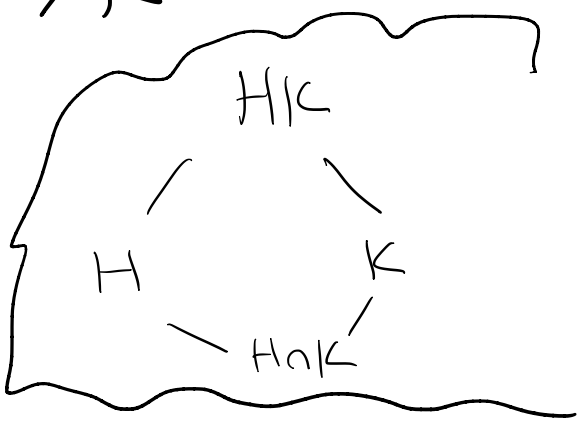
Last time

- Normal subgroups
- Quotient groups
- Universal property
- 1st isomorphism theorem
- FTGT2

Given $H, K \leq G$, write $HK = \{hk \mid h \in H, k \in K\}$.
If $K \trianglelefteq G$, then HK is a subgroup (exercise).

Corollary ("Second isomorphism theorem")
Suppose $H \leq G$ and $K \trianglelefteq G$. Then
$H \cap K \trianglelefteq H$ and $H/_{H \cap K} \cong HK/_K$.



Proof The homomorphism

$$f: H \hookrightarrow HK \twoheadrightarrow HK/_K$$

has kernel $H \cap K$, so $H/_{H \cap K} \cong \bar{\text{im}}(f)$.
But f is surjective, since every coset of K in HK has a representative in H; indeed, $hkK = hK$. □

Corollary ("third isomorphism theorem")

Suppose $H, K \trianglelefteq G$ and $K \subseteq H$. Then

$H/K \trianglelefteq G/K$ and

$$\frac{G/K}{H/K} \cong G/H$$

Proof Since $K \subseteq H = \ker(\pi_H)$, the universal property gives

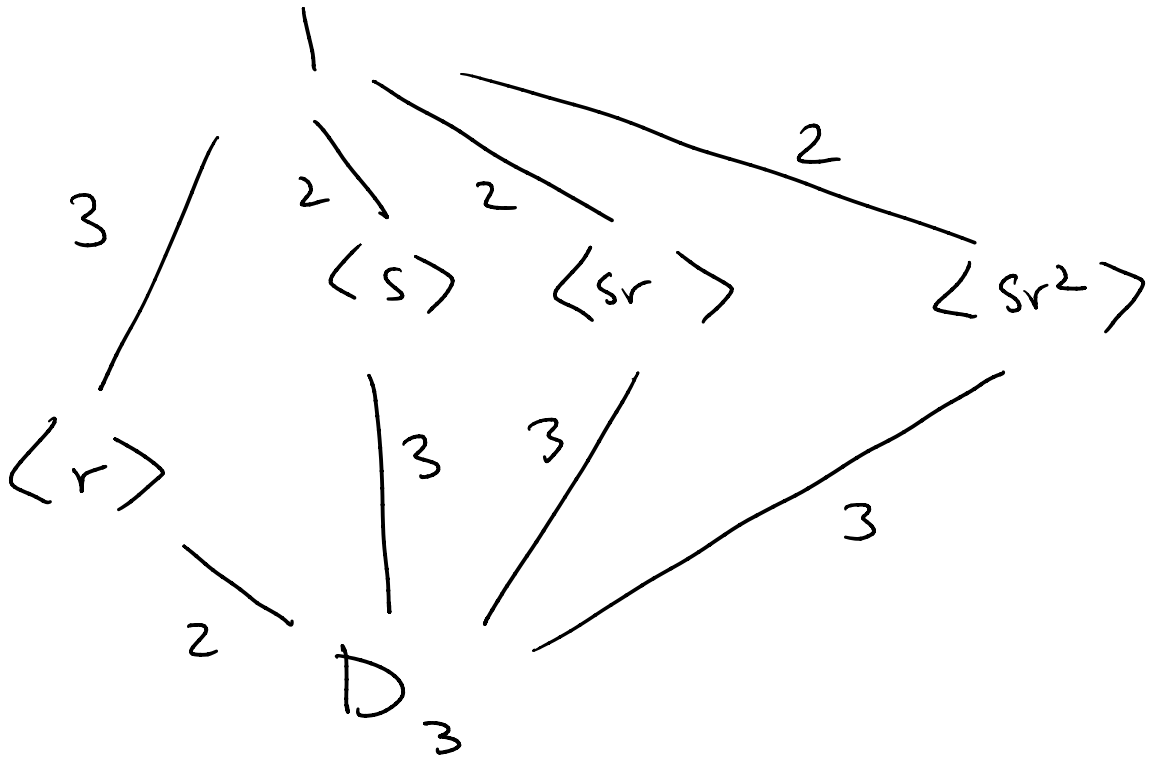
$$\begin{array}{ccc} G & \twoheadrightarrow & G/H \\ \downarrow & \nearrow_{f} & \\ G/K & & \end{array}$$

