note! ascending chain condition and Noetherian are equivalent conditions (proved last semester).

- Theorem. Let R be a PID, M a free module of rank n and $N \subset M$ then N is a free submodule of rank $m \le n$. Moreover there is a basis $y_1, ..., y_n$ of M such that $a_1 y_1, ..., a_m y_m$ is a basis of N and a_1 divides a_2 divides ... divides a_m.

  Proof. take $\phi : M \to R$ then $\phi(N) =\subset R$ is a principle ideal i.e. there is $a_\phi \in R$ with $\phi(N) = (a_\phi)$. now let $\Sigma = \{(a_\phi) : \phi \in Hom_R(M, R)\}$. Now for any 2 elements $(a_\phi), (a_\psi)$ there is d the GCD of a_ϕ and a_ψ, $(d) = \{r_\phi a_\phi + r_\psi a_\psi : r\phi, r\psi \in R\}$ and we have $(a_\phi) \subset (d)$ and $(a_\psi) \subset (d)$. Then by noetherianess we have that σ will have maximal elements. let $\nu(N) = (a_\ni)$ be a maximal element. Then $a_\nu \not\subset (a_\phi)$ for $\Sigma \ni (a_\phi) \neq (a_{nu})$. Set $a_1 = a_\nu$. Let $x_1, ..., x_n$ be a basis of M then there is $u \in N$ with $\nu(y) = a$. The map $\pi_i : M \to R$ by $\pi_i(b_1 x_1 + ... + b_n x_n = b_i$. Now since $a_1 \neq 0$, $N \neq 0$ so $\pi_i(N) \neq 0$ for at least 1 i.

  We need to show for any $\phi \in Hom_R(M, R)$, $a_1 | \phi(y)$. Now $(d) = (a_1, \phi(y))$ and $d = r_1 a_1 + r_2 \phi(y)$. Let $\psi(r_1 \nu + r_2 \psi$. then $\psi(y) = r_1 a_1 + r_2 \phi(y) = d$. So $d \in \psi(N)$, but also $(d) \subset \psi(N)$ and $(a_1) \subset (d) \subset \psi(N)$. so $\psi(N) \subset (a_1) \Rightarrow (d) = (a_1)$ so $a_1 | \phi(y)$.

Now $a_1|\pi_i(y)$ for all i. Then $\pi_1(y) = a_i b_i$. Let $y_1 = \sum_{i=1}^{n} b_i x_i$. then $a_1 y_1 = \sum a_1 b_i x_i = \sum \pi_i(y) x_i = y$. Since $a_1 = \nu(y) = \nu(a_1 y_1) = a_1 \nu(y_1)$ so $\nu(y_1) = 1$. So we may write $M = Ry_1 \oplus Ker(\nu)$ since for $x \in M$ we have $x = \underbrace{\nu(x)y_1}_{\in Ry_1} + \underbrace{(x - \nu(x)y_1)}_{\in ker(\nu)}$. NOw if $r_1 y_1 = ker\nu \cap Ry_1$ then $r_1 = r_1\nu(y_1 = \nu(r_1 y_1) = 0$.

Then $N = Ra_1 y_1 \oplus ker\nu \cap N$.

Can repeat this process to get direct sum decomposition.

$\square$

14 Feb 21

14.1 midterm 1 review

- sections 10.1- 10.5, 11.3, 11.5.
- Major topics:
  1. $Hom_R(N, M)$
  2. free modules (Universal property)
  3. direct sums
  4. tensor products (universal property)
  5. diagram chasing (definitely on test, look at unassigned diagram chasing problem)
  6. projective modules
  7. injective modules
  8. flat modules.
  9. dual vector spaces.
  10. tensor algebras
- recall $A^2(V) =< v \otimes v : v \in V >$
- basis for $T^2(V)$, $V = F^3$ with $char(F) \neq 2$. then basis of V is e_1, e_2, e_3 and basis for $T^2(v) = e_1 \otimes e_1, e_1 \otimes e_2, e_1 \otimes e_3, e_2 \otimes e_2, e_2 \otimes e_2, e_2 \otimes e_3, e_3 \otimes e_1, e_3 \otimes e_2, e_3 \otimes e_3, e_1 \otimes e_2$.

  In C^2 we identify $e_j \times e_i$ with $e_i \otimes e_j$ so basis for $S^2(V) = T^2/C^2$ is $e_1 \otimes e^1 + C^2, e_2 \otimes e_2 + C^2(V), e_3 \otimes e_3 + C^2, e_1 \otimes e_2 + C^2(V), e_1 \otimes e_3 + C^2(V), e_2 \otimes e_3 + C^2(V)$.
- example on flatness: R comm ring. M flat right R-module, N and (R, S) bimodule a flat S module. (from homework).

  if $0 \longrightarrow L \longrightarrow K$ injection of S modules. Then $0 \longrightarrow N \otimes_S L \longrightarrow N \otimes_s K$ is an injection of R modules since N is flat S-module

  then $0 \longrightarrow M \otimes_R (N \otimes_S L) \longrightarrow M \otimes_R (N \otimes_s K)$ is an injection since M is flat R module.

  but by prop of tensors $M \otimes_R (N \otimes_S L) \cong (M \otimes_R N) \otimes_S L$ and $M \otimes_R (N \otimes_S K) \cong (M \otimes_R N) \otimes_S K$ so

  $0 \longrightarrow (M \otimes_R N) \otimes_S L \longrightarrow (M \otimes_R N) \otimes_S K$ in an injection as well.
- 10.5 problem 1d see book for statement:

  There is $c \in C$ with $\gamma(c) = 0$. since ϕ is surjective there is $b \in B$ with $\phi(b) = x$ then $0 = \gamma(x) = \gamma \circ \phi(b) = \phi' \circ \beta(b)$. then $\beta(b) \in ker(\phi') = im(\psi')$. Now there is $a' \in A'$ with $\psi'(a') = \beta(b)$ since α is surjective there is $a \in A$ with $\alpha(a) = a'$ then $\beta \circ \psi(a) = \psi' \circ \alpha(a) = \psi'(a') = \beta(b)$. Since β is injective $b = \psi(a)$ and $\phi(b) = \phi \circ \psi(a) = 0$ but $\phi(b) = c = 0$ so γ is injective.

  Note to show a map is injective when diagram chasing start in top row. to show a map is surjective start in bottom row.
- know examples, how to identify which modules are projective, injective, flat i.e. free $\Rightarrow$ flat, projective $\Rightarrow$ flat.

  Ex: $\mathbb{Z}_2[x]$ as a $\mathbb{Z}$-module. Not free $\mathbb{Z}$ module since it has torsion. Since it has torsion not projective. not divisible so its not injective. Also not flat (has torsion).

  Ex: $\mathbb{Z}_2[x]$ as a $\mathbb{Z}_6$-module. then is projective since Z_2 is a direct summand of $\mathbb{Z}_6$. is divisible so it is injective. and is flat (since it is projective).

