EQUATIONS IN FREE METABELIAN GROUPS

ROGER C. LYNDON[1]

Baumslag and Mahler [1] have shown that, for F a free group and hence $G=F/F''$ a free metabelian group, and p any prime, the relation $a^pb^p=c^p$ cannot hold for elements a, b, and c of G such that aG' and bG' are independent elements of the free abelian group G/G'. In answer to a question they raised, we show by their methods that, if p, q, and r are three primes, not all the same, then there exist solutions of the equation $a^pb^q=c^r$ in G, with a and b independent modulo G'.

We may suppose that $r\neq p$, q. If such a solution exists at all, one exists in G, free metabelian on two generators x and y, and such that, modulo G', $a\equiv x^{mr}$, $b\equiv y^{nr}$, and $c\equiv x^{mp}y^{nq}$, for some positive integers m and n. Let L be the ring of Laurent polynomials over the integers in x and y (that is, admitting both positive and negative integer exponents). Then G' is naturally the free L module with generator $k=x^{-1}y^{-1}xy$, that is, with $u^x=x^{-1}ux$, $u^y=y^{-1}uy$, and $u^{A+B}=u^Au^B$, for all u in G' and A, B in L. In this notation, we have

$$a = x^{mr}k^A, \quad b = y^{nr}k^B, \quad \text{and} \quad c = x^{mp}y^{nq}k^C,$$

for certain elements A, B, and C of L. Let $\Gamma_h(z)$ be the cyclotomic polynomial with roots all primitive hth roots of unity. The condition $a^pb^q=c^r$ reduces by straightforward computation to the condition on A, B, and C that

$$A\Gamma_p(x^{mr})y^{nr} + B\Gamma_q(y^{nr}) = C\Gamma_r(x^{mp}y^{nq}) + D(x, y),$$

where

$$D(x,y) = (1+x+ \cdots + x^{mp-1})(1+y+\cdots+y^{nq-1})x^{-mp}E(x^{mp}, y^{nq}),$$

and

$$E(u, v) = \sum_{i=0}^{r-1} (uv)^i \frac{u^{r-i}-1}{u-1}\,.$$

Collecting terms in $X=x^m$ and $Y=y^n$ gives an equation

$$A_1\Gamma_p(X^r)Y^r + B_1\Gamma_q(Y^r) = C_1\Gamma_r(X^pY^q) + X^{-p}D_1(X, Y)$$

where

Received by the editors October 4, 1965.

[1] Work supported in part by a grant from the National Science Foundation.

$$D_1(X, Y) = \Gamma_p(X)\Gamma_q(Y)E(X^p, Y^q).$$

It is easy to see that, conversely, the existence of a solution A_1, B_1, C_1 of this last equation implies that of a solution of $a^p b^q = c^r$ with a and b independent modulo G'.

It remains, then, to show that D_1 belongs to the ideal in L generated by $\Gamma_p(X^r)$, $\Gamma_q(Y^r)$, and $\Gamma_r(X^p Y^q)$. Since all elements concerned lie in the polynomial ring $Z[X, Y]$, this comes to showing that D_1 belongs to the ideal J of this ring generated by the same three elements. Since $\Gamma_p(X^r) = \Gamma_{pr}(X)\Gamma_p(X)$, the ring $Z[X]/\Gamma_p(X^r)$ decomposes into $Z[X]/\Gamma_{pr}(X)$ and $Z[X]/\Gamma_p(X)$, and $Z[X, Y]/J$ decomposes correspondingly. Since $\Gamma_p(X)$ divides $D_1(X, Y)$, it suffices to consider the first component only. A similar argument for Y enables us to replace J by the ideal J_1 generated by $\Gamma_{pr}(X)$, $\Gamma_{qr}(Y)$, and $\Gamma_r(X^p Y^q)$.

We may identify $Z[X]/\Gamma_{pr}(X)$ with the ring $Z[\xi]$ where ξ is a primitive prth root of unity. Over this ring, $\Gamma_{qr}(Y)$ splits into factors $(Y^q - \omega)/(Y - \omega)$, where ω runs through the $r-1$ primitive rth roots of unity. Therefore $Z[X, Y]$ is a subdirect product of rings $Z[\xi, \eta]$ of algebraic integers, where ξ runs through the primitive prth roots of unity and η through the primitive qrth roots of unity. We shall show that, in each such ring, $\gamma = \Gamma_r(\xi^p \eta^q)$ divides $\delta = \Gamma_p(\xi)\Gamma_q(\eta)E(\xi^p, \eta^q)$.

Both $\omega = \xi^p$ and $\zeta = \eta^q$ are primitive rth roots, and we consider two cases, according as $\omega\zeta = 1$ or not. If $\omega\zeta \neq 1$, then $\omega\zeta$ is a primitive rth root, whence we find that

$$E(\omega, \zeta) = \sum_0^{r-1} \frac{\omega^r \zeta^i - (\omega\zeta)^i}{\omega - 1} = \left(\sum \zeta^i - \sum (\omega\zeta)^i\right)/(\omega - 1) = 0,$$

that $\delta = 0$, and so γ divides δ. Suppose henceforth that $\omega\zeta = 1$. Then $\gamma = \Gamma_r(1) = r$, while

$$E(\omega, \zeta) = \sum \frac{\omega^{-i} - 1}{\omega - 1} = \left(\sum \omega^{-i} - \sum 1\right)/(\omega - 1) = -r/(\omega - 1),$$

and hence

$$\delta = \Gamma_p(\xi)\Gamma_q(\eta)E(\omega, \zeta) = \frac{\omega - 1}{\xi - 1}\,\frac{\omega - 1}{\eta - 1}\,\frac{-r}{\omega - 1} = -r\,\frac{\omega - 1}{(\xi - 1)(\eta - 1)}\,.$$

It suffices to show that $\xi - 1$, and similarly $\eta - 1$, are units. Since ξ has minimal polynomial

$$\Gamma_{pr}(z) = \frac{z^{pr} - 1}{z^p - 1} \bigg/ \frac{z^r - 1}{z - 1},$$

the number $\xi-1$ has minimal polynomial $P(z)=\Gamma_{pr}(z+1)$, and hence norm $P(0)=\Gamma_{pr}(1)=1$, and is therefore a unit. This provides $U(X, Y)$ in $Z[X, Y]$ such that $D_1(\xi, \eta)=U(\xi, \eta)\Gamma_r(\xi^p\eta^p)$ holds for ξ and η as in the case last considered; it is easily checked that the same hold if ξ and η are any roots of $\Gamma_p(X^r)$ and $\Gamma_q(Y^r)$, whence it follows that this equation holds in $Z[X, Y]/(\Gamma_p(X^r), \Gamma_q(Y^r))$, and that D_1 is in J. This completes the proof.

Bibliography

1. Gilbert Baumslag and Kurt Mahler, *Equations in free metabelian groups*, Michigan Math J. **12** (1965), 417–420.

Queen Mary College, London and
University of Michigan