Oct. 27, 2006 (Fri.)

Proposition 2.8.14. *Let H be a subgroup of a solvable group G, then H is solvable.*

Let N be a normal subgroup of G. Then G is solvable if and only if both N and G/N are solvable.

Sketch. G has a solvable series, intersecting the series with H gives a solvable series of H.

If $N \lhd G$, then we have $\pi : G \to G/N$. Projecting the solvable series of G to G/N gives a solvable series of G/N.

Finally, if N and G/N are solvable, they have solvable series respectively. Apply π^{-1} to the solvable series of G/N gives a series from N to G. Combine this series with the serious of H gives a solvable series of G. □

Example 2.8.15.

We will prove in the coming subsection that A_5 is not solvable, hence so is S_n for $n \geq 5$. □

2.9. **normal and subnormal series.** We turning back to series a little bit more. A subnormal series is called a composition series if every quotient is a simple group.

Definition 2.9.1. *For a subnormal series, $\{e\} = H_n < ... < H_0 = G$, the factors of the series are the quotient groups H_{i-1}/H_i and the length is the number of non-trivial factors. A refinement is a series obtained by finite steps of one-step refinement which is $\{e\} = H_n < . < K < .. < H_0 = G$.*

Definition 2.9.2. *Two series are said to be equivalent if there is a one-to-one correspondence between the non-trivial factors. And the corresponding factors groups are isomorphism.*

It's clear that this defines an equivalent relation on subnormal series. The main theorems are

Theorem 2.9.3 (Schreier)**.** *Any two subnormal (resp. normal) series of a group G have a subnormal (resp. normal) refinement that are equivalent.*

An immediate corollary is the famous Jordan-Hölder theorem.

Theorem 2.9.4 (Jordan-Hölder)**.** *Any two composition series of a group are equivalent.*

The main technique is the Zassenhaus Lemma, or sometimes called butterfly Lemma.

Lemma 2.9.5 (Zassenhaus)**.** *Let $A^* \lhd A$ and $B^* \lhd B$ be subgroups of G. Then*

(1) $A^*(A \cap B^*) \lhd A^*(A \cap B)$.
(2) $B^*(A \cap B) \lhd B^*(A \cap B)$.
(3) $A^*(A \cap B)/A^*(A \cap B^*) \cong B^*(A \cap B)/B^*(A^* \cap B)$.

Sketch. It's clear that $A \cap B^* = (A \cap B) \cap B^* \lhd A \cap B$. And similarly, $A^* \cap B \lhd A \cap B$. Let $D = (A \cap B^*)(A^* \cap B) \lhd A \cap B$. One can have a well-defined homomorphism $f : A^*(A \cap B) \to A \cap B/D$ with kernel $A^*(A \cap B^*)$. And similarly for the other homomorphism. □

proof of Schreier's theorem. Let $\{e\} = G_{n+1} < ... < G_0 = G$ and $\{e\} = H_{m+1} < ... < H_0 = G$ be two subnormal series. Let $G(i,j) := G_{i+1}(G_i \cap H_j)$ (resp. $H(i,j) := H_{j+1}(G_i \cap H_j)$). Then one has a refinement

$$G = G(0,0) > G(0,1) > ... > G(0,m) > G(1,0) > ... > G(n,m),$$

$$G = H(0,0) > H(1,0) > ... > H(n,0) > H(0,1) > ... > H(n,m).$$

By applying Zaseenhaus Lemma to $G_{i+1}, G_i, H_{j+1}, H_j$, one has

$$G(i,j)/G(i,j+1) \cong H(i,j)/H(i+1,j).$$

□

2.10. **simplicity of A_5.** An element in S_n is said to be have cycle structure $(m_1, .., m_r)$ with $m_1 \geq m_2 \geq ... \geq m_r$, $m_1 + ... + m_r = n$ if its cycle decomposition is of length $m_1, ..., m_r$ respectively. For example, $(1,2)(3,4) \in S_4$ has cycle structure $(2,2)$ and $(1,2) \in S_4$ has cycle structure $(2,1,1)$.

