10. POWER AUTOMORPHISMS

§10.1. Definition and Examples

This section is based on work I did in the late 1960s. A **power automorphism** of a group G is an automorphism that maps every subgroup of G *onto* itself.

Under such an automorphism every element is mapped to some power, though not necessarily the same power for each element.

We denote the group of power automorphisms of G by $\mathcal{P}$**(G).**

Power automorphisms are relevant to the study of the auto-projectivities (automorphisms of the lattice of subgroups). The power automorphisms are precisely those group automorphisms that induce the trivial auto-projectivity in the lattice of subgroups. The group of auto-projectivities of G is thus isomorphic to Aut(G)/$\mathcal{P}$(G).

Theorem 1: If G is generated by elements of order 2 then $\mathcal{P}(G) \cong \mathbf{1}$.

Proof: If g has order 2 and θ is a power automorphism then $g^\theta \in \langle g \rangle$, and since $1^\theta = 1$, $g^\theta = g$. So power automorphisms fix elements of order 2 and so, if G is generated by them, the only power automorphism is the identity function.

Example 1: Since dihedral groups are generated by elements of order 2, $\mathcal{P}(\mathbf{D}_{2n}) \cong \mathbf{1}$ for all n.

Example 2: $\mathcal{P}(\mathbf{C}_n) \cong \mathbb{Z}_n^{\#}$. The power automorphisms are the maps $x \to x^n$ for n coprime to n.

We can identify $\mathcal{P}(\mathbf{C}_n)$ as a direct product of cyclic groups by using the following facts:

(1) $\mathbb{Z}_{mn}^{\#} \cong \mathbb{Z}_n^{\#} \times \mathbb{Z}_n^{\#}$ if m, n are coprime,

(2) $\mathbb{Z}_{p^n}^{\#} \cong \mathbf{C}_{p^{n-1}} \times \mathbf{C}_{p-1}$ if p is odd,

(3) $\mathbb{Z}_{2^n}^{\#} \cong \mathbf{C}_{2^{n-2}} \times \mathbf{C}_2$ if $n \geq 3$,

(3) $\mathbb{Z}_4^{\#} \cong \mathbf{C}_2$.

[See my notes on *Number Theory*, Chapter 6]

Example 3:

$\mathcal{P}(\mathbf{C}_{2000}) \cong \mathbb{Z}_{2000}^{\#} \cong \mathbb{Z}_{16}^{\#} \times \mathbb{Z}_{125}^{\#} \cong \mathbf{C}_4 \times \mathbf{C}_2 \times \mathbf{C}_{25} \times \mathbf{C}_4$.

Theorem 2: If $\theta \in \mathcal{P}(G)$ and $g \in G$ has infinite order then

$$g^{\theta} = g^{\pm 1}.$$

Proof: Suppose $g^{\theta} = g^{n}$ and $g^{\theta^{-1}} = g^{m}$.
Then $(g^{\theta})^{\theta^{-1}} = (g^{n})^{\theta^{-1}} = g^{mn}$.
But this is just g and so $g^{mn-1} = 1$.
Since g has infinite order we must have $mn = 1$.

If $\theta \in \mathrm{Aut}(G)$ and $g \in G$ then $[g, \theta]$ denotes $g^{-1}g^{\theta}$.

Theorem 3: If $\theta \in \mathcal{P}(G)$ and $g \in G$ then the inner automorphism generated by $[g, \theta]$ is in $\mathcal{P}(G)$.
Proof: Let $H \leq G$ and $g \in G$.
Then $(H^{g})^{\theta} = H^{g} = H^{(g^{\theta})}$ whence $H^{[g,\theta]} = H$.

§10.2. Homogeneous and Universal Power Automorphisms

A **homogeneous power automorphism**, θ, is one where for all $m \in \mathbb{Z}$ there exists $n \in \mathbb{Z}$ such that if $|x| = m$ then $x^{\theta} = x^{n}$. In other words, under a homogeneous power automorphism elements of the same order map to the same power. We denote the set of homogeneous power automorphisms of G by $\mathcal{H}(G)$.

If $n \in \mathbb{Z}$, we denote the map $g \to g^{n}$ by θ_n. If θ_n is an automorphism of G and $\theta_n^{-1} = \theta_m$ for some m then we call θ_n a **universal power automorphism** for G. We

denote the set of universal power automorphisms for G by $\mathcal{U}(G)$.

You may be wondering why the definition of universal power automorphisms refers to inverses while those for power automorphisms did not. You'll find out soon.

