Additional notes for Galois Theory
Math 128B

1 Orbit-Stabilizer and conjugation

Definition. Let G be a group. For $x \in X$, we define the *orbit of x under conjugation by G* to be

$$\operatorname{orb}_G(x) = \left\{gxg^{-1} \mid g \in G\right\} = \left\{y \in X \mid y = gxg^{-1} \text{ for some } g \in G\right\} \tag{1}$$

and we define the *stabilizer of x under conjugation by G* to be

$$\operatorname{stab}_G(x) = \left\{g \in G \mid gxg^{-1} = x\right\} \leq G. \tag{2}$$

In other words, $\operatorname{orb}_G(x)$ is the conjuagacy class of x in G, and since $gxg^{-1} = x$ exactly when $gx = xg$, $\operatorname{stab}_G(x)$ is precisely

$$C(x) = \{g \in G \mid gx = xg\} \leq G, \tag{3}$$

the *centralizer* of x in G.

Theorem. *Considering conjugation on G, for any $x \in X$, let S be the set of all left cosets of the coset $\operatorname{stab}_G(x)$ in G. Then the function $\Phi : S \to \operatorname{orb}_G(x)$ defined by*

$$\Phi(a \operatorname{stab}_G(x)) = axa^{-1} \tag{4}$$

is well-defined and bijective. In particular, if $\operatorname{orb}_G(x)$ is finite, then

$$|\operatorname{orb}_G(x)| = |G : \operatorname{stab}_G(x)|. \tag{5}$$

Proof. The only possible ambiguity in the definition of Φ comes in the choice of coset representative a in the coset $a \operatorname{stab}_G(x)$. However, if a' is another representative for $a \operatorname{stab}_G(x)$, then $a' = ah$ for some $h \in \operatorname{stab}_G(x)$ (Gallian, Ch. 7), and

$$a'xa'^{-1} = ahx(ah)^{-1} = ahxh^{-1}a^{-1} = axa^{-1}, \tag{6}$$

by the definition of what it means to have $h \in \operatorname{stab}_G(x)$.

To see that Φ is surjective, for $y \in \operatorname{orb}_G(x)$, by definition of orbit, $y = gxg^{-1}$ for some $g \in G$, which means that $y = \Phi(g \operatorname{stab}_G(x))$. To see that Φ is injective, suppose $\Phi(a \operatorname{stab}_G(x)) = \Phi(b \operatorname{stab}_G(x))$. Then $axa^{-1} = bxb^{-1}$, which means that

$$x = b^{-1}axa^{-1}b = (b^{-1}a)x(b^{-1}a)^{-1}. \tag{7}$$

Therefore, $b^{-1}a \in \operatorname{stab}_G(x)$, which means that $a \operatorname{stab}_G(x) = b \operatorname{stab}_G(x)$ (Gallian, Ch. 7). $\square$

2 The Cycle-Shape Theorem

Theorem. *For $\alpha, \sigma \in S_n$, let $\beta = \sigma\alpha\sigma^{-1}$. Then β has the same cycle-shape as α, except renumbered by σ; that is, conjugation by σ turns each cycle of α of the form*

$$(a\ b\ c\ \ldots\ z) \tag{8}$$

to a cycle of the form

$$(\sigma(a)\ \sigma(b)\ \sigma(c)\ \ldots\ \sigma(z)). \tag{9}$$

Consequently, for $\alpha, \beta \in S_n$, there exists some $\sigma \in S_n$ such that $\beta = \sigma\alpha\sigma^{-1}$.

In other words, conjugation by σ "renumbers" the cycles of α by applying σ to them.

Proof. Observe that if we apply the permutation $\sigma\alpha\sigma^{-1}$ to the point $\sigma(x) \in \{1, \ldots, n\}$, we get

$$\sigma\alpha\sigma^{-1}(\sigma(x)) = \sigma(\alpha(x)). \tag{10}$$

It follows that if the disjoint cycle form of α contains a cycle of the form $(a\ b\ c\ \ldots)$, where $\alpha(a) = b$, $\alpha(b) = c$, and so on, then the disjoint cycle form of $\sigma\alpha\sigma^{-1}$ contains a cycle of the form $(\sigma(a)\ \sigma(b)\ \sigma(c)\ \ldots)$. Therefore, since σ is a bijection, the set $\{1, \ldots, n\}$ consists of points of the form $\sigma(x)$, and $\sigma\alpha\sigma^{-1}$ is a product of disjoint cycles of the form $(\sigma(a)\ \sigma(b)\ \sigma(c)\ \ldots)$, as claimed.

