Foreword

Usage

- Notes are presented in two columns: main notes on the left, and sidenotes on the right. Main notes will have a larger margin.
- The following is the color code for the notes:

Blue	Definitions
Red	Important points
Yellow	Points to watch out for / comment for incompletion
Green	External definitions, theorems, etc.
Light Blue	Regular highlighting
Brown	Secondary highlighting

- The following is the color code for boxes, that begin and end with a line of the same color:

Blue	Definitions
Red	Warning
Yellow	Notes, remarks, etc.
Brown	Proofs
Magenta	Theorems, Propositions, Lemmas, etc.

- Hyperlinks are underlined in magenta. If your PDF reader supports it, you can follow the links to either be redirected to an external website, or a theorem, definition, etc., in the same document. Note that this is only reliable if you have the full set of notes as a single document, which you can find on: `https://japorized.github.io/TeX_notes`

17 Lecture 17 Jun 08 2018

17.1 Group Action (Continued 2)

17.1.1 Group Action (Continued 2)

Note (Recall Theorem 46)

Let G act on a finite set $X \neq \emptyset$. Let[1]

$$X_f = \{x \in X : a \cdot x = x,\, a \in G\}$$

Let $G \cdot x_1, G \cdot x_2, ..., G \cdot x_n$ be distinct nonsingleton orbits (ie. $|G \cdot x_i| > 1$). Then

$$|X| = \left|X_f\right| + \sum_{i=1}^{n} [G : S(x_i)].$$

[1] X_f is also called the set of elements of X that are fixed by the action of G.

Example 17.1.1 (Conjugacy Class & Centralizer)

Let G be a finite group acting on itself by ***conjugation****. In the context of Theorem 46, we have that*

$$\begin{aligned} X &= G \\ G_f &= \{x \in G : gxg^{-1} = x,\, g \in G\} \\ &= \{x \in G : gx = xg,\, g \in G\} = Z(G), \end{aligned}$$

where we recall that $Z(G)$ is the center of G. Now for any $x \in G$, we have

$$G \cdot x = \{gxg^{-1} : g \in G\},$$

which is known as the ***conjugacy class*** *of x. We also have*

$$S(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = C_G(x),$$

which is called the ***centralizer*** *of x.*

Putting the above example with Theorem 46, we have the following corollary.

Corollary 47 (Class Equation)

Let G be a finite group and $\{gx_1g^{-1} : g \in G\}$, ..., $\{gx_ng^{-1} : g \in G\}$ denote the distinct nonsingleton conjugacy classes. Then

$$|G| = |Z(G)| + \sum_{i=1}^{n}[G : C_G(x_i)].$$

Lemma 48

Let G be a group of order o^m, where p prime and $m \in \mathbb{N}$, which acts on a finite set X. Let

$$X_f = \{x \in X : a \cdot x = x,\, a \in G\}.$$

Then we have

$$|X| \equiv \left|X_f\right| \mod p$$

Proof

By the Orbit Decomposition Theorem, we have that

$$|X| = \left|X_f\right| + \sum_{i=1}^{n}[G : S(x_i)],$$

where $[G : S(x_i)] > 1$ for $1 \leq i \leq n$. For any x_i, by Lagrange's Theorem, $[G : S(x_i)] \mid |G| = p^m$. Since $[G : S(x_i)] > 1$, we have, by the ***Fundamental Theorem of Arithmetic****, that $[G : S(x_i)]$ must be a multiple of p, i.e. p divides $[G : S(x_i)]$, for all i. Therefore, $p \mid \left(|X| - \left|X_f\right|\right)$, i.e.*

$$|X| \equiv \left|X_f\right| \mod p,$$

as required. $\square$

RECALL Lagrange's Theorem: If G is finite and $g \in G$, then

$$o(g) \mid |G|.$$

An interesting question to ask here is: Is the converse true? I.e., given a group G with an integer m such that $m \mid |G|$, does G contain an element of order m?

Consider K_4, the Klein 4-group. Note that all elements of K_4 have order at most 2, but $4 \mid |K_4| = 4$.

Now if m is some prime, is the converse still true?

Theorem 49 (Cauchy)

Let p be a prime, G be a finite group. If $p \mid |G|$, then G contains an element of order p.

Proof (McKay)

Let $|G| = n$. Suppose $p \mid n$. Let

$$X = \{(a_1, ..., a_p) : a_i \in G,\ a_1 \dots a_p = 1\}.$$

Note that $X \neq \emptyset$, since $(1, ..., 1) \in X$ (so the proof is not vacuous). Take any $a_1, ..., a_{p-1} \in G$, then a_p is uniquely determined, i.e.

$$a_p = (a_1 \dots a_{p-1})^{-1}.$$

Now for each a_i, we have n choices, thus $|X| = n^{p-1}$.[2]

[2] Convince yourself why this is true.

Let $\mathbb{Z}_p = (\mathbb{Z}_p, +)$ act on X by "cycling", i.e. $\forall k \in \mathbb{Z}_p$,

$$k \cdot (a_1, a_2, ..., a_p) = (a_{k+1}, a_{k+2}, ..., a_p, a_1, ..., a_k).$$

[3] *Note that*

[3] We want to use Theorem 46 from here.

$$\begin{aligned}(a_1, ..., a_p) \in X_f &\iff \text{every cycled shift of } (a_1, ..., a_p) \text{ is itself} \\ &\iff a_1 = a_2 = \dots = a_p \text{ and } a_1 a_2 ... a_p = 1\end{aligned}$$

i.e. all of the components of the p-tuple are the same. Now if $(a_1, ..., a_p)$ has at least 2 distinct components, then its orbits must have p elements. In other words, for some $r \in \mathbb{N}$, for each $1 \leq i \leq r$, we have that $[G : S(x_i)] = p$.

Then, by the Orbit Decomposition Theorem,

$$n^{p-1} = |X| = \left|X_f\right| + \sum_{i=1}^{r}[G : S(x_i)]$$
$$\left|X_f\right| = n^{p-1} - rp.$$

We observe that $\left|X_f\right|$ *is indeed divisible by* p *and is non-zero, since* $(1, ..., 1) \in X_f$. *Therefore, there exists some* $a \neq 1 \in G$, *such that* $(a, ..., a) \in X_f$, *i.e.* $a^p = 1$. *We know that* p *is the smallest power by construction, and therefore* $o(a) = p$ *as required.* $\square$