Theorem 4: $\mathcal{U}(G) \leq \mathcal{K}(G) \leq \mathcal{P}(G) \leq \text{Aut}(G)$ and all are normal subgroups of Aut(G).

Proof: It's obvious that $\mathcal{U}(G) \subseteq \mathcal{K}(G) \subseteq \mathcal{P}(G) \subseteq \text{Aut}(G)$. Moreover it's easy to show that all these sets are closed under composition, or multiplication of functions. We need to be careful when it comes to inverses.

The inverse of a power automorphism is a power automorphism because we insist that power automorphisms map every subgroup *onto* itself.

If $\theta \in \mathcal{K}(G)$, then for all $g, h \in G$ with the same order m, there exists $n \in \mathbb{Z}$ such that $g^\theta = g^n$ and $h^\theta = h^n$. Now GCD(m, n) = 1, so $mh + nk = 1$ for integers h, k.

Now $(g^n)^{\theta^{-1}} = g = g^{mh + nk} = g^{nk}$.

Hence $g^{\theta^{-1}} = ((g^n)^{\theta^{-1}})^k = g^k$.

Similarly $h^{\theta^{-1}} = g^k$ and so $\theta^{-1} \in \mathcal{K}(G)$.

So $\mathcal{U}(G)$, $\mathcal{K}(G)$ and $\mathcal{P}(G)$ are all subgroups of Aut(G). The fact that they are all normal in Aut(G) will be left as an exercise.

In a later section we will discuss power automorphisms of the Prüfer *p*-groups. Here there automorphisms of the form θ_n where θ_n^{-1} is homogeneous but not universal.

Theorem 5: $\mathcal{H}(G) \leq Z(\text{Aut}(G))$.
Proof: Let $\theta \in \text{Aut}(G)$ and suppose that $\sigma \in \mathcal{U}(G)$.
Let $g \in G$. Then $|g^\theta| = |g|$ and so there exists an integer n such that $g^\sigma = g^n$ and $(g^\theta)^\sigma = (g^\theta)^n$.
Then $g^{\theta\sigma} = (g^\theta)^\sigma = (g^\theta)^n = (g^n)^\theta = g^{\sigma\theta}$.

Example 4: $\text{Aut}(\mathbf{Q}_8) \cong \mathbf{S}_4$, as shown in Example 5 of Chapter 9.
$\mathbf{Q}_8 = \langle A, B \mid A^4, B^2 = A^2, BA = A^{-1}B\rangle$.
If α is the map that sends $A \to A^{-1}$, $B \to B$ and
β is the map that sends $A \to A$, $B \to B^{-1}$ then
$\mathcal{P}(\mathbf{Q}_8) = \langle \alpha, \beta \mid \alpha^2, \beta^2, \beta\alpha = \alpha\beta\rangle \cong \mathbf{V}_4$.
$\mathcal{H}(\mathbf{Q}_8) = \mathcal{U}(\mathbf{Q}_8) = \langle \alpha\beta\rangle \cong \mathbf{C}_2$.

§10.3. Power Automorphisms of Abelian Groups

Theorem 6: If G is a non-periodic abelian group then $\mathcal{P}(G) = \mathcal{H}(G) = \mathcal{U}(G) \cong \mathbf{C}_2$, consisting of 1 and θ_{-1}.
Proof: Let $x \in G$ with infinite order and let $y \in G$.
Let $\theta \in \mathcal{P}(G)$. Then $x^\theta = x^n$ where $n = \pm 1$.
Let $y^\theta = y^m$ and $(xy)^\theta = (xy)^t$.
Suppose that $x^\theta = x$.

Case I: y has infinite order and $y^\theta = y^{-1}$:
Then $(xy)^\theta = xy^{-1} = (xy)^t$.
In that case $x^{1-t} = y^{1+t}$.
Applying θ to both sides $x^{1-t} = y^{-(1+t)}$ and so $y^{2(1+t)} = 1$.
Since y has infinite order we would have $t = -1$. But then $x^{1-t} = 1$ which gives $t = 1$, a contradiction.
Case II: y has finite order:
Then $(xy)^\theta = xy^m = (xy)^t$.
Then $x^{t-1} = y^{m-t}$.
Since y^{m-t} has finite order, $t = 1$ and so $y^\theta = y$.

So for all $y \in G$, $y^\theta = y$ and hence $\theta = 1$.

