Tues Oct 29

HW 4 due Tues Nov 12

Today: Finite Fields

Let R be a ring. Then $\exists!$ ring map $\varphi : \mathbb{Z} \to R$.

Proof: Since φ is a ring map we must have $\varphi(1_{\mathbb{Z}}) = 1_R$. It follows that

$$\begin{aligned}\varphi(n) &= \varphi(1_{\mathbb{Z}} + \cdots + 1_{\mathbb{Z}}) \\ &= \varphi(1_{\mathbb{Z}}) + \cdots + \varphi(1_{\mathbb{Z}}) \\ &= 1_R + \cdots + 1_R \\ &= \text{“}n 1_R\text{”}\end{aligned}$$

and $\varphi(-n) = -\varphi(n) = -n1_R$.

This determines the map. ///

Highbrow Translation:

$\mathbb{Z}$ is an (the) initial object in the category of rings.

Now consider a domain R (i.e. no zero-divisors) and the unique map $\varphi: \mathbb{Z} \to R$

The kernel is an ideal of $\mathbb{Z}$, hence $\ker\varphi = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.
We also have:

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker\varphi \approx \operatorname{im}\varphi \leq R.$$

Since R is a domain, so is $\operatorname{im}\varphi$, hence $n\mathbb{Z}$ is a prime ideal.

We conclude that

$$n = 0 \quad \text{or} \quad n = p \text{ prime}.$$

Def: We say $\operatorname{char}(R) := n$ is the characteristic of the domain R

In particular, we define the characteristic $\operatorname{char}(K)$ of a field K.

Def: We say a field K is prime if it has no proper subfield.

Theorem (Classification of Prime Fields):

Every prime field is isomorphic to

$$\underset{(\text{char } 0)}{\mathbb{Q}} \quad \text{or} \quad \underset{(\text{char } p)}{\mathbb{Z}/p\mathbb{Z}} \text{ for } p \text{ prime}$$

Proof: Let K be a prime field and consider the unique ring map $\varphi: \mathbb{Z} \to K$. If $\text{char}(K) = p > 0$ then we have

$$\mathbb{Z}/p\mathbb{Z} \approx \text{im}\,\varphi \leq K.$$

Since $\mathbb{Z}/p\mathbb{Z}$ is a field (Euclid) we see that $\text{im}\,\varphi$ is a sub<u>field</u> of K. Since K is prime we have $\text{im}\,\varphi = K$.

If $\text{char}(K) = 0$ then we have

$$\mathbb{Z} \approx \mathbb{Z}/0\mathbb{Z} \approx \text{im}\,\varphi \leq K$$

The smallest subfield of K containing $\text{im}\,\varphi \,(\approx \mathbb{Z})$ is isomorphic to $\mathbb{Q}$. Since K is prime we have $\mathbb{Q} \approx K$.

$\blacksquare$

Def: Given a field K, the intersection of all subfields is called the prime subfield of K.

Note that the prime subfield is prime. It is isomorphic to $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$, depending on the characteristic of K.

Idea (Steinitz, 1910):

To classify fields we should classify extensions of $\mathbb{Q}$ and $\mathbb{Z}/p\mathbb{Z}$.

This problem includes Galois theory and birational algebraic geometry, so it is "too hard".

However, finite fields can be classified.

Let F be a finite field, so $\mathrm{char}(F) = p > 0$. Let $K \cong \mathbb{Z}/p\mathbb{Z}$ be the prime subfield.

The multiplication map $\mu : K \times F \to F$ defines a K-module structure on F with "scalar multiplication" μ.

Since F is finite, it is certainly finitely generated as a K-module. Hence

$$F \approx K^n \text{ (as } K\text{-modules)}$$

for some $n \in \mathbb{N}$. It follows that

$$|F| = |K^n| = |K|^n = p^n.$$

In summary, every finite field has order p^n for some prime p and $n \in \mathbb{N}$.

With some work, one can show the following.

☆ Classification of Finite Fields:

Given prime p and $n \in \mathbb{N}$, there <u>exists</u> a field of order $q := p^n$ and this field is <u>unique</u> up to isomorphism.

We call it $\mathbb{F}_q$.

Alternative notation: $\mathbb{F}_q = GF(q)$
"Galois field"

Proof Omitted. (See my ADE book for the existence part.)

Linear algebra over $\mathbb{F}_q$ has an extra kick.

Example:

Let V be an n-dimensional $\mathbb{F}_q$ module and let U be a k-dimensional submodule. In particular, $U \leq V$ is a finite subgroup so we can apply Lagrange's Theorem.

Since $V \cong \mathbb{F}_q^n$ and $U \cong \mathbb{F}_q^k$ we have

$$|V/U| = |V|/|U|$$

$$= q^n/q^k = q^{n-k}$$

But V/U is itself a f.g. $\mathbb{F}_q$-module.

Hence

$$\dim(V/U) = n-k$$
$$= \dim(V) - \dim(U).$$

In summary, if V is a f.g. $\mathbb{F}_q$-module then we have

$$\dim(V) = \log_q |V|$$

and in this case we see that

$$\text{Lagrange's Theorem} \underset{\exp}{\overset{\log}{\rightleftarrows}} \text{Rank-Nullity Theorem}$$

Moral: There is a strong analogy between finite sets and finite-dimensional vector spaces. Vector spaces over $\mathbb{F}_q$ provide a bridge.

The General Linear Group.

Let K be a field and let $V = K^n$. Then we write

$$GL(V) = GL(n,K).$$

If $V = \mathbb{F}_q^n$, then we write

$$GL(V) = GL(n, q).$$

Q: $|GL(n,q)| = ?$

<u>Theorem</u>: For any field K we have a bijection.

$$GL(n,K) \longleftrightarrow \{\text{ordered bases of } K^n\}$$

<u>Proof</u>: Let $(\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n)$ be an ordered basis for K^n. Define a map $\varphi: K^n \to K^n$ by $\varphi(\vec{e}_i) := \vec{b}_i$ and extend linearly. This map is invertible with inverse given by $\varphi^{-1}(\vec{b}_i) = \vec{e}_i$.

Conversely, let $\varphi \in GL(n,K)$. Then

$$(\varphi(\vec{e}_1), \varphi(\vec{e}_2), \ldots, \varphi(\vec{e}_n))$$

is an ordered basis of K^n ▨

[In Coordinates: The columns of an invertible matrix form an ordered basis.]

Corollary:

$$|GL(n,q)| = q^{\frac{n(n-1)}{2}}(q-1)(q^2-1)\cdots(q^n-1).$$

Proof: We will count ordered bases $(\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n)$ of K^n.

First choose $\vec{b}_1 \in \mathbb{F}_q^n - 0$ in $q^n - 1$ ways.

Then choose $\vec{b}_2 \in \mathbb{F}_q^n - \mathbb{F}_q(\vec{b}_1)$ in $q^n - q$ ways.

Then choose $\vec{b}_3 \in \mathbb{F}_q^n - \mathbb{F}_q(\vec{b}_1, \vec{b}_2)$ in $q^n - q^2$ ways.

