Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 34 (1993), No. 2, 157-161.

Is Whaples' Theorem a Group Theoretical Result?

Arne Ledet
Mathematical Institute, University of Copenhagen
Universitetsparken 5, DK - 2100 Copenhagen

A theorem by Whaples (see [2] or [3]) states, that if a field admits a cyclic extension of degree p, where p is an odd prime, it admits a pro-cyclic extension of degree p^∞. Similarly, the existence of a cyclic extension of degree 4 implies the existence of a procyclic extension of degree 2^∞.

This can be formulated as a statement about the absolute Galois group G of the field: If G has the cyclic group $\mathbf{Z}/p\mathbf{Z}$ as a factor, it has the pro-cyclic group $\widehat{\mathbf{Z}}_p$ of p-adic integers as a factor, and similarly for $\mathbf{Z}/4\mathbf{Z}$ and the 2-adic integers $\widehat{\mathbf{Z}}_2$.

This property does not hold for pro-finite groups in general. (With $\mathbf{Z}/p\mathbf{Z}$ and $\mathbf{Z}/4\mathbf{Z}$ as obvious counter-examples.) But unless the field is formally real the absolute Galois group is torsion free, and it is therefore natural to ask whether Whaples' result generalizes to torsion free pro-finite groups.

It does not.

Let p be a prime. For $h \geq 0$, $k, m > 0$, $h + k \geq m$, we define

$$\mathfrak{M}_{h,k,m} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\widehat{\mathbf{Z}}_p) \;\middle|\; \begin{matrix} ad - bc = 1, \ d \equiv 1 \pmod{p^m}, \\ b \equiv 0 \pmod{p^h}, \ c \equiv 0 \pmod{p^k} \end{matrix} \right\}.$$

It is easily seen that $\mathfrak{M}_{h,k,m}$ is a closed p-subgroup of

$$\mathrm{SL}_2(\widehat{\mathbf{Z}}_\mathrm{p}) = \varprojlim \mathrm{SL}_2(\mathbf{Z}/\mathrm{p}^\mathrm{n}\mathbf{Z}).$$

For odd primes p these groups are investigated in [1, III.§17], where the following theorems are proved:

Theorem 1. *Let*

$$B(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \quad C(x) = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}, \quad D(x) = \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix},$$

and consider the following subgroups of $\mathfrak{M}_{h,k,m}$*:*

$$\begin{aligned}\mathfrak{B}_h &= \{B(x) \mid x \equiv 0 \pmod{p^h}\},\\ \mathfrak{C}_k &= \{C(x) \mid x \equiv 0 \pmod{p^k}\},\\ \mathfrak{D}_m &= \{D(x) \mid x \equiv 1 \pmod{p^m}\}.\end{aligned}$$

Every element $x \in \mathfrak{M}_{h,k,m}$ *can be written in one and only one way as* $x = bcd$, $b \in \mathfrak{B}_h$, $c \in \mathfrak{C}_k$, $d \in \mathfrak{D}_m$.

$$[\mathfrak{M}_{h,k,m} : \mathfrak{M}_{h+h',k+k',m+m'}] = p^{h'+k'+m'}.$$

An easy consequence of the decomposition $\mathfrak{M}_{h,k,m} = \mathfrak{B}_h\mathfrak{C}_k\mathfrak{D}_m$ is the following: $\mathfrak{M}_{h+h',k+k',m+m'} \triangleleft \mathfrak{M}_{h,k,m}$, if $h' \le m+m' \le h+k+k'$ and $k' \le m+m' \le k+h+h'$.

Theorem 2. $\mathfrak{M}'_{h,k,m} = \mathfrak{M}_{h+m,k+m,h+k}$.

Theorem 1 is also valid for $p = 2$, whereas Theorem 2 holds for odd primes only. The analogue of Theorem 2 for $p = 2$ (and $m > 1$) is Theorem 4 below.

Lemma 3. *Let* $p = 2$ *and* $m > 1$*. Then*

$$\begin{aligned}[\mathfrak{B}_h, \mathfrak{D}_m] &= \mathfrak{B}_{h+m+1} \quad \text{and}\\ [\mathfrak{C}_k, \mathfrak{D}_m] &= \mathfrak{C}_{k+m+1}.\end{aligned}$$

Also $[B(b), C(c)] = B(b)C(c)B(-b)C(-c) = B(-b^2ce^{-1})C(bc^2e)D(e)$, *where* $e = 1 - bc$.