Suppose that $x^\theta = x^{-1}$.
Now $\theta_{-1} \in \mathcal{P}(G)$ and hence so is $\theta\theta_{-1}$. But $\theta\theta_{-1}$ fixes x and so by the above, $\theta\theta_{-1} = 1$, and so$\theta = \theta_{-1}$.

Theorem 7: Let G be a finite abelian p-group of exponent p^n. Then $\mathcal{P}(G) = \mathcal{H}(G) = \mathcal{U}(G) \cong \mathbb{Z}_{p^{n^\#}}$.
Proof: G is a direct product of its Sylow p-subgroups.
Let $a \in G$ of order p^n. Then $G = \langle a \rangle \times B$ for some B.
Let $\theta \in \mathcal{P}(G)$ and suppose that $a^\theta = a^r$. Let $b \in B$.
Then $b^\theta = b^k$ for some k.
Then $(ab)^\theta = a^r b^k = (ab)^t$ for some t.
Hence $a^{r-t} = b^{t-k}$. Since $\langle a \rangle$, B are disjoint, $a^{r-t} = b^{t-k} = 1$.
$\therefore\ b^t = b^k$ and $p^n \mid r - t$. Since $|b|$ divides p^n, $b^k = b^t = b^r$.
Hence $\theta = \theta_r$.

Theorem 8: For all finite abelian groups G, $\mathcal{P}(G) = \mathcal{U}(G)$.
Proof: For each prime p, let G_p denote the Sylow p-subgroup of G and suppose that the exponent of G_p is m_p. Let $\theta \in \mathcal{P}(G)$. Then θ restricted to G_p is a power automorphism of the form $x \to x^{n_p}$. By the Chinese Remainder Theorem (see my notes on *Number Theory*), there exists N such that $N \equiv n_p \pmod{m_p}$ for each prime p dividing |G|.

§10.4. Automorphisms of the Prüfer Groups

In Chapter 7 we discussed the Prüfer p-groups.

$$\mathbb{Z}_{p^\infty} = \langle A_1, A_2, \ldots \mid A_1^p, A_2^p = A_1, A_3^p = A_2, \ldots \rangle.$$

This is an infinite abelian group, but although the commuting relations are missing they can be deduced from the power relations.

The elements have the form A_i^k with $0 \le k < p$. It is **locally cyclic** meaning that any finite subset is contained in a cyclic subgroup. For if $X = A_i^k$ and $Y = A_j^h$, with $i \le j$ then $A_i = A_j^{p^{j-i}}$ and so [X, Y] = 1. In fact the only subgroups are 1, $\langle A_1 \rangle$, $\langle A_2 \rangle$, …, $\langle A_i \rangle$, …, $\mathbb{Z}_{p^\infty}$. Since no two of these are isomorphic, every automorphism of $\mathbb{Z}_{p^\infty}$ must fix every subgroup. Hence $\mathrm{Aut}(\mathbb{Z}_{p^\infty}) = \mathcal{P}(\mathbb{Z}_{p^\infty})$.

Let $\alpha = (k_1, k_2, \ldots)$ be an infinite sequence where for each i, $0 \le k_i < p$ and $k_1 > 0$. Define $\theta_\alpha: \mathbb{Z}_{p^\infty} \to \mathbb{Z}_{p^\infty}$ to

be the automorphism induced by mapping each A_h to A_h^N where $N = k_1 + pk_2 + p^2k_2\ldots + p^{h-1}k_h$.

This is well-defined because $A_h^p = A_{h-1}$ and, under θ_α, $A_h \rightarrow A_h^N$ and so $A_h^p \rightarrow A_h^{pN} = A_{h-1}{}^N = A_{h-1}{}^M$ where $M = k_1 + pk_2 + p^2k_2\ldots + p^{h-2}k_{h-1}$ since $|A_{h-1}| = p^{h-1}$.

It is easy to check that θ_α is a power homomorphism. Moreover it is clearly a homogeneous power homomorphism. But unless there exists K such that $k_n = 0$ for all $n \geq K$, θ_α is not a universal power homomorphism.

The expressions of the form α are usually written as formal series as $\sum_{n=1}^{\infty} k_1 p^{n-1}$ where for each n, $0 \leq k_n < p$. These can be made into a ring called the ring of p-adic integers and $\mathrm{Aut}(\mathbb{Z}_{p^\infty}) = \mathcal{P}(\mathbb{Z}_{p^\infty}) = \mathcal{H}(\mathbb{Z}_{p^\infty})$ is isomorphic to the group of units of this ring. However $\mathcal{U}(\mathbb{Z}_{p^\infty})$ is isomorphic to the group of integers that are coprime to p.

