II.J. Automorphisms

II.J.1. DEFINITION. An isomorphism $\varphi\colon G \overset{\cong}{\to} G$ is called an **automorphism** of G.

II.J.2. EXAMPLES. (i) The identity map id_G is an automorphism of any group.

(ii) Conjugation by $g \in G$ is denoted $\imath_g\colon G \overset{\cong}{\to} G$; automorphisms of this type are called **inner**. (The conjugation must be by an element *of* G, not by an element of some larger group it sits in!) Abelian groups have no non-identity inner automorphisms.

(iii) If $G \trianglelefteq G'$, then conjugation by $g' \in G'$ does give *an* automorphism of G (but this may or may not be inner).

(iv) In Example II.I.22(e), $\mathfrak{S}_4$ acted by conjugation on the ccl

$$\{(12)(34),\ (13)(24),\ (14)(23)\} = V_4 \backslash \{1\}.$$

That is, for each $\sigma \in \mathfrak{S}_4$, $\imath_\sigma$ induces a permutation of $V_4\backslash\{1\}$ ($\Longrightarrow$ element of $\mathfrak{S}_3$ — we got all elements of $\mathfrak{S}_3$ this way). In fact, each $\imath_\sigma$ induces an automorphism of V_4 (since $V_4 \trianglelefteq \mathfrak{S}_4$) and [except for the identity] these are *non*-inner (as V_4 is abelian).

Write

$$\begin{aligned} \mathrm{Aut}(G) &:= \text{ the set of automorphisms of } G, \text{ and} \\ \mathrm{Inn}(G) &:= \text{ the set of inner automorphisms of } G. \end{aligned}$$

II.J.3. PROPOSITION-DEFINITION. $\mathrm{Aut}(G)$ *is a group under composition of maps, as is* $\mathrm{Inn}(G)$*; and* $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$*. So we can define the group of* ***outer automorphisms*** *by* $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$*. If* G *is abelian, then* $\mathrm{Out}(G) = \mathrm{Aut}(G)$.

PROOF. The composition of two isomorphisms is again an isomorphism; isomorphisms are invertible; and Id_G is an isomorphism. The same goes for inner automorphisms: e.g.,

$$(\imath_g \circ \imath_h)(x) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \imath_{gh}(x).$$

Finally, for $x \in G$ and $\alpha \in \mathrm{Aut}(G)$,

$$\begin{aligned}(\alpha \circ \imath_x \circ \alpha^{-1}(g) &= \alpha(x\alpha^{-1}(g)x^{-1}) \\ &= \alpha(x)\underbrace{\alpha(\alpha^{-1}(g))}_{=g}\alpha(x)^{-1} \\ &= \imath_{\alpha(x)}(g)\end{aligned}$$

$\implies \alpha\mathrm{Inn}(G)\alpha^{-1} \subseteq \mathrm{Inn}(G)$. □

II.J.4. EXAMPLES. (i) $\mathrm{Aut}(V_4) \cong \mathfrak{S}_3$, so we can see Ex. II.I.22(e) in terms of a surjective homomorphism $\mathfrak{S}_4 \overset{\imath_{(\cdot)}}{\twoheadrightarrow} \mathrm{Aut}(V_4)$ (with kernel V_4). So we see that the automorphism group of an abelian group need not be abelian.

(ii)[20] $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$. To see this, consider

$$\begin{aligned}\mu \colon \mathbb{Z}_n^* &\to \mathrm{Aut}(\mathbb{Z}_n) \\ \bar{a} &\longmapsto \mu_{\bar{a}} := \text{multiplication by } \bar{a}.\end{aligned}$$

For injectivity of μ: suppose $\mu_{\bar{a}} = \mathrm{id}_{\mathbb{Z}_n}$; then $\mu_{\bar{a}}(\bar{b}) = \bar{b}$ for any $\bar{b} \in \mathbb{Z}_n$, and taking $\bar{b} = \bar{1}$ gives $\bar{a} = \bar{1}$.

For surjectivity of μ: let $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$, and set $\bar{a} = \alpha(\bar{1})$. Now

$$\begin{aligned}(\mu_{\bar{a}} - \alpha)(\bar{b}) &= \mu_{\bar{a}}(\bar{b}) - \alpha(\bar{b}) \\ &= \bar{a}\bar{b} - \alpha(\underbrace{\bar{1} + \cdots + \bar{1}}_{b \text{ times}}) \\ &= \bar{a}\bar{b} - \underbrace{\alpha(\bar{1})}_{\bar{a}} \cdot \bar{b} \\ &= \bar{0} \quad (\forall \bar{b})\end{aligned}$$

$\implies \mu_{\bar{a}} = \alpha$, so $\alpha \in \mathrm{im}(\mu)$. □

We finish this section with a striking result.

---

[20] Here we recall that $\mathbb{Z}_n^* = \{\bar{a} \mid (a,n) = 1\}$ under multiplication mod n. It's a group because the gcd being 1 means that there exist $r, s \in \mathbb{Z}$ such that $ra + sn = 1$, i.e. $\bar{r}\bar{a} \underset{(n)}{\equiv} \bar{1}$ and so $\bar{r} = \bar{a}^{-1}$. Similarly, $\mu_{\bar{a}}$ below — which is a homomorphism from $\mathbb{Z}_n \to \mathbb{Z}_n$ by the distributive law — has inverse $\mu_{\bar{a}^{-1}}$, making it an automorphism of $\mathbb{Z}_n$.

