§1 Matrices A any ring.

Recall from prev. lecture: $\mathrm{Hom}_A(A^m, A^n) \cong M_{n\times m}(A)$

$$f \longmapsto (f(e_1) \cdots f(e_m))$$

view as column vectors

In particular, the general linear group of A

$$GL_n(A) := M_n(A)^\times := \{ S \in M_n(A) \mid \exists T \text{ s.th. } ST = 1_n \}$$

agrees with the automorphism group $\mathrm{Aut}_{A\text{-Module}}(A^n)$.

For a matrix $S \in M_n(A)$, one defines by the usual formulas

$$\det(S),\ \mathrm{tr}(S) \in A$$

$$\mathrm{char}(S, X) := \det(X\cdot 1_n - S) \in A[X].$$

These are $GL_n(A)$-conjugation invariant, just like for vector spaces.

__Lem 1__ The matrix $S \in M_n(A)$ is invertible

$\Longleftrightarrow$ $\det(S)$ lies in $A^\times$, i.e. is invertible.

__Proof__ $\Rightarrow$ If $S\cdot T = 1_n$, then $\det(S)\cdot\det(T) = 1$

$\Leftarrow$ If $\det(S) \in A^\times$, then we may write down its inverse:

$$S^{-1} = \frac{1}{\det(S)} \hat{S}$$

where $\hat{S} = (t_{ij})$ is the <u>adjoint matrix</u>

$$t_{ij} = (-1)^{i+j} \det(S_{ji}) \qquad \text{leave out } j\text{-th row and } i\text{-th column.}$$

The point is that definition of $\hat{S}$ does not involve further division. Moreover, the check that $S \cdot \hat{S} = \det(S) \cdot 1_n$ is purely algebraic and holds in any ring. $\square$

For an ideal $\mathfrak{a} \subseteq A$ and an A-module M, we define

$$\mathfrak{a}M := \left(a \cdot m \mid a \in \mathfrak{a},\ m \in M \right)$$

This is an A-submodule. Moreover, the construction is compatible with A-linear maps: Any $f : M \to N$ restricts to a map $f : \mathfrak{a}M \to \mathfrak{a}N$.

<u>Observation</u>:

$$(f : M \to N \text{ surjective}) \Rightarrow (\bar{f} : M/\mathfrak{a}M \to N/\mathfrak{a}N \text{ surjective})$$

<u>Cor 2</u> Assume $f : A^m \twoheadrightarrow A^n$ is surjective. Then $m \geq n$.

In particular, $A^m \cong A^n \Leftrightarrow n = m$. $(A \neq 0)$

<u>Proof</u> Pick any max ideal $\mathfrak{m} \subseteq A$. Then $k := A/\mathfrak{m}$ is

a field and $\overline{f} : A^m/\mathfrak{m}^m = \kappa^m \twoheadrightarrow A^n/\mathfrak{m}^n = \kappa^n$ surjective by the observation. Now we are in the case of vector spaces, and the claim is clear. $\square$

<u>Recall</u> An $(i\times i)$-minor of an $(n\times m)$-matrix S is an $(i\times i)$-matrix that arises by striking $n-i$ rows & $m-i$ columns. Write $S_{I,J}$ $I \subseteq \{1,\dots,n\}$, $J \subseteq \{1,\dots,m\}$, $|I| = |J| = i$ for the minor of rows I and cols J.

<u>Cor 3</u> Let $S : A^m \to A^n$ be an A-linear map. Let $I(S) = \left(\det(S_{I,J}) \;\middle|\; |I| = |J| = n \right)$. Then

$$S \text{ surjective} \Longrightarrow I(S) = A.$$

<u>Proof</u> Assume S surjective, let $\mathfrak{m} \subset A$ be a max ideal. By previous observation, $(S \bmod \mathfrak{m}) : \kappa(\mathfrak{m})^m \to \kappa(\mathfrak{m})^n$ is a surjective map of $\kappa(\mathfrak{m})$-vector spaces. Hence $(S \bmod \mathfrak{m}) \in M_{n\times m}(\kappa(\mathfrak{m}))$ has an invertible $(n\times n)$-minor, meaning $\det(S_{I,J}) \notin \mathfrak{m}$ for suitable I, J.

Thus $I(S) \not\subseteq \mathfrak{m}$. This applies to all max ideals $\mathfrak{m}$, so $I(S) = A$. $\square$

Rmk The converse implication $I(S) = A \Rightarrow S$ surjective holds as well. We will discuss this in detail soon.

Example $A^m \to A$, $e_i \mapsto f_i$ being surjective is equivalent to $(f_1, \ldots, f_m) = A$.

