# On groups of order $p^3$, $p$ is an odd prime

by Felix Lazebnik

January 18, 2011

The presentation below is based on Dummit and Foote [2], Hall [3], and Conrad [1]. The motivation was to make it as close as possible to the course I teach at the University of Delaware, to use as few facts as possible, and to prove existence of exactly two isomorphism classes in nonabelian case. The latter is achieved by obtaining the description of the groups in terms of semidirect products.

Let $G$ be a group of order $p^3$, $p$ is an odd prime. If $G$ is abelian, using the Fundamental Theorem for Finite Abelian Groups, we get three isomorphism classes:

$$\mathbb{Z}/(p^3), \quad \mathbb{Z}/(p^2) \times \mathbb{Z}/(p) \quad \text{and} \quad \mathbb{Z}/(p) \times \mathbb{Z}/(p) \times \mathbb{Z}/(p).$$

Suppose $G$ is not abelian. Then $G$ contains no element of order $p^3$. We use the fact that every maximal subgroup of a finite $p$-group is normal, which implies that every subgroup of order $p^2$ is normal in $G$. (See Corollary 7 from Lecture 9, or Theorem 22 (ii) from the Lecture Notes). Therefore our analysis can be reduced to the following two cases.

**Case 1.** $G$ has an element $a$ of order $p^2$.

Let $N = \langle a \rangle$. Being of order $p^2$, $N$ is normal. As $G/N$ is of order $p$, and so cyclic, there must be an element $b \in G \setminus N$ such that $b^p \in N$.

**Case 1.1.** $|b| = p$. Let $B = \langle b \rangle$. As $G = NB$, and $N \cap B = \langle e \rangle$,

$$G = N \underset{f}{\rtimes} B \quad \text{for some homomorphism} \quad f : B \to \operatorname{Aut} N$$

Every automorphism $\phi$ of $N$ is of the form $\phi_i : a \mapsto a^i$, where $(i, p^2) = 1$. Hence, there are $p^2 - p = p(p-1)$ such automorphisms. If $f(b) = \phi_1$, then $\phi_1$ is trivial, and so $G$ is abelian as a direct product of abelian groups. Let $i = mp + r$, where $1 \le r < p$, and $f(b) = \phi_i$. Then $|\phi_i| = |b| = p$, and therefore $a = \phi_i^p(a) = a^{i^p}$. Hence, $i^p \equiv 1 \pmod{p^2}$. As $i^p = (mp + r)^p \equiv r^p \equiv r \pmod{p}$, the latter by Fermat's theorem, and $i^p \equiv 1 \pmod{p}$, we obtain $r \equiv 1 \pmod{p}$, and so $r = 1$. Hence $f(b) = \phi_{mp+1}$, for some $m$, $1 \le m < p$. For $m = 1$, we obtain $f(b) = \phi_{p+1}$. This gives us the first example of the operation in $G$:

$$(a^i, b^j)(a^{i'}, b^{j'}) = (a^{i+i'(p+1)}, b^{j+j'}),$$

or, identifying the set of elements of $G$ with $\mathbb{Z}/(p^2) \times \mathbb{Z}/(p)$,

$$(i, j)(i', j') = (i + i'(p+1), j + j').$$

Note that all $\phi_{mp+1} = \phi_{p+1}^m$ form a cyclic group of order $p$. We leave it for the reader to check that that the semidirect product corresponding to $f(b) = \phi_{mp+1}$ for $1 < m < p$, leads to an isomorphic group. One can do it in a way similar to the one in our solution of Problem 3 of Lecture 14 (classification of nonabelian groups of order $pq$, where $p$ and $q$ are primes and $p < q$. )

**Case 1.2.** $|b| = p^2$. Our goal is to show that there exists $b_1 \in G \setminus N$ or order $p$, and this will reduce the problem to Case 1.1.

As $G = N + bN + \cdots + b^{p-1}N$, every element of $G \setminus N$ can be written in the form $b^y a^x$ for some $1 \le x \le p-1$ and $1 \le y \le p^2 - 1$. Hence, it is sufficient to show that for some such $x$ and $y$, $|b^y a^x| = p$ and $b^y a^x$ is not in $N$. The latter is equivalent to $b^y$ not in $N$. As $N \lhd G$, and $b$ is not in $N$, $bab^{-1} = a^i$ for some $i$, where $(i, p^2) = 1$. Hence $b^j a b^{-j} = a^{i^j}$ for every $j$, and $b^y a^x b^{-y} = a^{xi^y}$, or $b^y a^x = a^{xi^y} b^y$. Taking $j = p$, we conclude, as we did in Case 1.1, then $i = mp+1$ for some $1 \le m \le p-1$. We have:

$$(b^y a^x)^p = (b^y a^x) \cdot (b^y a^x) \cdot \ldots \cdot (b^y a^x) = a^{xi^y} b^y \cdot (b^y a^x) \cdots (b^y a^x) =$$

$$a^{xi^y} (b^{2y} a^x)(b^y a^x) \cdots (b^y a^x) = a^{xi^y + xi^{2y}} b^{2y} (b^y a^x) \cdots (b^y a^x) = \cdots =$$

$$a^{xi^y + xi^{2y} + \cdots + xi^{(p-1)y}} b^{py} = a^{x \frac{i^{py} - i^y}{i^y - 1}} b^{py}$$

