When is a finite abelian group cyclic?

In Corollary 5.6.4 (p.300), Fraleigh proves that any finite group of units in a field F is cyclic, by noting that for any integer m, the equation $a^m = 1$ can have at most m solutions in F, and then showing that this fact, together with the Fundamental Theorem on finitely generated abelian groups (Theorem 2.4.12, proved in section 4.4), forces such a group to be cyclic. Since we did not cover the proof of the Fundamental Theorem, we will have to get this result by a different argument.

I will prove below that a finite abelian group A which, for each prime p, has no more than p elements a satisfying $a^p = e$, must be cyclic (a slightly stronger result than Fraleigh notes), and deduce Corollary 5.6.4 from this.

To show a group A of order n to be cyclic is the same as showing that it contains an element a of order n (since such an a will generate an n-element subgroup, and such a subgroup can only be the whole group A). So the result we intend to prove relates elements of ''small'' orders, i.e., elements satisfying equations $a^p = 1$, with elements of ''large'' order, namely, generators of A. The next result will be our key to relating elements of larger and smaller orders.

3.2.13 LEMMA Let A be an abelian group, written multiplicatively. Then

(i) For each positive integer m, the map $\alpha_m : A \to A$ defined by $\alpha_m(a) = a^m$ is a homomorphism.

Let us denote by A_m the kernel of this map, i.e., let

$$A_m = \{a \in A \mid a^m = e\}.$$

Then if A is finite one has, for all positive integers m_1 and m_2

(ii) $|A_{m_1 m_2}| \leq |A_{m_1}|\,|A_{m_2}|$, and

(iii) If equality holds in (ii), then $\alpha_{m_1}[A_{m_1 m_2}] = A_{m_2}$.

PROOF Because A is abelian, we can rewrite $\alpha_m(ab) = (ab)^m = (ab)(ab)\dots(ab)$ as $(aaa\dots a)(bbb\dots b) = a^m b^m = \alpha_m(a)\,\alpha_m(b)$, proving (i).

To prove (ii), let us first note that given m_1 and m_2, the law of exponents $(a^{m_2})^{m_1} = a^{m_1 m_2}$ says that $\alpha_{m_1}\alpha_{m_2} = \alpha_{m_1 m_2}$. I claim this implies

$$\alpha_{m_1}[A_{m_1 m_2}] \leq A_{m_2}.$$

Indeed, let $a \in A_{m_1 m_2} = \mathrm{Ker}(\alpha_{m_1 m_2})$; we want to show that $\alpha_{m_1}(a) \in A_{m_2} = \mathrm{Ker}(\alpha_{m_2})$; in other words, that $\alpha_{m_2}(\alpha_{m_1}(a)) = e$. But as we have just seen, the left-hand side equals $\alpha_{m_1 m_2}(a)$, which is e by assumption on a.

Let us now regard α_{m_1} as a homomorphism from $A_{m_1 m_2}$ into A_{m_2}. Since the kernel of α_{m_1} is A_{m_1}, the First Isomorphism Theorem says that the image of the map is isomorphic to $A_{m_1 m_2}/A_{m_1}$. Hence assuming A is finite, so that these subgroups are finite, the order of this image will be $|A_{m_1 m_2}|/|A_{m_1}|$. Since A_{m_2} contains this image, we get $|A_{m_2}| \geq |A_{m_1 m_2}|/|A_{m_1}|$, and if equality holds, the image is precisely A_{m_2}. Multiplying by $|A_{m_1}|$, we conclude that $|A_{m_1}|\,|A_{m_2}| \geq |A_{m_1 m_2}|$, proving (ii), and that if equality holds, then $\alpha_{m_1}[A_{m_1 m_2}] = A_{m_2}$, proving (iii). $\square$

We can now prove the desired result:

3.2.14 THEOREM Let A be a finite abelian group such that for every prime p, the equation $a^p = e$ has $\leq p$ solutions $a \in A$. Then A is cyclic.

PROOF The assumption on solutions of $a^p = e$ says, in the notation of the preceding lemma, that for each prime p, $|A_p| \leq p$. Hence using that lemma we see that for every integer m, $|A_{pm}| \leq |A_p|\,|A_m| \leq p\,|A_m|$. Thus, $|A_{pm}| \leq p\,|A_m|$, and if equality holds, then both of the preceding inequalities must be equalities; in particular, the first must be, so by the preceding lemma, the map α_p must carry A_{pm} onto A_m.

