Homework #10, due 11/11/09 = **5.1.10**, **5.1.18**, **5.4.1**, **5.4.2**, **5.4.3**

5.1.10 Let p be a prime. Let A and B be two cyclic groups of order p with generators x and y, respectively. Set $E = A \times B$ so that E is the elementary abelian group of order p^2: E_{p^2}. Prove that the distinct subgroups of E of order p are $\langle x\rangle$, $\langle xy\rangle$, $\langle xy^2\rangle$, ..., $\langle xy^{p-1}\rangle$, $\langle y\rangle$. (Note that there are $p+1$ of them.)

Identify the group A with the subgroup $A \times 1$, and identify the group B with the subgroup $1 \times B$. By this identification and the hypotheses, we have $\langle x\rangle = A = A \times 1$, $\langle y\rangle = B = 1 \times B$, and $|x| = |y| = |A \times 1| = |1 \times B| = p$. Then $\langle x\rangle$ and $\langle y\rangle$ are distinct subgroups of E of order p. We must show that $\langle xy\rangle$, $\langle xy^2\rangle$, ..., $\langle xy^{p-1}\rangle$ are also subgroups of order p, and that there are no other subgroups of order p.

Consider the subgroup $\langle xy^k\rangle$ generated by $z = xy^k$, where $0 \le k \le p-1$. We compute the order of z. Let $n \in \mathbb{Z}^+$ and suppose $z^n = 1$. This means that $1 = (xy^k)^n$, so $1 = x^n y^{kn}$ since E is abelian. Then $x^{-n} = y^{kn} \in \langle x\rangle \cap \langle y\rangle = 1$, so $x^{-n} = 1 = y^{kn}$. Since $|x| = |y| = p$, this tells us that $p| - n$, so $p|n$. On the other hand, $(xy^k)^p = x^p y^{kp} = 1(y^p)^k = 1^k = 1$. Thus the order of xy^k is p.

To prove that the groups $\langle x\rangle$, $\langle xy\rangle$, $\langle xy^2\rangle$, ..., $\langle xy^{p-1}\rangle$, $\langle y\rangle$ are all distinct from each other, it is enough to show that no generator of one of these groups is in another one of these groups. Let us assume otherwise, say $xy^k \in \langle xy^l\rangle$ with $0 \le k, l \le p-1$ and $\langle xy^k\rangle \ne \langle xy^l\rangle$. Then there is some m such that $xy^k = (xy^l)^m$, hence, since E is abelian, $x^{1-m} = y^{lm-k}$. But this element must belong to both $\langle x\rangle$ and $\langle y\rangle$, and hence $x^{1-m} = 1 = y^{lm-k}$. From the first of these two equations we know p divides $1-m$, and from the second we know p divides $lm-k$. But $lm - k = l(m-1) + l - k$, so p must also divide $l-k$. However, we assumed $0 \le k, l \le p-1$, so the fact that p divides $l-k$ implies that $l = k$. This contradicts our assumption $\langle xy^k\rangle \ne \langle xy^l\rangle$.

If H is any subgroup of E that has order p, then H is isomorphic to $\mathbb{Z}_p$ and is generated by a single element z of E. We have found $p+1$ subgroups of E, each of order p, each isomorphic to $\mathbb{Z}_p$. The intersection of any two of them is the trivial subgroup 1. Hence the number of elements of E that fall into the union of these subgroups is $1 + (p+1)(p-1) = p^2$. But $p^2 = |E|$, so the union of these subgroups is all of E. Therefore z belongs to one of the subgroups, say $\langle xy^k\rangle$, which implies that H is a subgroup of $\langle xy^k\rangle$, but both H and $\langle xy^k\rangle$ have the same order, so they are equal. Thus the list of $p+1$ subgroups of order p is complete.

5.1.18 In each of (a)–(e) give an example of a group with the specified properties.

(a) an infinite group in which every element has order 1 or 2: $\mathbb{Z}_2^\omega$ (the countable direct power of the 2-element cyclic group $\mathbb{Z}_2$)

(b) an infinite group in which every element has finite order but for each positive integer n there is an element of order n. Use the subgroup of $\prod_{n=1}^{\omega} \mathbb{Z}_n$ which is generated by the elements of $\prod_{n=1}^{\omega} \mathbb{Z}_n$ that are non-zero in only finitely many places.