§10.5. The Centrality Theorem

I denote the image of an element g under the function θ by $\boldsymbol{g^\theta}$ and I define $\boldsymbol{g^{-\theta}}$ to be $(g^\theta)^{-1}$. I also define $\mathbf{[g, \theta]} = g^{-1}g^\theta$ and $\mathbf{[g, \theta, h]} = [[g, \theta], h]$.

Theorem 8: If θ is a power automorphism of G and $g \in G$ then the inner automorphism induced by $[g, \theta]$ is also power automorphism of G.

Proof: Let $H \leq G$ and let $g \in G$.

Then $(H^g)^\theta = H^g = H^{g^\theta}$ whence

$$H = H^{g^\theta g^{-1}} = H^{g^{-1}g^\theta} = H^{[g,\theta]}.$$

Theorem 9: If θ is a power automorphism of G and $g, h \in G$ then $[g, \theta, h][h, \theta, g] = 1$ and

$$[g, \theta, h] \in \langle g \rangle \cap \langle h \rangle.$$

Proof: Since $g^\theta h^\theta = (gh)^\theta \in \langle gh \rangle$, $g^\theta h^\theta$ commutes with gh. Hence

$$\begin{aligned}[g, \theta, h][h^{-1}, \theta, g^{-1}] &= gg^{-\theta}h^{-1}g^{-1}(g^\theta h^\theta)(gh)h^{-\theta}g^{-1} \\ &= gg^{-\theta}h^{-1}g^{-1}(gh)(g^\theta h^\theta)h^{-\theta}g^{-1} \\ &= 1.\end{aligned}$$

By Theorem 6, $[g, \theta, h] \in \langle h \rangle$ and $[h^{-1}, \theta, g] \in \langle g \rangle$. Hence for all $g, h \in G$, $[g, \theta, h] \in \langle g \rangle \cap \langle h \rangle$. Finally,

$$\begin{aligned}[h^{-1}, \theta, g^{-1}] &= [[h, \theta]^{-1}, g]^{-1} \\ &= [h, \theta, g]^{[h, \theta]^{-1}} \\ &= [h, \theta, g] \text{ since } [h, \theta, g] \in \langle h \rangle.\end{aligned}$$

An automorphism of a group G is **central** if $[\theta, g] \in Z(G)$ for all $g \in G$.

Theorem 10: If $\theta \in \mathfrak{P}(G)$ and $[g_i, \theta, h_j] = 1$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ then

$$\left[\prod_{i=1}^{n} g_i, \theta, \prod_{j=1}^{m} h_j\right] = 1.$$

Proof: By Theorem 2 we may assume that $m \geq n$.
We prove this by induction on m.
If $m = 1$ then $n = 1$ and $[g_1, \theta, h_1] = 1$ by assumption.

Suppose $m > 1$. Then

$$\left[\prod_{i=1}^{n} g_i, \theta, \prod_{j=1}^{m} h_j\right] = \left[\prod_{i=1}^{n} g_i, \theta, h_m\right]\left[\prod_{i=1}^{n} g_i, \theta, \prod_{j=1}^{m-1} h_j\right]^{h_m} = 1,$$

by the induction hypothesis.

Theorem 11: Suppose $G = \langle x, y\rangle$ is an abelian p-group, written additively, where $|x| = p^m$ and $|y| = p^n$ and where $n \le m$. Then $G = \langle x\rangle \oplus \langle ux + y\rangle$ for some u.
Proof: Choose u so that $ux + y$ has minimal order p^t. Clearly $t \le n \le m$.
Suppose $\langle ux + y\rangle \cap \langle x\rangle \neq 0$.
Then $p^{t-1}(ux + y) = p^{n-1}rx$ for some x.
Hence $p^{t-1}[(u - p^{m-t}r)x + y] = 0$, a contradiction.

The following is one of my own theorems, proved as part of my PhD thesis.

Theorem 12 (COOPER): Every power automorphism is central.
Proof: Let F be a group with a non-central power automorphism θ.
Then for some $g, h \in F$, $d = [g, \theta, h] \neq 1$.
By Theorem 9, $d \in \langle g\rangle \cap \langle h\rangle \le Z(K)$ where $K = \langle g, h\rangle$ and so $|g|$, $|h|$ are both finite or both infinite.