Continuing in this way gives

$$|GL(n,q)| = (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})$$

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

$$= q^{1+2+\cdots+(n-1)}(q-1)(q^2-1)\cdots(q^n-1).$$

$$= q^{\frac{n(n-1)}{2}}(q-1)(q^2-1)\cdots(q^n-1).$$

$\blacksquare$

Example: $|GL(2,2)| = 2^{\frac{2\cdot 1}{2}}(2-1)(2^2-1)$
$= 2 \cdot 1 \cdot 3$
$= 6$

$$GL(2,2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$

Define $SL(n,K)$ as the kernel of the determinant homomorphism

$$\det : GL(n,K) \to K^\times$$

Note that $\mathrm{im}(\det) = K^\times$, Hence

$$GL(n,K)/SL(n,K) \cong K^\times$$

as multiplicative groups.

If $K = \mathbb{F}_q$ then we conclude that

$$|SL(n,q)| = |GL(n,q)| \,/\, |\mathbb{F}_q^\times|$$

$$= \frac{q^{\frac{n(n-1)}{2}} \cancel{(q-1)} (q^2-1) \cdots (q^n-1)}{\cancel{(q-1)}}$$

$$= q^{\frac{n(n-1)}{2}} (q^2-1)(q^3-1) \cdots (q^n-1).$$

We will see in general that

$$Z(GL(n,K)) = \underbrace{\{aI : a \in K^\times\}}_{= \text{"scalar matrices"}}$$

and $Z(SL(n,K)) = \{I\}$ or $\{\pm I\}$.

<u>Define</u>: $PSL(n,K) := SL(n,K) / Z(SL(n,K))$.

We will prove later that

$PSL(n,K)$ is <u>simple</u> $\forall\, n \geq 2$ and all fields K, unless

$$n = 2 \text{ and } K = \mathbb{F}_2 \text{ or } \mathbb{F}_3$$

Thurs Oct 31

HW 4 due Tues Nov 12

Current Goal: Prove the following

☆ <u>Theorem</u>: $\forall n \geq 2$ and all fields K,

$$\boxed{PSL(n, K) \text{ is simple}}$$

unless $n=2$ and $K = \mathbb{F}_2$ or $\mathbb{F}_3$ ///

These are the simple groups of "Type A", part of the ABCDEFG classification scheme of Wilhelm Killing (1888)

To prove the Theorem we must investigate the internal structure of GL.

Let K be a field and consider $V \approx K^n$.

After choosing a basis
$\beta = \vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in K^n$
we can represent each $\vec{x} \in K^n$ as a <u>column</u> <u>vector</u>:

$$\vec{x} = x_1\vec{b}_1 + \cdots + x_n\vec{b}_n \longleftrightarrow [\vec{x}]_\beta = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Then given an endomorphism $\varphi \in End(K^n)$ we have

$$[\varphi(\vec{x})]_\beta = [\varphi(x_1\vec{b}_1 + \cdots + x_n\vec{b}_n)]_\beta$$

$$= [x_1\varphi(\vec{b}_1) + \cdots + x_n\varphi(\vec{b}_n)]_\beta$$

$$= x_1[\varphi(\vec{b}_1)]_\beta + \cdots + x_n[\varphi(\vec{b}_n)]_\beta$$

$$= [\varphi]_\beta [\vec{x}]_\beta ,$$

where $[\varphi]_\beta$ is the $n \times n$ matrix with jth column $[\varphi(\vec{b}_j)]_\beta$. In this way we identify $End(K^n)$ with the K-algebra of $n \times n$ matrices

$$End(K^n) \approx Mat_n(K).$$

However, the isomorphism is NON-CANONICAL. It depends on an arbitrary choice of basis

Q: How do the different choices relate?

Given two bases $\alpha = \vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n \in K^n$
$\beta = \vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in K^n$,

define the matrix

$$[\alpha \to \beta] := \left([\vec{a}_1]_\beta \; [\vec{a}_2]_\beta \; \cdots \; [\vec{a}_n]_\beta \right).$$

Then for all $\vec{x} = x_1\vec{a}_1 + \cdots + x_n\vec{a}_n \in K^n$ we have

$$[\alpha \to \beta][\vec{x}]_\alpha = \left([\vec{a}_1]_\beta \cdots [\vec{a}_n]_\beta \right) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$= x_1[\vec{a}_1]_\beta + x_2[\vec{a}_2]_\beta + \cdots + x_n[\vec{a}_n]_\beta$$

$$= [x_1\vec{a}_1 + x_2\vec{a}_2 + \cdots + x_n\vec{a}_n]_\beta$$

$$= [\vec{x}]_\beta.$$

Similarly, we define

$$[\beta \to \alpha] := \left([\vec{b}_1]_\alpha \; [\vec{b}_2]_\alpha \; \cdots \; [\vec{b}_n]_\alpha \right).$$

and we see that $\forall \vec{x} \in K^n$,

$$[\beta \to \alpha][\vec{x}]_\beta = [\vec{x}]_\alpha .$$

In other words, $[\alpha \to \beta]$ is an invertible matrix with

$$[\alpha \to \beta]^{-1} = [\beta \to \alpha] \qquad ///$$

Now consider an endomorphism $\varphi \in \mathrm{End}(K^n)$. Then $\forall \vec{x} \in K^n$ we have

$$[\varphi(\vec{x})]_\beta = [\alpha \to \beta][\varphi(\vec{x})]_\alpha$$

$$[\varphi]_\beta [\vec{x}]_\beta = [\alpha \to \beta][\varphi]_\alpha [\vec{x}]_\alpha$$

$$\underbrace{[\varphi]_\beta [\alpha \to \beta]}[\vec{x}]_\alpha = \underbrace{[\alpha \to \beta][\varphi]_\alpha}[\vec{x}]_\alpha$$

Since this holds for all $\vec{x} \in K^n$ we conclude that

$$[\varphi]_\beta [\alpha \to \beta] = [\alpha \to \beta][\varphi]_\alpha$$

$$\boxed{[\varphi]_\beta = [\alpha \to \beta][\varphi]_\alpha [\alpha \to \beta]^{-1}}$$

Definition: Given $A, B \in Mat_n(K)$, we say that A and B are conjugate if $\exists\, P \in GL(n,K)$ such that

$$B = PAP^{-1}$$

We have seen that matrices that represent the same endomorphism in different coordinates are conjugate.

Conversely, given $P = (\vec{p}_1\ \vec{p}_2 \cdots \vec{p}_n) \in GL(n,K)$, note that $\rho = \vec{p}_1, \vec{p}_2, \dots, \vec{p}_n \in K^n$ are a basis, and we have

$$P = ([\vec{p}_1]_\mathcal{E}\ [\vec{p}_2]_\mathcal{E} \cdots [\vec{p}_n]_\mathcal{E}) = [\rho \to \mathcal{E}],$$

where $\mathcal{E}$ is the standard basis of K^n.

Thus if $B = PAP^{-1}$ for some $A, B \in Mat_n(K)$ then A and B represent the same endomorphism in different coordinates.

Abstractly: $GL(n,K)$ acts on $Mat_n(K)$ by conjugation (this is called the adjoint representation of GL)

The orbits are equivalence classes of endomorphisms

Goal: we would like to parametrize the orbits, to find a standard representative from each orbit.

This is tricky in general, but has a nice solution if K is algebraically closed:

Given $A \in Mat_n(K)$ we say $\vec{x} \in K^n$ is an eigenvector of A if

- $\vec{x} \neq \vec{0}$
- $A\vec{x} = \lambda \vec{x}$ for some $\lambda \in K$, called the eigenvalue.