§2 The elementary divisor theorem

Lem 4 Let $S, T \in M_{n\times m}(A)$. Assume there are $L \in Gl_n(A)$, $R \in Gl_m(A)$ s.th. $LSR = T$. Then L and R induce isomorphisms

$$\overline{L} : \operatorname{coker}(S) \xrightarrow{\sim} \operatorname{coker}(T)$$

$$R|_{\ker(T)} : \ker(T) \xrightarrow{\sim} \ker(S).$$

Proof The middle square commutes, hence the dotted arrows exist:

$$\begin{tikzcd}
\ker(S) \arrow[r] \arrow[d, dashed, "R^{-1}|_{\ker(S)}"'] & A^m \arrow[r, "S"] \arrow[d, "R^{-1}"'] & A^n \arrow[r] \arrow[d, "L"] & \operatorname{coker}(S) \arrow[d, dashed, "\overline{L}"] \\
\ker(T) \arrow[r] & A^m \arrow[r, "T"] & A^n \arrow[r] & \operatorname{coker}(T)
\end{tikzcd}$$

R, L isomorphisms $\Rightarrow R|_{\ker(T)}, \overline{L}$ isomorphisms. $\square$

<u>Conclusion</u> We can classify finitely presented A-modules (to some degree) by classifying the double cosets

$$GL_n(A) \backslash M_{n\times m}(A) / GL_m(A).$$

Write $S \sim S' \underset{def}{=} \exists\, L \in GL_n(A),\ R \in GL_m(A)$ s.th.

$$S' = LSR.$$

<u>Thm 5 (Elementary Divisor Thm)</u> Let A be a PID and $S \in M_{n\times m}(A)$. Then there are unique up to units $a_1 \mid a_2 \mid \cdots \mid a_k \in A$, $k = \min\{n,m\}$, s.th.

$$S \sim \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_k \\ & 0_{(n-k)\times m} & \end{pmatrix} \quad \text{resp.} \quad S \sim \begin{pmatrix} a_1 & & & \\ & \ddots & & 0_{n\times(m-k)} \\ & & a_k & \end{pmatrix}.$$

<u>Thm 6</u> (Structure Thm for fin. gen. modules over PIDs)

Let A be a PID and M a fin. gen. A-module. Then there are unique $l, r \geq 0$ and unique up to units $a_1 \mid a_2 \mid \cdots \mid a_l \neq 0$ s.th.

$$M \cong A/(a_1) \oplus \cdots \oplus A/(a_l) \oplus A^r$$

Proof of Thm 6 Since M is fin gen, can find a surjection $\varphi : A^m \twoheadrightarrow M$.

A PID $\Rightarrow$ A noetherian $\Rightarrow$ $\ker(\varphi)$ is fin gen,

so can find $S : A^n \twoheadrightarrow \ker(\varphi)$, which

means $M \cong \mathrm{coker}(S)$.

By Lem 4, M up to isomorphism only depends on S up to equivalence $\sim$. So by Thm 5, may assume S diagonal with elementary divisors $a_1 | a_2 | \cdots | a_\ell \neq 0$, $a_{\ell+1} = \cdots = a_k = 0$. Then

$$M \cong A/(a_1) \oplus \cdots \oplus A/(a_\ell) \oplus A^{m-\ell}$$

The uniqueness is part of Exercise Sheet 4. $\square$

Proof of Thm 5 Write $g = \gcd$ in the following, see the appendix for a recap on the gcd.

Claim Put $a_1 := g(S)$. Then there is $S_1 \in M_{(n-1)\times(m-1)}(A)$ s.th.

$$S \sim \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & S_1 & \\ 0 & & & \end{pmatrix}.$$

Proving this claim proves the theorem:

•) If $L \in M_n(A)$, $R \in M_m(A)$ are any, then $g(S) \mid g(LSR)$ because the gcd of some elements divides all their linear combinations. If $L \in Gl_n(A)$, $R \in Gl_m(A)$, then also

$$g(LSR) \mid g(L^{-1}LSRR^{-1}) = g(S), \text{ so } g(S) = g(LSR)$$

Thus if $S \sim \begin{pmatrix} a_1 & \\ & S_1 \end{pmatrix}$ as in the claim, then $a_1 = g(S) = g\begin{pmatrix} a_1 & \\ & S_1 \end{pmatrix} \mid g(S_1)$. Then an inductive argument implies existence of $a_1 \mid a_2 \mid \cdots \mid a_k$.

•) The same argument however shows the uniqueness:

Namely, if $S \sim \begin{pmatrix} a_1 & & & \\ & \ddots & & \\ & & a_k & \\ & 0 & & \end{pmatrix}$ or $\begin{pmatrix} a_1 & & & \\ & \ddots & & 0 \\ & & a_k & \end{pmatrix}$,

then $a_1 = g\begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_k \end{pmatrix} = g(S)$, so a_1 is uniquely determined up to unit.

Moreover, if $\begin{pmatrix} a & 0 \cdots 0 \\ 0 & \\ \vdots & S_1 \\ 0 & \end{pmatrix} \sim \begin{pmatrix} a & 0 \cdots 0 \\ 0 & \\ \vdots & \tilde{S}_1 \\ 0 & \end{pmatrix}$, then

$S_1 \sim \tilde{S}_1$, so uniqueness of $a_2 \mid \cdots \mid a_k$ follows again by induction.

It is left to prove the claim, which requires the:

<u>Construction of suitable (2×2)-matrices:</u>

·) Let $a, b \in A$, not both $= 0$.