Suppose $|g|$, $|h|$ are both infinite.
Then $g^\theta = g^{-1}$ and $h^\theta = h^{-1}$, for if $g^\theta = g$ or $h^\theta = h$ we would obtain a contradiction by Theorem 2.

Hence $[g, \theta] = g^{-2}$ and $[h, \theta] = h^{-2}$.
By Theorem 7, $h^{[g,\theta]} = h^{-1}$, since $d \neq 1$.
Hence $[g, \theta, h] = h^2$. Similarly $[h, \theta, g] = g^2$.
By Theorem 8, $g^2h^2 = 1$ whence
$[g, \theta, h] = [g^{-2}, h] = 1$, a contradiction.

So $|g|$ and $|h|$ are both finite. By Theorem 9 we may assume that they both have prime power order. By Theorem 2 the prime must be the same, say p. in each case. Since θ is non-central on $K/\langle d^p \rangle$ we may assume that $d^p = 1$.

Let $H = \langle [g, \theta], [h, \theta] \rangle$.
We may suppose that $|[g, \theta]| \geq |[h, \theta]|$.
Now $[h, \theta] = h^r$ for some integer r.
Hence $[[g, \theta], [h, \theta]] = [g, \theta, h^r] = [g, \theta, h]^r$
$\in \langle d \rangle \leq Z(H)$.
Hence H is nilpotent of class at most 2.
Being finitely generated H is finite.

If $p = 2$ and $|h| = 2^s$, it follows that $[h^{2^{s-1}}, \theta] = 1$ whence r is even and H is abelian.
If $p > 2$ then H being nilpotent, it is a finite regular p-group.
Hence, by Theorem 6, H is verbally abelian, so
$\langle [g, \theta] \rangle \cap \langle [g, \theta]^u [h, \theta] \rangle$ for some u.
Now d and $[g, \theta]$ are both contained in $\langle g \rangle$ and so one is a power of the other.
However d commutes with h while $[g, \theta]$ does not.
Hence $d = [g, \theta]^t$ for some t.

Then if $v = u(1 - t)$,

$[g^v, h, \theta] = [g^{-ut}g^u h, \theta] = (g^u h)^{-1}[g^{-ut}, \theta](g^u h)[g^u h, \theta]$

$= d^{-u}[g^u, \theta][g^u, \theta, h][h, \theta]$

$= [g, \theta]^u[h, \theta].$

So $\langle [g, \theta] \rangle \cap \langle [g^v h, \theta] \rangle = 1$ and so either $[g, \theta] = 1$ or $[g^v h, \theta] = 1$ or $\langle g \rangle \cap \langle g^v h \rangle = 1$.

Therefore by Theorem 2 $[g, \theta, g^v h] = 1$.

But $\langle g, h \rangle = \langle g, g^v h \rangle$ and so, by Theorem 3, θ restricted to $\langle g, h \rangle$ is central, a contradiction.

Corollary 1:
Power automorphisms fix the elements of G′.

Corollary 2: Conjugates map to the same power under a power automorphism.

Proof: Suppose that $\theta \in \mathcal{P}(G)$ and that $g^\theta = g^r$.

Let $h \in G$.

Then $(h^{-1}gh)^\theta = (g\,[\,g,h])^\theta$

$= g^\theta[g, h]$

$= g^{r-1}h^{-1}gh$

$= h^{-1}g^r h$, since $g^{r-1} \in Z(G)$

$= (h^{-1}gh)^r$.

The **kern** of a group G is the intersection of all the normalisers of the subgroups of G. It is the set of elements of G that induce inner automorphisms that are power automorphisms.

Corollary 3: $K(G) \leq Z_2(G)$.

§10.6. Hamiltonian Groups

A **Dedekind group** is a group in which every subgroup is normal. In such a group every inner automorphism is a power automorphism. Clearly all abelian groups are Dedekind. A **Hamiltonian group** is defined to be a non-abelian Dedekind group.

Clearly G is Dedekind if and only if it is equal to its kern.

Let $\mathcal{K}$ be the class of Dedekind groups.
Then $\mathcal{A} \subset \mathcal{K}$. The Quaternion group $\mathbf{Q}_8$ is non-abelian and Hamiltonian.

Theorem 13: $\mathcal{K}$ is S-closed and Q-closed.
Proof: Let $G \in \mathcal{K}$ and let $H \leq G$.
If $K \leq H$ then $K \leq G$ and so K is normal in G, and hence normal in H. Hence $H \in \mathcal{K}$.
Let $H \trianglelefteq G$ and let $K/H \leq G/H$ for some K.
Since $K \leq G$, K is normal in G and hence $K/H \trianglelefteq G/H$.
Hence $G/H \in \mathcal{K}$.

