Homework #7, due 10/14/09 = **3.2.4**, **3.2.8**, **3.3.3**, **3.3.7**

3.2.4 Show that if $|G| = pq$ for some primes p and q (not necessarily distinct), then either G is abelian or $Z(G) = 1$.

First we recall the solution to problem **3.1.36**, that if $G/Z(G)$ is cyclic then G is abelian.

Assume $G/Z(G)$ is cyclic with generator $xZ(G)$. Let $g_1, g_2 \in G$. Then $g_1 \in g_1Z(G) = (xZ(G))^{a_1} = x^{a_1}Z(G)$ for some $a_1 \in \mathbb{Z}$, so there is some $z_1 \in Z(G)$ such that $g_1 = x^{a_1}z_1$. Similarly, there are $a_2 \in \mathbb{Z}$ and $z_2 \in Z(G)$ such that $g_2 = x^{a_2}z_2$. Then

$$\begin{aligned}
g_1g_2 &= x^{a_1}z_1x^{a_2}z_2 \\
&= x^{a_1}x^{a_2}z_1z_2 && \text{since } z_1 \in Z(G) \\
&= x^{a_1+a_2}z_2z_1 && \text{since } z_1 \in Z(G) \\
&= x^{a_2}x^{a_1}z_2z_1 \\
&= x^{a_2}z_2x^{a_1}z_1 && \text{since } z_2 \in Z(G) \\
&= g_2g_1
\end{aligned}$$

Since the center $Z(G)$ is a subgroup of G, the order of $Z(G)$ must be either 1, or p, or q, or pq. If the order of $Z(G)$ is 1 then $Z(G)$ has only one element, which must be the identity element of G, so $Z(G) = 1$ and we're done. If the order of $Z(G)$ is pq, then $Z(G)$ is a finite subset of the finite set G of the same cardinality, so $G = Z(G)$, which implies that G is abelian and again we're done. So assume that the order of $Z(G)$ is either p or q, that is, $1 < Z(G) < G$.

Let's suppose that the order of $Z(G)$ is q. Since $Z(G)$ is a *normal* subgroup of G, we have a quotient group $G/Z(G)$ whose order is $|G : Z(G)| = pq/q = p$, a prime. There is (up to isomorphism) exactly one group of prime order p, and that is the cyclic group $\mathbb{Z}_p$ of order p. Therefore $G/Z(G) \cong \mathbb{Z}_p$. Since $G/Z(G)$ is cyclic, it follows from problem **3.1.36** that G is abelian.

3.2.8 Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.

First of all, the intersection of any two subgroups is a subgroup, and 1 is in every subgroup, so we have $1 \in H \cap K$.

Let $g \in H \cap K$. Then $|g|$ divides both $|H|$ and $|K|$, but by hypothesis $(|H|, |K|) = 1$, that is, $|H|$ and $|K|$ have no common divisors other than 1, so $|g| = 1$, hence $g = 1$. (The only element of a group that has order 1 is the identity element of the group.)

3.3.3 Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either (i) $K \leq H$ or (ii) $G = HK$ and $|K : K \cap H| = p$.

Since H is a normal subgroup we have a quotient group G/H whose order $|G : H|$ is the prime number p. Let K be an arbitrary subgroup of G. Then, since H is normal, HK is a subgroup of G by **3.2, Cor. 15**. Since $1 \in K$ we have $H \subseteq H1 \subseteq HK$, so H is a subgroup of HK. Then $p = |G : H| = |G : HK||HK : H|$, but p is prime, so either $p = |G : HK|$ and $1 = |HK : H|$, or else $1 = |G : HK|$ and $p = |HK : H|$. In the first case we get $HK = H$ (hence $K \subseteq H$ and we're done) from $1 = |HK : H|$. So assume we are in the second case. We get $G = HK$ from $1 = |G : HK|$. By the Second Isomorphism Theorem, $HK/H \cong K/H \cap K$, but we know $p = |HK : H|$ so we have $p = |HK/H| = |K/H \cap K| = |K : H \cap K|$.

3.3.7 Let M and N be normal subgroups of G such that $G = MN$. Prove that $G/(M \cap N) \cong (G/M) \times (G/N)$.

By the Second Isomorphism Theorem, we have $MN/M \cong N/(M \cap N)$ and $MN/N \cong M/(M \cap N)$, so

$$(G/M) \times (G/N) = (MN/M) \times (MN/N) \cong N/(M \cap N) \times M/(M \cap N).$$

To complete the proof it will therefore be enough to find an isomorphism from $N/(M \cap N) \times M/(M \cap N)$ to $G/(M \cap N)$. Define φ on $N/(M \cap N) \times M/(M \cap N)$ by $\varphi(X, Y) = XY$ for all $(X, Y) \in N/(M \cap N) \times M/(M \cap N)$. Then φ is a homomorphism because, for all $n_1, n_2 \in N$ and all $m_1, m_2 \in M$, we have

$$\begin{aligned}
&\varphi((n_1(M \cap N), m_1(M \cap N))\varphi((n_2(M \cap N), m_2(M \cap N))) && \\
&= n_1(M \cap N)m_1(M \cap N)n_2(M \cap N)m_2(M \cap N) && \text{def. of } \varphi \\
&= n_1(M \cap N)(m_1Mn_2 \cap m_1Nn_2)(M \cap N)m_2(M \cap N) && \text{dist} \\
&= n_1(M \cap N)(Mn_2 \cap m_1N)(M \cap N)m_2(M \cap N) && m_1 \in M \leq G,\ n_2 \in N \leq G \\
&= n_1(M \cap N)(n_2M \cap Nm_1)(M \cap N)m_2(M \cap N) && M \lhd G,\ N \lhd G \\
&= n_1(M \cap N)(n_2Mm_1 \cap n_2Nm_1)(M \cap N)m_2(M \cap N) && m_1 \in M \leq G,\ n_2 \in N \leq G \\
&= n_1(M \cap N)n_2(M \cap N)m_1(M \cap N)m_2(M \cap N) && \text{distribution (see below)} \\
&= \varphi((n_1(M \cap N), n_2(M \cap N)))\varphi((m_1(M \cap N), m_2(M \cap N))) && \text{def. of } \varphi
\end{aligned}$$

We used here the distribution principles proved in class, namely, for any subsets $X, Y \subseteq G$ of a group G, and any element $a \in G$, we have $(X \cap Y)a = Xa \cap Ya$ and $a(X \cap Y) = aX \cap aY$.