$(a,b) = (g(a,b))$ implies there are

r, s with $ra + sb = g(a,b)$. Then necessarily

$(r,s) = 1$, e.g. by the 2nd description in Lem 6.

·) This means there are u, v s.th. $ur + sv = 1$,

so $\begin{pmatrix} r & s \\ -v & u \end{pmatrix} \in GL_2(A)$.

·) If $\begin{pmatrix} r & s \\ -v & u \end{pmatrix} \in GL_2(A)$, then

$g(ra+sb, -va+ub) = g(a,b)$ for all $a, b \in A$.

(This is a special case of $g(S) = g(LSR)$ $\forall L, R$.)

<u>Proof of the claim:</u> Apply the following algorithm.

If $S = 0$, then we are done.

Otherwise, swap rows/cols s.th. $s_{11} \neq 0$ and proceed

as follows:

1) Pick $T = \begin{pmatrix} r & s \\ -v & u \end{pmatrix} \in GL_2(A)$ s.th. $rs_{11} + ss_{21} = g(s_{11}, s_{21})$.

Via $\begin{pmatrix} T & \\ & 1_{n-2} \end{pmatrix}$, $S \sim \begin{pmatrix} g(s_{11}, s_{21}) & * \\ \tilde{s}_{21} & \\ * & * \end{pmatrix}$.

2) via $\begin{pmatrix} 1 & 0 \\ -\frac{\tilde{s}_{21}}{g(s_{11}, s_{21})} & 1 \end{pmatrix}$, $S \sim \begin{pmatrix} g(s_{11}, s_{21}) & * \\ 0 & \\ * & * \end{pmatrix}$

3) Repeat for first column: $S \sim \begin{pmatrix} g(1^{st} \text{ col}) & * \\ 0 & \\ \vdots & * \\ 0 & \end{pmatrix}$

4) Same with top row by right multiplication: $S \sim \begin{pmatrix} g(1^{st} \text{ col}, 1^{st} \text{ row}) & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \tilde{S} & \\ 0 & & & \end{pmatrix}$.

5) Let $a :=$ top left corner. If $a = g(S)$, we are done. Otherwise, there is some $\tilde{s}_{ij}$ s.th. $g(a, \tilde{s}_{ij})$ divides a properly. In this case, add col of $\tilde{s}_{ij}$ to 1st column and start over at 1). The new top left corner obtained in step 4) properly divides a, so the algorithm terminates after finitely many iterations. $\square$ Claim + Thm.

__Example 1__ $\begin{pmatrix} 2 & \\ & 3 \\ 4 & 5 \end{pmatrix} \; -2 \quad \sim \begin{pmatrix} 2 & \\ & 3 \\ & 5 \end{pmatrix} \qquad @$

$\gcd(2,3,5) = 1$, so not yet done in upper left corner.

$$\sim \begin{pmatrix} 2 & \\ 3 & 3 \\ 5 & 5 \end{pmatrix} \; -1 \quad \sim \begin{pmatrix} 2 & \\ 1 & 3 \\ 5 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 \\ 2 & \\ 5 & 5 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 3 \\ & -6 \\ & -10 \end{pmatrix} \sim \begin{pmatrix} 1 & \\ & -6 \\ & -10 \end{pmatrix} \sim \begin{pmatrix} 1 & \\ & 2 \\ & \end{pmatrix}$$

In ptic, $\operatorname{coker} \begin{pmatrix} 2 & \\ & 3 \\ 4 & 5 \end{pmatrix} \cong \mathbb{Z}/2 \oplus \mathbb{Z}$.

__Rmk__ At @, one could have continued more directly. The order here follows instead the algorithm on the previous page.

__Example 2__ $\begin{pmatrix} 2 & \\ & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & \\ 3 & 3 \end{pmatrix} \sim \begin{pmatrix} -1 & -3 \\ 3 & 3 \end{pmatrix}$

$\sim \begin{pmatrix} -1 & -3 \\ & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & \\ & 6 \end{pmatrix}$. This reflects the isomorphism

$\mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/3$.

§ Appendix on the gcd: For $0 \neq a \in A$ any, $\pi \in A$ prime,

put $v_\pi(a) := \sup\{n \geq 0 \mid \pi^n \mid a\}$.

Let $PI/\sim := \{\pi \in A \text{ prime}\}/A^\times$.

Thus $a = \text{unit} \cdot \prod_{\pi \in PI/\sim} \pi^{v_\pi(a)}$ is the prime factorization of a.

Lem 6 The following three definitions of the gcd, which is only defined up to unit, coincide:

1) $(a,b) = (g_1(a,b))$

2) $g_2(a,b) = \prod_{\pi \in PI/\sim} \pi^{\min\{v_\pi(a),\, v_\pi(b)\}}$

3) $g_3(a,b)$ = any element of A s.th.

$c \mid a,\ c \mid b \implies c \mid g_3(a,b)$.

Proof $g_2 = g_3$ is clear. For $g_1 = g_2$:

$(a/g_2, b/g_2) = A$ because a/g_2 and b/g_2 have no common prime factor, so are not contained in a common max ideal. Thus $(a,b) = (g_2)$ $\square$