Math 122 Monday, December 12

recall for a rng R can define an R-module M e.g. a $\mathbb{Z}$-module is an abelian group

An R-module M is finitely generated if $\exists\ m_1,\dots,m_n \in M$ such that any $m \in M$ has the form $m = r_1m_1 + \cdots + r_nm_n$ for some $r_1,\dots,r_n \in R$. Equivalently there is a surjective R-module homomorphism $f: R^n \to M$ $(r_1,\dots,r_n) \longmapsto \sum r_im_i$.

If f is injective then $R^n \simeq M$ say M is free of rank n. In general have a submodule $N = \ker f \subset R^m$ and $R^m/\ker f \simeq M$

Future If R is Euclidean we will show that $\ker f$ is also free of rank $m \le n$. In fact any R-submodule of R^n is free of rank $m \le n$.

Step back and study R-module homomorphisms between free modules (R arbitrary) $f: R^n \to R^m$. Give R^n the standard basis $e_i = (0,\dots,1,\dots,0)$. Then f is completely determined by the n elements $f(e_i) \in R^m$ and these are arbitrary in R^m. Call $f(e_i) = (r_{1i},\dots,r_{mi}) \in R^m$. Then f is determined by mn elements $r_{ij} \in R$.

A is determined by the matrix $A = (r_{ij})$ with m rows and n columns where the i-th column is $f(e_i)$.

When is f invertible as an R-module homomorphism?
Invertible iff $\{e_i^* = f(e_i)\}$ form a basis for R^m so $g(e_i^*) = g(e_i)$ is the inverse
$\iff$ A is an invertible $n \times n$ matrix (so $m = n$)

Fact In any commutative rng, $\det(AB) = \det A \times \det B$ where $\det A = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}$.

Let A^* be the $n \times n$ matrix of cofactors. Then can compute $A \cdot A^* = \det A \cdot I$. So if $\det A \in R^\times$ is a unit then $A^{-1} = \frac{1}{\det A} A^*$ and A is invertible. Conversely if A is invertible $A \cdot A^{-1} = I \Rightarrow \det A \cdot \det A^{-1} = 1 \Rightarrow \det A \in R^\times$ is a unit.

ex. An $n \times n$ matrix with entries in $R = \mathbb{Z}$ is invertible (in $\mathbb{Z}$) iff $\det A = \pm 1$

As before $GL_n(R) \subset M_{n \times n}(R)$ is the subgroup of invertible $n \times n$ matrices.

e.g. $\exists$ finite groups $GL_n(\mathbb{Z}/m\mathbb{Z})$. Challenge: what is the order?

e.g. Also have infinite groups $GL_n(\mathbb{Z}) \subset GL_n(\mathbb{R})$, as a discrete subgroup of a real lie group. $GL_1(\mathbb{Z}) = \{\pm 1\}$ but for $n = 2$ and larger this is interesting

How to construct invertible matrices $P \in GL_n(R)$ any ring R?

1) $P = \begin{pmatrix} r_1 & & 0 \\ & \ddots & \\ 0 & & r_n \end{pmatrix}$ diagonal. $\det P = r_1 \cdots r_n \iff$ all $r_i \in R^\times$. Then $P^{-1} = \begin{pmatrix} r_1^{-1} & & 0 \\ & \ddots & \\ 0 & & r_n^{-1} \end{pmatrix}$

This gives a subgroup of $GL_n(R)$ isomorphic to $(R^\times)^n$.

2) P = permutation matrices (get $n!$ of these) $P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & \ddots & \\ 0 & & 1 \end{pmatrix}$ etc. $\det P = \operatorname{sign}(\sigma) = \pm 1 \in R^\times$.

The product (diag)(Perm) $\subset GL_n(R)$ is isomorphic to $(R^\times)^n \rtimes S_n$.

3) possibly infinite order $P = \begin{pmatrix} 1 & & c_{ij} & \\ & \ddots & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$ $c_{ij} \in R$ $i \neq j$ called <u>unipotent</u>. Note $\det P = 1$

If A is an $n \times m$ matrix and P is an invertible $n \times n$ matrix then $A' = PA$ is an $n \times m$.
Say $P = (1 \cdots v_i \cdots 1)$. Then PA multiplies i-th row of A by v_i and leaves the rest unchanged.
AP — i-th column — —
Say P a permutation matrix. Then PA permutes the rows of A.
AP — — columns — —
Say $P = (1 \cdots c_{ij} \cdots 1)$. Then PA adds $c \cdot j$th row of A to ith row of A.
AP — $c \cdot i$th column — — jth column — —

Yoga: We can perform any sequence of <u>row and column operations</u> of A to transform it to a matrix $A' = PAQ$ (A a $m \times n$, $P \in GL_m(R)$, $Q \in GL_n(R)$ products of types 1,2,3)

Prop Let A be a $m \times n$ matrix over $\mathbb{Z}$. Then there are invertible matrices P and Q such that $A' = PAQ = \begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & \ddots & \\ 0 & & & d_k \\ & 0 & & \end{pmatrix}$ where $d_1 | d_2 | \cdots | d_k$ and all are positive integers.
("divides")

Start: find P and Q such that $PAQ = \begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$ such that d divides everything in B.

Note this is easy for a field because you can divide but it turns out it can be done if R is Euclidean. Look at Artin before next class.