In this case we have

$$A\vec{x} = \lambda\vec{x}$$
$$A\vec{x} - \lambda\vec{x} = \vec{0}$$
$$A\vec{x} - \lambda I\vec{x} = \vec{0}$$
$$(A - \lambda I)\vec{x} = \vec{0}.$$

$\Rightarrow$ $\underbrace{\ker(A-\lambda I)}_{\text{The "}\lambda\text{-eigenspace"}}$ is nontrivial

In summary:

$$\lambda \in K \text{ is an eigenvalue of } A.$$
$$\Updownarrow$$
$$\ker(A-\lambda I) \text{ is nontrivial}$$
$$\Updownarrow$$
$$\underbrace{\det(A-\lambda I)}_{\text{the "characteristic polynomial"}} = 0.$$

<u>Define</u>:

$$\chi_A(x) := \det(A - xI) \in K[x]$$

The characteristic polynomial is an invariant of adjoint orbits:

Given $A, B \in Mat_n(K)$, $P \in GL(n,K)$ with

$$B = PAP^{-1}$$

we have

$$\begin{aligned}
\chi_B(x) &= \det(B - xI) \\
&= \det(PAP^{-1} - xPIP^{-1}) \\
&= \det(P(A - xI)P^{-1}) \\
&= \cancel{\det(P)} \det(A - xI) \cancel{\det(P)^{-1}} \\
&= \det(A - xI) \\
&= \chi_A(x).
\end{aligned}$$

But it is not a complete invariant.

Example

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in Mat_2(\mathbb{C})$$

have $\chi_A(x) = \chi_B(x) = (x-1)^2$

$\downarrow$

But suppose $\exists P$ with $B = PAP^{-1}$. Then

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = P \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} P^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times$$

Hence A, B are not conjugate.

If K is algebraically closed (i.e. every polynomial in $K[x]$ splits into linear factors), then $\exists$ a complete invariant called the Jordan Normal Form.

☆ <u>Theorem</u>: If K is alg. closed then every $A \in \mathrm{Mat}_n(K)$ is conjugate to a <u>unique</u> matrix of the form

$$\begin{pmatrix} J_{n_1}(\lambda_1) & & & 0 \\ & J_{n_2}(\lambda_2) & & \\ & & \ddots & \\ 0 & & & J_{n_k}(\lambda_k) \end{pmatrix}$$

where each

$$J_n(\lambda) = \underbrace{\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & 1 & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}}_{n} \Bigg\} n$$

is called a Jord<u>an</u> block.

<u>Proof</u>: This is a consequence of the Fundamental Theorem for f. g. modules over a PID (Postponed)

///

Highbrow Translation:

☆ Jordan-Chevalley Decomposition:

Let K be algebraically closed (more generally, let K be "perfect").
Then for all $A \in \mathrm{Mat}_n(K)$ there exist <u>unique</u> $S, N \in \mathrm{Mat}_n(K)$ such that

↓

- $A = S + N$
- S is semisimple (diagonalizable)
- N is nilpotent ($N^k = 0$ for some k)
- $SN = NS$

//

Example

$$\left(\begin{array}{cc|ccc} 2 & 1 & & & \\ & 2 & & & \\ \hline & & 3 & 1 & \\ & & & 3 & 1 \\ & & & & 3 \end{array}\right) = \left(\begin{array}{cc|ccc} 2 & & & & \\ & 2 & & & \\ \hline & & 3 & & \\ & & & 3 & \\ & & & & 3 \end{array}\right) + \left(\begin{array}{cc|ccc} 0 & 1 & & & \\ & 0 & & & \\ \hline & & 0 & 1 & \\ & & & 0 & 1 \\ & & & & 0 \end{array}\right)$$

$$A \qquad = \qquad S \qquad + \qquad N$$

Check that

$$SN = NS = \left(\begin{array}{cc|ccc} 0 & 2 & & & \\ & 0 & & & \\ \hline & & 0 & 3 & \\ & & & 0 & 3 \\ & & & & 0 \end{array}\right)$$

Tues Nov 5

HW 4 is due Tues Nov 12

Recall from last time:

The group $GL(n, K)$ acts on the algebra $Mat_n(K)$ by conjugation

$$P \cdot A = PAP^{-1}$$

and the orbits are equivalence classes of endomorphisms.

Definition: We say A is diagonalizable if it is equivalent to a diagonal matrix

$$P^{-1}AP = \begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}$$

Suppose $P = (\vec{p}_1\ \vec{p}_2 \cdots \vec{p}_n)$.

Then we have

$$A\vec{p_j} = P\begin{pmatrix}\lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n\end{pmatrix}P^{-1}\vec{p_j}$$

$$= P\begin{pmatrix}\lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n\end{pmatrix}\vec{e_j}$$

$$= P\begin{pmatrix}0\\ \vdots \\ 0 \\ \lambda_j \\ 0 \\ \vdots \\ 0\end{pmatrix} = \lambda_j \vec{p_j},$$

hence the columns of P are a basis of eigenvalues for A.

The diagonalizable matrices are "Zariski dense" in $\mathrm{Mat}_n(K) \approx K^{n^2}$, so almost all matrices are diagonalizable.

Furthermore, if K is algebraically closed we have the following.

Jordan Decomposition:

For all $A \in Mat_n(K)$ $\exists !$ $N \in Mat_n(K)$ such that

- $A + N$ is diagonalizable
- N is nilpotent ($N^k = 0$ for some k)
- $AN = NA$.

Proof: Next semester. //

Today we'll consider the space of rectangular matrices

$$Mat_{n,m}(K) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ a_{21} & \cdots & a_{2m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} : a_{ij} \in K \right\}$$

If $U \approx K^m$ and $V \approx K^n$ then by choosing bases

$$\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_m \in K^m$$
$$\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n \in K^n$$

we get a bijection

$$\mathrm{Hom}(U,V) \longleftrightarrow \mathrm{Mat}_{n,m}(K)$$

defined by sending the linear map $\varphi : U \to V$ to the matrix with entries a_{ij} such that

$$\varphi(\vec{u}_j) = \sum_{k=1}^{n} a_{kj} \vec{v}_k$$

The group $GL(n,K) \times GL(m,K)$ acts on $\mathrm{Mat}_{n,m}(K)$ by simultoneously changing coordinates on U and V.

In matrix notation, given $A \in \mathrm{Mat}_{n,m}(K)$ and $(P,Q) \in GL(n,K) \times GL(m,K)$ we have

$$(P,Q) \cdot A := P A Q^{-1}$$

The orbits are equivalence classes of linear maps.

Goal: Find a canonical representative for each orbit.