Remark 2.10.1. *There is a one-to-one correspondence between cycle structures of S_n and partition of the integer n.*

A key observation is that any two elements are conjugate to each other if and only if they have the same cycle structure. Let's call the set of all elements of cycle structure $(m_1, ..., m_r)$ the cycle class of $(m_1, ...m_r)$. A consequence of this fact is that a subgroup $N < S_n$ is normal if and only if N is union of cycle classes.

Let's put it another way, given a group G, we can always consider the group action $G \times G \to G$ by conjugation. The conjugate classes are the orbits. A subgroup $H < G$ is normal if and only if it is union of orbits. If $G = S_n$, then orbits are cycle classes.

Example 2.10.2. *In S_4, V is the union of class $(1,1,1,1)$ and $(2,2)$. A_4 is the union of V and the class $(3,1)$.*

The purpose of this subsection is to show that A_5 is a simple non-abelian group, hence a non-solvable group.

Theorem 2.10.3. *A_5 is a simple non-abelian group.*

Proof. One note that in S_5, possible cycle structures are $(5),(4,1)$,$(3,1$ $,1)$,$(3,2),(2,2,1),(2,1,1,1),(1,1,1,1,1)$ with $24,30,20,20,15,10,1$ elements in each class. While A_5 is the union of classes of $(5),(3,1,1),(2,$ $2,1),(1,1,1,1,1)$.

We consider the actions of conjugation $\alpha : S_5 \times A_5 \to A_5$ and its restriction $\beta : A_5 \times A_5 \to A_5$. For $\sigma \in A_5$, let $\mathcal{O}_{\alpha,\sigma}$ be the orbit of the α and $\mathcal{O}_{\beta,\sigma}$ be the orbit of the β. And let $G_{\alpha,\sigma}, G_{\beta,\sigma}$ be the stabilizer.

It's clear that $G_{\alpha,\sigma} = C_{S_5}(\sigma)$ and $G_{\beta,\sigma} = C_{A_5}(\sigma) = C_{S_5}(\sigma) \cap A_5$. Thus we have either $|G_{\beta,\sigma}| = \frac{1}{2}|G_{\alpha,\sigma}|$ or $|G_{\beta,\sigma}| = |G_{\alpha,\sigma}|$. Hence $|\mathcal{O}_{\beta,\sigma}| = |\mathcal{O}_{\alpha,\sigma}|$ or $|\mathcal{O}_{\beta,\sigma}| = \frac{1}{2}|\mathcal{O}_{\alpha,\sigma}|$.

case 1. If σ has cycle structure (5), then $|\mathcal{O}_{\alpha,\sigma}| = 24, |G_{\alpha,\sigma}| = 5$. It follows that $|G_{\beta,\sigma}| = 5$ and hence $|\mathcal{O}_{\beta,\sigma}| = 12$.

case 2. If σ has cycle structure $(3,1,1)$, then $|\mathcal{O}_{\alpha,\sigma}| = 20, |G_{\alpha,\sigma}| = 6$. However, one notice that there is an element $\tau \in C_{S_5}(\sigma) - C_{A_5}(\sigma)$ (e.g. $(45)(123) = (123)(45)$). Hence $|G_{\beta,\sigma}| \neq |G_{\alpha,\sigma}|$ and must be $\frac{1}{2}|G_{\alpha,\sigma}| = 3$. Therefore $|\mathcal{O}_{\beta,\sigma}| = 20$.

case 3. If σ has cycle structure $(2,2,1)$,then $|\mathcal{O}_{\alpha,\sigma}| = 15, |G_{\alpha,\sigma}| = 8$. It follows that $|\mathcal{O}_{\beta,\sigma}| = 15$.

Combining all this, if $H < A_5$ is a normal subgroup, then $|H| = 1 + 12r_1 + 20r_2 + 15r_3$, where r_i are integers. Moreover $|H| \mid |A_5| = 60$, which is impossible unless $|H| = 1$ or 60. □

2.11. **simple linear groups.** We have seen that A_5 is a simple group. Another important source of simple groups is via the linear groups.

