Let H be a subgroup of G and fix $g \in G$, then $H \cong gHg^{-1}$.

Proof: Letting ϕ_g denote conjugation by g, we have for $h_1, h_2 \in H$ that

$$\phi(h_1h_2) = gh_1h_2g^{-1} = gh_1(gg^{-1})h_2g^{-1} = \phi(h_1)\phi(h_2),$$

thus ϕ_g is a homomorphism. If $x \in gHg^{-1}$, then $x = ghg^{-1}$ for some $h \in H$, and thus is mapped to by h, showing that ϕ_g is surjective. Finally, suppose $\phi(h_1) = \phi(h_2)$, then

$$gh_1g^{-1} = gh_2g^{-1} \implies (g^{-1}g)h_1(g^{-1}g) = (g^{-1}g)h_2(g^{-1}g) \implies h_1 = h_2,$$

thus showing that ϕ_g is injective, which proves $H \cong gHg^{-1}$. ■

4.4 Automorphisms

1) Given a group G, let $\sigma \in \mathrm{Aut}(G)$ and denote ϕ_g as conjugation by $g \in G$, then we have that $\sigma\phi_g\sigma^{-1} = \phi_{\sigma(g)}$. As a corollary, $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Proof: Fixing $h \in G$, we see that

$$(\sigma\phi_g\sigma^{-1})(h) = \sigma(\phi_g(\sigma^{-1}(h))) = \sigma(g\sigma^{-1}(h)g^{-1}),$$

and because σ is an automorphism,

$$\sigma(g\sigma^{-1}(h)g^{-1}) = \sigma(g)\sigma(\sigma^{-1}(h))\sigma(g^{-1}) = \sigma(g)h\sigma(g)^{-1} = \phi_{\sigma(g)}(h),$$

thus $\sigma\phi_g\sigma^{-1} = \phi_{\sigma(g)}$. Since $\phi_{\sigma(g)} \in \mathrm{Inn}(G)$, we have that $\sigma\phi_g\sigma^{-1} \in \mathrm{Inn}(G)$ for every $\sigma \in \mathrm{Aut}(G)$, thus $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. ■

2) If G is an abelian group of order pq where p and q are distinct primes, then G is cyclic.

Proof: Since p and q are distinct, we can assume $p < q$ without loss of generality. By Cauchy's theorem, there exist elements $x, y \in G$ with orders p and q respectively. Clearly $|xy| \neq 1$, else the order of x or y would be 1. We can also see that $|xy| \neq p$, else we would have that

$$e = (xy)^p = x^py^p = y^p,$$

which is impossible since $|y| = q > p$. Finally, $|xy| \neq q$, since if we did we would have

$$e = (xy)^q = x^q y^q = x^q,$$

and because $p \nmid q$, we have that $q = pn + r$ for some $n, r \in \mathbb{Z}$ and $0 < r < p$, thus

$$e = x^q = x^{pn+r} = (x^p)^n x^r = x^r,$$

which violates $|x| = p > r$. Thus, our only choice for the order of xy is pq, which shows that G is cyclic. $\blacksquare$

15) In $(\mathbb{Z}/5\mathbb{Z})^\times$, we have $\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{3}, \bar{1}\} = (\mathbb{Z}/5\mathbb{Z})^\times$, thus $\mathbb{Z}/5\mathbb{Z}$ is cyclic.

In $(\mathbb{Z}/9\mathbb{Z})^\times$, we have $\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{8}, \bar{7}, \bar{5}, \bar{1}\} = (\mathbb{Z}/9\mathbb{Z})^\times$, thus $\mathbb{Z}/9\mathbb{Z}$ is cyclic.

4.5 Sylow's Theorem

3) If G is a group and p a prime that divides the order of G, then there exists an element $x \in G$ of order p.

Proof: Fix a group G with order $p^\alpha m$, where p is prime, $\alpha \geq 1$, and $p \nmid m$. By Sylow's theorem, there exists a subgroup H of G with order p^α. Let $x \in H$ where $x \neq e$. Since $|x|$ divides p^α, we have that $|x| = p^n$ for some $1 \leq n \leq \alpha$. Consider the element $y = x^{p^{n-1}}$. Because $p^{n-1} < p^n$, we have that $y \neq e$. We can see that

$$y^p = \left(x^{p^{n-1}}\right)^p = x^{p^{n-1}p} = x^{p^n} = e,$$

thus $|y| \leq p$. Since no integer $2 \leq k < p$ divides p^α, we must have that $|y| = p$, thus proving Cauchy's theorem. $\blacksquare$

7) The Sylow 2-subgroups of S_4 are given by

$$H_1 = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$$

$$H_2 = \{e, (1\ 3), (2\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4), (1\ 4\ 3\ 2), (1\ 2\ 3\ 4)\}$$

$$H_3 = \{e, (1\ 4), (2\ 3), (1\ 4)(2\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2)\}$$

We have that $H_1 = (2\ 3)H_2(2\ 3)^{-1} = (2\ 4)H_3(2\ 4)^{-1}$, $H_2 = (2\ 3)H_1(2\ 3)^{-1} = (3\ 4)H_3(3\ 4)^{-1}$, and $H_3 = (2\ 4)H_1(2\ 4)^{-1} = (3\ 4)H_2(3\ 4)^{-1}$.

13) If G is a group with order 56, then there exists a normal Sylow p-subgroup where p is a prime divisor of $|G|$.

Proof: The prime factorization of 56 is $2^3 \cdot 7$. We know that $n_7 \equiv 1 \pmod{7}$ and that $n_7 \mid 2^3$, thus the possible options for n_7 are 1 and 8. If $n_7 = 8$, then there are 8 Sylow 7-subgroups, each having 6 elements of order 7 that are unique to that group, plus the identity element. This means that there can be only one Sylow 2-subgroup, since such a group would have 7 non-identity elements whose orders are powers of two. Since $8 \cdot 6 + 7 + 1 = 56$, we have accounted for all elements in G and thus know that $n_2 = 1$, proving that G has a normal Sylow 2-subgroup. Otherwise, $n_7 = 1$, and G has a normal Sylow 7-subgroup, completing the proof. ■

23) No group G of order 462 is simple.

Proof: The prime factorization of 462 is $2 \cdot 3 \cdot 7 \cdot 11$. We have that $n_{11} \equiv 1 \pmod{11}$ and that $n_{11} \mid 42$, thus the possible values for n_{11} are $1, 12, 23, 34, 45, \ldots$, but the only one of these that divides 42 is 1, showing that G has a normal Sylow 11-subgroup, and thus is not simple. ■

26) If a group G of order 105 has a normal Sylow 3-subgroup, then it is abelian.

Proof: -