Start by only changing coordinates only on the target space. i.e. let $GL(n,k) \curvearrowright Mat_{n,m}(k)$ act by left multiplication

$$P \cdot A = PA.$$

Now define the elementary matrices.

for all $0 \neq k \in K$ we define

$$E_{ij}(k) = \begin{array}{c c} & \begin{array}{ccccc} & & & j & \end{array} \\ \begin{array}{c} \\ i \\ \\ \\ \end{array} & \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ \cdots & 1 & \cdots & k & \cdots \\ & & & 1 & \\ & & & & \ddots \; 1 \end{pmatrix} \end{array} \qquad i \neq j$$

$$E_{ii}(k) = \begin{array}{c c} & \begin{array}{ccccc} & & i & & \end{array} \\ \begin{array}{c} \\ \\ i \\ \\ \end{array} & \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ \cdots & \cdots & k & \cdots & \\ & & & 1 & \\ & & & & 1 \end{pmatrix} \end{array}$$

$$P_{ij} = \begin{array}{c c} & \begin{array}{ccccc} & i & & j & \end{array} \\ \begin{array}{c} \\ i \\ \\ j \\ \\ \end{array} & \begin{pmatrix} 1 & & & & \\ \cdots & 0 & \cdots & 1 & \\ & & 1 & & \\ \cdots & 1 & \cdots & 0 & \\ & & & & 1 \end{pmatrix} \end{array} \qquad i < j$$

Note that $\det(E_{ij}(k)) = 1 \neq 0$

$\det(E_{ii}(k)) = k \neq 0$

$\det(P_{ij}) = -1 \neq 0$

So elementary matrices are invertible.

Suppose $A = \begin{pmatrix} \vec{a}_{1\cdot} \\ \vdots \\ \vec{a}_{n\cdot} \end{pmatrix}$ has ith row $\vec{a}_{i\cdot}$

Note that

$$E_{ij}(k)A = \begin{pmatrix} \vec{a}_{1\cdot} \\ \vdots \\ \vec{a}_{i-1\cdot} \\ \vec{a}_{i\cdot} + k\vec{a}_{j\cdot} \\ \vec{a}_{i+1\cdot} \\ \vdots \\ \vec{a}_{n\cdot} \end{pmatrix} \begin{matrix} \\ \\ \\ \leftarrow \\ \\ \\ \\ \end{matrix}$$

replace $\vec{a}_{i\cdot}$ by $\vec{a}_{i\cdot} + k\vec{a}_{j\cdot}$.

$$E_{ii}(k)A = \begin{pmatrix} \vec{a}_{1\cdot} \\ \vdots \\ \vec{a}_{i-1\cdot} \\ k\vec{a}_{i\cdot} \\ \vec{a}_{i+1\cdot} \\ \vdots \\ \vec{a}_{n\cdot} \end{pmatrix} \begin{matrix} \\ \\ \\ \leftarrow \\ \\ \\ \\ \end{matrix}$$

replace $\vec{a}_{i\cdot}$ by $k\vec{a}_{i\cdot}$

$$P_{ij}A = \begin{pmatrix} \vec{a}_{1\cdot} \\ \vdots \\ \vec{a}_{i-1\cdot} \\ \vec{a}_{j\cdot} \\ \vec{a}_{i+1\cdot} \\ \vdots \\ \vec{a}_{j-1\cdot} \\ \vec{a}_{i\cdot} \\ \vec{a}_{j+1\cdot} \\ \vdots \\ \vec{a}_{n\cdot} \end{pmatrix} \begin{matrix} \\ \\ \\ \leftarrow \\ \\ \\ \\ \leftarrow \\ \\ \\ \\ \end{matrix}$$

swap rows $\vec{a}_{i\cdot}$ and $\vec{a}_{j\cdot}$

These are called <u>elementary row operations</u>

<u>Def</u>: We say the matrix $A = (a_{ij}) \in Mat_{n,m}(K)$ is in <u>reduced</u> <u>row</u> <u>echelon</u> <u>form</u> (RREF) if

- First nonzero entry in each row $= 1$; this entry is called a "pivot"
- The pivot in row i is to the right of the pivot in row $i+1$.
- The entries above each pivot are 0.
- The zero rows are at the bottom.

<u>Eg</u>.

$$A = \begin{pmatrix} 0 & 1 & * & 0 & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{is in RREF}$$

"<u>E</u>chelon" = "Staircase"

☆ <u>Theorem</u>:

Every orbit of $GL(n,K) \curvearrowright M_{n,m}(K)$ contains a unique matrix in RREF.

Proof of Existence:

(1) Start at the bottom left (non-standard)

Current column := 1

Find the lowest nonzero entry in curr. col. that is not in a previous pivot row. This entry is the new pivot.

Scale the new pivot row with $E_{ii}(k)$ to make the pivot = 1.

Use $E_{ij}(k)$ with $i<j$ to eliminate all entries above the pivot that are not in previous pivot rows.

Current Column := current column + 1

Repeat.

The result looks like

$$T_1 A = \begin{array}{c} (1) \\ (2) \\ (3) \\ (4) \end{array} \begin{pmatrix} 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & * & * & * \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Note: T_1 is a product of E_{ii} and E_{ij} $(i<j)$ so it is upper triangular.

(2) Permute the rows to put the matrix in upper echelon form.

The result looks like

$$PT_1A = \begin{array}{c} (3) \\ (1) \\ (2) \\ (4) \end{array} \begin{pmatrix} 0 & 1 & * & * & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Note: P is a product of P_{ij} so it is a permutation matrix.

(3) Eliminate the entries above the pivots using $E_{ij}(k)$ $(i<j)$.

The result looks like

$$T_2PT_1A = \begin{pmatrix} 0 & 1 & * & 0 & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Note: T_2 is again upper triangular.

Proof of Uniqueness: Postponed. $\blacksquare$

Corollary (Bruhat Decomposition):

Let $G = GL(n,k)$.
Let $B \leq G$ be the subgroup of upper-triangular matrices (called a Borel subgroup).
Let $W \leq G$ be the subgroup of permutation matrices (called the Weyl group)

Then the group G is generated by the elementary matrices (called Chevalley generators)

and moreover we have

$$\begin{aligned} G &= BWB \\ &= \{ b_1 w b_2 : b_1, b_2 \in B, w \in W \}. \end{aligned}$$

Proof: Let $A \in GL(n,k)$. Then the RREF of A is the identity matrix. Applying the (nonstandard) reduction algorithm gives $T_2 P T_1 A = I$

$$\begin{aligned} A &= T_1^{-1} P^{-1} T_2^{-1} \\ &\in BWB \end{aligned}$$

$\blacksquare$

Thurs Nov 7

HW 4 due next Tuesday

Topic: Double Cosets.

Let $H, K \leq G$ be subgroups. Then the direct product $H \times K$ acts on G by

$$(h,k) \circ g := hgk^{-1}.$$

Proof: We have

$$(1,1) \circ g = 1 g 1^{-1} = g$$

and for $(h_1,k_1), (h_2,k_2) \in H \times K$ we have

$$\begin{aligned}
(h_1,k_1) \circ \left[(h_2,k_2) \circ g\right] &= (h_1,k_1) \circ h_2 g k_2^{-1} \\
&= h_1 h_2 g k_2^{-1} k_1^{-1} \\
&= (h_1 h_2) g (k_1 k_2)^{-1} \\
&= \left[(h_1,k_1)(h_2,k_2)\right] \circ g.
\end{aligned}$$

The orbits of this action are called double cosets

$$HgK := \{ hgk : h \in H, k \in K \}$$

Notation: We let

$$H \backslash G / K := \{ HgK : g \in G \}$$

Recall that if G is finite then

$$|HgK| = \frac{|H||K|}{|H \cap gKg^{-1}|}$$

Proof: Orbit-Stabilizer. $\blacksquare$

Now let K be a field and consider the general linear group.

$$G := GL(n, K)$$

Let $B \leq G$ be the group of upper triangular matrices (called the standard <u>Borel</u> subgroup)

Let $W \leq G$ be the group of permutation matrices (called the Weyl group)

Consider the action $B \times B \curvearrowright G$ by $(b_1, b_2) \circ g := b_1 g b_2^{-1}$ and the double coset decomposition $B \backslash G / B$.