  Ex: $\mathbb{Z}$ as a $\mathbb{Z}$ module is projective but not projective

  Ex: $\mathbb{Q}$ is injective but not projective

  Ex: $\mathbb{Q}/\mathbb{Z}$ is injective but not flat.

15 Feb 26

- Note about test: For tensor product problem:

$$\begin{tikzcd} A \times (B \otimes_R C) \arrow[r, "i"] \arrow[d, "\phi_1"'] & A \otimes_R (B \otimes_R C) \arrow[dl, "\Phi_1"] \\ (A \otimes_R B) \otimes_R C & \end{tikzcd}$$

for $\phi_1(a, b \otimes c) \to (a \otimes b) \otimes c$ need to show that ϕ_1 is bilinear. Then make similar diagram switching A and C to get Φ_2. Then $\Phi_1 \circ \Phi_2 = \Phi_2 \circ \Phi_1 = Id$.

15.1 Fundamental theorem for finitely generated PIDs

- Suppose M is a finitely generated module over a PID. Then M is isomorphic to $R^k \oplus R/(a_i) \oplus ... \oplus R/(a_m)$ where $a_1|a_2|...|a_m$. In order to produce such a decomposition we can use the matrix game.

- $F[x]$ is a PID when F is a field. If V is an F vector space and T a linear transformation then there is a 1-1 correspondence between $F[x]$ modules and the pairs (V, T).

- Recall some facts from linear algebra: λ is an eigenvalue of T if there is a non-zero vector $v \in V$ with $Tv = \lambda v$. In this case we say that v is an eigenvector of T.

  The eigenspace of λ is $E_\lambda = \{v \in V : Tv = \lambda v\}$.

  Note the following are equivalent:

  1. λ is an eigenvalue of T
  2. $T - \lambda I = 0$. is non-singular linear transformation.
  3. $det(T - \lambda I) = 0$.

  The characterisitc polynomial for a linear transformation $T : V \to V$ is $C_T(x) = det(xI - T)$. Note that if λ is an eigenvalue of T then $C_T(\lambda) = 0$. By Fundamental theorem of fintely generated modules over PIDs we have $V \cong \dfrac{F[x]}{a_1(x)} \oplus ... \oplus \dfrac{F[x]}{a_m(x)}$ with $a_1(x)|a_2(x)|....|a_m(x)$. Then we have $a_m(x)V = 0$. We say the annihilator of V is the biggest ideal of $F[x]$ such that $IV = 0$. In this case we have $(a_m(x)) = AnnV$.

  The monic polynomial which is an associate of $a_m(x)$ is called the minimum polynomial of T.

  Consider $F[x]/(a(x))$ with $a(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ monic. $x\bar{1} = \bar{x}$. $x\bar{x} = \bar{x}^2$ and so on until $x\bar{x}^{n-1} = \bar{x}^n = -a_0 - a_1\bar{x} - ...a_{n-1}\bar{x}^{n-1}$.

  So as an operator on $F[x]/(a(x))$, x can be represented by the matirx

$$x = \begin{pmatrix} 0 & 0 & .... & 0 & -a_0 \\ 1 & 0 & .... & 0 & -a_1 \\ 0 & 1 & .... & 0 & -a_2 \\ \vdots & & \ddots & & \\ 0 & 0 & .... & 1 & -a_{n-1} \end{pmatrix}$$

  This is called the companion matrix to $a(x)$, $C_{a(x)}$

  The rational canonical form (RCF) for $\dfrac{F[x]}{a_1(x)} \oplus ... \oplus \dfrac{F[x]}{a_m(x)}$ with each $a_i(x)$ monic is

$$\begin{pmatrix} C_{a_1(x)} & 0 & ... & 0 \\ 0 & C_{a_2(x)} & ... & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & C_{a_m(x)} \end{pmatrix}$$

given $T: V \to V$ create the matrix $XI - T$ with respect to some basis $(T(b_1)...T(b_n)) = A$ each $T(b_i)$ is a column of A. then play the matrix game on $xI - A$ to produce

$$\begin{pmatrix} 1 & & 0 & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & a_1(x) & & \\ & & & & \ddots & \\ & & & & & a_m(x) \end{pmatrix}$$

Matrix game with $A = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$

$$\begin{pmatrix} x-2 & -1 \\ -3 & x-4 \end{pmatrix} \to \begin{pmatrix} -1 & x-2 \\ x-4 & -3 \end{pmatrix} \to \begin{pmatrix} 1 & 2-x \\ x-4 & -3 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 2-x \\ 0 & -x^2-6x+5 \end{pmatrix} \to \begin{pmatrix} 1 & 00 & x^2-6x+5 \end{pmatrix}$$

rcf is $\begin{pmatrix} 0 & -5 \\ 1 & 6 \end{pmatrix}$

16 Feb 28

16.1 More on rational Cannonical form

- Rational Canonical form is unique.

  will show $C_{a(x)}$ companion matrix for $a(x)$ is unique. Given T, multiplying by $x(T)$ generates all the basis elements. If we have subspaces D_i which are T invariant it is enough to determine the e_i for that particular polynomial. i.e. given $F[x]/(b_i(x)) \cong D_i$. Then $T^j e_i$ will give us the rest of the basis elements for the block. So given $b_1|b_2|....|b_t$ such that $V \cong F[x]/(b_1) \oplus ... \oplus F[x]/(b_t)$ and $F[x]/(b_i(x)) \cong D_i$. There is a basis $e_1, Te_1, ..., T^{m-1}e_1, e_2, Te_2, ..., T^{n_t-1}e_t$. which puts T into the form

$$\begin{pmatrix} C_{b_1(x)} & & 0 \\ & \cdots & \\ 0 & & C_{b_t(x)} \end{pmatrix}$$

  If $m_T(x) = a_m(x)$ then $b_t(x)|a_m(x)$ and $a_m(x)|b_t(x)$ can work backwards to see that $a_i(x) = b_i(x)$.

  If S and T are similar matrices then they have the same invariant factors so the same rational canonical form.

  In particular if $S \sim T$ then There is $UinV$ such that $S = U^{-1}TU$ so $US = TU$. Now if $Sx \subseteq W$ for some $x \in W$ then UW is a subspace isomorphic to W (by invrtibility of U. Then $TU(x) \subset UW$ (since if $Sx = w \in W$ then $T(Ux) = USx = Uw \in UW$.

- Theorem: (Cayley Hamilton) if $C_T(x) = a_1(x) \cdots a_m(x)$ then a_m is the minimum polynomial $m_T(x)$. In parituclar if $C_T(T) = 0$ then $M_T(T) = 0$. More generally $m_T(x)|C_T(x)$ and $C_T(x)|M_T(x)^m$ and $M_T(x)^n$ for $n \geq m$.

