Jan Snellman




# Abstract Algebra, Lecture 9

## The Class Equation

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet


Linköping, fall 2019

Lecture notes availabe at course homepage
`http://courses.mai.liu.se/GU/TATA55/`

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Summary

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Summary

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Summary

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Summary

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Lemma

*Let the group $G$ act on itself by conjugation,*

$$g.x = gxg^{-1}$$

*Then*

1. $\mathbf{Orb}(x) = \left\{ gxg^{-1} \middle| g \in G \right\}$. *We call this the conjugate class containing $x$ and denote it by $Cl(x)$.*
2. $\mathbf{Stab}(x) = \left\{ g \in G \middle| gxg^{-1} = x \right\} = \{ g \in G | gx = xg \}$. *We call this subgroup the centralizer of $x$ and denote it by $C_G(x)$.*
3. $\mathbf{Fix}(g) = \left\{ x \in G \middle| gxg^{-1} = x \right\} = \{ x \in G | gx = xg \} = C_G(g)$
4. $\mathbf{Fix}(G) = \left\{ x \in G \middle| gxg^{-1} = x \text{ for all } x \in X \right\} = \cap_{g \in G} \mathbf{Fix}(g) = \cap_{g \in G} C_G(g) = \{ x \in G | gx = xg \text{ for all } g \in G \}$. *We call this subgroup the center of $G$ and denote it $Z(G)$.*

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



**Lemma**

*The center of $G$ is the union of all singleton conjugacy classes.*

**Proof.**

$Cl(g) = \{g\}$ if and only if $g$ commutes with everything. □

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Theorem (Class equation)

*If $G$ is finite, then*

$$|G| = |Z(G)| + \sum_{i=1}^{r} |Cl(x_i)| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C_G(x_i)|} \tag{1}$$

*where the $x_i$'s are a choice of exactly one group element from each conjugacy class with more than one element.*

## Proof.

The conjugacy classes are equivalence classes of an equivalence realtion on $G$, thus they partition $G$. The center is, as stated before, the union of the conjugacy classes that consist of a single element. □

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Example

If $G$ is abelian, then the class equation reads

$$|G| = |Z(G)|$$

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Example

In $S_3$, there is one conjugacy class containing the transpositions, and one containing the 3-cycles, and a singleton class containing the identity. The class equation is thus

$$\begin{aligned} |S_3| &= |Z(S_3)| + |Cl((1,2))| + |Cl((1,2,3))| \\ &= |\langle () \rangle| + \frac{|S_3|}{C_{S_3}((1,2))} + \frac{|S_3|}{C_{S_3}((1,2,3))} \\ &= 1 + 3 + 3 \\ &= |\langle () \rangle| + \frac{|S_3|}{C_{S_3}((1,2))} + \frac{|S_3|}{C_{S_3}((1,2,3))} \end{aligned}$$

from which we conclude that $C_{S_3}((1,2)) = \langle (1,2) \rangle$, $C_{S_3}((1,2,3)) = \langle (1,2,3) \rangle$.

For general $n$, the conjugacy classes of $S_n$ are easy to describe:

**Theorem**

1. *Two permutations in $S_n$ are conjugate iff they have the same cycle type.*
2. *The number of permutations in $\S_n$ with cycle type $\lambda$ is given by $c(\lambda, n)$ (hand-in exam batch 2).*
3. *Thus, there are exactly $\frac{n!}{c(\lambda,n)}$ permutations in $S_n$ commuting with a given permutation $\sigma$ with cycle type $\lambda$*
4. $Z(S_n) = \langle () \rangle$
5. *The class equation for $S_n$ is*

$$n! = 1 + \sum_{\lambda \vdash n} c(\lambda, n) \tag{2}$$

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Example

For $n = 4$, the numerical partitions of 4, and the corresponding conjugacy classes, are

| $\lambda$ | $\sigma$ | $c(\lambda, 4)$ |
|---|---|---|
| $(4)$ | $(1,2,3,4)$ | 6 |
| $(3,1)$ | $(1,2,3)(4)$ | 8 |
| $(2,2)$ | $(1,2)(3,4)$ | 3 |
| $(2,1,1)$ | $(1,2)(3)(4)$ | 6 |
| $(1,1,1,1)$ | $(1)(2)(3)(4)$ | 1 |

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



**Theorem (Cauchy)**

*If $G$ is a finite group with $|G| = n$, and $p$ is a prime number dividing $n$, then $G$ contains en element of order $p$.*