(c) a group with an element of infinite order and an element of order 2: $\mathbb{Z} \times \mathbb{Z}_2$

(d) a group G such that every finite group is isomorphic to some subgroup of G: let S be the set of finite groups whose underlying set is a subset of $\mathbb{Z}$. Then S is a countable set, and the direct product of all the groups in S is a group which has copy of every group in S as a normal subgroup. But every finite group is isomorphic to some group in S.

(e) a nontrivial group G such that $G \cong G \times G$: Let G be $\mathbb{Z}_2^\omega$.

5.4.1 Prove that if $x, y \in G$ then $[y, x] = [x, y]^{-1}$. Deduce that for any subsets A and B of G, $[A, B] = [B, A]$ (where $[A, B]$ is the subgroup generated by the commutators $[a, b]$, $a \in A$, $b \in B$).

First, we have

$$\begin{aligned}[y,x] &= y^{-1}x^{-1}yx \\ &= y^{-1}x^{-1}(y^{-1})^{-1}(x^{-1})^{-1} \\ &= (x^{-1}y^{-1}xy)^{-1} \\ &= [x,y]^{-1}\end{aligned}$$

Next we will show that all the generators of $[A, B]$ belong to $[B, A]$. Since $[A, B]$ and $[B, A]$ are both subgroups, this is enough to show $[A, B] \subseteq [B, A]$. (The opposite inclusion will also hold by the same reasoning.) Consider an arbitrary generator $[a, b]$ of $[A, B]$, where $a \in A$ and $b \in B$. Then, by the computation above, $[a, b]^{-1} = [b, a] \in [B, A]$. Now $[B, A]$ is a subgroup, so $[a, b] = ([a, b]^{-1})^{-1} \in [B, A]$.

5.4.2 Prove that a subgroup H of a group G is normal iff $[G, H] \leq H$.

Assume $H \triangleleft G$. We wish to show $[G, H]$ is a subgroup of H. Because H is a subgroup, we need only show that the generators of $[G, H]$ belong to H. Consider an arbitrary generator $g^{-1}h^{-1}gh \in [G, H]$, where $g \in G$ and $h \in H$. Then $h^{-1} \in H$ since H is a subgroup, and $g^{-1}h^{-1}g \in H$ since H is a normal subgroup and $g^{-1}h^{-1}g$ is the conjugate of $h^{-1} \in H$ by g^{-1}. From $g^{-1}h^{-1}g \in H$ and $h \in H$ we get $g^{-1}h^{-1}gh \in H$ since H is a subgroup.

Assume $[G, H] \leq H$. To show H is normal, we assume $h \in H$, $g \in G$, and will show $ghg^{-1} \in H$. First we note that $g^{-1} \in G$ and $h^{-1} \in H$, hence $[g^{-1}, h^{-1}] \subseteq [G, H] \leq H$, which implies $(g^{-1})^{-1}(h^{-1})^{-1}g^{-1}h^{-1} \in H$, hence $ghg^{-1}h^{-1} \in H$. But $h \in H$, so $ghg^{-1} = ghg^{-1}(h^{-1}h) = (ghg^{-1}h^{-1})h \in H$, as desired.

5.4.3 Let $a, b, c \in G$. Prove that **(a)** $[a, bc] = [a, c](c^{-1}[a, b]c)$ **(b)** $[ab, c] = (b^{-1}[a, c]b)[b, c]$

$$\begin{aligned}[a,c](c^{-1}[a,b]c) &= (a^{-1}c^{-1}ac)(c^{-1}(a^{-1}b^{-1}ab)c) \\ &= a^{-1}c^{-1}(a(cc^{-1})a^{-1})b^{-1}abc \\ &= a^{-1}c^{-1}(aa^{-1})b^{-1}abc \\ &= a^{-1}c^{-1}b^{-1}abc \\ &= a^{-1}(bc)^{-1}a(bc) \\ &= [a,bc]\end{aligned}$$

$$\begin{aligned}(b^{-1}[a,c]b)[b,c] &= (b^{-1}(a^{-1}c^{-1}ac)b)(b^{-1}c^{-1}bc) \\ &= b^{-1}a^{-1}c^{-1}a(c(bb^{-1})c^{-1})bc \\ &= b^{-1}a^{-1}c^{-1}a(cc^{-1})bc \\ &= b^{-1}a^{-1}c^{-1}abc \\ &= (ab)^{-1}c^{-1}(ab)c \\ &= [ab,c]\end{aligned}$$