II.J.5. THEOREM. *Let $n > 2$.*
(i) $\mathrm{Inn}(\mathfrak{S}_n) \cong \mathfrak{S}_n$.
(ii) *Assume $n \neq 6$. Then* $\mathrm{Aut}(\mathfrak{S}_n) \cong \mathrm{Inn}(\mathfrak{S}_n)$.
(iii) *For $n = 6$, this is* false (*and* $\mathrm{Out}(\mathfrak{S}_6) \cong \mathbb{Z}_2$).

PROOF. (i) We want to show that $\imath\colon \mathfrak{S}_n \to \mathrm{Aut}(\mathfrak{S}_n)$, the map sending $g \mapsto \imath_g$, is injective — in other words, that $C(\mathfrak{S}_n) = \{1\}$. Let $\sigma \in \mathfrak{S}_n \backslash \{1\}$ be given; it moves at least one number in $\{1, \ldots, n\}$, say $a \mapsto b$. Take any $c \neq a, b$ in $\{1, \ldots, n\}$; then $(bc)\sigma$ sends $a \mapsto c$, while $\sigma(bc)$ sends $a \mapsto b$. So $\sigma \notin C(\mathfrak{S}_n)$, done.

(ii) Any $\alpha \in \mathrm{Aut}(\mathfrak{S}_n)$ sends conjugate elements to conjugate elements (why?). Hence if α is going to move an element of one conjugacy class ccl_1 into a different conjugacy class ccl_2, it must send all of ccl_1 into ccl_2, and its inverse does the reverse. So we would have to have $|\mathrm{ccl}_1| = |\mathrm{ccl}_2|$, and moreover (since automorphisms send elements of order k to elements of order k) that *elements* of ccl_1 have the same orders as those in ccl_2. The goal of this proof is to show that these constraints on an automorphism messing with ccl's are so tight that it never happens except for $n = 6$.

Now the ccl's in $\mathfrak{S}_n$ with elements of order 2 are the

$$C_k := \left\{ \sigma \in \mathfrak{S}_n \;\middle|\; \begin{array}{c} \sigma \text{ has cycle structure} \\ \underbrace{(\cdot\cdot)\cdots(\cdot\cdot)}_{k}\underbrace{(\cdot)\cdots(\cdot)}_{n-2k} \end{array} \right\}$$

(i.e. products of k disjoint transpositions) for $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$, with

$$|C_k| = \frac{n!}{(n-2k)!k!2^k}.$$

We have

$$\begin{aligned} |C_k| = |C_1| &\iff \frac{n!}{(n-2k)!k!2^k} = \frac{n!}{(n-2)!2} \\ &\iff \frac{(n-2)!}{(n-2k)!} = k!2^{k-1} \\ &\iff \binom{n-2}{2k-2} = \frac{k!2^{k-1}}{(2k-2)!}; \end{aligned}$$

but the binomial symbol is an integer, whereas $\frac{k!2^{k-1}}{(2k-2)!}$ is not an integer for $k \geq 4$. Moreover, the $k = 2$ case $\binom{n-2}{2} = 2$ is also impossible. This leaves $k = 3$, and $\binom{n-2}{4} = 1$, which holds $\iff$ $n = 6$. We conclude that for $n \neq 6$, $\alpha(C_1) = C_1$.

Now assume that $n \neq 6$, and let an automorphism α be given. We have just shown that α sends transpositions to transpositions. Suppose $\alpha((12)) = (ab)$, and $x \in \{3, \ldots, n\}$; then

$$\begin{aligned}(12)(1x) = \text{3-cycle} &\implies \alpha((12)(1x)) = (ab)\alpha((1x)) = \text{3-cycle} \\ &\implies \alpha((1x)) = (ac) \text{ or } (bc) \quad c \neq a, b\end{aligned}$$

Without loss of generality (by swapping a and b if necessary) we may assume $\alpha((1x)) = (ac)$. With this assumption in place, we make the

<u>Claim</u>: $\alpha((1y)) = (ad)$ (for some $d \neq a$) for any $y \in \{2, \ldots, n\}$. [HW]

Taking this claim for granted, define a permutation of $\{1, \ldots, n\}$ by $\sigma(1) := a$, $\sigma(y) :=$ this "d" for each $y \neq 1$, and compute $\imath_{\sigma^{-1}}\alpha((1y)) = \imath_{\sigma^{-1}}((ad)) = (1y)$. So $(\imath_{\sigma^{-1}} \circ \alpha)$ is the identity on all $(1y)$'s. But transpositions generate $\mathfrak{S}_n$, and since $(yy') = (1y')(1y)(1y')$, the $(1y)$'s generate $\mathfrak{S}_n$ all by themselves. It follows that $\imath_{\sigma^{-1}} \circ \alpha = \mathrm{id}_{\mathfrak{S}_n}$, and so $\alpha = \imath_{\sigma^{-1}}$ is an inner automorphism.

(iii) If α is inner, it has to stabilize ccl's, not permute them. The computation above suggests that there may be an automorphism α with $\alpha(C_1) = C_3$, which would have to be outer. Constructing this will be an application of Sylow theory, so we defer the proof of this part. $\square$