Theorem (Bruhat Decomposition):

Every double coset BgB contains a unique permutation, so we get a bijection

$$\begin{aligned} W &\longleftrightarrow B \backslash G / B \\ w &\longmapsto BwB \end{aligned}.$$

Proof of Existence (RREF):

I described the "Bruhat algorithm" last time. Today we'll use it to compute the RREF of

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

(1) start at bottom left. Eliminate up and to the right.

$$\begin{matrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 0 & 2 \end{matrix} \longrightarrow \begin{matrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 1 & 0 & 1 \end{matrix} \longrightarrow \begin{matrix} 0 & 2 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{matrix}$$

$$\longrightarrow \begin{matrix} 0 & 1 & \cancel{1/2} \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{matrix} \longrightarrow \begin{matrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{matrix}$$

Matrix form

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

$$= \begin{pmatrix} 1/2 & -1/2 & 1/4 \\ & 1 & -1/2 \\ & & 1/2 \end{pmatrix} A$$

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

(2) Permute the rows to put pivots on the main diagonal

$$\begin{matrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{matrix} \longrightarrow \begin{matrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{matrix} \longrightarrow \begin{matrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}$$

Matrix Form

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

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

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

(3) Eliminate above the pivots.

$$\begin{matrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} \longrightarrow \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}$$

Matrix Form

$$\begin{pmatrix} 1 & & -1 \\ & 1 & \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & & 1 \\ & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$$

DONE.

Summary.

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

$$U_2 P U_1 A = I.$$

$$\Longrightarrow \quad A = U_1^{-1} P^{-1} U_2^{-1}$$

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

Bruhat Decomposition

[Bonus: Let $U \leq B$ be the group of upper-unitriangular matrices, i.e with 1's on the diagonal. Then $\forall g \in G$ we can write.

$$g = bwu$$

where $b \in B$, $w \in W$, $u \in U$.]

Proof of Uniqueness:

Given $g \in GL(n,K)$ we have shown that $\exists$ $b \in B$, $w \in W$, $u \in U$ such that

$$g = bwu.$$

We will show that the permutation w is uniquely determined by g.

Little tweak: Consider the anti-diagonal matrix

$$J = \begin{pmatrix} & & & 1 \\ & & \cdot & \\ & 1 & & \\ 1 & & & \end{pmatrix}$$

Note that $J^2 = I$ so we have

$$Jg = JbJJwu$$
$$g' = b'w'u$$

where $g' = Jg$, $b' = JbJ$, $w' = Jw$.

Crucial Observation: $b' = JbJ$ is rotated by $180°$ so it is now <u>lower triangular</u>.

Now given $A \in GL(n,K)$ and $1 \leq s,t \leq n$, let $[A]_{st}$ = upper left $s \times t$ corner of A.

$$A = \begin{array}{c c} & \begin{array}{cc} t & n-t \end{array} \\ \begin{array}{c} s \\ n-s \end{array} & \left(\begin{array}{c|c} [A]_{st} & * \\ \hline * & * \end{array}\right) \end{array}$$

Use this to write equation $g' = b'w'u$ in block form:

$$\left(\begin{array}{c|c} [g']_{st} & * \\ \hline * & * \end{array}\right) = \left(\begin{array}{c|c} [b']_{ss} & 0 \\ \hline * & * \end{array}\right)\left(\begin{array}{c|c} [w']_{st} & * \\ \hline * & * \end{array}\right)\left(\begin{array}{c|c} [u]_{tt} & * \\ \hline 0 & * \end{array}\right)$$

$$= \left(\begin{array}{c|c} [b']_{ss}[w']_{st} & * \\ \hline * & * \end{array}\right)\left(\begin{array}{c|c} [u]_{tt} & * \\ \hline 0 & * \end{array}\right)$$

$$= \left(\begin{array}{c|c} [b']_{ss}[w']_{st}[u]_{tt} & * \\ \hline * & * \end{array}\right)$$

Hence $[g']_{st} = [b']_{ss}[w']_{st}[u]_{tt}$

Since $[b']_{ss}$, $[u]_{tt}$ are invertible, $[g']_{st}$ and $[w']_{st}$ represent the same linear map in different coordinates. In particular, we have

$$\operatorname{rank}[g']_{st} = \operatorname{rank}[w']_{st} \quad \forall s,t.$$

But a permutation is uniquely determined by these ranks

Example:

$$\begin{pmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix} \xrightarrow{\text{ranks}} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\longleftarrow$$

Thus g determines $g' = Jg$, which determines $w' = Jw$, which determines w. $\blacksquare$

The Bruhat algorithm also proves that $GL(n,k)$ is generated by elementary matrices

$E_{ij}(k)$ "transvections"
$E_{ii}(k)$ "diagonal matrices"
P_{ij} "permutations".

Theorem: Actually, the permutations are not necessary.

Proof: We have $P_{ij} = E_{jj}(-1)E_{ij}(1)E_{ji}(-1)E_{ij}(1)$ because

$$\begin{pmatrix} \vec{a}_{i\cdot} \\ \vec{a}_{j\cdot} \end{pmatrix} \longrightarrow \begin{pmatrix} \vec{a}_{i\cdot} + \vec{a}_{j\cdot} \\ \vec{a}_{j\cdot} \end{pmatrix} \longrightarrow \begin{pmatrix} \vec{a}_{i\cdot} + \vec{a}_{j\cdot} \\ \cancel{\vec{a}_{j\cdot}} - (\vec{a}_{i\cdot} + \cancel{\vec{a}_{j\cdot}}) \end{pmatrix} = \begin{pmatrix} \vec{a}_{i\cdot} + \vec{a}_{j\cdot} \\ -\vec{a}_{i\cdot} \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} \cancel{\vec{a}_{i\cdot}} + \vec{a}_{j\cdot} - \cancel{\vec{a}_{i\cdot}} \\ -\vec{a}_{i\cdot} \end{pmatrix} = \begin{pmatrix} \vec{a}_{j\cdot} \\ -\vec{a}_{i\cdot} \end{pmatrix} \longrightarrow \begin{pmatrix} \vec{a}_{j\cdot} \\ \vec{a}_{i\cdot} \end{pmatrix}$$

$\blacksquare$

We have

$$GL(n,K) = \langle E_{ij}(k), E_{ii}(k) : \forall i,j, \forall k \in K \rangle$$

If K is topological, note that

$$\left.\begin{array}{l} E_{ij}(k) \to I \\ E_{ii}(1+k) \to I \end{array}\right\} \text{ as } k \to 0$$

☆ Harder Theorem: Let $\varepsilon > 0$. Then $GL(n,\mathbb{C})$ is generated by the set