We will prove this important result twice, first using the class equation, then using an action by a cyclic group.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Proof (by Class Equation)

- Induction over $n$, assuming $n \geq p$.
- If $n = p$ then $G$ is cyclic, done.
- So assume $n > p$, $p|n$.
- If $H \leq G$ proper subgroup, $p||H|$, then by induction $H$ contains element of order $p$.
- So suppose that $p \not| |H|$ for all proper subgroups $H$.
- Class equation is

$$n = Z(G) + \sum_{j=1}^{r} \frac{|G|}{|C_G(x_i)|},$$

where $C_G(x_i)$ are proper subgroups, hence their order is not divisible by $p$, hence each term in the sum is, hence so is $Z(G)$.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Prrof (contd)

- So $p|Z(G)$.
- $Z(G)$ finite abelian, so $Z(G) \simeq \prod_{j=1}^{s} \mathbb{Z}_{p_j^{r_j}}$.
- Some $p_j = p$, say $p_1 = p$.
- The generator $a$ of the factor $Z_{p_1^{r_1}}$ has order $p^{r_1}$.
- The element $a^{p^{r_1-1}}$ has order $p^{r_1}/\gcd(p^{r_1}, p^{r_1-1}) = p$.
- Inject this element of $\mathbb{Z}_{p_1^{r_1}}$ into the direct product, it will still have order $p$.
- Done.

□

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Proof using group action

- Recall $|G| = n$, $p|n$, $p$ prime
- Let $C_p = \langle r \rangle$, the cyclic group with $p$ elements.
- Let $X = \{ (g_1, \ldots, g_p) | g_i \in G,\ g_1 \cdots g_p = 1 \}$
- Clearly $|X| = n^{p-1}$
- $|\mathbf{Orb}((g_1, \ldots, g_p))| = \frac{|C_p|}{|\mathbf{Stab}((g_1, \ldots, g_p))|}$
- $\mathbf{Stab}((g_1, \ldots, g_p)) = \begin{cases} C_p & \text{if } g_1 = g_2 = \cdots = g_p \\ \{1\} & \text{if some } g_i \neq g_j \end{cases}$
- Thus $|\mathbf{Orb}((g_1, \ldots, g_p))| = \begin{cases} 1 & \text{if } g_1 = g_2 = \cdots = g_p \\ p & \text{if some } g_i \neq g_j \end{cases}$

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Proof (contd

- Denote by $a$ the number of singleton orbits, $b$ the number of orbits of size $p$
- Since $(1, 1, \ldots, 1) \in X$, $a > 0$
- Orbits partition $X$, so $n^{p-1} = a + bp$
- $p|n$, so $p|a$
- Thus exist other singleton orbit $(g, \ldots, g) \in X$ apart from $(1, \ldots, 1)$
- This means that $g^p = 1$, hence $o(g) = p$.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Example

Take $G = S_3$. Then $|G| = 6$, which is divisible by 3. Let us prove that there is some element in $S_3$ of order 3.

Put

$$X = \left\{ (g, h, h^{-1}g^{-1}) \middle| g, h \in S_3 \right\}$$

Then $|X| = 6^2 = 36$.

Study the sequence $\mathbf{v} = ((12), (13), (123)) \in X$. All cyclic permutations except the identity change $\mathbf{v}$, so $\mathbf{Stab}(\mathbf{v}) = \{1\}$, and $\mathbf{Orb}(\mathbf{v}) = \{((12), (13), (123)),\ ((13), (123), (12)),\ ((123), (12), (13))\}$.

Study the sequence $\mathbf{w} = ((123), (123), (123)) \in X$. All cyclic permutations preserve $\mathbf{w}$, so $\mathbf{Stab}(\mathbf{w}) = \left\{1, r, r^2\right\}$, and $\mathbf{Orb}(\mathbf{w}) = \{((123), (123), (123))\}$.

There are 3 elements in $S_3$ whose orders are divisible by 3, so orbit partition of $X$ becomes

$$36 = 3 + 3 * 11$$

Can you find these eleven orbits of size 3?