We wish to have

$$a^{x \frac{i^{py} - i^y}{i^y - 1}} b^{py} = 1.$$

For $y = 1$, and using $i = mp + 1$, the last equality gives

$$a^{x \frac{(mp+1)^p - (mp+1)}{mp}} b^p = a^{x(kp^2 + p)} b^p = a^{xp} b^p = 1.$$

As $|b| = |a| = p^2$, and $b^p \in N$, we have $b^p = a^{pu}$ for some $u = 1, \ldots, p-1$. Therefore taking $x = -u$, and setting $b_1 = a^{-u} b$, we obtain the element we were looking for![1]

**Case 2.** Every nonidentity element of $G$ has order $p$.

A normal subgroup $H$ of $G$ of order $p^2$ exists. We know that $H$ must be abelian. As $G$ contains no element of order $p^2$, $H \simeq \mathbb{Z}/(p) \times \mathbb{Z}/(p)$. Let $K = \langle k \rangle$, where $k \in G \setminus H$. Then $|K| = p$, $G = HK$, and $H \cap K = \langle k \rangle$. Therefore

$$G = H \underset{g}{\rtimes} K \quad \text{for some homomorphism} \quad g : K \to \operatorname{Aut} H.$$

We know that $\operatorname{Aut} H \simeq GL_2(\mathbb{Z}/(p))$. If $g(k)$ is the identity automorphism, then $G$ is abelian. Hence, $|g(k)| = p$. We know that $|GL_2(\mathbb{Z}/(p))| = (p^2-1)(p^2-p) = p(p-1)^2(p+1)$. Hence $g(k)$ generates a Sylow $p$-subgroup of $GL_2(\mathbb{Z}/(p))$. Choosing a particular Sylow $p$-subgroup

$$\left\langle\ g(k) = A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\ \right\rangle < GL_2(\mathbb{Z}/(p)),$$

[1] Just trying this form of $b_1$ from the beginning would do, but it would not be clear how one could find it in a natural way.

we obtain an operation in $G$:

$$(v, k^j)(v', k^{j'}) = (v + v'^{g(k)}, k^{j+j'}) = (v + v'A, k^{j+j'}).$$

Identifying the set of elements of $G$ with $(\mathbb{Z}/(p) \times \mathbb{Z}/(p)) \times \mathbb{Z}/(p)$, we obtain

$$((a,b),j)((a',b'),j') = ((a,b) + (a',b')^{g(k)}, j + j') =$$

$$((a,b) + (a',b')A, j + j') = ((a,b) + (a', a' + b'), k^{j+j'}) =$$

$$((a + a', b + a' + b'), j + j').$$

As all Sylow $p$-subgroups of $GL_2(\mathbb{Z}/(p))$ are conjugate, they are generated by matrices similar to $A$. Let $g' : K \to \operatorname{Aut} H$ be defined by $k \mapsto CAC^{-1}$ for some $C \in GL_2(\mathbb{Z}/(p)$. Then

$$\phi : H \underset{g}{\rtimes} K \to H \underset{g'}{\rtimes} K, \quad (v, j) \mapsto (vC^{-1}, j),$$

is a group isomorphism, which is easily verified. Hence, all nonabelian semidirect products of $H$ and $K$ are isomorphic.

Therefore there are two isomorphism classes of non-abelian groups of order $p^3$, for odd prime $p$. □

Though the existence of exactly two isomorphism classes in the nonabelian case is proven, it is always nice to find their examples among familiar groups. One can show that our first construction is isomorphic to the group

$$G_p = \left\{ \begin{pmatrix} 1 + (p) & b \\ 0 & 1 \end{pmatrix}, \ \ (p) = p\,\mathbb{Z}/(p^2), \text{ and } b \in \mathbb{Z}/(p^2) \right\},$$

and our second construction is isomorphic to the $UT_3(\mathbb{Z}/(p))$, also known as Heisenberg group:

$$UT_3(\mathbb{Z}/(p)) = \operatorname{Heis}(\mathbb{Z}/(p)) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \ \ a, b, c \in \mathbb{Z}/(p). \right\}$$

We leave it to the reader to find subgroups of $G_p$ isomorphic to $N$ and $B$, subgroups of $\operatorname{Heis}(\mathbb{Z}/(p))$ isomorphic to $H$ and $K$, and establish related isomorphisms. In case of difficulties, one can consult [1].

# References


[1] K. Conrad, Groups of order $p^3$,
`http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/groupsp3.pdf`

[2] D.S. Dummit, R.M. Foote, Abstract Algebra, 3rd edition, John Willey & Sons, 2004.

[3] M. Hall, Jr., Theory of Groups, The Macmillian Company, New York, 1959.