We first introduce some notions. Let V be a m-dimensional vector space over a field K. Then the **general linear group** $GL(V)$ is the group of all non-singular linear transformations on V. If we choose a basis $\{e_1, ..., e_m\}$ of V, then a non-singular linear transformation can be represented as a non-singular matrix in $GL(m, K)$. If K is a field of q elements (thus unique up to isomorphism, which we will see later), then we may write $GL(m, q)$ instead.

Proposition 2.11.1. $|GL(m, q)| = (q^m - 1)(q^m - q)...(q^m - q^{m-1})$.

Proof. Let $\{e_1, ..., e_m\}$ be a basis and A a $m \times m$ matrix. A is non-singular if and only $\{Ae_1, ..., Ae_m\}$ is again a basis. Or equivalently, $\{Ae_1, ..., Ae_m\}$ is linearly independent. Ae_1 can have anything but zero, thus there are $q^m - 1$ choices. And then Ae_2 can be anything independent of Ae_1, thus there are $q^m - q$ choices. Inductively, we get the formula. □

A matrix (or linear transformation) is called **unimodular** if determinant is 1. Let $SL(V)$, (resp. $SL(m, K)$) be the subgroups of unimodular matrices. An *elementary transvection* $B_{ij}(\lambda)$ is a matrix which is 1 along diagonal, λ as its ij entry, and 0 elsewhere. A **transvection** is a matrix B such that is similar (which is conjugate in group theory) to some $B_{ij}(\lambda)$. Note that $B_{ij}(\lambda)^{-1} = B_{ij}(-\lambda)$.

Lemma 2.11.2. *If $A \in GL(m, K)$ with $\det A = \mu$, then $A = UD(\mu)$, where U is a product of elementary transvections and $D = diag(1, ..., 1, \mu)$.*

Sketch. Performing elementary row operations by multiplying elementary transvections on the left. One sees that it reaches a matrix of type $D(\mu)$.

For example, we look at first column. Assume that $a_{21} \neq 0$. Then multiply $B_{12}(a_{21}^{-1}(1 - a_{11}))$, one gets a matrix A' with $A'_{11} = 1$. Then multiply $B_{21}(-a_{21})$, the one gets a matrix A'' with $A''_{11} = 1, A''_{21} = 0$. □

Proposition 2.11.3. *We have:*
1. $GL(m, K)$ is a semi-direct product of $SL(m, K)$ by K^*.
2. $SL(m, K)$ is generated by elementary transvections.

Proof. 1. Consider $\det : GL(m, K) \to K^*$. It's clear that this is a group homomorphism with kernel $SL(m, K)$. Hence $SL(m, K) \lhd GL(m, K)$. On the other hand, $\Delta := \{D(\mu) | \mu \in K^*\} < GL(m, K)$ and $\Delta \cong K^*$. One can verify that $GL(m, K) = SL(m, K)\Delta$ by the abbove Lemma. And it's clear that $SL(m, K) \cap \Delta = \{e\}$. Thus, we are done.
2. This follows immediately from above Lemma. □

We now introduce more notations. Let $Z(m, K)$ (resp. $Z(V)$) be the center of $GL(m, K)$. Then it's easy to see that $Z(m, K)$ is nothing but scalar matrices. Let $SZ(m, K) = Z(m, K) \cap SL(m, K)$, the group of unimodular scalar matrices. One can also verify that $Z(SL(m, K)) = SZ(m, K)$.

In order to compute the cardinality of $SZ(m, K)$, we recall the following fact:

Proposition 2.11.4. *Let K be a field.*
1. $x^n = 1$ has at most n solutions in K.
2. Every finite subgroup of K^* is cyclic. In particular, if K is finite, then K^* is cyclic.

As a result, if K is a finite field of q elements, then $x^m = 1$ has exactly $(q - 1, m)$ solutions. Thus $SZ(m, q) = (q - 1, m)$.

Let $PGL(V) := GL(V)/Z(V)$ and $PSL(V) := SL(V)/SZ(V)$. Then we have

$$|PGL(m, q)| = |SL(m, q)| = (q^m - 1)(q^m - q)...(q^m - q^{m-1})/(q - 1),$$

$$|PSL(m, q)| = (q^m - 1)(q^m - q)...(q^m - q^{m-1})/d(q - 1),$$

where $d = (q - 1, m)$.