As for the last statement, if α and β have the same cycle-shape, then there must exist some way of putting the cycles of α in bijection with cycles of β of the same length. Then if (for example) the cycle $(a\ b\ c\ \ldots)$ of α is matched with the cycle $(x\ y\ z\ \ldots)$ of β, choose $\sigma \in S_n$ such that $\sigma(a) = x$, $\sigma(b) = y$, and so on. By the first part of the theorem, it then follows that $\sigma\alpha\sigma^{-1} = \beta$, and the theorem follows. $\square$

One subtlety in the Cycle-Shape Theorem: If G is a subgroup of S_n and $\alpha, \beta \in G$ then the following statements are both true.

- If α and β are conjugate in G, then α and β must have the same cycle-shape (since they are conjugate in S_n).
- But if α and β have the same cycle-shape, they need not be conjugate in G, even though they are conjugate in S_n.

For a very direct example of the second statement, take $\alpha = (1\ 2\ 3)$, $\beta = (1\ 3\ 2)$, and $G = A_3 = \langle(1\ 2\ 3)\rangle$. Since α and β have the same cycle-shape, they are conjugate in S_3, but they are *not* conjugate in A_3, since A_3 is abelian, and therefore, elements are only conjugate to themselves. For a more interesting example, take $\alpha = (1\ 2\ 3)$, $\beta = (1\ 3\ 2)$, and $G = A_4$. Again, α and β are conjugate in S_4, but they are *not* conjugate in A_4, as the reader can check by brute force. More specifically, the conjugacy class in S_4 consisting of 8 3-cycles splits into two conjugacy classes of size 4 in A_4: the conjugates of $\alpha = (1\ 2\ 3)$ and the conjugates of $\beta = (1\ 3\ 2)$.

3 The Fundamental Theorem of Galois Theory (expanded statement)

Definition. Let F be a field, and let E be an extension field of F. An *automorphism* of E is a ring isomorphism $\varphi : E \to E$. The *Galois group of E over F* is defined to be

$$\mathrm{Gal}(E/F) = \{\varphi \in \mathrm{Aut}(E) \mid \varphi(x) = x \text{ for all } x \in F\}. \tag{11}$$

If $H \leq \mathrm{Gal}(E/F)$, we define the *fixed field of H* to be

$$E_H = \{x \in E \mid \varphi(x) = x \text{ for all } \varphi \in H\}. \tag{12}$$

Theorem (Fundamental Theorem of Galois Theory (expanded))**.** *Let F be a field of characteristic 0 or a finite field, and let E be the splitting field of some $f(x) \in F[x]$. Let $\mathcal{S}$ be the set of all subgroups of $\mathrm{Gal}(E/F)$, and let $\mathcal{F}$ be the set of all subfields of E containing F. Define functions $\Phi : \mathcal{S} \to \mathcal{F}$ and $\Psi : \mathcal{F} \to \mathcal{S}$ by*

$$\Phi(H) = E_H = \text{the fixed field of } H, \tag{13}$$

$$\Psi(K) = \mathrm{Gal}(E/K) = \text{the group of all automorphism of } E \text{ fixing } K. \tag{14}$$

Then Φ and Ψ are inverses of each other, and therefore, bijections. (I.e., for K a subfield of E containing F, $E_{\mathrm{Gal}(E/K)} = K$, and for H a subgroup of $\mathrm{Gal}(E/F)$, $\mathrm{Gal}(E/E_H) = H$.) Furthermore, if K and L are subfields of E containing F:

1. *We have that $K \subseteq L$ if and only if $\mathrm{Gal}(E/K) \geq \mathrm{Gal}(E/L)$. (I.e., Φ and Ψ are inclusion-reversing bijections.)*

2. *$[E : K] = |\mathrm{Gal}(E/K)|$, and therefore,*

$$[K : F] = |\mathrm{Gal}(E/F) : \mathrm{Gal}(E/K)| = \frac{|\mathrm{Gal}(E/F)|}{|\mathrm{Gal}(E/K)|}. \tag{15}$$

3. *K is a splitting field of some $g(x) \in F[x]$ if and only if $\mathrm{Gal}(E/K)$ is normal in $\mathrm{Gal}(E/F)$. In that case,*

$$\mathrm{Gal}(K/F) \approx \mathrm{Gal}(E/F)/\,\mathrm{Gal}(E/K). \tag{16}$$

4. *The group $\mathrm{Gal}(E/F)$ acts on (permutes) the set $X = \{a_1, \ldots, a_n\}$ of all zeros of $f(x)$ in E.*

5. *If $f(x)$ is irreducible over F, then $\mathrm{Gal}(E/F)$ acts transitively on $X = \{a_1, \ldots, a_n\}$; i.e., for $i \neq j$, there exists some $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(a_i) = a_j$.*