Non-abelian groups of order p^3

Let G be a non-abelian group of order p^3 with p a prime. Then we know that its center Z is non-trivial. Furthermore if a group is a central extension with a cyclic quotient, then the group is commutative. Thus we have an extension

$$1 \to Z \to G \to A \to 1$$

where A is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ and $Z \sim \mathbb{Z}_p$. Furthermore we also conclude that the commutator of G is contained in the center Z. As it is non-trivial by assumption, we must have equality. We are now ready to set up the structure theory.

Pick x, y two non-commuting elements, and set $1 \neq c = xyx^{-1}y^{-1}$ which is hence a generator for the cyclic group Z.

We can write

$$xy = cyx$$

And thus by repetition

$$x^2y = x(xy) = cx(yx) = c(xy)x = c^2yx^2$$

and easily derive by induction the relations

$$x^m y = c^m y x^m$$

and more generally

$$x^m y^n = c^{mn} y^n x^m$$

In particular we note, what could of course been seen directly, that for any element x we have $x^p \in Z$. The structure of the group would be completly determined by setting numbers q, r such that $x^p = c^q, y^p = c^r$

Similarly we can compute

$$(xy)(xy) = x(yx)y = c^{-1}x^2y^2$$

or more generally

$$(xy)^n = c^{-n(n+1)/2} x^n y^n$$

Let us now assume p is odd and postpone a discussion of $p = 2$.

If we replace x by x^α and y by y^β then by the above c will be replaced by $c^{\alpha\beta}$. We thus get

$$(x^\alpha y^\beta)^p = c^{-\alpha\beta p(p+1)/2} c^{\alpha q + \beta r} = c^{\alpha q + \beta r}$$

The right-hand side can be made to 1 by a judicious choice of α, β and hence we can assume that there exists an element x not in the center such that $x^p = 1$.

We conclude that in the odd case we have two cases. Either we have two non-commuting elements of order p or we have just one non-central element (up to a power). In both cases we can exhibit G as a semi-direct product

$$1 \to B \to G \to C \to 1$$

where C is a cyclic group of order p disjoint from B where B is generated by the center and an element y. In the first case y is any non-central element, while in the second case it is one not of order p. The structure of B will in the first case be $\mathbb{Z}_p \times \mathbb{Z}_p$ and in the second $\mathbb{Z}_{p^2}$. To describe the semi-direct product we need to determine the representation of $\mathbb{Z}_p$ on the automorphism group of B.

Case I.

Any element of B can be written uniquely as $y^\alpha c^\beta$ pick x such that the commutator $< x, y >= c$ and consider

$$x(y^\alpha c^\beta)x^{-1} = (xy^\alpha)x^{-1}c^\beta = c^\alpha y^\alpha x x^{-1} c^\beta = y^\alpha c^{\beta+\alpha}$$

This corresponds to sending x to the matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ identifying in the process the only subgroup of $GL(2, \mathbb{F}_p)$ of order p. In particular G is uniquely determined.

Case II.

Any element of B can now be writen as y^α we may choose x of order p such that $< x, y >= y^p = c$ a similar calculation as above yields

$$xy^\alpha x^{-1} = c^\alpha y^\alpha x x^{-1} = y^{\alpha(p+1)}$$

identifying in the same way the only subgroup of $\mathcal{A}\mathrm{ut}(\mathbb{Z}_{p^2}) \sim \mathbb{Z}_{p(p-1)}$ of order p. Once again G is uniquely determined.

Note that both constructions also make sense for $p = 2$ but then they coincide.

Now let us turn to $p = 2$ we then have

$$(xy)^2 = cx^2y^2$$

where c is a non-trivial element of order two. Thus we conclude that not both x and y can be of order two. In particular we can always find elements of order 4.

Case 1. There is a non-central element of order two, then as above we can form a semi-direct product of $\mathbb{Z}_2$ with $\mathbb{Z}_4$. This is given by the canonical identification of $\mathbb{Z}_2$ with $\mathcal{A}\mathrm{ut}(\mathbb{Z}_4)$ and the construction obviously yields the dihedral group of order 8.

Case 2. There is no non-central element of order two. We then have $x^2 = y^2 = c$ and the structure of the group is completly determined. In fact if we set $c = -1$ (an element of order two) and $x = i, y = j$ we get $ij = -ji$ and if we set $k = ij$ we exhaust the possible elements of G naturally represented as

$$\begin{array}{ccc} i & j & k \\ & -1 & \\ -i & -j & -k \\ & 1 & \end{array}$$

and we have in fact defined the so called Quaternionic group representing the units of the integral quaternions.