Proof. We have

$$\begin{aligned}[B(b), D(d)] &= B(b)D(d)B(b)^{-1}D(d)^{-1}\\ &= \begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\begin{pmatrix}d^{-1} & 0\\ 0 & d\end{pmatrix}\begin{pmatrix}1 & -b\\ 0 & 1\end{pmatrix}\begin{pmatrix}d & 0\\ 0 & d^{-1}\end{pmatrix}\\ &= \begin{pmatrix}1 & b(1-d^{-2})\\ 0 & 1\end{pmatrix} = B(b(1-d^{-2})).\end{aligned}$$

If $d \equiv 1 \pmod{2^m}$, we have $1 - d^{-2} = (1+d^{-1})(1-d^{-1}) \equiv 0 \pmod{2^{m+1}}$. Hence $[\mathfrak{B}_h, \mathfrak{D}_m] = \mathfrak{B}_{h+m+1}$. $[\mathfrak{C}_k, \mathfrak{D}_m] = \mathfrak{C}_{k+m+1}$ is proved similarly. □

Theorem 4. *Let* $p = 2$ *and* $m > 1$*. If* $h + k > m$,

$$\mathfrak{M}'_{h,k,m} = \mathfrak{M}_{h+m+1,k+m+1,h+k}.$$

If $h + k = m$,

$$\mathfrak{M}'_{h,k,m} = \mathfrak{M}_{h+m+1,k+m+1,m+1}\left\langle B(2^{h+m})C(2^{k+m})D(1+2^m)\right\rangle.$$

Proof. $h+k>m$: If $b \equiv 0 \pmod{2^h}$ and $c \equiv 0 \pmod{2^k}$, we have $-b^2ce^{-1} \equiv 0 \pmod{2^{2h+k}}$ and $bc^2e \equiv 0 \pmod{2^{h+2k}}$. Since $2h+k \geq h+m+1$ and $h+2k \geq k+m+1$, we have $D(e) \in \mathfrak{M}'_{h,k,m}$ by Lemma 3. $\mathfrak{D}_{h+k}$ is generated by these elements $D(e)$, and we conclude, that $\mathfrak{D}_{h+k} \subseteq \mathfrak{M}'_{h,k,m}$. Hence

$$\mathfrak{M}_{h+m+1,k+m+1,h+k} \subseteq \mathfrak{M}'_{h,k,m}.$$

Since $\mathfrak{M}_{h+m+1,k+m+1,h+k} \lhd \mathfrak{M}_{h,k,m}$ and $\mathfrak{M}_{h,k,m}/\mathfrak{M}_{h+m+1,k+m+1,h+k}$ is abelian, we have

$$\mathfrak{M}'_{h,k,m} = \mathfrak{M}_{h+m+1,k+m+1,h+k}.$$

$h+k=m$: We still have $\mathfrak{B}_{h+m+1} \subseteq \mathfrak{M}'_{h,k,m}$ and $\mathfrak{C}_{k+m+1} \subseteq \mathfrak{M}'_{h,k,m}$. If $b \equiv 0 \pmod{2^{h+1}}$ and $c \equiv 0 \pmod{2^k}$, we get $D(e) \in \mathfrak{M}'_{h,k,m}$ and $e \equiv 1 \pmod{2^{m+1}}$. Hence

$$\mathfrak{M}_{h+m+1,k+m+1,m+1} \subseteq \mathfrak{M}'_{h,k,m}$$

These subgroups are both normal.

We know that $B(-2^{2h}2^k(1-2^m)^{-1})C(2^h2^{2k}(1-2^m))D(1-2^m) \in \mathfrak{M}'_{h,k,m}$, and $B(2^{h+m})C(2^{k+m})D(1+2^m) \equiv B(-2^{2h}2^k(1-2^m)^{-1})C(2^h2^{2k}(1-2^m))D(1-2^m) \pmod{\mathfrak{M}_{h+m+1,k+m+1,m+1}}$. If we let $B=B(2^{h+m})$, $C=C(2^{k+m})$ and $D=D(1+2^m)$ this gives

$$\mathfrak{M}_{h+m+1,k+m+1,m+1}\langle BCD\rangle \subseteq \mathfrak{M}'_{h,k,m}.$$