  Ex: Suppose that A is a 3×3 matirix with $C_A(x) = (x-1)^2(x+1)$. How many rational canonical forms correspond to this characteristic polynomial?

invariant factors	RCF
$(x-1)^2(x+1)$	$\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$
$(x-1), x^2-1$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

  Ex. Find all 4×4 matrices with minimum polynomial $x^2 - 1$.

invariant factors	RCF
x^2-1, x^2-1	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
$(x-1), (x-1), x^2-1$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
$(x+1), (x+1), x^2-1$	$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Ex: Problem from jan qual: A is a 10×10 matrix satisfying $A^{10000} = 0$ show $A^{10} = 0$ let $f(x) = x^{10000}$ only irreducible factor of x^{10000} is x. So characteristic polynomial divides x^{10000} and has degree 10 so $C_A(x) = x^{10}$ is the only polynomial dividing f having degree 10. Since the matrix has to be a zero of the characteristic polynomial it follows that $A^{10} = 0$.

- To find the RCF of a matrix A we play the matrix game on $XI - A$.

  Rules for matrix game:

  1. Can swap rows or cols
  2. Multiply by any non-zero element of F
  3. replace a row/column by sum of multiple of that row/column with multiple of another row/column.

- note if you keep track of ROW ops (not col) then you can reconstruct invariant factors.
- EX:

$$A = \begin{pmatrix} 2 & -3 & 3 \\ 0 & -3 & 5 \\ 0 & 1 & 1 \end{pmatrix}$$

$$XI - A = \begin{pmatrix} x-2 & 3 & -3 \\ 0 & x+3 & -5 \\ 0 & -1 & x-1 \end{pmatrix} \to (R_1 \leftrightarrow R_3)$$

$$XI - A = \begin{pmatrix} 0 & -1 & x-1 \\ 0 & x+3 & -5 \\ x-2 & 3 & -3 \end{pmatrix} \to (C_1 \leftrightarrow C_2)$$

$$XI - A = \begin{pmatrix} -1 & 0 & x-1 \\ x+3 & 0 & -5 \\ 3 & x-2 & -3 \end{pmatrix} \to (-R_1)$$

$$XI - A = \begin{pmatrix} 1 & 0 & 1-x \\ x+3 & 0 & -5 \\ 3 & x-2 & -3 \end{pmatrix} \to (-(x+3)R_1 + R_2 \to R_2, -3R_1 + R_3 \to R_3)$$

$$XI - A = \begin{pmatrix} 1 & 0 & 1-x \\ 0 & 0 & x^2+2x-8 \\ 0 & x-2 & 3x-6 \end{pmatrix} \to ((x-1)C_1 + C_3 \to C_3)$$

$$XI - A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & x^2+2x-8 \\ 0 & x-2 & 3x-6 \end{pmatrix} \to (R_2 \leftrightarrow R_3)$$

$$XI - A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-2 & 3x-6 \\ 0 & 0 & x^2+2x-8 \end{pmatrix} \to (-3C_2 + C_3 \to C_3)$$

$$XI - A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & x^2+2x-8 \end{pmatrix}$$

So we have

$$RCF = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 8 \\ 0 & 1 & -2 \end{pmatrix}$$

.

To get invariant factors start with identity matrix and modify step by step with an operation for each row operation in the order in which they came.

modification:

If we $R_i \leftrightarrow R_j$ then swap $C_i \leftrightarrow C_j$.

If we $uR_i \to R_i$ then modify $u^{-1}C_i \to C_i$

If we $a(x)R_i + R_j \to R_j$ then modify $-a(x)C_j + C_i \to C_i$.

The result of this will provide a matrix with the generators of the invariant factors

17 March 2

17.1 More on RCF/matrix game

- last time we had
$$\begin{pmatrix} 2 & -3 & 3 \\ 0 & -3 & 5 \\ 0 & 1 & 1 \end{pmatrix}$$
and performed the sequence of row operations
  1. $R_4 \leftrightarrow R_3$
  2. $-R_1$
  3. $-(x+3)R_2 + R_2 \to R_2$
  4. $-3R_1 + R_3 \to R_3$
  5. $R_2 \leftrightarrow R_3$.

  on $xI - A$.

  Now if we start with identity matrix and perform these on columns we get generators of the invariant factors.
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \to (C_1 \leftrightarrow C_3)$$
$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \to (-C_1)$$
$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$$
  Now $x + 3 \sim A + 3I = \begin{pmatrix} 5 & -3 & 3 \\ 0 & 0 & 5 \\ 0 & 1 & 4 \end{pmatrix}$ so to perform $((x+3)C_2 + C_1 \to C_1)$ we replace $(x+3)C_2$ with the column generated by $(A+3I)c_2$ the resulting matrix is
$$\begin{pmatrix} -3 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \to (3c_3 + c_1 \to c_1$$
$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \to (c_2 \leftrightarrow c_1)$$
$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$
  So can produce basis from e_1 and e_2

  Now $Ae_1 = 2e_1$, $Ae_2 = \begin{pmatrix} -3 \\ -3 \\ 1 \end{pmatrix}$ and so $U = \begin{pmatrix} 1 & 0 & -3 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix}$, $U^{-1} = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}$ and $U^{-1}AU = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 8 \\ 0 & 1 & -2 \end{pmatrix}$ which is a rational canonical form which corresponds to $(x-2), x^2 + 2x - 8 = (x-2)(x+4)$ as desired.

17.2 Jordan Canonical Form

- Assume elementry divisors are powers of linear factors and we have $a_1(x)|a_2(x)|...|a_m(x)$. The eigenvalues are $\lambda_1, ..., \lambda_t$ so we may write

$$a_1(x) = (x-\lambda_1)^{\alpha_{11}} \cdots (x-\lambda_t)^{\alpha_{1t}}$$

$$\vdots$$

$$a_j(x) = (x-\lambda_1)^{\alpha_{j1}} \cdots (x-\lambda_t)^{\alpha_{jt}}$$

  where the α_{ik} may be zero. For $i = 0, ..., j-1$.

- Suppose we have $F[x]/(x-\lambda)^k$ can choose basis as $(\bar{x}-\lambda)^{k-1}, (\bar{x}-\lambda)^{k-2}, ..., (\bar{x}-\lambda), 1$. now we can compute

$$x(\bar{x}-\lambda)^{k-1} = \lambda(\bar{x}-\lambda)^{k-1} + (\bar{x}-\lambda)^k = \lambda(\bar{x}-\lambda)$$

  , similarly

$$x(\bar{x}-\lambda)^{k-2} = \lambda(\bar{x}-\lambda)^{k-2} + (\bar{x}-\lambda)^{k-1}$$

  and

$$x(\bar{x}-\lambda)^{i} = \lambda(\bar{x}-\lambda)^{i} + (\bar{x}-\lambda)^{i+1}$$

  until finally

$$x \cdot 1 = \lambda + \bar{x} - \lambda$$

  Hence multiplication by x is represented by the matrix

$$\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ 0 & & \ddots & & \\ 0 & 0 & 0 & 0 & \lambda \end{pmatrix}$$

  called the JOrdan block for $(x-\lambda)^k$. A Jordan Canonical form for a matrix A is

$$\begin{pmatrix} J_1 & & & 0 \\ & J_2 & & \\ & & \ddots & \\ 0 & & & J_s \end{pmatrix}$$

  where each J_i is a Jordan block.