1.1. *Automorphism groups of non-abelian groups of order* p^3

As we have noted any two non-commuting elements x, y generate the group G (abstractly as all proper subgroups are abelian) it is enough to determine an automorphism by specifying the action of the automorphism on those two elements alone. Thus set

$$\begin{aligned} x \mapsto & c^a x^{m_1} y^{n_1} = x' \\ y \mapsto & c^b x^{m_2} y^{n_2} = y' \end{aligned}$$

Set $\phi = \begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix}$ and it is easy to check

$$< x', y' >= c^{\det \phi}$$

Thus we get the condition that $\det(\phi) \neq 0(p)$ and hence we get an exact sequence

$$0 \to \mathbb{Z}_p \times \mathbb{Z}_p \to \mathcal{A}\mathrm{ut}(G) \to GL(2,p)$$

Where $\mathbb{Z}_p \times \mathbb{Z}_p$ is given by the automorphisms

$$\begin{aligned} x \mapsto & c^a x \\ y \mapsto & c^b y \end{aligned}$$

So let us as usual distinguish betwen the even and odd case. So from now on let us assume p is odd, until explicitly assumed even. In the case I, every element has order p so there are no obstructions, hence the righthand map is surjective and we have indeed a short exact sequence.

$$0 \to \mathbb{Z}_p \times \mathbb{Z}_p \to \mathcal{A}\mathrm{ut}(G) \to GL(2,p) \to 1$$

Where the quotient $GL(2,p)$ clearly denotes the induced automorphism of the quotient $\mathbb{Z}_p \times \mathbb{Z}_p$. All automorphisms preserve the center Z and those that act trivial on the center make up an extension

$$0 \to \mathbb{Z}_p \times \mathbb{Z}_p \to \mathcal{A}\mathrm{ut}_0(G) \to SL(2,p) \to 1$$

and we have

$$1 \to \mathcal{A}\mathrm{ut}_0(G) \to \mathcal{A}\mathrm{ut}(G) \to \mathbb{Z}_p^* \to 1$$

where the righthandside map $\mathcal{A}\mathrm{ut}(G) \to \mathbb{Z}_p$ is given by the determinant.(The image is clearly isomorphic to the automorphism group of the center).

Furthermore we have a natural split of $\mathcal{A}\mathrm{ut}(G)$ in inner and outer automorphisms. The inner automorphisms are clearly given by $G/Z = \mathbb{Z}_p \times \mathbb{Z}_p$ and to identify it we have to make a slight calculation, conjugating by the element $x^m y^n$.

$$\begin{aligned} (x^m y^n)x(y^{-n}x^{-m} &= c^{-mn}x \\ (x^m y^n)y(y^{-n}x^{-m} &= c^m y \end{aligned}$$

Thus we identify the outer automorphisms with $GL(2,p)$ given by the first natural splitting.

We note in passing that the order of the automorphism group is $p^3(p+1)(p-1)^2$.

In case 2. We note that the induced automorphisms on the quotient $\mathbb{Z}_p \times \mathbb{Z}_p$ must have a fixed eigenspace, namely those elements of order p. Thus the image will not be the full group $GL(2,p)$ but a subgroup conjugate to lower triangular matrices, which we will denote by $GL_0(2,p)$ this is a group of $p(p-1)^2$ elements so the total automorphismgroup will have order $p^3(p-1)^2$. The rest of the above discussion goes through, in particular $GL_0(2,p)$ will be indentified with the outer automorphisms.

Finally the case of $p = 2$. In the dihedral case we are now considering $GL_0(2,2) \sim \mathbb{Z}_2$

1.2. Conjugacy classes

As is obvious the elements of the center split up into conjugacy classes of just one element each. For the non-central elements, the centralizers are groups of order p^2 (generated by the elements and the central elements; or alternatively coinciding with the normalizers of the generated cyclic subgroups) and hence the conjugacy classes have p elements. As

$$xyx^{-1} = cy$$

for some central element c we can describe those simply as the cosets of the center.

Obviously an inner automorphism preserves the conjugacy classes. In this case we also see that the automorphisms that do preserve conjugacy classes are indeed inner.