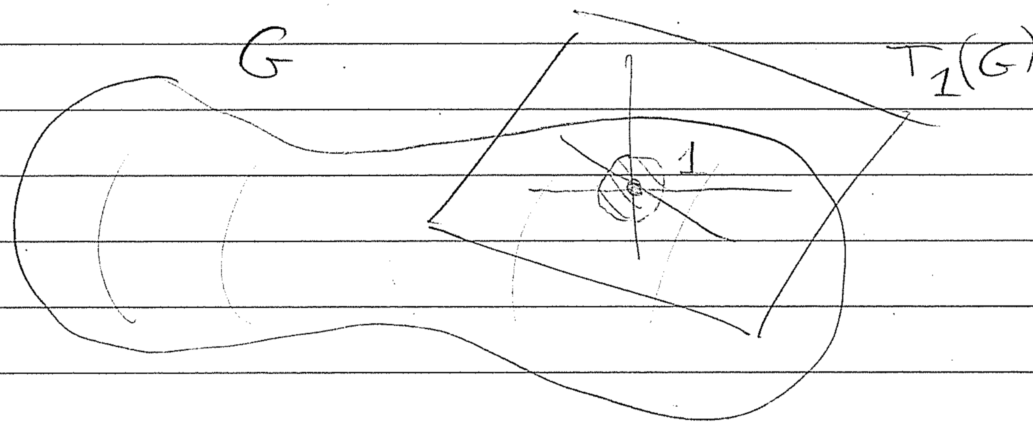
$$\{ E_{ij}(k), E_{ii}(1+k) : \forall i,j, \forall |k| < \varepsilon \}$$

☆☆ Harder Theorem: If G is a connected Lie group, then G is generated by any neighborhood of the identity $1 \in G$.

[Remark:

$GL(n,\mathbb{C})$ is connected but $GL(n,\mathbb{R})$ has two connected components.
]

Picture:



The whole algebraic structure of G is contained near the identity.

Idea (Sophus Lie):

Consider the tangent space at $1 \in G$,

$$\mathfrak{g} := T_1(G)$$

This is called the "Lie algebra" of G.

Tues Nov 12

HW 4 due today.

Let K be a field. Recall that the general linear group $GL(n,K) = \mathrm{Aut}(K^n)$ is generated by

$E_{ij}(k)$ "transvections"
$E_{ii}(k)$ "diagonal matrices"

If $K = \mathbb{C}$, note that

$$\left.\begin{array}{l} E_{ij}(k) \longrightarrow I \\ E_{ii}(1+k) \to I \end{array}\right\} \text{ as } k \to 0.$$

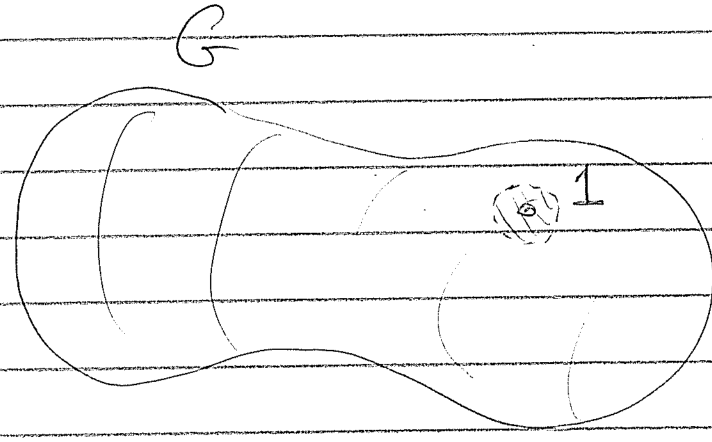
Topological Theorem:

Let $\varepsilon > 0$. Then $GL(n,\mathbb{C})$ is generated by the matrices

$$\{E_{ij}(k), E_{ii}(1+k) : |k| < \varepsilon\}.$$

More generally a connected topological group G is generated by any open neighborhood of the identity $1 \in G$.

Picture:



The algebraic structure of G is local.

Today we will discuss

$SL(n,K)$ and $PSL(n,K)$.

Recall that $SL(n,K)$ is the kernel of the determinant

$$\det : GL(n,K) \to K^\times,$$

so $SL(n,K) \triangleleft GL(n,K)$.

Theorem: For all K and $n \geq 2$, $SL(n,K)$ is generated by the transvections $E_{ij}(k)$, $i \neq j$.

Proof: We have $\det E_{ij}(k) = 1$, hence $E_{ij}(k) \in SL(n,K)$. We will show that diagonal matrices $E_{ii}(k)$ are not necessary to generate $SL(n,k)$.

[It's not trivial because $SL(n,K)$ does contain diagonal matrices:

$$\begin{pmatrix} k & 0 \\ 0 & 1/k \end{pmatrix} \in SL(2,K) \quad . \quad]$$

We will use induction on n. Assume $SL(n-1,K)$ is generated by transvections and consider $A=(a_{ij}) \in SL(n,K)$.

Since A is invertible, some entry in the first column is nonzero. There are two cases.

Case 1: $a_{j1} \neq 0$ for some $j > 1$. Then we replace row 1 by

$$(\text{row } 1) + \frac{1-a_{11}}{a_{j1}} (\text{row } 2).$$

In matrix notation we get

$$E_{1j}\left(\frac{1-a_{11}}{a_{j1}}\right)A = \left(\begin{array}{c|c} 1 & * \\ \hline * & * \end{array}\right)$$

<u>Case 2</u>: If $a_{j1} = 0 \;\forall\; j > 1$ then we must have $a_{11} \neq 0$, hence

$$E_{21}\left(\frac{1}{a_{11}}\right)A = \left(\begin{array}{c|c} a_{11} & * \\ 1 & \\ \hline * & * \end{array}\right)$$

Then we apply Case 1 to get

$$E_{12}(1-a_{11})\,E_{21}\left(\frac{1}{a_{11}}\right)A = \left(\begin{array}{c|c} 1 & * \\ \hline * & * \end{array}\right)$$

//

In either case we now have 1 in the top left corner. Multiplying on the left by suitable $E_{j1}(k)$ with $j > 1$ gives

$$\left(\begin{array}{c|c} 1 & * \\ \hline 0 & \\ \vdots & * \\ 0 & \end{array}\right)$$

Then multiplying on the right by suitable $E_{ij}(k)$ with $j \geq 1$ gives

$$\left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right)$$

[Note: multiplying on the right by $E_{ij}(k)$, $i \neq j$, replaces column j by

(column j) + k(column i).]

Since $\det E_{ij}(k) = 1$ $\forall i \neq j$ and since det is multiplicative, we have

$$\det \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right) = 1$$

$$\Longrightarrow \det A' = 1$$

$$\Longrightarrow A' \in SL(n-1, K).$$

By induction, A' is a product of $(n-1) \times (n-1)$ transvections $E'_{ij}(k)$.