Since f is surjective, it suffices to show $\ker(f) = H/K$, but $\ker(f)$ is the set of cosets of K in H with representatives in H. $\square$

We return to Galois theory with an example.

Ex Setting $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, we have seen that $\mathrm{Gal}(K/\mathbb{Q}) \cong D_3 = \{s^\varepsilon r^k\}$.

The "obvious" subgroups of D_3 are



(we reind the indices). We claim there are no other subgroups. Indeed (exercise),

(1) if $H \leq D_3$ contains r ($\Leftrightarrow r^2$) and

sr^k, then $s \in H \Rightarrow H = D_3$, and

(2) if H contains sr^k and sr^ℓ for $k \neq \ell$, then $r^{-k}s \in H \Rightarrow 1 \neq r^{\ell-k} \in H \Rightarrow r \in H$

$\Rightarrow s \in H \Rightarrow H = D_3$.

The corresponding automorphisms are

α	$r(\alpha)$	$s(\alpha)$
$\sqrt[3]{2}$	$\sqrt[3]{2}\,\zeta$	$\sqrt[3]{2}$
$\sqrt[3]{2}\zeta$	$\sqrt[3]{2}\,\zeta^2$	$\sqrt[3]{2}\zeta^2$
$\sqrt[3]{2}\zeta^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\,\zeta$

,

from which we see that

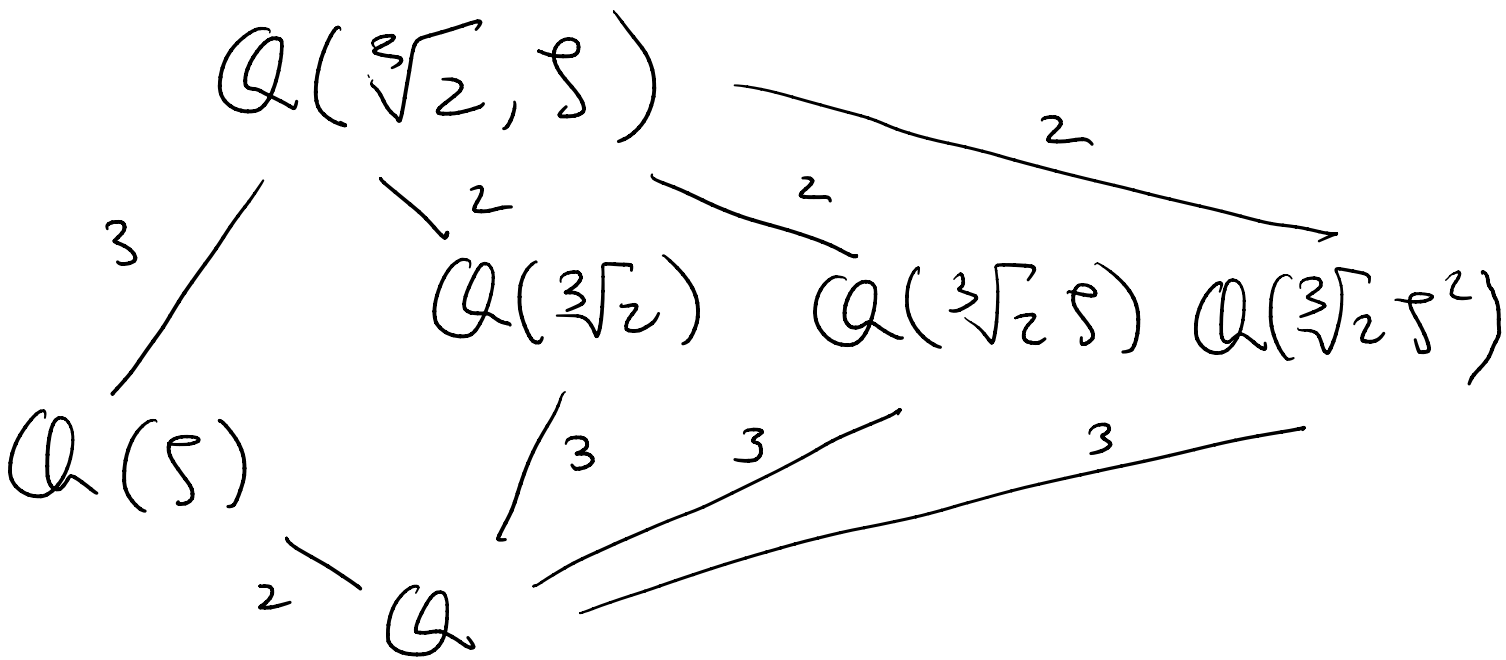
(a) r fixes $\zeta = \sqrt[3]{2}\zeta / \sqrt[3]{2}$