Now let a prime factorization of $|A|$ be $|A| = p_1 p_2 \cdots p_n$, where some factors may be repeated. Then by repeated application of the above observations, we have

$$|A| \;=\; |A_{p_1 p_2 \cdots p_n}| \;\leq\; |A_{p_1 p_2 \cdots p_{n-1}}|\, p_n \;\leq\; \ldots \;\leq\; |A_{p_1}|\, p_2 \cdots p_n \;\leq\; |A_1|\, p_1 p_2 \cdots p_n \;=\; p_1 p_2 \cdots p_n,$$

where at the last stage we use the observation that $A_1 = \{e\}$. But since $p_1 p_2 \cdots p_n$ is a factorization of $|A|$, the first and last terms above are equal, hence we must have equality at *all* the ''$\leq$'' signs.

From this we conclude, on the one hand, that for each $i \in \{0, \ldots, n\}$ we have

$$|A_{p_1 \cdots p_i}|\, p_{i+1} \cdots p_n \;=\; p_1 p_2 \cdots p_n,$$

i.e., that

(1) $$|A_{p_1 \cdots p_i}| \;=\; p_1 \cdots p_i,$$

and on the other hand, using the preceding lemma, that for each such i

(2) the homomorphism α_{p_i} carries $A_{p_1 \cdots p_i}$ onto $A_{p_1 \cdots p_{i-1}}$.

We can now prove by induction that for each i, $A_{p_1 p_2 \cdots p_i}$ contains an element of order $p_1 p_2 \cdots p_i$. The case $i = 0$, i.e., the fact that the group $A_1 = \{e\}$ has an element of order 1, namely e, is clear. Taking any $i > 0$, let

$$m \;=\; p_1 p_2 \cdots p_{i-1},$$

and let us assume inductively that A_m has an element a of order m; we need to prove from this that A_{mp_i} has an element of order mp_i. Now by (2), the element $a \in A_m$ can be written

$$a \;=\; \alpha_{p_i}(b) \;=\; b^{p_i}$$

for some $b \in A_{mp_i}$. Thus $\langle a\rangle \leq \langle b\rangle$, so the order of b must be a multiple of the order of a, which is m. Also, the order of b must divide the order of A_{mp_i}, which is mp_i. So the order of b is either m or mp_i.

If the order of b is mp_i, then we are done. Moreover, I claim that if p_i divides m, (i.e., if p_i is a repetition of one of p_1, p_2, ..., p_{i-1}), then b must indeed have order mp_i. For let us write $m = m' p_i$, and suppose b only had order m. Then we would have $a^{m'} = (b^{p_i})^{m'} = b^m = e$, contradicting the assumption that a has order m.

It remains to consider the case where b has order m, in which case, by what we have just shown, m is not divisible by p_i. By Cauchy's Theorem we can find an element $c \in A_{mp_i}$ of order p_i. Now what can be said about the order of the product bc? On the one hand, the subgroup it generates contains $(bc)^{p_i} = b^{p_i} c^{p_i} = a\,e = a$, so its order is a multiple of $|\langle a\rangle| = m$. On the other hand, $(bc)^m = b^m c^m = c^m \neq e$ (because m is not divisible by p_i, the order of c), so the order of bc is not m; hence being a multiple of m and a divisor of $|A_{mp_i}| = mp_i$; it must be exactly mp_i.

This completes the induction. Taking $i = n$, we have that $A_{p_1 p_2 \cdots p_n} = A$ contains an element a of order n, which therefore generates A, showing A cyclic, and proving the lemma. □

Thus we can now get the result in Fraleigh,

5.6.4 COROLLARY If G is a finite subgroup of the multiplicative group $\langle F^*, \cdot\rangle$ of a field F, then G is cyclic. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

PROOF By the preceding theorem, it suffices to show that for each prime p, the equation $a^p = 1$ has at most p solutions in G. But the solutions to this equation are the zeroes of the polynomial $x^p - 1$, and Corollary 5.6.3 tells us that a polynomial of degree p has at most p zeroes. □