But then $\left(\begin{array}{c|c} 1 & 0 \cdots 0 \\ \hline 0 & \\ \vdots & A' \\ 0 & \end{array}\right)$ is a product of

$$E_{i+1,j+1}(k) = \left(\begin{array}{c|c} 1 & 0 \cdots 0 \\ \hline 0 & \\ \vdots & E_{ij}'(k) \\ 0 & \end{array}\right)$$

$\blacksquare$

<u>Example</u>: Express $\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} \in SL(2,K)$ in terms of transvections.

$$\begin{pmatrix} 1 & \\ 1/a & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 1 & 1/a \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1-a \\ & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 1 & 1/a \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{a}-1 \\ 1 & \frac{1}{a} \end{pmatrix}$$

$$\begin{pmatrix} 1 & \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{a}-1 \\ 1 & \frac{1}{a} \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{a}-1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & \frac{1}{a}-1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1-\frac{1}{a} \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \checkmark$$

In summary

$$E_{21}(-1)E_{12}(1-a)E_{21}\left(\tfrac{1}{a}\right)\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}E_{12}\left(1-\tfrac{1}{a}\right) = I$$

$$\Longrightarrow \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} = E_{21}\left(\tfrac{1}{a}\right)^{-1}E_{12}(1-a)^{-1}E_{21}(-1)^{-1}E_{12}\left(1-\tfrac{1}{a}\right)^{-1}$$

$$= E_{21}\left(-\tfrac{1}{a}\right)E_{12}(a-1)E_{21}(1)E_{12}\left(\tfrac{1}{a}-1\right)$$

$$= \begin{pmatrix} 1 & \\ -1/a & 1 \end{pmatrix}\begin{pmatrix} 1 & a-1 \\ & 1 \end{pmatrix}\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & \frac{1}{a}-1 \\ & 1 \end{pmatrix}$$

That was not trivial

You will show on HW5 that

$$Z(GL(n,K)) = \{kI : k \in K^\times\} \approx K^\times$$

"scalar matrices"

and hence

$$Z(SL(n,K)) = \{kI : k^n = 1\}$$

"n-th roots of 1"

Our next goal is to prove that

$$PSL(n,K) := SL(n,K) / Z(SL(n,K))$$

is a simple group for all fields K and all $n \geq 2$, except

$$PSL(2,\mathbb{F}_2) \text{ and } PSL(3,\mathbb{F}_q),$$

which are not simple.

We will use a general method due to Kenkichi Iwasawa (1917 – 1998)

Def: We say that an action $G \curvearrowright X$ is doubly tranitive if

$\forall\ (x_1, x_2), (y_1, y_2) \in X \times X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$, $\exists\ g \in G$ such that

$$gx_1 = y_1 \quad \text{and} \quad gx_2 = y_2$$

Lemma 1: If $G \curvearrowright X$ is doubly transitive then $\forall x \in X$, $Stab(x)$ is a maximal subgroup of G.

Proof: Since $G \curvearrowright X$ is doubly transitive, in particular it is transitive, so $\forall x \in X$ we have

$$X \approx G/Stab(x) \quad \text{as } G\text{-sets}.$$

Assume for contradiction that $\exists H \leq G$ such that

$$Stab(x) \lneqq H \lneqq G.$$

Then $\exists\ g \in G - H$ and $h \in H - Stab(x)$. Since $Stab(x) \neq hStab(x)$ and $Stab(x) \neq gStab(x)$ and since $X \approx G/Stab(x)$ is doubly trans., $\exists\ u \in G$ such that

$$u(Stab(x)) = Stab(x) \text{ and } u(hStab(x)) = gStab(x).$$

i.e. $u \in Stab(x)$ and $g^{-1}uh \in Stab(x)$.
But then we have $uh \in H$ and $g^{-1}uh \in H$, hence

$$uh(g^{-1}uh)^{-1} = \cancel{uhh^{-1}u^{-1}}g = g \in H.$$

CONTRADICTION. $\blacksquare$

Lemma 2: If $G \curvearrowright X$ is doubly transitive, then any normal $N \triangleleft G$ acts either trivially or transitively on X.

Proof: Suppose $N \curvearrowright X$ is not trivial, i.e. $\exists\, n \in N, x \in X$ with $nx \neq x$.

Now pick any $y \neq y'$ in X. Then by double transitivity $\exists\, g \in G$ with

$$gx = y \quad \text{and} \quad g(nx) = y'.$$

But then we have

$$\begin{aligned} y' &= gnx \\ &= gng^{-1}y. \end{aligned}$$

Since $gng^{-1} \in N$, we conclude that $N \curvearrowright X$ is transitive $\boxtimes$

To state Iwasawa's criterion, we need one more concept.

To be continued...

Thurs Nov 14

HW 5 due ?
NO CLASS Nov 25 → 29 (Thanksgiving)
Final Exam scheduled for
Thurs Dec 12, 2:00 – 4:30pm

... continued.

We are proving that $PSL(n,k)$ is simple using a method of Kenkichi Iwasawa.

Recall: Given an action $G \curvearrowright X$ we define the diagonal action $G \curvearrowright X \times X$ by $g(x_1, x_2) = (gx_1, gx_2)$. We say that $G \curvearrowright X$ is doubly transitive if

$$G \curvearrowright \left(X \times X - \{(x,x) : x \in X\}\right)$$

is transitive. (G sends any pair to any other pair)

Lemma 1: If $G \curvearrowright X$ is doubly transitive then $\forall x \in X$, $Stab(x)$ is a maximal subgroup of G.

///

Lemma 2: If $G \curvearrowright X$ is doubly transitive then any normal $N \trianglelefteq G$ acts either trivially or transitively on X. ///

To state Iwasawa's Theorem we need one more idea.

Given group G and $g, h \in G$ we define the commutator $[g,h] := ghg^{-1}h^{-1}$. Note

$$gh = hg \iff [g,h] = 1$$

We define the commutator subgroup

$$[G,G] := \langle [g,h] : g,h \in G \rangle$$

You will prove on HW5 that $[G,G] \trianglelefteq G$. The quotient

$$G^{ab} := G/[G,G]$$

is called the abelianization of G.

It is abelian (by construction) and it has the following universal property:

if A is abelian then $\forall$ group homs. $\varphi : G \to A$ $\exists !$ hom. $\tilde{\varphi} : G^{ab} \to A$ such that

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & A \\ G/[G,G] \arrow[ur, dashed, "\tilde{\varphi}"'] & \end{tikzcd} \qquad \varphi = \tilde{\varphi} \circ \pi$$

☆ Theorem (Iwasawa, 1941)
[in Proc. Imperial Acad. Tokyo, in German]

Let $G \curvearrowright X$ be doubly transitive. If

- For some x, $\mathrm{Stab}(x)$ has an abelian normal subgroup whose conjugates generate G,
- $[G,G] = G$

then G/K is simple, where K is the kernel of $G \curvearrowright X$.

Proof:

To show G/K is simple we will show that $K \leq N \leq G$ and $N \trianglelefteq G$ imply that $N = K$ or $N = G$. The result follows from Correspondence.

So assume $K \leq N \leq G$ and $N \trianglelefteq G$. Let $H = \mathrm{Stab}(x)$ for some $x \in X$. Since N is normal, NH is a subgroup of G. Since $H \leq NH$ and H is maximal by Lemma 1 we have $NH = H$ or $NH = G$.