Example 6: $\mathcal{K}$ is not closed under P because $\mathbf{S}_3/\mathbf{A}_3$ and $\mathbf{A}_3$ are both cyclic, and hence belong to H. Yet $\mathbf{S}_3$ is not Hamiltonian.

Theorem 14: Hamiltonian groups are class 2-nilpotent.
Proof: Suppose that G is a Hamiltonian group.
Every inner automorphism, being a power automorphism, is central.
So, if $x, y \in G$ then $x^y = xz$ for some $z \in Z(G)$.
Hence $G' \leq Z(G)$ and so $G/Z(G)$ is abelian.
This means that $Z(G/Z(G)) = G/Z(G)$ and so $Z_2(G) = G$.

Theorem 15: Hamiltonian groups are periodic.
Proof: Let $G \in \mathfrak{D} - \mathfrak{A}$. We begin by showing that elements of infinite order, if there are any, must commute. Suppose that x, y are elements of infinite order that do not commute.
Then $x^{-1}yx = y^{-1}$ and $y^{-1}xy = x^{-1}$.
Hence $[x, y] = x^{-1}(y^{-1}xy) = x^{-2}$.
But $[x, y] = (x^{-1}yx)y = y^2$ so $x^{-2} = y^2$.
It follows that y^2 commutes with x and so

$$[x, y^3] = [x, y] = 1.$$

But by the above argument this will mean that $x^{-2} = y^6$ and so $y^4 = 1$, a contradiction.

Recall that τG denotes the torsion subgroup of G. Now if $\tau G < G$, G will be generated by elements of infinite order and so will be abelian, a contradiction. Hence G is periodic.

Being a periodic nilpotent group of class 2 or less, a Hamiltonian group is the direct sum of its Sylow

subgroups, each of which will be Hamiltonian. So now we must investigate Hamiltonian p-groups.

Theorem 16: There are no Hamiltonian p-groups if p is odd.

Proof: Suppose G is a Hamiltonian p-group, where p is an odd prime. G is verbally abelian, and every power automorphism of G, including the inner ones, is a power automorphism of G_*, the corresponding abelian group.

Let g, h be two non-commuting elements of G and let $H = \langle g, h \rangle$ and suppose that $|h|$ divides $|g|$.

Let θ be the power automorphism of G_* induced by conjugation by g in G. Then θ restricted to H is a power automorphism of H and hence it has the form $x \to x^n$ for some n. So $g = g^n$ and $g^{-1}hg = h^n$.

Since $|g|$ divides $n - 1$, $|h|$ divides $n - 1$ and so $h^n = h$, a contradiction.

Theorem 17:

Suppose $G = \langle a, b \rangle$ is a nilpotent 2-group of class 2 where $\langle a \rangle$ is normal in G, $|a| \geq |b|$ and $\langle a \rangle \cap \langle b \rangle > 1$.

Then $G \cong \mathbf{Q}_8$.

Proof: Let $|a| = 2^n$ and $|b| = 2^m$ where $n \geq m$.

Let $|G:\langle a \rangle| = 2^t$. Then $t < m \leq n$.

Now $[b, a] = a^{2^r k}$ for some odd k and some r.

Since G is non-abelian, $r \geq 1$.

Now $b^{2^t} = a^{s2^q}$ for some odd s and some q.

[**NOTE:** For $G = \mathbf{Q}_8 = \langle a, b \mid a^4, b^2 = a^2, ba = a^{-1}b \rangle$,

$t = 1, m = n = 2, r = 1, k = 1, s = q = 1]$

Then $|a2^q| = 2^{n-q}$ and $|b2^t| = 2^{m-t}$. Hence $q = n + t - m$.
Let $c = a^v 2^{n-m} b$ for some v.
$\therefore\ c^{2^t} = a^{2^{n-m+t}} b^t [b, a^v 2^{n-m}] 2^{t-1}(2^t - 1)$
$= a^{2^q [v+s+k2^{r-1}v(2^t-1)]}$.
If $v[1 + k2^{r-1}(2^t - 1)] \equiv -s \pmod{2^{m-t}}$ then c has order 2^t.
If $r \geq 2$ then $1 + k2^{r-1}(2^t - 1)$ is odd and so this congruence can be solved for v. For such an element v, $|c| = 2^t$ and so $G = \langle a, b\rangle = \langle a, c\rangle$. Since $|G| = 2^{n+t} = |a|.|c|$, $\langle a\rangle \cap \langle c\rangle = 1$.
Hence $r = 1$, $[b, a] = a^{2k}$. Hence $b^{-1}ab = a^{1-2k}$.
Since $[b, a] \in Z(G)$, a^{2k}, and hence $a^2 \in Z(G)$.
Now $a^2 = (a^2)^b = (a^b)^2 = a^{2-4k}$, from which we conclude that $a^{4k} = 1$. Again, since k is odd, $a^4 = 1$.
Since $\langle a\rangle \cap \langle b\rangle > 1$, $b^2 = a^2 \neq 1$.
So $G \cong \mathbf{Q}_8$.
This proof is based on one in *Group Theory* by Eugene Schenkman (page 192).