- Ex for the matrix $\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$ we had $RCF = \begin{pmatrix} 0 & -5 \\ 1 & 6 \end{pmatrix}$ so eigenvalues were $2, 3$ so jordan form is $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$.

- Ex we did RCF of 3×3 matrices with char poly $(x-1)^2(x+1)$ has ele divisors $(x-1), (x-1), (x+1)$ or $(x-1)^2, x+1$ these correspond to $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 00 & 0 & -1 \end{pmatrix}$

- Ex: 4×4 with minimal poly $x^2 - 1$. had 3 sets of invariant factors

  1. x^2-1, x^2-1
  2. $x-1, x-1, x^2-1$
  3. $x+1, x+1, x^2-1$.

  which correspond to elementary divisors

  1. $x-1, x-1, x+1, x+1$
  2. $x-1, x-1, x-1, x+1$
  3. $x+1, x+1, x+1, x-1$

and JCFs of

1. $\begin{pmatrix} 1 & & & \\ 0 & 1 & & \\ 0 & 0 & -1 & \\ 0 & 0 & 0 & -1 \end{pmatrix}$

2. $\begin{pmatrix} 1 & & & \\ 0 & 1 & & \\ 0 & 0 & 1 & \\ 0 & 0 & 0 & -1 \end{pmatrix}$

3. $\begin{pmatrix} 1 & & & \\ 0 & -1 & & \\ 0 & 0 & -1 & \\ 0 & 0 & 0 & -1 \end{pmatrix}$

- In example finished at beginning of class we have invariant factors of $(x-2), x^2+2x-8$ so elementary divisors $x-2, x-2, x+4$ and JCF $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -4 \end{pmatrix}$

  Can get this if we don't already have RCF by following procedure:

  In this case we had e_1 generated a cyclic submodule of dim 1 and e_2 generate a cyclic submodule of dim 2.

  Suppose that f generates $V \cong F[x]/(a(x))$ with $a(x) = (x-\lambda_1)^{\alpha_1} \cdots (x-\lambda_t)^{\alpha_t}$. then $\dfrac{a(x)}{(x-\lambda_i)}^{\alpha_i}$ gives generators for submodule $F[x]/(x-\lambda_i)^{\alpha_i}$.

  Apply this to case above we have $\dfrac{x^2+2x-8}{x-2}e_2 = (x+4)e_2 = (A+4I)w_2 = (-3,1,1)$ and $\dfrac{x^2+2x-8}{x+4}e_2 = (x-2)e_2 = (-3,-3,1)$ then $U = \begin{pmatrix} 1 & -3 & -3 \\ 0 & 1 & -5 \\ 0 & 1 & 1 \end{pmatrix}$ and $U^{-1}AU = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & -4 \end{pmatrix}$

18 March 4

18.1 More on Jordan Form

- To find P such that $P^{-1}AP = J$ where J is the Jordan form of A. let $C_A(x) = det(A - xI)$ is char polynomial $C_A(x) = (x - \lambda_1)^{m_1}...(x - \lambda_s)^{m_s}$. F algebraically closed. Follow the process

  1. For each λ_i calculate $N(A - \lambda_i I)$. $dim(N(A - \lambda_i I))$ tells how many cyclic subspaces there are of the form $F[x]/(x - \lambda_i)^{s_{ij}}$ there are. $s_{i1} + ...s_{ir_i} = m_i$.
  2. Compute the null space $N(A - \lambda_i I)^k)$ for $2 \le k$ until $dim(N(A - \lambda_i I)^k) = m_i$ the multiplicity of λ_i. Stop at the smallest k where this happens - $k = \max\{s_{ij} : 1 \le j \le i_r\}$.

     denote by $E_{\lambda_i} = \{v : \lambda_i v = Av\}$ the eigenspace of λ_i. and let $G_{\lambda_i} = \{v : \exists\ k\ s.t.\ (A - \lambda_i I)^k v = 0\}$ the generalized eigenspace of λ.
  3. Choose $v_{i1} \in G_{\lambda_i}$, $v_{i1} \in N((A - \lambda_i I)^k) \setminus N((A - \lambda_i I)^{k-1})$ then $v_{i1}, (A - \lambda_i I)v_{i1}, ..., (A - \lambda_i I)^{k-1}v_{i1}$ generate a cyclic subspace isomorphic to $F[x]/(x - \lambda_i)^k$.
  4. If $k = m_i$, done. If not there is $v_{i2} \in N(A - \lambda_i I)^k \setminus N((A - \lambda_i I)^{k-1} \cup span\{(A - \lambda_i I)^j v_{i1}\}_{j=0}^{k-1}$. generate $v_{i2}, (A - \lambda_i I)v_{i2}, ...(A - \lambda_i I)^{k-1}v_{i2}$ repeat if necessary. If there is not $v_{i2} \in N(A - \lambda_i I)^k \setminus N((A - \lambda_i I)^{k-1} \cup span\{(A - \lambda_i I)^j v_{i1}\}_{j=0}^{k-1}$ the search next in $N(A - \lambda_i I)^{k-1})$ for such vectors. generate $v_{i2}, (A - \lambda_i I)v_{i2}, ...(A - \lambda_i I)^{k-2}v_{i2}$. Keep going until we have a basis of G_{λ_i} formed by the cyclic subspace bases.

- Ex: $A = \begin{pmatrix} 3 & 1 & 4 & 2 \\ -1 & 1 & -3 & 3 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$ char poly is $(x - 2)^3(x - 3)$.

  Now

  $$A - 3I = \begin{pmatrix} 0 & 1 & 4 & 2 \\ -1 & -2 & -3 & 3 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

  which has row eschelon form of

  $$\begin{pmatrix} 1 & 0 & 0 & -7 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

  which gives $(7, -2, 0, 1)$ as the eigenvalue for 3.

  Now

  $$A - 2I = \begin{pmatrix} 1 & 1 & 4 & 2 \\ -1 & -1 & -3 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

  which has row eschelon form of

  $$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

  which gives $(-1, 1, 0, 0)$ as the eigenvalue for 2.

  Now

  $$(A - 2I)^2 = \begin{pmatrix} 0 & 0 & 1 & 9 \\ 0 & 0 & -1 & -2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

which has row eschelon form of

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

which has null space of $span\{(1,0,0,0),(0,1,0,0)\}$. Now $(-1,1,0,0)$ is in this space, so we need to continue.