Case $NH = H$: Then $N \leq H$ implies that N fixes x, hence $N \curvearrowright X$ is not transitive. By Lemma 2, $N \curvearrowright X$ is trivial which means $N \leq K$. We conclude $N = K$. ///

Case $NH = G$: Let $U \trianglelefteq H$ be abelian such that $G = \langle gUg^{-1} : g \in G \rangle$, which exists by hypothesis. Since $N \trianglelefteq G$ and $U \trianglelefteq H$ we have $NU \trianglelefteq NH = G$. Then $\forall g \in G$, $gUg^{-1} \subseteq g(NU)g^{-1} = NU$. It follows that $NU = G$, and hence

$$\frac{G}{N} = \frac{NU}{N} \approx \frac{U}{N \cap U}.$$

Since U is abelian this means G/N is abelian. By universal property of $[G,G]$ we have $[G,G] \leq N$. Then since $[G,G] = G$ by hypothesis, we have $N = G$.

$\blacksquare$

Now we apply Iwasawa to $SL(n,K)$.

Note that $SL(n,K)$ acts on the set of 1-dim subspaces of K^n:

$$Gr_K(1,n) = K\mathbb{P}^{n-1}$$

"projective space"

Given $A \in SL(n,K)$, suppose that $Al = l$ for all $l \in K\mathbb{P}^{n-1}$. Then we have

$$A\vec{x} \in K(\vec{x})$$

$$A\vec{x} = \lambda\vec{x} \qquad \forall x \in K^n$$

(Every vector is an eigenvector.) Suppose $A\vec{e}_i = \lambda_i \vec{e}_i$ where $\vec{e}_i$ is the standard basis. So we have

$$A = \begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}.$$

Suppose $A(\vec{e}_i + \vec{e}_j) = \lambda(\vec{e}_i + \vec{e}_j) = \lambda\vec{e}_i + \lambda\vec{e}_j$.
Then we have

$$\lambda\vec{e}_i + \lambda\vec{e}_j = A(\vec{e}_i + \vec{e}_j) = A\vec{e}_i + A\vec{e}_j = \lambda_i\vec{e}_i + \lambda_j\vec{e}_j$$

$\Longrightarrow \lambda_i = \lambda = \lambda_j$. We conclude that A is a scalar matrix $A = kI$.
Thus the kernel of action $SL(n,K) \curvearrowright K\mathbb{P}^{n-1}$ is the center

$$Z(SL(n,K)) = \{ kI : k^n = 1 \}. \quad ///$$

[We obtain an action $PSL(n,K) \curvearrowright K\mathbb{P}^{n-1}$, which explains the "P" in PSL.]

Now we show $SL(n,K) \curvearrowright K\mathbb{P}^{n-1}$ is doubly transitive. Choose lines $K(\vec{v}_1) \neq K(\vec{v}_2)$ and $K(\vec{u}_1) \neq K(\vec{u}_2)$ and extend these to bases

$$\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$$
$$\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n$$

Then the map φ defined by $\varphi(\vec{u}_i) := \vec{v}_i$ $\forall$ i sends

$$\varphi(K(\vec{u}_1)) = K(\vec{v}_1)$$
$$\varphi(K(\vec{u}_2)) = K(\vec{v}_2)$$

Unfortunately we may have $\det \varphi \neq 1$. This can be fixed by scaling the nth column. We define

$$\tilde{\varphi}(\vec{u}_i) = \begin{cases} \varphi(\vec{u}_i) & 1 \leq i \leq n-1 \\ \frac{1}{\det \varphi} \varphi(\vec{u}_i) & i = n \end{cases}$$

Then $\tilde{\varphi} \in SL(n, K)$. ///

Now let P be the stabilizer of the line $K\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ We know that

$$P = \left\{ \left(\begin{array}{c|c} a & * \\ \hline 0 & B \end{array} \right) : a = \frac{1}{\det B} \right\}$$

"parabolic subgroup"

The projection $P \to GL(n-1,K)$ defined by

$$\left(\begin{array}{c|c} a & * \\ \hline 0 & B \end{array}\right) \longmapsto B$$

has abelian kernel

$$U = \left\{ \left(\begin{array}{c|c} 1 & * \cdots * \\ \hline 0 & \\ \vdots & I \\ 0 & \end{array}\right) \right\} \approx (K^{n-1}, +)$$

///

To finish the proof that $PSL(n,K)$ is simple, we must show.

- The conjugates of U generate $SL(n,K)$.
- $[SL(n,K), SL(n,K)] = SL(n,K)$.

We already know that $SL(n,K)$ is generated by transvections $E_{ij}(k)$

Theorem: Every transvection $E_{ij}(k)$ is conjugate to $E_{12}(\pm k) \in U$.

Proof: If w is a permutation sending $i \mapsto w(i)$ then the corresponding permutation matrix satisfies

$$w E_{ij}(k) w^{-1} = E_{w(i),w(j)}(k).$$

Choose w such that $w(i)=1$ and $w(j)=2$, so

$$w E_{ij}(k) w^{-1} = E_{12}(k).$$

If $\det w = 1$ we're done. Otherwise, let

$$d = \begin{pmatrix} -1 & & 0 \\ & 1 & \\ 0 & & \ddots & \\ & & & 1 \end{pmatrix}$$

Then $(dw) E_{ij}(k) (dw)^{-1} = E_{12}(\pm k)$ with $dw \in SL(n,K)$.

$\blacksquare$

Example:

$$\begin{pmatrix} & & 1 \\ & 1 & \\ -1 & & \end{pmatrix} \begin{pmatrix} 1 & & \\ & 1 & \\ & k & 1 \end{pmatrix} \begin{pmatrix} & & 1 \\ & 1 & \\ -1 & & \end{pmatrix}^{-1} = \begin{pmatrix} 1 & k & \\ & 1 & \\ & & 1 \end{pmatrix}$$

So far we have made no hypothesis on n or the field K (except assuming $n \geq 2$)

Theorem: If $n \geq 2$, then every $E_{ij}(k)$ is a commutator of elements of $SL(n, K)$ except when $n=2$ and $K = \mathbb{F}_2$ or $\mathbb{F}_3$. It follows that

$$[SL(n,K), SL(n,K)] = SL(n,K)$$

Proof: In general, we have

$$[E_{ij}(\alpha), E_{jl}(\beta)] = E_{il}(\alpha\beta)$$

when i, j, l are distinct. Thus for $n \geq 3$ we get

$$E_{ij}(k) = [E_{il}(k), E_{lj}(1)], \quad l \notin \{i, j\}.$$

If $n = 2$ then we have

$$\begin{pmatrix} a & \\ & 1/a \end{pmatrix} \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} \begin{pmatrix} a & \\ & 1/a \end{pmatrix}^{-1} \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & b(a^2-1) \\ & 1 \end{pmatrix}$$

which gives all $E_{12}(k)$ if $|K| > 3$. Similarly for $E_{21}(k)$. $\blacksquare$

We are done!

Summary: If $n \geq 2$, then

$$PSL(n,K) = SL(n,K) / Z(SL(n,K))$$

is simple except when $n=2$ and $K = \mathbb{F}_2$ or $\mathbb{F}_3$.

This accounts for all the finite simple groups we have known.

order	name
60	$PSL(2,4) = PSL(2,5)$
168	$PSL(3,2) = PSL(2,7)$
360	$PSL(2,9)$
504	$PSL(2,8)$
660	$PSL(2,11)$
1092	$PSL(2,13)$
2448	$PSL(2,17)$
$\vdots$	

The smallest one we haven't met is

$$|PSU(3,3)| = 6048$$