Theorem 18: Let G be a Hamiltonian 2-group.
Then $G \cong \mathbf{Q}_8 \times A$ where A is an elementary abelian group.
Proof: By Theorem G is nilpotent of class 2.
Let $a, b \in G$ such that $ab \neq ba$. Let $Q = \langle a, b\rangle$.
Now $\langle a\rangle$, $\langle b\rangle$ are normal subgroups of G, and hence of Q, and if they are disjoint then $Q = \langle a\rangle \times \langle b\rangle$. Hence $ab = ba$, a contradiction, so $\langle a\rangle \cap \langle b\rangle > 1$.

By the Theorem 16 Q ≅ $\mathbf{Q}_8$.

Let K = $C_G(H)$. The cosets of K in G are thus:

K, Ka, Kb, Kab

since 1, a, b and ab induce different inner automorphisms on Q. Suppose that $k \in$ K of order 4.

Then $\langle ak \rangle = \{1, ak, a^2k^2, a^3k^3\}$.

Now $b^{-1}(ak)b = a^{-1}k = a^3k$, which is not one of the powers of ak, a contradicting the fact that G is Hamiltonian. Hence K has no element of order 4. It must therefore be an elementary abelian group.

It can be viewed as a vector space over $\mathbb{Z}_2$.

Now $\langle a^2 \rangle \leq$ K and so can be viewed as a 1-dimensional subspace of K. The only basis for $\langle a^2 \rangle$ is $\{a^2\}$ and this can be extended to a basis, $\mathfrak{B}$, for K.

Let $\mathfrak{L} = \mathfrak{B} - \{a^2\}$ and let A be the subspace spanned by $\mathfrak{L}$. Additively L is an elementary abelian 2-group. Clearly G = Q × A which has the required form.

Theorem 19: A Hamiltonian group is isomorphic to $\mathbf{Q}_8 \times$ H where H is an abelian group with no element of order 4.

Proof: Let G be a Hamiltonian 2-group.

By Theorem 13, G is nilpotent of class 2.

By Theorem 14, G is periodic.

Hence G is the direct product of its Sylow subgroups, each of which is a Dedekind group.

By Theorem 15 the Sylow *p*-subgroups for odd primes *p*, are abelian. Let P be the Sylow 2-subgroup. It must be Hamiltonian.
By Theorem 17, $P \cong \mathbf{Q}_8 \times A$ where A is elementary abelian. Hence $G \cong \mathbf{Q}_8 \times A \times B$ where B is the direct product of the Sylow *p*-subgroups for odd primes *p*. Now take $H = A \times B$.

Note that in Theorem 17 we used the standard theorem of vector spaces that every linearly independent subset of a vector space can be extended to a basis.

However the proof that you've seen only works for finite-dimensional vector spaces. To prove it for *all* vector spaces one needs Zorn's Lemma, which is equivalent to the Axiom of Choice.

It can be shown that there cannot possibly exist a proof that the Axiom of Choice is true, nor a proof that it is false. Therefore you're logically free to accept or reject the Axiom of Choice!

If you prefer to be an Axiom of Choice agnostic then I'm afraid that you will have to limit Theorem 18 to finitely generated Hamiltonian groups.

EXERCISES FOR CHAPTER 10

Exercise 1: For each of the following statements determine whether it is true or false.
(1) The only power automorphisms for a dihedral group is the trivial one.
(2) $\mathcal{P}(\mathbb{R}) \cong \mathbb{R}^{\#}$.
(3) For all periodic abelian groups all power automorphisms are universal.
(4) Homogeneous power automorphisms commute with any automorphism.
(5) The kern of a group is the intersection of the normalisers of all the subgroups of G.
(6) If θ is a power automorphism of G then for all $g \in G$ there exists $z \in Z(G)$ such that $g^{\theta} = gz$.
(7) $\mathbf{Q}_8$ is the only finite Hamiltonian 2-group.
(8) There are no Hamiltonian groups of finite odd order.