Now

$$(A-2I)^3 = \begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

which has row eschelon form of

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

which has null space of $span\{(1,0,0,0),(0,1,0,0),(0,0,1,0)\}$. Now e_3 is not in the previous null space so can use it to compute rest of basis.

we have $(A-2I)e_3 = (4,-3,0,0)$, and $(A-2I)e_3 = (1,-1,0,0)$. note this last one must be the eigenvector (a good way to check work). Now we can write down P with these vectors as columns.

$$P = \begin{pmatrix} 1 & 4 & 0 & 7 \\ -1 & -3 & 0 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and one may compute $P^{-1} = \begin{pmatrix} -3 & -4 & 0 & 29 \\ 1 & 1 & 0 & -9 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ and $P^{-1}AP = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$ which is a jordan form.

18.2 The field theory

- Let $F \subset K$ be fields. We say that F is a subfield of K and K is a field extension of F. Let $\alpha \in K \setminus F$. could have $1, \alpha, ...\alpha^{n-1}$ be linearly independent over F and $\alpha^n = -(b_{n-1}\alpha^{n-1} + ...b_0)$. with $b_i \in F$. then α is the zero of $x^n + b_{n-1}x^{n-1} + ... + b_0 \in F[x]$. Then $f(x)$ is irreducible so $F[x]/(f(x))$ is a field and a field extension of F.

19 March 6

19.1 Field theory continued

- F, K fields with $F \subseteq K$ then K is called a field extension of F. for each $r \in F$ we have $rK \subset K$ so multiplication by F gives scalar multiplication of F on K and K can be viewed as an F-vector space.

- Def: the index or degree of F in a field extension K is $[K : F] = dim_F K$. (The dimension of K considered as a vector space over F.)

- Prop: Let $\phi : F \to F'$ be a homomorphism of fields. Either ϕ is 1-1 or ϕ is the trivial homomorphism.

  Proof. A field F has only the ideals 0 and F, so $ker(\phi) = 0$ or $ker(\phi) = F$. If $ker(\phi) = 0$ then ϕ is one to one and if $ker(\phi) = F$ then ϕ is the trivial map. □

  If we have a 1-1 homomorphism of fields $\phi : F \to F'$ then $\phi(F) \subseteq F'$ is an isomorphism. So often we call $\phi(F)$ F since they are isomorphic.

- Prop. Given F a field $p(x) \in F[x]$ an irreducible polynomial there is a field extension K of F having a zero of $f(x)$ in it.

  Proof. Consider $K = F[x]/(p(x))$. then K is a field since $(p(x))$ is a maximal ideal. Define $\pi : F[x] \to K$ by $\pi(g(x)) = g(x) + (p(x))$ and consider $\pi|_F : F \to K$ which is a homomorphism $F \to K$. Moreover $\pi|_F$ is not trivial since $\pi(1) = 1 + (p(x)) \neq (p(x))$ so $\pi|_F(1) = 1 + (p(x)) \neq (p(x))$. So $\pi|_f$ is not trivial and therefore 1-1 so $\pi|_F \cong F$ and can view the image as F. So we have $F \subset K$. Let $\bar{x} = x + ((p(x))$, then $p(\bar{x}) = p(x) + ((p(x)) = (p(x)) = 0$ in K. So $\bar{x}$ is a zero of $p(x)$ living in K. □

- Theorem: Let F be a field and $K \subseteq F$ be an extension of F. Suppose that $\alpha \in K$ is the zero of some polynomial $f(x) \in F(x)$. Then there is monic a polynomial $m_{\alpha,F}(x)$ with minimal degree and $m_{\alpha,F}(x)$ divides $f(x)$.

  Let $S = \{g(x) : g(\alpha) = 0\}$ then $deg(g) \in \mathbb{N}$ and since $\mathbb{N}$ is well ordered it has a smallest element and so $\{deg(g) : g \in S\}$ also has a smallest element. Let $g(x)$ be a monic polynomial smallest degree (we can attain this by dividing by leading coefficient if g weren't monic). We need to show that g is irreducible. Suppose $deg(g) = n$.

  Suppose g is not irreducible, $g(x) = a(x)b(x)$ then $1 \leq deg(a), deg(b) < deg(g)$. Then $g(\alpha) = a(\alpha)b(\alpha) \Rightarrow a(\alpha)$ or $b(\alpha) = 0$, but then g was not such a polynomial of least degree, a contradiction, so g was irreducible.

  Now we can use the division algorithm to write $f(x) = q(x)g(x) + r(x)$ where $r(x) = 0$ or $deg(r) < deg(g)$. then

  $$0 = f(\alpha) = q(\alpha)g(\alpha 0 + r(\alpha) = r(\alpha)$$

  so $r(x) = 0$ (again my minimal degree of g. and we have that $g(x)$ divides $f(x)$.

- Def: The monic polynomial of minimal degree with coefficients in F with α as a zero is called the minimal polynomial of α over F. this is denoted in different ways $m_{\alpha,F}(x)$, $irr(\alpha, F)$, etc...

- Cor: $F \subseteq K \subseteq E$, $\alpha \in E$ with α the zero of a minimal polynomial with coefficients in F then $m_{\alpha,K}(x) | m_{\alpha,F}(x)$. We have $m_{\alpha,F}(x) \in F[x] \subseteq K[x]$ and $m_{\alpha,k}(x) \subset K[x]$ and α is a zero of $m_{\alpha,K}(x)$. Since $m_{\alpha,K}$ is the min poly for α with coefficients in K we have $m_{\alpha,K}(x) | m_{\alpha,F}(x)$.

- Ex: $x^2 + 1 \in \mathbb{Q}[x]$. then i is a zero and $x^2 + 1 = m_{i,\mathbb{Q}}(x)$. If $K = Q(i)$ then $m_{i,K}(x) = x - i$.

- Thm: If $K = F[x]/((p(x))$ with $p(x)$ irreducible over F then $\theta = x + ((p(x))$ then θ is a zero of $p(x)$ and $1, \theta, \theta^2, ..., \theta^{n-1}$ where $n = deg(p)$ is a basis for K over F.

Proof. We have already seen that θ is a zero of p. Need to show that $1, \theta, ..., \theta^{n-1}$ spans K and are linearly independent.

Take $f(x) \in F[x]$ then $f(x) + ((p(x)) = r(x) + ((p(x))$ where $f(x) = q(x)p(x) + r(x)$ where $deg(r) < n$. and $f(\theta) = r(\theta) = a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1}$, so the θ_i span $F[x]$.

