2) Suppose $n=pq$, $p<q$ prime and $p \nmid q-1$. Then there is a non-Abel. group of order n.

Pf: Let $K = C_p = \langle x \rangle$, $H = C_q$.

$\mathrm{Aut}(H) \cong (\mathbb{Z}/q\mathbb{Z})^\times \cong C_{q-1}$ (prim. root thm, since q is prime)

Since $p \mid q-1$, $\mathrm{Aut}(H)$ has an element ψ of order p.

Let $\varphi: K \to \mathrm{Aut}(H)$ be the hom determined by $\varphi(x) = \psi$.

Since φ is not the identity, $H \times_\varphi K$ is a non-Abelian group of order pq.

Def: If $H \leq G$, a <u>complementary subgroup</u> is a subgroup $K \leq G$ with $HK = G$ and $H \cap K = \{e\}$.

Recognition Theorem: If H and K are complementary subgroups of G, and if $H \trianglelefteq G$, then $G \cong H \times_\varphi K$ with $\varphi: K \to \mathrm{Aut}(H)$ defined by $k \mapsto (h \mapsto khk^{-1})$.

Pf: The facts that $HK = G$ and $H \cap K = \{e\}$ guarantee that every element $g \in G$ has a unique rep. as $g = hk$, $h \in H, k \in K$.

(Suppose $hk = h'k'$. Then $(h')^{-1}h = k'k^{-1} \in H \cap K = \{e\}$

$\Rightarrow h' = h$ and $k' = k$.)

Define $\tau: G \to H \rtimes_\varphi K$ by $\tau(hk) = (h,k)$.

This map is bijective. To see that it is a hom.:

$$\tau(hkh'k') = \tau\big((hkh'k^{-1})kk'\big) = (h(khk^{-1}), kk')$$

($khk^{-1} = \varphi_k(h')$)

$$= (h,k)(h',k') \quad (\text{in } H \rtimes_\varphi K). \qquad \square$$

Final example:

3) Suppose $n = pq$, $p < q$ prime.

i) If $p \nmid q-1$ then the only group of order n, up to isom., is C_n.

ii) If $p \mid q-1$ then there are exactly 2 groups of order n: C_n and a non-Abel. gp. of order n.

Pf: Suppose G is a group of order n. Let $H \leq G$ be a subgroup of order q, and $K \leq G$ a subgroup of order p. (These exist by Cauchy's thm.)

Then $H \trianglelefteq G$, since $|G:H| = p$ is the smallest prime dividing $|G|$, and $|H \cap K| = 1 \Rightarrow |HK| = |G| \Rightarrow HK = G$.

By the thm., $G \cong H \rtimes_\varphi K$.

What are the possible homs. $\varphi: K \to \mathrm{Aut}(H)$?

Since $|K| = p$ and $\mathrm{Aut}(H) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ is a cyclic group of order $q-1$:

i) If $p \nmid q-1$ then the only hom. $\varphi: K \to \mathrm{Aut}(H)$ is the trivial one, so $G = HK \cong H \times K$ (Abelian).

ii) If $p \mid q-1$ then since $\mathrm{Aut}(H)$ is cyclic, it has exactly one subgroup of order p, call it $\langle \psi \rangle$. The hms. $\varphi: K \to \mathrm{Aut}(H)$ (i.e. $= \langle \psi \rangle$) are determined by $\varphi(x) = \psi^k$, $0 \le k \le p-1$.

- If $k = 0$ then $HK \cong H \times K$.
- For $1 \le k \le p-1$, all of the groups $H \times_\varphi K$ are non-Abelian and are isomorphic to each other.

One more def., for homework:

If $K = \mathrm{Aut}(H)$ and $\varphi: K \to \mathrm{Aut}(H)$ be the identity map. Then $H \times_\varphi K$ is called the holomorph of H, denoted $\mathrm{Hol}(H)$.

Rings

Def: A ring is a set R together with binary operations $+$ and $\times$ satisfying:

- $(R, +)$ is an Abelian group. (0 = additive identity)
- $\times$ is associative
- $+$ and $\times$ must satisfy distributive laws:

  $\forall a, b, c \in R$,

  $$(a+b)\times c = (a\times c) + (b\times c)$$

  and $$a\times(b+c) = (a\times b) + (a\times c).$$