Justin Willson
Andrew Doumont
Bob Kuo

11. Let G be a finite, 2-step nilpotent, p-group.

(a) Show that if p is odd, then G has an abelian word $w(x, y)$. That is, if $x \oplus y = w(x, y)$, then $\langle G; x \oplus y\rangle$ is an abelian group.

(b) Is the same assertion true if p is even?

(c) Is the same assertion true if G is 3-step nilpotent?

Proof.

(a) Let c be an integer such that $2c+1 = |G'|$. Then, c is well defined because G is a finite p-group, with p odd so $|G'|$ is also odd and finite. Now, we can define

$$x \oplus y = xy[x, y]^c.$$

We claim that $\langle G; x \oplus y\rangle$ is an abelian group. Observe, $1 \in G$ is the identity element for the relation since

$$x \oplus 1 = x \cdot 1 \cdot [x, 1]^c = x \cdot (x^{-1}x)^c = x = 1 \cdot x \cdot [1, x]^c = 1 \oplus x.$$

Further, we have,

$$x \oplus x^{-1} = xx^{-1}[x, x^{-1}] = (x^{-1} \cdot x \cdot x \cdot x^{-1})^c = 1 = x^{-1}x[x^{-1}, x] = x^{-1} \oplus x,$$

so the operation has inverses. Next, we can see that the relation is commutative by observing that

$$(x \oplus y)(y \oplus x)^{-1} = xy[x, y]^c(yx[y, x]^c)^{-1} = xy[x, y]^c[x, y]^c y^{-1}x^{-1} = [x^{-1}, y^{-1}]^{2c+1} = 1.$$

Here, the second to last equality comes from expanding the commutators and noticing that the pattern $xyx^{-1}y^{-1} = [x^{-1}, y^{-1}]$ repeats $2c + 1$ times in the expansion. Finally, to see that the relation is associative observe that

$$x \oplus (y \oplus z) = xyz[y, z]^c[x, yz[y, z]^c]^c = xyz[y, z]^c[x, yz]^c = xyz[x, y]^c[x, z]^c[y, z]^c$$

and

$$(x \oplus y) \oplus z = xy[x, y]^c z[xy[x, y]^c, z]^c = xyz[x, y]^c[xy, z]^c = xyz[x, y]^c[x, z]^c[y, z]^c$$

where the equalites follow from the realization that all elements of G commute with commutators in G since

$$a[b, c] = [b, c]a[a, [b, c]] = [b, c]a$$

due to G being 2-step nilpotent. Thus $\oplus$ is associative, hence, $\langle G; x \oplus y\rangle$ is an abelian group.

Justin Willson
Andrew Doumont
Bob Kuo

(b) The assertion is not true if p is even, that is, it is not true if $p = 2$. This is because there is no integer c such that $2c + 1 \equiv 0 \mod |G'|$ when the order of G is a power of 2. One might ask if there is another word that works, however, because G is 2-step nilpotent, every word can be written as

$$w(x, y) = x^a y^b [x, y]^c,$$

so we will show that the only possible abelian word is the one from part (a). If $w(x, y) = x^a y^b [x, y]^c$, we claim that the only possible identity for w is 1. Let $e \in G$ be an identity for $w(x, y)$ and let e^{-1} be its inverse with respect to the original multiplication in G. We see

$$1 = w(e, 1) = e^a \quad \text{and} \quad 1 = w(1, e) = e^b.$$

So, the order of e in G divides both a and b. Then, we see

$$e^{-1} = w(e, e^{-1}) = e^a (e^{-1})^b = 1,$$

where the first equality follows from the identity property of e, the second equality follows from the definition of w and the last equality comes from the fact that $e^a = 1$ and that the order of e^{-1} is the same as the order of e, hence, $(e^{-1})^b = 1$ as well. Thus, the only candidate for an identity for our word is the identity in the group. From this we deduce that a must be equal to b in order for the word to have an inverse and that $a \equiv 1 \mod \exp(G)$ for the word to have an identity[1]. This is because if a is larger, we see that

$$w(x, 1) = x^a 1^b [x, 1]^c = x^a,$$

which is not always equal to x unless $a \equiv 1 \mod \exp(G)$ since G is a p-group. We get that $a = b$ by observing

$$x^b = w(1, x) = w(x, 1) = x^a.$$

Finally, we see that c must satisfy $2c + 1 \equiv 0 \mod |G'|$ by the computation we used in part (a) to show commutativity.

(c) The same assertion is not true if G is 3-step nilpotent since the assertion fails for $p = 3$. To see this, we provide a counter example. Consider the group with the presentation

$$G := \langle \alpha, \beta, \gamma \mid \alpha^9 = \beta^3 = \gamma^3 = 1, \alpha\beta = \beta\alpha, \gamma\alpha\gamma^{-1} = \alpha\beta^{-1}, \gamma\beta\gamma^{-1} = \alpha^3\beta \rangle,$$

which is a 3-step nilpotent group of order $3^4 = 81$. By way of contradiction, assume that G has an abelian word

$$w(x, y) = x^a y^b [x, y]^c [x, y, x]^d [y, x, y]^e.$$

We will show that $\langle G; w(x, y) \rangle$ is not isomorphic to any abelian group of order 81. By the arguments made in part (b), we see that $a = b = 1$. This tells us that under $w(x, y)$, the element α has order 9 in $\langle G; w(x, y) \rangle$ since it has order 9 in $\langle G; \cdot \rangle$. This tells us that $\langle G; w(x, y) \rangle$ is not isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

[1] Here, $\exp(G)$ is the exponent of G

Justin Willson
Andrew Doumont
Bob Kuo

Next, since $w(x,y)$ is composed of multiplication and inverses, every subgroup of $\langle G; \cdot\rangle$ is also a subgroup of $\langle G; w(x,y)\rangle$. Using GAP, we found that $\langle G; \cdot\rangle$ has 50 distinct subgroups. Since each distinct subgroup of $\langle G; \cdot\rangle$ is also a subgroup $\langle G; w(x,y)\rangle$, we can eliminate $\mathbb{Z}_{81}$, $\mathbb{Z}_3 \times \mathbb{Z}_{27}$, and $\mathbb{Z}_9 \times \mathbb{Z}_9$ as they all have less than 50 distinct subgroups. Now, the only abelian group we have left to eliminate is $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9$. This can be eliminated by observing that $\langle G; w(x,y)\rangle$ has 31 subgroups of order 3, while $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9$ has 13, which is too few. Thus no such $w(x,y)$ exists.

$\square$