Suppose that $a_0 + a_1\theta + ...a_{n-1}\theta^{n-1} = 0$ then θ is a zero of $g(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$. but then $p(x)|g(x)$ but this is impossible since $deg(p) = n > deg(g) = n - 1$. So each $a_i = 0$ so the θ_i are linearly independent. □

- Let $K = F[x]/((p(x))$ and $\theta = x + p(x)$. Sometimes we write this as $K = F(\theta) = \{a_0 + a_1\theta + ...a_{n-1}\theta^{n-1} : a_i \in F\}$. if we take $a(\theta), b(\theta) \in K$ then $a(\theta)b(\theta)$ is a polynomial. If $deg(ab) > n$ then $ab \equiv r \mod p$ with $deg(r) < n$.

- Ex $\mathbb{Z}_2[x]/(x^3+x+1)$, θ is a zero of x^3+x+1. Consider $\theta^2(\theta^2+1) = \theta^4+\theta^2$. Then $\theta^3+\theta+1 = 0 \Rightarrow \theta^3 = \theta+1$. So $\theta^4 = \theta^2 + \theta$. then $\theta^2(\theta^2 + 1) = \theta^2 + \theta + \theta^2 = \theta$. Which tells us that remainder of $x^4 + x^2$ divided by $x^3 + x + 1$ is x (can confirm with long division).

- ex θ^{-1}?

  $p(x) = b_0 + b_1x + ... + x^n$ then

$$0 = p(\theta) = b_0 + b_1\theta + .. + \theta^n$$

$$-b_0 = \theta(b_1 + b_2\theta + ... + \theta^{n-1}$$

so

$$1 = \theta \underbrace{\frac{-1}{b_0}(b_1 + b_2\theta + ... + \theta^{n-1})}_{\theta^{-1}}$$

Given $a(\theta)$ with $deg(a) < n$ then to find $(a(\theta))^{-1}$ use the euclidean algorithm to express $1 = a(\theta)b(\theta) + p(\theta)c(\theta)$.

For example the inverse of $(\theta^2 + \theta + 1)$ from above is $(\theta^2 + \theta + 1)^{-1} = \theta^2$.

20 March 9

20.1 More on Fields

- To construct a field with p^n elements where p is prime we construct $\mathbb{Z}_p[x]/(p(x))$ where $p(x)$ is irreducible in $\mathbb{Z}_p[x]$ of degree n.
- Ex: In $\mathbb{Z}_2[x]$ x^3+x+1 is irreducible, so $\mathbb{Z}_2[x]/(x^3+x+1)$ is a field with 8 elements.

  $K = \mathbb{Z}_2[x]/(x^2+x+1)$ field with 4 elements. There is no subfield of K isomorphic to L. If θ is a root x^2+x+1 then we have $\theta^2+\theta+1 = 0 \Rightarrow \theta^2 = \theta+1$. We can produce the following multiplication table.

$\cdot$	0	1	θ	$\theta+1$
0	0	0	0	0
1	0	1	θ	$\theta+1$
θ	0	θ	$\theta+1$	1
$\theta+1$	0	$\theta+1$	1	θ

- if $F \subset K$ is a field extension $A = \{a_i\}, A \subset K$ the subfield of K generated by F and A is $F(A)$ - the smallest subfield of K containing F and A. If $A \in \{\alpha_1, ..., \alpha_s\}$ then $F(A) = F(\alpha_1, ..., \alpha_s)$. IN this case we call $F(A)$ a finitely generated subfield of K (does not imply finite basis).

  Ex: $F = \mathbb{Q}$ $K = \mathbb{C}$ and $A = \{e\}$. Since e is not algebraic, e is not the zero of any polynomial with coefficients in Q. The smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and e will be $\mathbb{Q}(e) = \{\frac{p(e)}{q(e)} : p, q \in \mathbb{Q}[x], q \neq 0\} \cong \mathbb{Q}(x)$.
- Def: A simple extension of F is of the form $F(\alpha)$.
- $F \subseteq K \cong \dfrac{F[x]}{m_{\alpha,F}(x)} := F(\alpha) = \{b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}\}$.
- Isomorphism extension Theorem: Let F, F' be fileds and $\phi : F \to F'$ be an isomorphism. Suppose $p(x) = a_0+a_1x+...a_{n-1}x^{n-1}+x^n$ is irreducible with $a_i in F$ and $p'(x) = \phi(a_0)+\phi(a_1)x+...+\phi(a_{n-1})x^{n-1}+x^n$ is irreducible in $F'[x]$ then there is an isomorphism $\Phi : F(\alpha) \to F(\beta)$ where α is a root of $p(x)$ and β is a root of $p'(x)$ such that $\Phi|_F = \phi$.

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\Phi} & F'(\beta) \\ \downarrow & & \downarrow \\ F & \xrightarrow{\phi} & F' \end{array}$$

  Proof. ϕ extends to an isomorphism $\psi : F[x] \to F'[x]$ by $\psi(c_0 + c_1x + ... + c_mx^m) = \phi(c_0) + \phi(c_1)x + ... + \phi(c_m)x^m$. Clearly we ahve $\psi(g(x)+h(x)) = \psi(g(x)) + \psi(h(x))$ and $\psi(g(x)h(x)) = \psi(g(x))\psi(h(x))$ and ψ is a bijection. Now let $\Phi : F[x]/(p(x)) \to F'[x]/(p(x))$ since we have $\psi(p(x)) = p'(x)$. then $\tilde{\psi} : F[x] \to \dfrac{F'[x]}{(p(x))}$ with $ker(\tilde{\psi}) = (p(x))$ so by the first isomorphism theorem $F(\alpha) \cong F[x]/(p(x)) \cong F'[x]/(p'(x)) \cong F'(\beta)$. $\square$

- example: $\mathbb{Q}(\sqrt[3]{2} \cong \mathbb{Q}[x]/(x^3-2)$. Then $\sqrt[3]{2}$ is a zero of $x^3 - 2 = 0$. Other roots of this are $\sqrt[3]{2}\zeta_3^i$ where ζ_3 is third root of unity $i = 1, 2$. We have $\mathbb{Q}(\sqrt[3]{2}\zeta_3) \cong \mathbb{Q}[x]/(x^3-2)$ but these fields are not equal.
- We say a field extension K of F if for every $\alpha \in K$ there is a polynomial $f \in F[x]$ with $f(\alpha) = 0$.
- example of extension where you only get 1 zero: $K = \mathbb{Z}_2(t)$, $Z_2(t^4) = F$. then $x^4 - t^4$ is irreducible but $x^4 - t^4 = (x-t)^4 \in K[x]$ so the only root is t.
- Prop: If α is algebraic then $F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$ and $[F(\alpha) : F] = deg(m_{\alpha,F}(x)$.

  Proof. $1, \alpha, ..., \alpha^{n-1}$ is a basis for $F(\alpha)$ then $1, \alpha, ..., \alpha^n$ are linearly dependent. so $\alpha^n+a_{n-1}\alpha^{n-1}+...+a_0 = 0$ is the minimum polynomial is the minimum polynomial for α, F. $\square$

- Prop: Every finite extension of a field F is an algebraic extension.

