EXAMPLE: Recall Klein-four $V_4 = \{e, (12)(34), (13)(24), (14)(23)\} < S_4$

which has index $[S_4 : V_4] = \frac{24}{4} = 6$.

Not hard to check $V_4 \trianglelefteq S_4$ directly, but let's show this and identify the quotient group S_4/V_4 as isomorphic to S_3 by exhibiting a (surjective) homomorphism $S_4 \xrightarrow{\varphi} S_3$ with $\ker\varphi = V_4$:

$$S_4 \xrightarrow{\varphi} S_3 = S_{\{A,B,C\}} \quad \text{where}$$

$$p \longmapsto \varphi(p) = \text{the permutation } \begin{pmatrix} A & B & C \\ p(A) & p(B) & p(C) \end{pmatrix}$$

$A := \{\{1,2\},\{3,4\}\}$ $\circlearrowleft (12)$, $\circlearrowleft (12)(34)$

$B := \{\{1,3\},\{2,4\}\}$ $\circlearrowleft (12)(34)$

$C := \{\{1,4\},\{2,3\}\}$ $\circlearrowleft (23)$, $\circlearrowleft (12)(34)$

$A \xleftrightarrow{(23)} B$, $B \xleftrightarrow{(12)} C$

$$e, (12)(34), (13)(24), (14)(23) \longmapsto \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} = e$$

$$(12) \longmapsto \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} = (BC)$$

$$(23) \longmapsto \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} = (AB)$$

$\vdots$

having these two in $\operatorname{im}\varphi$ already shows $\operatorname{im}\varphi = S_3$, since $\langle (AB), (BC) \rangle = S_{\{A,B,C\}}$

Since $\ker\varphi = V_4$ and $\operatorname{im}\varphi = S_3$, $S_4/V_4 \cong S_3$, which was not obvious.

10/12/18 >

More modular arithmetic (not in Artin Ch. 2)

Recall $\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{(n-1)}\}$ where $\bar{a} := a + n\mathbb{Z}$

had both $+$ and $\times$ operations, so we get two (abelian) groups

- $(\mathbb{Z}/n\mathbb{Z})^+$, which is just a cyclic group of size n, since we have an isomorphism

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\varphi} G = \langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$$

$$\bar{a} \longmapsto g^a$$

$$\underbrace{\bar{a} + \bar{b}}_{=\overline{a+b}} \longmapsto g^{a+b} = g^a \cdot g^b$$

- $(\mathbb{Z}/n\mathbb{Z})^\times := \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \bar{a} \text{ has a multiplicative inverse } \bar{b} \text{ with } \bar{a}\bar{b} = \bar{1}\}$

a little more interesting...

PROPOSITION: $(\mathbb{Z}/n\mathbb{Z})^\times = \{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1 \}$

In particular, $\varphi(n)$ (the Euler phi function

$:= |(\mathbb{Z}/n\mathbb{Z})^\times|$

$= |\{ a = 1, 2, \ldots, n-1 : \gcd(a,n) = 1 \}|$

proof: $\bar{a} \in \mathbb{Z}/n\mathbb{Z} \iff \exists\, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ with $\bar{a}\bar{b} = \bar{1}$

$\iff \exists\, b \in \mathbb{Z}$ with $ab = 1 + kn$ for some $k \in \mathbb{Z}$

$\iff \exists\, b, k \in \mathbb{Z}$ with $ab - kn = 1$

$\iff \mathbb{Z}a + \mathbb{Z}n = \mathbb{Z}\cdot 1$, i.e. $\gcd(a,n) = 1$ ∎

EXAMPLES: ① $(\mathbb{Z}/5\mathbb{Z})^\times = \{\cancel{\bar{0}}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$, $\varphi(5) = 4$

and generally for p prime

$(\mathbb{Z}/p\mathbb{Z})^\times = \{\cancel{\bar{0}}, \bar{1}, \bar{2}, \bar{3}, \ldots, \overline{p-1}\}$, $\varphi(p) = p-1$

② $(\mathbb{Z}/\underbrace{15}_{3\cdot 5}\mathbb{Z})^\times = \{\cancel{\bar{0}}, \bar{1}, \bar{2}, \cancel{\bar{3}}, \bar{4}, \cancel{\bar{5}}, \cancel{\bar{6}}, \bar{7}, \bar{8}, \cancel{\bar{9}}, \cancel{\overline{10}}, \overline{11}, \cancel{\overline{12}}, \overline{13}, \overline{14}\}$

$\varphi(15) = 8 = 2\cdot 4$

$= \mathbb{Z}/15\mathbb{Z} - \underbrace{\{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}\}}_{\text{multiples of } \bar{3}} - \underbrace{\{\bar{0}, \bar{5}, \overline{10}\}}_{\text{multiples of } \bar{5}}$

and generally for p, q distinct primes

$(\mathbb{Z}/pq\mathbb{Z})^\times = \mathbb{Z}/pq\mathbb{Z} - \underbrace{\{\overset{\bar{0}, \bar{p}, 2\bar{p}, \ldots, \overline{(q-1)p}}{\text{multiples of } \bar{p}}\}}_{q \text{ of these}} - \underbrace{\{\overset{\bar{0}, \bar{q}, 2\bar{q}, \ldots, \overline{(p-1)q}}{\text{multiples of } \bar{q}}\}}_{p \text{ of these}}$

$\varphi(pq) = pq - q - p + 1$ because $\bar{0}$ was removed twice!