Exercise 2: How many power automorphisms of order 2 are there for $\mathbf{C}_{1440}$?

Exercise 3: Let $G = \langle A, B \mid A^3, B^4, BA = A^{-1}B \rangle$.
Find $\mathcal{P}(G)$ and $\mathcal{U}(G)$.

Exercise 4: Let $G = \langle A, B \mid A^{16}, B^{16}, [A, B] = B^8 \rangle$.
(a) Show that G is nilpotent of class 2.
(b) Show that $A^{\theta} = A^3$, $B^{\theta} = B^{11}$ induces an automorphism of G.

(c) Show that $\theta \in \mathcal{P}(G)$.
(d) Is $\theta \in \mathcal{K}(G)$?
(e) Find the order of θ.

SOLUTIONS FOR CHAPTER 10

Exercise 1:
(1) TRUE: All non-trivial dihedral groups are generated by elements of order 2.
(2) Remember that $\mathbb{R}$ is normally written additively, so that a homogeneous power automorphism would be written as $x \to nx$ for some non-zero n. Now it is true that all such maps are automorphisms, but they are not power automorphisms because the do not map every subgroup **onto** itself. For example $x \to 2x$ maps $\mathbb{Z}$ to $2\mathbb{Z}$. An element, x, of infinite order can only be mapped to x or $-x$ by a power automorphism and, in fact, the only non-trivial power automorphism of $\mathbb{R}$ is $x \to -x$.
(3) FALSE: The Prüfer groups have non-universal power automorphisms.
(4) TRUE
(5) TRUE
(6) TRUE: This is the Centrality Theorem
(7) FALSE: $\mathbf{Q}_8 \times \mathbf{C}_2$, $\mathbf{Q}_8 \times \mathbf{C}_2 \times \mathbf{C}_2$, … are all Hamiltonian 2-groups.
(8) TRUE
Exercise 2: $\mathcal{P}(\mathbf{C}_{1440}) \cong \mathbb{Z}_{1440}^{\#}$. Now $1440 = 2^5.3^2.5$ so

$\mathcal{P}(\mathbf{C}_{1440}) \cong \mathbb{Z}_{32}{}^{\#} \times \mathbb{Z}_9{}^{\#} \times \mathbb{Z}_5{}^{\#} \cong C_8 \times C_2 \times C_3 \times C_2 \times C_4$.
The Sylow 2-subgroup has 4 direct factors so the number of elements of order 2 is $2^4 - 1 = 15$.

Exercise 3: $\mathcal{P}(G) \cong \mathbf{C}_2$ where generated by θ where $A^\theta = A$ and $B^\theta = B^{-1}$.
$\mathcal{U}(G) \cong \mathbf{1}$.

Exercise 4:
(a) $G' = \langle B^8 \rangle$.
Since $A^{-1}B^{-1}AB = B^8$, $A^{-1}B^{-1}A = B^7$ and so $A^{-1}BA = B^9$.
Then $A^{-1}B^8A = B^{72} = B^8$, so $B^8 \in Z(G)$.
Hence $G' \leq Z(G)$ and so G is nilpotent of class 2.
(b) Under θ: $A \to A^3$ and $B \to B^{11}$.
So Now $(A^3)^{16} = A^{48} = 1$, $(B^{11})^{16} = 1$.
$A^{-3}B^{11}A^3 = B^{11.9^3} = B^{8019} = B^3$ and $(B^9)^{11} = B^{99} = B^3$.
So A^θ and B^θ satisfy the same relations as A, B and hence θ is an automorphism.
(c) $(A^rB^s)^\theta = A^{3r}B^{11s} = \begin{cases} (A^rB^s)^3 \text{ if } r \text{ is even} \\ (A^rB^s)^{11} \text{ if } r \text{ is odd} \end{cases}$.
Hence θ is a power automorphism.
(d) Since A, B have the same order, and $A^\theta = A^3$ and $B^\theta = B^{11}$, θ is not homogeneous.
(e) Under θ: $A \to A^3 \to A^9 \to A^{27} = A^{11} \to A^{33} = A$ and $B \to B^{11} \to B^{121} = B^9 \to B^{99} = B^3 \to B^{33} = B$.
Hence θ has order 4.