  Proof. Let $[K : F] = n$ be finite. Take $\alpha \in K$ then $1, \alpha, ..., \alpha^n$ must be linearly dependent so there are a_i with so $\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0$ and α is a root of a polynomial in $F[x]$.

  $\square$

- Note: Algebraic extensions are not always finite: $A = \{\sqrt{p} : p\ prime\}$ then $\mathbb{Q}(A)$ is algebraic but not finite.

  Ex: $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(A)$. then can write

$$\alpha = \sqrt{2} + \sqrt{3} \Rightarrow$$
$$\alpha - \sqrt{2} = \sqrt{3} \Rightarrow \alpha^2 - 2\alpha\sqrt{2} + 2 = 3 \Rightarrow$$
$$\alpha^2 - 1 = 2\alpha\sqrt{2} \to \alpha^4 - 10\alpha^2 + 1 = 0$$

  .

- next time: Thm: if $F \subseteq K \subseteq L$ with $[L : K] < \infty$ and $[K : F] < \infty$ then $[L : F] = [L : K][K : F] < \infty$.

21 March 11

21.1 Tower theorem, degrees of field extensions

- Homework: 13.1 2,6,7, 13.2 4,7,9,14
- Thm: if $F \subseteq K \subseteq L$ with $[L : K] < \infty$ and $[K : F] < \infty$ then $[L : F] = [L : K][K : F] < \infty$.

  Proof. Suppose $n = [L : K]$, $m = [K : F]$. Then there are $\alpha_1, ...\alpha_n$ that form a basis for L over K and there are $\beta_1, ..., \beta_m$ which form a basis over F.

  Claim: $\{\alpha_i\beta_j\}_{ij\in\{1,...,n\}}$ form a basis of L over F. Pick $a \in L$ then $a = \sum a_i\alpha_i$ with $a_i \in K$ then $a_i = \sum_{j=1}^{m} b_{ij}\beta_j$ with $b_{ij} \in F$ then

$$a = \sum_{i=1}^{n}(\sum_{j=1}^{m} b_{ij}\beta_j)\alpha_i = \sum_{i=1}^{n}\sum_{j=1}^{m} b_{ij}\beta_j\alpha_i =$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m} b_{ij}\alpha_i\beta_j$$

  so the α_i, β_j span L over F. So need to show $\alpha_i\beta_j$ are linearly independent. if $\sum b_{ij}\alpha_i\beta_j = 0$ then $\sum_{i=1}^{n}(\sum_{j=1}^{m} b_{ij}\beta_j)\alpha_i =$ but then each $\sum_{j=1}^{m} b_{ij}\beta_j = 0$ since α_i are linearly indep. but then $b_{ij} = 0$ since β_j are linearly indep. Now there are mn products in $\{\alpha_i\beta_j\}$ and the result follows. □

- K is a finite extension of F if and only if K is generated by finitely many algebraic elements. If $K = F(\alpha_1, ..., \alpha_s)$ with $degm_{\alpha_i,F}(x) = n_i$ then $[K : F] \le n_1n_2 \cdots n_s$.

  Proof. if $[K : F] = n < \infty$ then there is a basis $\alpha_1, ..., \alpha_n$ with α_i algebraic. α_i are the zero of polynomials of degree $\le n$. so $K = F(\alpha_1, ...\alpha_n)$.

  $(\Rightarrow)$ $K = F(\alpha_1, .., \alpha_n)$ with α_i algebraic. Then $F[\alpha_i) : F] = n_i$ then $[K : F(\alpha_1, ..., \alpha_{s-1})][F(\alpha_1, ..., \alpha_{s-1}) : F(\alpha_1, ..., \alpha_{s-2})] \cdots [F(\alpha_1) : F]$.

  If $K_i = F(\alpha_1, ..., \alpha_i$ then $K_s = K$ and since $m_{\alpha_i,K_{i-1}}(x)$ divides $m_{\alpha_i,F(x)}$ so $[K_i : K_{i-1}] \le [F(\alpha_i) : F]$ so $[K : F] = [K_s : K_{s-1}]...[K_1 : F] \le n_sn_{s-1}...n_1$. □

- example where degree is less. Take $\mathbb{Q} = F$, $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\zeta_3$. Then $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = [\mathbb{Q}(\alpha_2 : \mathbb{Q}] = 3$ but $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] = 6 \le 9$ since a basis for $\mathbb{Q}(\alpha_1, \alpha_2)/\mathbb{Q}$ is $1, \sqrt[3]{2}, \sqrt[3]{4}, \zeta_3, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3$.
- Prop: If $\alpha, beta \in K$ algebraic over F then $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ are all algebraic over F.

  Proof. α, β are algebraic then $F(\alpha, \beta)$ is algebraic over F, $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in F(\alpha, \beta)$ so are algebric over F. □

- Prop: IF $F \subseteq K \subseteq L$ and K is algebraic over F and L is algebraic over K then L is algebraic over F.

  Proof. Take $\alpha \in L$. Since L is algebraic over K there is a polynomial $p(x) = a_0 + a_1x + ...a_nx^n \in K[x]$ with $p(\alpha) = 0$. Since $a_0, a_1, ..., a_n\ inK$ and K algebraic over F then $[F(a_0, ..., a_n : F] < \infty$ so we have produced a finite extension then $[F(a_0, ..., a_n, \alpha) : F(a_0, ..., a_n] \le n$. Then $[F(a_0, ..., a_n, \alpha) : F] = [F(a_0, ..., a_n, \alpha) : F(a_0, ..., a_n)][F(a_0, ..., a_n] : F] < \infty$ so $F(a_0, ..., a_n, \alpha)$ is algebraic over F so α is algebraic over F. □

- Suppose K_1 and K_2 are fields. The composite field K_1K_2 is the smallest field containing K_1 and K_2. If $\{K_i\}_{i\in I}$ are fields then $\prod_{i\in I} K_i$ (finite sums of finite products) is the smallest field containing each K_i.

- Prop: Let K_1, K_2 be field extensions of F with $[K_1 : F] < \infty$ and $[K_2 : F] < \infty$ then $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$.

  Proof. $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F] = [K_1K_2 : K_2][K_2 : F]$. but $[K_1K_2 : K_1] \leq [K_2 : F]$ and $[K_1K_2 : K_2 \leq [K_1 : F]$ so we have $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$ $\square$

21.2 splitting fields

- def: a polynomial $f(x) \in F[x]$ splits in K if $F(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in K[x]$ with $\alpha_i \in K$ (not necessarily distinct).
- Def: A field E (an extension of F) is a splitting field of $f(x) \in F[x]$ over F if E is the smallest field where f splits. Similarly given $\{f_i\}_{i \in I}$ a collection of polynomials we say E is the splitting field of $\{f_i\}$ if E is the smallest field where all f_i split.
- Example: $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ The splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$.
- Example $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$ has roots $\pm 1 \pm i$ so the splitting field is $\mathbb{Q}(i)$
- Theorem: Splitting fields exist.