$= (p-1)(q-1)$

e.g. $\varphi(15) = \varphi(3\cdot 5) = (3-1)(5-1) = 8$

③ For a prime power p^k,

$(\mathbb{Z}/p^k\mathbb{Z})^\times = \mathbb{Z}/p^k\mathbb{Z} - \underbrace{\{\overset{\bar{0}, \bar{p}, 2\bar{p}, \ldots, (p^{k-1}-1)\bar{p}}{\text{multiples of } \bar{p}}\}}_{p^{k-1} \text{ of these}}$ e.g. $\mathbb{Z}/2^3\mathbb{Z} = \{\cancel{\bar{0}}, \bar{1}, \cancel{\bar{2}}, \bar{3}, \cancel{\bar{4}}, \bar{5}, \cancel{\bar{6}}, \bar{7}\}$

so $\varphi(p^k) = p^k - p^{k-1}$

Recall that Lagrange's Thm told us any $g \in G$ a finite group has $\text{ord}(g)$ dividing $|G|$, so $g^{|G|} = \left(g^{\text{ord}(g)}\right)^{\frac{|G|}{\text{ord}(g)}} = 1^{\frac{|G|}{\text{ord}(g)}} = 1$

COROLLARY: (a) Euler's Theorem: In $(\mathbb{Z}/n\mathbb{Z})^\times$, every $\bar{a}$ has $\bar{a}^{\varphi(n)} = \bar{1}$.

(b) Fermat's "Little" Theorem: For any prime p, in $(\mathbb{Z}/p\mathbb{Z})^\times$, every $\bar{a}$ has $\bar{a}^{p-1} = \bar{1}$ } mult. by $\bar{a}$

so in $\mathbb{Z}/p\mathbb{Z}$, every $\bar{a}$ has $\bar{a}^p = \bar{a}$

i.e. in $\mathbb{Z}$, $a^p \equiv a \bmod p$.

EXAMPLE: In $(\mathbb{Z}/15\mathbb{Z})^\times$,

$\varphi(15) = |(\mathbb{Z}/15\mathbb{Z})^\times| = 8$

$\bar{a}$	$\text{ord}(\bar{a})$
$\bar{1}$	1
$\bar{2}$	4
$\bar{4}$	2
$\bar{7}$	4
$\bar{8}$	4
$\bar{11}$	2
$\bar{13}$	4
$\bar{14} = \bar{-1}$	2

all divide 8 (but none are 8 itself, i.e. $(\mathbb{Z}/15\mathbb{Z})^\times$ is not cyclic of order 8, $(\mathbb{Z}/15\mathbb{Z})^\times \not\cong (\mathbb{Z}/8\mathbb{Z})^+$

To understand $(\mathbb{Z}/n\mathbb{Z})^\times$ better, it will help to look at ...

§2.11 Product groups (& Sun Ze's Theorem)

DEF'N: (-PROPOSITION) Given two groups G, G' their Cartesian product $G \times G' = \{(g, g') : g \in G, g' \in G'\}$ becomes a group via componentwise composition:

$$(G \times G') \times (G \times G') \longrightarrow (G \times G')$$
$$(g_1, g_1') \times (g_2, g_2') \longmapsto (g_1 g_2, g_1' g_2')$$

Note $1_{G \times G'} = (1_G, 1_{G'})$

and $(g, g')^{-1} = (g^{-1}, (g')^{-1})$

(67) EXAMPLES: Let's compute orders in $\underbrace{(\mathbb{Z}/3\mathbb{Z})^\times}_{\{\bar 1,\bar 2\}} \times \underbrace{(\mathbb{Z}/5\mathbb{Z})^\times}_{\{\bar 1,\bar 2,\bar 3,\bar 4\}}$:

$(\bar a, \bar b)$	$\mathrm{ord}(\bar a,\bar b)$
$(\bar 1,\bar 1)$	1
$(\bar 1,\bar 2)$	4
$(\bar 1,\bar 3)$	4
$(\bar 1,\bar 4)$	2
$(\bar 2,\bar 1)$	2
$(\bar 2,\bar 2)$	4
$(\bar 2,\bar 3)$	4
$(\overline{-1},\overline{-1}) = (\bar 2,\bar 4)$	2

Looks similar to $(\mathbb{Z}/15\mathbb{Z})^\times$! Not a coincidence...

3rd century AD.?

Sun Ze's Theorem ("Chinese Remainder Thm")
(PROP 2.11.3 + more)

Given m,n $\boxed{\text{with } \gcd(m,n)=1,}$ the map

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{f} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
$$\underset{(\mathrm{mod}\ mn)}{\bar a} \longmapsto (\underset{(\mathrm{mod}\ m)}{\bar a}, \underset{(\mathrm{mod}\ n)}{\bar a})$$

is well-defined, a bijection, and respects both + and ×, so that it gives group isomorphisms

$$(\mathbb{Z}/mn\mathbb{Z})^+ \cong (\mathbb{Z}/m\mathbb{Z})^+ \times (\mathbb{Z}/n\mathbb{Z})^+$$
$$\text{and } (\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

10/12/2018 > proof: Well-defined-ness of f comes from $\bar a = \bar a'$ in $\mathbb{Z}/mn\mathbb{Z}$
$\Rightarrow a - a' \in mn\mathbb{Z}$
$\Rightarrow a - a' \in m\mathbb{Z}, n\mathbb{Z}$
$\Rightarrow \bar a = \bar a'$ in $\mathbb{Z}/m\mathbb{Z}$
$\bar a = \bar a'$ in $\mathbb{Z}/n\mathbb{Z}$

Respecting +, × comes from their componentwise def'n on right.
Bijectivity of f comes from an explicit inverse map g, that comes from picking any $x, y \in \mathbb{Z}$ with $xm + yn = 1$ (since $\gcd(m,n)=1$).