## Theorem

*If $|G| = p^n$, with $p$ prime, then $Z(G)$ is non-trivial.*

## Proof.

- $z = |Z(G)|$
- If $a \in G$ then $C_G(a) \leq G$, so $|C_G(a)| = p^k$.
- If $G$ abelian, then $Z(G) = G$, done.
- If $G$ not abelian then $z < p^n$, and

$$p^n = z + \sum_j \frac{p^n}{p^{k_j}}$$

- $p|LHS$, $p|\frac{p^n}{p^{k_j}}$, so $p|z$.
- Since $z > 0$, we get that $z > 1$, so $Z(G)$ non-trivial.

□

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Theorem

*Let $|G| = p^2$, where $p$ is a prime. Then $G$ is abelian.*

## Proof.

- $|\mathbb{Z}(G)| \in \{p, p^2\}$ since the center is a non-trivial subgroup.
- If $|\mathbb{Z}(G)| = p^2$ then done.
- Assume, towards a contradiction, that $|Z(G)| = p$.
- Then $Z(G)$ cyclic, and normal in $G$, so $G/Z(G)$ also cyclic.
- Let $G/Z(G) = \langle aZ(g) \rangle$.
- Take $g, h \in G$, their images in the quotient are $gZ(G) = a^m Z(G)$ and $hZ(G) = a^n Z(G)$.
- So $g = a^m x$, $h = a^n y$, $x, y \in Z(G)$.
- So $gh = a^m x a^n y = x a^m a^n y = x a^{m+n} y = x y a^{m+n} = y x a^{m+n} = y a^{m+n} x = y a^n a^m x = a^n y x a^m = hg$.

□

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



Recall:

**Definition**

A group is a $p$-group if every element has order which is a power of $p$.

**Lemma**

*A finite group is a p-group iff its size is a power of p.*

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



**Definition**

Let $|G| = n$, and suppose that $p^k | n$ but $p^{k+1} \not| n$. A subgroup $H \leq G$ with $|H| = p^k$ is called a $p$-Sylow subgroup.

**Theorem (First Sylow thm)**

*If $|G| = n$, with $p|n$, then $G$ has a $p$- Sylow subgroup. Furthermore, any $p$-subgroup of $G$ is contained in some $p$-Sylow subgroup.*

**Proof.**

Omitted, read the textbook. □

**Corollary**

*If $|G| = n$, with $p^k|n$, then $G$ has a subgroup of size $p^k$.*

**Remark**

Note that this does not guarantee the existence of elements of order $p^k$.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



**Example**

If $|G| = 12$, then there are surely subgroups of size $2, 3, 4$. In the dihedral group with 12 elements, there are no elements of order 4, however, there are subgroups of size 4. You can take the subgroup generated by a reflection through a line through two vertices, a reflection through a line perpendicular to the first line, and the antipodal map.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



**Theorem (Sylow's second thm)**

*Any two $p$-Sylow subgroups $H, K$ of $G$ are conjugate, i.e., there exists $g \in G$ such that*

$$K = gHg^{-1}.$$

**Proof.**

Omitted, read the textbook. □

**Remark**

If there is a single $p$-Sylow subgroup $H$, then Sylows's second thm shows that $H \triangleleft G$.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



**Theorem (Sylow's third thm)**

*Let $G = m$, $p$ prime, $p|m$. Let $r$ denote the number of $p$-Sylow subgroups. Then*

$$r|m$$

*and*

$$r \equiv 1 \mod p$$

**Proof.**

Omitted, read the textbook. □

## Example (Svensson Ex. 12.57)

- Suppose $|G| = 56 = 2^3 * 7$.
- Claim: $G$ has (at least) one proper normal subgroup.
- $n_2$ number 2-Sylow, $n_7$ number 7-Sylow.
-

$$\begin{aligned} n_2 &\equiv 1 \mod 2 \\ 2^3 * 7 &\equiv 0 \mod n_2 \\ n_7 &\equiv 1 \mod 7 \\ 2^3 * 7 &\equiv 0 \mod n_7 \end{aligned}$$

- Soln to above: $(n_2, n_7) \in \{(1,1), (1,8), (7,1), (7,8)\}$
- If we can exclude $n_2 = 7$, $n_7 = 8$ then done, since unique $p$-Sylow is normal

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET



## Example (Svensson Ex. 12.57 cont.)

- Suppose that we have 7 2-Sylow and 8 7-Sylow
- Each 7-Sylow is cyclic
- Two such intersect in the identity, only, by Lagrange.
- Picture!
- So $8 * 6 = 48$ elements of order 7
- Only $56 - 48 = 8$ elems left, can't make 7 groups of order $2^3 = 8$.