(b) s fixes $\sqrt[3]{2}$

(c) sr fixes $\sqrt[3]{2}\zeta$

(d) sr^2 fixes $\sqrt[3]{2}\zeta^2$

Since the degrees match the indices, these are the fixed fields:



Then $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ is Galois over $\mathbb{Q}(\zeta)$ with Galois group C_2 and Galois over $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}\zeta)$, and $\mathbb{Q}(\sqrt[3]{2}\zeta^2)$ with Galois group C_3. The only proper, nontrivial normal subgroup is $\langle r \rangle$ (exercise), so $\mathbb{Q}(\zeta)$ is Galois over $\mathbb{Q}$ with Galois group $D_3/\langle r \rangle \cong C_2$. The other three extensions are not Galois over $\mathbb{Q}$; in fact, $\mathrm{Aut}(E/\mathbb{Q}) = \{id\}$ for these E. Instead, elements

of $\mathrm{Gal}(K/\mathbb{Q})$ restrict to isomorphisms among the three.

In the example, the smaller Galois groups were all cyclic. We now generalize this observation.

Def An extension K of F is called cyclic if it is Galois and $\mathrm{Gal}(K/F)$ is a cyclic group.

Thm Let F be a field with $\mathrm{char}(F) \nmid n$, and suppose that F contains the n^{th} roots of unity. For $a \in F$, the extension $F(\sqrt[n]{a})$ is cyclic of degree dividing n. Conversely, if K is a cyclic extension of F with $[K:F] = n$, then $K = F(\sqrt[n]{a})$ for some $a \in F$.

Lemma Any $H \leq C_n$ is isomorphic to C_d for some $d \mid n$.

Def The order of $g \in G$, denoted $|g|$, is the least $r \in \mathbb{N}$ such that $g^r = 1$, if such exists. Otherwise, $|g| = \infty$.

Exercise $\langle g \rangle \cong C_{|g|}$, where $C_\infty := \mathbb{Z}$.

Prop $|g| \mid |G|$.

Proof By the exercise, $|g| = |\langle g \rangle|$, which divides $|G|$ by Lagrange's theorem. $\square$

In particular, it follows that $g^{|G|} = 1$.

Lemma 2 Every subgroup of $\mathbb{Z}$ is of the form $k\mathbb{Z}$ for some $k \in \mathbb{Z}$.

Proof WLOG $\{0\} \neq H \leq \mathbb{Z}$. Let $k \in H$ be the least positive element of H. Then $k\mathbb{Z} = \langle k \rangle \subseteq H$. Given $\ell \in H$, we have

$$\gcd(\ell, k) = ak + b\ell \in H$$

so $k \leq \gcd(\ell, k)$ by minimality. Thus, $k = \gcd(\ell, k)$ and $k \mid \ell$, so $\ell \in k\mathbb{Z}$.

□

Proof of Lemma 1 Given $H \leq C_n$, let

$H' = f^{-1}(H) \subseteq \mathbb{Z}$, where

$$f : \mathbb{Z} \longrightarrow C_n$$
$$m \longmapsto r^m.$$

Then H' is a subgroup (exercise), so $H' = k\mathbb{Z}$ by Lemma 2, so $H = \langle r^k \rangle$, whence $H \cong C_{|r^k|}$, but $|r^k| \mid n$. □