$\mathfrak{M}_{h,k,m}$ is generated by $b=B(2^h)$, $c=C(2^k)$ and $d=D$, so to prove normality of $\mathfrak{M}_{h+m+1,k+m+1,m+1}\langle BCD\rangle$ one directly verifies that $[x,BCD] \in \mathfrak{M}_{h+m+1,k+m+1,m+1}$ for $x=b,c,d$. This is easily done, and we conclude

$$\mathfrak{M}_{h+m+1,k+m+1,m+1}\langle BCD\rangle \lhd \mathfrak{M}_{h,k,m}.$$

Since $\mathfrak{M}_{h,k,m}/\mathfrak{M}_{h+m+1,k+m+1,m+1}\langle BCD\rangle$ is abelian, we have

$$\mathfrak{M}_{h+m+1,k+m+1,m+1}\langle BCD\rangle = \mathfrak{M}'_{h,k,m}.$$ □

Proposition 5. *Let p be an odd prime. Then*

$$\mathfrak{M}_{h,k,m}/\mathfrak{M}'_{h,k,m} \simeq \mathbf{Z}/p^m\mathbf{Z} \times \mathbf{Z}/p^m\mathbf{Z} \times \mathbf{Z}/p^{h+k-m}\mathbf{Z}.$$

Let $p=2$ and $m>1$. Then

$$\mathfrak{M}_{h,k,m}/\mathfrak{M}'_{h,k,m} \simeq \mathbf{Z}/2^{m+1}\mathbf{Z} \times \mathbf{Z}/2^{m+1}\mathbf{Z} \times \mathbf{Z}/2^{h+k-m}\mathbf{Z}.$$

Proof. p odd: $\mathfrak{M}_{h,k,m}$ is generated by $B(p^h)$, $C(p^k)$ and $D(1+p^m)$. It follows that $\mathfrak{M}_{h,k,m}/\mathfrak{M}'_{h,k,m}$ is the direct product of the subgroups generated by $B(p^k)\mathfrak{M}'_{h,k,m}$, $C(p^h)\mathfrak{M}'_{h,k,m}$ and $D(1+p^m)\mathfrak{M}'_{h,k,m}$.

$p = 2$ and $h + k > m$: The structure of $\mathfrak{M}_{h,k,m}/\mathfrak{M}'_{h,k,m}$ is obvious, since $\mathfrak{B}_h$, $\mathfrak{C}_k$ and $\mathfrak{D}_m$ are pro-cyclic with generators $B(2^h)$, $C(2^k)$ and $D(1 + 2^m)$.

$p = 2$ and $h + k = m$: Let the notation be as in the proof of Theorem 4. From $BCd, d^2 \in \mathfrak{M}'_{h,k,m}$ we get $d \equiv BC \pmod{\mathfrak{M}'_{h,k,m}}$, so $\mathfrak{M}_{h,k,m}/\mathfrak{M}'_{h,k,m}$ is generated by b and c. This gives

$$\mathfrak{M}_{h,k,m}/\mathfrak{M}'_{h,k,m} \simeq \mathbf{Z}/2^{m+1}\mathbf{Z} \times \mathbf{Z}/2^{m+1}\mathbf{Z}. \qquad \square$$

Proposition 6. i) *$\mathfrak{M}_{h,k,m}$ is torsion free for $p > 3$.*
ii) *For $p = 3$, $\mathfrak{M}_{h,k,m}$ is torsion free unless $(h, k, m) = (0, 1, 1)$. If $(h, k, m) = (0, 1, 1)$, every torsion element has order 3 and is of the form*

$$\begin{pmatrix} (x-1)/2 & b \\ c & -(x+1)/2 \end{pmatrix}, \quad \text{where } x^2 = 1 - 4(1 + bc).$$

iii) *For $p = 2$, $\mathfrak{M}_{h,k,m}$ is torsion free unless $m = 1$, in which case $-\mathbf{E}$ is a torsion element. If $m = 1$ and $h + k > 1$, $-\mathbf{E}$ is the only torsion element. If $m = 1$ and $h + k = 1$, there are in addition torsion elements of order 4, and any such torsion element is of the form*

$$\begin{pmatrix} x & b \\ c & -x \end{pmatrix}, \quad \text{where } bc \equiv 6 \pmod 8 \text{ and } x^2 = -(1 + bc).$$

Proof. Let $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\widehat{\mathbf{Z}}_\mathrm{p})$, and assume that $\mathbf{A}^{\mathbf{p}^\mathbf{k}} = \mathbf{E}$ for some $k \in \mathbf{N}$. The eigenvalues of $\mathbf{A}$ must be $p^{k\,\mathrm{th}}$ roots of unity, and also roots of the characteristic polynomial $\lambda^2 - (a + d)\lambda + 1$.

If 1 is the only eigenvalue, we have $\lambda^2 - (a + d)\lambda + 1 = \lambda^2 - 2\lambda + 1$, i.e., $a + d = 2$ and $ad = 1 + bc$. We can assume that

$$a = 1 + \sqrt{-bc} \quad \text{and} \quad d = 1 - \sqrt{-bc}.$$

An induction argument gives

$$\mathbf{A}^\mathbf{n} = \begin{pmatrix} 1 + n\sqrt{-bc} & nb \\ nc & 1 - n\sqrt{-bc} \end{pmatrix},$$

so $b = c = 0$ and $\mathbf{A} = \mathbf{E}$.