  Proof. Suppose that $f \in F[x]$ is a degree n polynomial. If $n = 1$ then f is linear so its roots are in F, so f splits over $E = F$. Now suppose $n > 1$ if f factors into linear polynomials in $F[x]$ then done. Otherwise there is an irreducible factor, $p(x)$ of degree ≥ 2. Then $f(x)/p(x) \cong F(\alpha)$ with α a root of $p(x)$ then $f(x) = (x - \alpha)f_1(x) \in F(\alpha)[x]$ so $f_1(x) \in F(\alpha)[x]$ with degree $f_1 < 1$ so by induction there is E such that f_1 factors into linear polynomials in $E[x]$. then $K = \cap E$ over all E such that f factors into linear polynomials in $E[x]$. then K is the smallest field over which f splits and K is the desired splitting field.

  $\square$

22 March 13

22.1 more on field extensions

- A field extension K of F is normal if K is the splitting field of a collection of polynomials $f_i(x) \in F(x)$.
- Prop: If K is a splitting field for a degree n polynomial $f \in F[x]$ then $[K : F] \leq n!$.

  Proof. Take $\alpha \in K$ then $[F(\alpha) : F] \leq n$ where α is a root of $f(x)$. Let $f(x) = (x-\alpha)f_1$, $deg(f_1) < n$ then by induction $[K : F(\alpha)] \leq (n-1)!$ so $[K : F] = [K : F(\alpha)][F(\alpha) : F] \leq (n-1)!n = n!$. □

- A cyclotomic field extension is one of the form $F(\zeta_n)$ where ζ_n is a primitive nth root of unity over F. If $F = \mathbb{Q}$ then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ where $\phi(n)$ is the Euler-ϕ function i.e the number of integers k such that $1 \leq k \leq n$ which are relatively prime to n.

  $F(\zeta_n)$ comes down to factoring $x^n - 1$ over F. we have

  $$x^n - 1 = (x-\zeta_n)(x-\zeta_n^2)\cdots(x-\zeta_n^n) = (x-1)(x-\zeta_n)\cdots(x-\zeta_n^{n-1})$$

  For example over $\mathbb{Q}$ we have $x^6 - 1 = (x-1)(x-\zeta_6)\cdots(x-\zeta_6^5)$ but these have relationships for example $\zeta_6^2 = \zeta_3$, $\zeta_6^3 = -1$. So the irreducible poly is $\Phi_n = \prod_{(a,n)=1, 1 \leq a < n} (x - \zeta_n^a)$

  Example: Consider $x^2 + 1 \in \mathbb{Z}_3[x]$ this is irreducible. If α is a root of then we have $\alpha^2 = -1$, and $\alpha^{-1} = -\alpha$, but α is not i since i lives in the complex plane and but $\mathbb{Z}_3$ does not.

  Example: $f(x) = x^p - 2$ (similar for $x^p - q$ where q is not a p-th power). f can be factored as

  $$f(x) = (x - \sqrt[p]{2})(x - \sqrt[p]{2}\zeta_p)\cdots(x - \sqrt[p]{2}\zeta_p^{p-1})$$

  so the splitting field over $\mathbb{Q}$ is $\mathbb{Q}[\sqrt[2]{p}, \zeta_p)$ and $[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = p(p-1)$. THen the irreducible poly $\Phi_p(x) = \prod_{1 \leq a < p} (x - \zeta_p^a) = x^{p-1} + x^{p-2} + ... + 1$. With $\zeta_p \in \mathbb{Q}(\sqrt[p]{2})$.

- Isomorphism extension theorem for splitting fields: Suppose F, F' are fields and $\phi : F \to F'$ is a isomorphism. If $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ and $f'(x) = \sum_{i=0}^{n} \phi(a_i) x^i$ then there is an extension of ϕ to the splitting fields of f, f'.

  $$\begin{tikzcd} K \arrow[r, "\Phi"] \arrow[d] & K' \arrow[d] \\ F \arrow[r, "\phi"] & F' \end{tikzcd}$$

  with $\Phi|_F = \phi$.

  Proof. By the isomorphism extension theorem there is $\psi : F(\alpha) \to F'(\beta)$ such that $\Psi|_F = \phi$. Where α is a root of f and β is a corresponding root of $f'(x)$.

  $$\begin{tikzcd} F(\alpha) \arrow[r, "\Phi"] \arrow[d] & F'(\alpha) \arrow[d] \\ F \arrow[r, "\phi"] & F' \end{tikzcd}$$

  Since $f(X) = (x-\alpha)f_1(x)$ and $f'(x) = (x-\beta)f_1'(x)$, f_1 and f_1' are degree $n-1$ polynomials so by induction there is an extension Φ of Ψ to K,

  $$\begin{tikzcd} K \arrow[r, "\Phi"] \arrow[d] & K' \arrow[d] \\ F(\alpha) \arrow[r, "\Psi"] \arrow[d] & F'(\alpha) \arrow[d] \\ F \arrow[r, "\phi"] & F' \end{tikzcd}$$

since $\Phi|_{F(\alpha)} = \Psi$ and $\Psi|_F = \phi$ we have $\Phi|_F = \phi$. so Φ is an isomorphism extension of ϕ.

□

- cor: If K and K' are splitting fields of f over F then $K \cong K'$

  Proof. Apply isomorphism extension theorem of splitting field to the identity

$$\begin{tikzcd} K \arrow[r] \arrow[d] & K' \arrow[d] \\ F \arrow[r, "id"] & F' \end{tikzcd}$$

□

- Example: Splitting field of x^3+x+1 over $\mathbb{Z}_2$. is $\mathbb{Z}_2(\alpha)$ where α is a root (can check by division algorithm).
- Def: Given field F the algebraic closure of F is the field $\bar{F}$ so that every polynomial $f(x) \in F[x]$ factors into linear factors in $\bar{F}[x]$ and $\bar{F}$ is an algebraic extension.
- Ex $\mathbb{C}$ is not the algebraic closure closure over $\mathbb{C}$ since $\pi \in \mathbb{C}$ is not algebraic over $\mathbb{Q}$ so $\mathbb{C}$ is not an algebraic extension. But $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$ and hence the algebraic closure.
- Def: we say a field K is algebraically closed if each $f(x) \in K[x]$ factors into linear factors.
- Prop: the algebraic closure of F is algebraically closed.

  Proof. $\bar{F}$ is the algebraic closure of F. $f(x) \in \bar{F}[x]$, α is a root of $f(x)$ then $\bar{F}(\alpha)$ an algebraic extension over $\bar{F}$ but $\bar{F}$ is algebraic over F so $\bar{F}(\alpha$ is algebriac over F so α is algebraic over F, $\alpha \in \bar{F}$, $\bar{F} = \bar{F}(\alpha)$, so $\bar{F}$ is algebraically closed.

□