We now give some more example of finite simple groups.

Theorem 2.11.5. *The group $PSL(2, q)$ are simple if and only if $q > 3$.*

Proof. If $q = 2, 3$, then $|PSL(2, 2)| = 6, |PSL(2, 3)| = 12$. Hence they are not simple.

Assume now that $q \geq 4$. Let $N \lhd PSL(2,q)$ and $H \lhd SL(2,q)$ be its preimage. It is enough to show that if $SZ(m,q) \subsetneq H < SL(m,q)$, then $H = SL(m,q)$.
1. For any matrix $A \in H - SZ(m,q)$. Then its rational canonical form is either $\begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}$ or $\begin{bmatrix} 0 & -1 \\ 1 & \beta \end{bmatrix}$.
2. In either case, H contains a matrix of the form $\begin{bmatrix} \alpha & 0 \\ \beta & \alpha^{-1} \end{bmatrix}$ with $\alpha \neq \pm 1$.
To see this, it remains to consider A in the second case. We assume $A = \begin{bmatrix} 0 & -1 \\ 1 & \beta \end{bmatrix}$. Then $TAT^{-1}A^{-1} = \begin{bmatrix} \alpha^{-2} & 0 \\ \beta(\alpha^2 - 1) & \alpha^2 \end{bmatrix} \in H$ for $T = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}$. We can pick α so that $\alpha^2 \neq \pm 1$ (unless $q = 5$, this case need some extra care).
3. Let $B = B_{21}(1)$, $A = \begin{bmatrix} \alpha & 0 \\ \beta & \alpha^{-1} \end{bmatrix}$ with $\alpha \neq \pm 1$. Then H contains $BAB^{-1}A^{-1} = B_{21}(1 - \alpha^{-2})$, an elementary tranvection with $1 - \alpha^{-2} \neq 0$.
4. If H contains $B_{21}(\mu)$, then $UB_{21}(\mu)U^{-1} = B_{12}(-\mu)$ for $U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.
5. It remains to show that H contains $B_{12}(\nu)$ for all $\nu \in K$ since $SL(m,q)$ is generated by transvections.
To see this, note that

$$\begin{bmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{bmatrix} \begin{bmatrix} 1 & \mu \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{bmatrix}^{-1} = \begin{bmatrix} 1 & \mu\alpha^2 \\ 0 & 1 \end{bmatrix}.$$

Let $G = \{0\} \cup \{\mu \in K | B_{12}(\mu) \in H\}$. It's clear that G is an additive group and contains all elements of the form $\mu(\alpha^2 - \beta^2)$.
We claim that $G = K$.
If $char(K) \neq 2$, then $\nu = (\frac{1}{2}(\nu+1))^2 - (\frac{1}{2}(\nu-1))^2$. Thus for given $\nu \in K$, $\nu\mu^{-1} = \xi^2 - \zeta^2$. It follows that $\nu \in G$.
If $char(K) = 2$, then $|K^*|$ is a cyclic group of odd order. Thus for $\nu \in K^*$, $\nu\mu^{-1} \in K^*$ and $\nu\mu^{-1} = \zeta^2$ for some ζ. Thus, $\nu = \mu\zeta^2 \in G$. □

Example 2.11.6.

On can even show that A_n is simple for $n \geq 5$. □

Example 2.11.7.

$|PSL(2,4)| = |PSL(2,5)| = 60$. And they are simple. So In fact, we have $PSL(2,4) \cong PSL(2,5) \cong A_5$.
$|PSL(2,7)| = 168$, so it can not be A_n.
$PSL(2,9) \cong A_6$. □

We finally give some more results concerning simple groups. However, we are not going to prove these.

Theorem 2.11.8 (Jordan-Dickson)**.** *If* $m \geq 3$ *and* V *is an* m*-dimensional vector space over a field* K*, then* $PSL(V)$ *is simple.*

Proposition 2.11.9. $PSL(3,4)$ *and* A_8 *are non-isomorphic simple groups of the same order.*