Abelian Forcing Sets

Michael Reid
Department of Mathematics
University of California, Berkeley
Berkeley, CA 94720
E-mail: reid@math.berkeley.edu

Joseph A. Gallian
Department of Mathematics
University of Minnesota, Duluth
Duluth, MN 55812
E-mail: jgallian@ua.d.umn.edu

September 19, 2008

Most readers of the MONTHLY have encountered particular cases of the following question. Suppose G is a group and n is an integer with the property that $(ab)^n = a^n b^n$ for all a and b in G. Which n implies that G is Abelian? Indeed, standard exercises in undergraduate abstract algebra textbooks ([1], [2], [3], [4]) are to show that $n = 2$ and $n = -1$ are two cases that do imply that G is Abelian. Are there others? Well, if p is any odd prime the group $G_p = \left\{ \left[\begin{array}{ccc} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{array} \right] \middle| \, a, b, c \in Z_p \right\}$ is a non-Abelian group with the property that $x^p = e$ for all x in G_p. And this implies that if n is any multiple of p (positive or negative) then $(ab)^n = a^n b^n$ for all a and b in G_p. Similarly, G_2 (which is isomorphic to the group of symmetries of a square) is a non-Abelian group for which $(ab)^n = a^n b^n$ when n is any multiple of 4. From these two observations it follows then that the identity $(ab)^n = a^n b^n$ for all a and b in a group implies that the group is Abelian if and only if $n = 2$ or $n = -1$.

More generally, let us call a set of integers T *Abelian forcing* if every group with the property that for all n in T

$$(ab)^n = a^n b^n \text{ for all } a \text{ and } b \text{ in } G$$

is Abelian. So far we have shown that the only singleton Abelian forcing sets are $\{-1\}$ and $\{2\}$. What about other sets? Both of Herstein's algebra textbooks ([3, p.31] and [4, p.57]) include the exercise that sets containing three consecutive integers are Abelian forcing. Moreover, one of Herstein's books ([4, p.57]) has an exercise that $\{3, 5\}$ is an Abelian forcing set. In contrast, the set $\{3, 7\}$ is not Abelian forcing.

So, what characterizes the Abelian forcing sets? Although we could not find the answer to this precise question in the literature, some of the essential features of our argument below can be gleaned from a paper by F. Levi [5] written in the group-theoretic language of fifty years ago. (Levi investigated the question of when the mapping $a \to a^n$ is a group endomorphism.) Our formulation of the question, the answer and the proof make the material more accessible to undergraduates.

Theorem. A set S of integers is an Abelian forcing set if and only if the greatest common divisor of the integers $n(n-1)$ as n ranges over S is 2.

Proof. Suppose that S is an Abelian forcing set and the greatest common divisor d of the integers $n(n-1)$ as n ranges over S is not 2. Since every integer of the form $n(n-1)$ is even, d has the form $2k$ where $k > 1$.

Let q be a prime that divides k. Then q divides $n(n-1)/2$ for every n in S. Thus $n(n-1) \equiv 0 \bmod 2q$ for all n in S. Next observe that for every odd prime p the elements of the group G_p satisfy

$$(ab)^{pk} = a^{pk} b^{pk} \text{ and } (ab)^{pk+1} = a^{pk+1} b^{pk+1}$$

for all integers k. Also, the elements of G_2 satisfy

$$(ab)^{4k} = a^{4k} b^{4k} \text{ and } (ab)^{4k+1} = a^{4k+1} b^{4k+1}$$

for all integers k. Since G_p and G_2 are non-Abelian we know that the sets

$$A = \{pk, pk+1 | k \in Z\} = \{n \in Z | n(n-1) \equiv 0 \bmod p\}$$

and

$$B = \{4k, 4k+1 | k \in Z\} = \{n \in Z | n(n-1) \equiv 0 \bmod 4\}$$

are not Abelian forcing sets. However, if q is odd, then S is a subset of A and if q is 2, then S is a subset of B. In either case, S can't be Abelian forcing since A and B aren't. This contradiction proves necessity.

To prove sufficiency suppose that the greatest common divisor of the integers $n(n-1)$ as n ranges over S is 2. We will show that S is Abelian forcing by showing that $2 \in S$. Let $n \in S$ and let a and b be arbitrary elements of a group G. We use $Z(G)$ to denote the center of G. The proof is bookkeeping.

Step 1. a^n commutes with b^{n-1}.
$(b^{-1}ab)^n = b^{-1}a^n b$ (since $(b^{-1}ab)^i = b^{-1}a^i b$ for all i)
$(b^{-1}ab)^n = b^{-n}a^n b^n$ (since $n \in S$).
Thus $b^{-1}a^n b = b^{-n}a^n b^n$ and $b^{n-1}a^n = a^n b^{n-1}$.

Step 2. b^n commutes with a^{n-1}.
Interchange a and b in Step 1.

Step 3. $1-n \in S$.
$ab = (ab)^n(ab)^{1-n} = a^n b^n (ab)^{1-n} \Rightarrow$
$b = a^{n-1}b^n(ab)^{1-n} = b^n a^{n-1}(ab)^{1-n}$ (Step 2).
So, $a^{1-n}b^{1-n} = (ab)^{1-n}$.

Step 4. $n(1-n) \in S$.
$(ab)^{n(1-n)} = (a^n b^n)^{1-n} = a^{n(1-n)}b^{n(1-n)}$ (Step 3).

Step 5. $a^{n(1-n)} \in Z(G)$.
$b^{-1}a^{n(1-n)}b = (b^{-1}ab)^{n(1-n)} = (b^{-1})^{n(1-n)}a^{n(1-n)}b^{n(1-n)}$ (Step 4)
$= (b^{n-1})^n a^{n(1-n)} (b^{1-n})^n = a^{n(1-n)}$ (Step 1).

Step 6. $H = \{n \in Z | (ab)^n = a^n b^n \text{ and } a^n \in Z(G)\}$ is a subgroup of Z.
Clear.

Step 7. $C = \{n(n-1) | n \in S\} \subseteq H$.
This follows directly from Steps 4 and 5.

Step 8. $2 \in S$.

Since $C \subseteq H$ and H is a subgroup of the integers, H contains the greatest common divisor of any subset of its elements. Thus, 2 is in H. Finally, since $H \subseteq S$ we are done.

References

1. J.B. Fraleigh, A First Course in Abstract Algebra, 4th ed., Addison-Wesley, Reading, MA, 1989.
2. J.A. Gallian, Contemporary Abstract Algebra, 2nd ed., D.C. Heath, Lexington, MA, 1990.
3. I.N. Herstein, Topics in Algebra, 2nd ed., John Wiley & Sons, New York, 1975.
4. I.N. Herstein, Abstract Algebra, 2nd ed., Macmillan, New York, 1990.
5. F.W. Levi, Notes on group theory. I, II. J. Indian Math. Soc. (N.S.), **8** (1944) 1-9.