$p > 3$: The $p^{i\,\mathrm{th}}$ cyclotomic polynomial is irreducible in $\widehat{\mathbf{Z}}_p[X]$ of degree $p^{i-1}(p-1) > 2$ for $i > 0$, so the only possible eigenvalue is 1, and we get $\mathbf{A} = \mathbf{E}$ by the above argument.

$p = 3$: If 1 is the only eigenvalue, we get $\mathbf{A} = \mathbf{E}$ as above. If the eigenvalues are ζ and ζ^{-1}, where ζ is a primitive third root of unity, we get $\lambda^2 - (a + d)\lambda + 1 = \lambda^2 + \lambda + 1$, i.e., $a + d = -1$ and $ad = 1 + bc$. We can assume that

$$a = \frac{-1 + \sqrt{1 - 4(1 + bc)}}{2} \quad \text{and} \quad d = \frac{-1 - \sqrt{1 - 4(1 + bc)}}{2}.$$

Since $a \equiv 1 \pmod{3^m}$ we get $bc \equiv -3 \pmod{3^m}$. $bc \equiv 0 \pmod{3^{h+k}}$ and $h+k \geq m$, so $m = 1$. If $h+k > 1$ we have $1 - 4(1-bc) \equiv -3 \pmod 9$, and since -3 is not a square in $\mathbf{Z}/9\mathbf{Z}$, $1-4(1-bc)$ is not a square in $\widehat{\mathbf{Z}}_3$. Therefore $h+k=1$, i.e., $h=0$ and $k=1$.

Now let $x = \sqrt{1-4(1+bc)}$. Then

$$\mathbf{A} = \begin{pmatrix} (x-1)/2 & b \\ c & -(x+1)/2 \end{pmatrix}$$

and direct calculation shows $\mathbf{A^3} = \mathbf{E}$.

Example: $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ -3 & -2 \end{pmatrix}$.

$p=2$: The eigenvalues are either 1, -1 or primitive fourth roots of unity. If 1 is the only eigenvalue, we have $\mathbf{A} = \mathbf{E}$. If -1 is the only eigenvalue, $-\mathbf{A} \in \mathrm{SL}_2(\widehat{\mathbf{Z}}_2)$ has 1 as its only eigenvalue, hence $-\mathbf{A} = \mathbf{E}$ and $\mathbf{A} = -\mathbf{E}$. This is obviously only possible for $m=1$.

Assume now, that the eigenvalues are primitive fourth roots of unity. Then $\lambda^2 - (a+d)\lambda + 1 = \lambda^2 + 1$, i.e., $a+d=0$. Since $a \equiv d \equiv 1 \pmod{2^m}$, we have $m=1$. We can assume

$$a = \sqrt{-(1+bc)}, \quad d = -\sqrt{-(1+bc)},$$

hence $\mathbf{A^2} = -\mathbf{E}$ and $\mathbf{A}$ has order 4.

Since $-(1+bc) \equiv -1 \pmod 2$, $-(1+bc)$ is a square in $\widehat{\mathbf{Z}}_2$, if and only if $-(1+bc) \equiv 1 \pmod 8$, if and only if $bc \equiv 6 \pmod 8$. Since $bc \equiv 0 \pmod{2^{h+k}}$, we get $h+k=1$.

Example: $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ -2 & -1 \end{pmatrix}$. □

It is now clear, that Whaples' Theorem does not generalize to arbitrary torsion free pro-finite groups: For an odd prime p and a natural number n we get examples of torsion free pro-p-groups with $\mathbf{Z}/p^n\mathbf{Z}$, but not $\mathbf{Z}/p^{n+1}\mathbf{Z}$, as a factor. For $p=2$ and $n \geq 3$ we get examples of torsion free pro-2-groups with $\mathbf{Z}/2^n\mathbf{Z}$, but not $\mathbf{Z}/2^{n+1}\mathbf{Z}$, as a factor.

Unfortunately, these groups do not give us an example of a torsion free pro-2-group with $\mathbf{Z}/4\mathbf{Z}$, but not $\mathbf{Z}/8\mathbf{Z}$, as a factor.

References

[1] Huppert, B.: *Endliche Gruppen I*, Springer 1967.

[2] Kuyk, W.; Lenstra, H.W. Jr.: *Abelian extensions of arbitrary fields.* Math. Ann. **216** (1975), 99–104.

[3] Whaples, G.: *Algebraic extensions of arbitrary fields*, Duke Math. J. **24** (1957), 201–204.