A NOTE ON THE CUP PRODUCT FOR PRO-p GROUPS

TILMANN WÜRFEL

(Communicated by Bhama Srinivasan)

ABSTRACT. Let $G$ be a pro-$p$ group and $g \in H^1(G)$. We give a group-theoretic description of the kernel of the cup product $\cup g : H^1(G) \to H^2(G)$.

In this note we exhibit a connection between the cup product $H^1(G) \times H^1(G) \to H^2(G)$ for a pro-$p$ group $G$ and certain subgroups of its Frattini group $G^*$. A typical result is the following (Corollary 1): If $S$ and $T$ are two different maximal subgroups of $G$, then $H^1(G/S) \cup H^1(G/T) = 0$ in $H^2(G)$ if and only if $S^*T^* \neq G^*$. We actually compute the annihilator of $H^1(G/S)$, with respect to the cup product, as $H^1(G/S)$ where $S$ is determined by certain commutator conditions (Proposition 1).

We use standard notations. The basic facts about pro-$p$ groups and their cohomology used here can be found in [1]. In particular, $p$ always denotes a prime, $G_i$ is the descending central series of a pro-$p$ group $G$, $G^* = GPGG^2$, $W(G) = H^1(G, 2/(p))$, $[x, y] = x^{-1}y^{-1}xy$, and $(\cdots)$ denotes closed subgroups.

PROPOSITION 1. Let $G$ be a pro-$p$ group and $S$ a maximal subgroup of $G$. Fix an element $g \in H^1(G)$ such that $S = \text{Ker}(g)$ and let $A_S = \{f \in H^1(G) | f \cup g = 0\}$. Denote by $\tilde{S}$ the subgroup $S^*(G^p)G^3$ if $p$ is odd, or $S^*G^2$ if $p = 2$. Then $A_S = H^1(G/\tilde{S})$, where $\tilde{S} = \{s \in S | [G, s] \subset \tilde{S}\}$ if $p$ is odd or if $p = 2$ and $S^*G^2 \neq G^*$, and $\tilde{S} = \{x \in G | [G, x] \subset S\}$ if $p = 2$ and $S^*G^2 = G^*$.

The proof will follow from Proposition 2. First, we need some information about certain maximal subgroups of the Frattini group.

LEMMA. Let $G$ be a pro-$p$ group and $S \leq G$ a maximal subgroup.

(a) If $T \leq G$ is a maximal subgroup different from $S$, then $S^*T^*$ is maximal in or equal to $G^*$ and contains $G_3$. If $p$ is odd, then $G^p \subset S^*T^*$. If $p = 2$ and $S^*T^* \neq G^*$, then $G_2 \not\leq S^*T^*$.

(b) Let $p$ be odd. If $W \leq G^*$ is a maximal subgroup containing $S^*(G^p)G_3$, then there exists a maximal $T \leq G$ such that $T \neq S$ and $W = S^*T^*$.

(c) Let $p = 2$. Every maximal subgroup $W \leq G^*$ such that $S^*G_3 \leq W$ and $G_2 \not\leq W$ is of the form $W = S^*T^*$ with some maximal $T \leq G$ different from $S$.

(d) $S^*G_2$ is maximal in or equal to $G^*$; if $p = 2$, then this depends on whether or not $g \cup g$ is zero where $g \in H^1(G)$ with $\text{Ker}(g) = S$.
PROOF. Everything follows from the congruence (cf. [1, Proposition 5])

\[(st)^p \equiv sp^t p[t, s] \mod (G^*)^p \]  

where \([G^*, G] = (G_2)^p G_3\).

(a) To see that \(G_3 \leq S^* T^*\), let \(\overline{G} = G/S^* T^*\). Since \(G = ST\), we can write \(\overline{G} = \overline{S} \overline{T}\) with \(\overline{S}, \overline{T}\) abelian and normal in \(\overline{G}\). So \(\overline{G_2} = [\overline{S}, \overline{T}] \leq \overline{S} \cap \overline{T}\) which is contained in the center of \(\overline{G}\). Hence \(G_3 = 1\).

Now pick an element \(t \in T \setminus S\) and define the map \(k: G \to G^*/S^* T^*\) by \(k(x) = [t, x]\). Since \(G_3 \leq S^* T^*\), \(k\) is homomorphism with \(T \leq \text{Ker}(k)\). If \(p\) is odd, then (1) yields \(G^p \subset S^* T^*\). Since \(G = \langle t \rangle S\), we can write \(G_2 = [G, S] = [t, S] S_2 G_3\) which implies that \(k\) is surjective. So \(S^* T^*\) is maximal in or equal to \(G^*\) if \(p\) is odd. If \(p = 2\), surjectivity of \(k\) follows from the congruence \((ta)^2 \equiv t^2 a^2 [s, t^a] \equiv [t, s^{-a}] \mod S^* T^*\). Still in the case \(p = 2\), assume that \(G_2 \leq S^* T^*\). Then the congruence \((st)^2 \equiv s^2 t^2 [s, t] \equiv 1 \mod S^* T^*\) shows that \(S^* T^* = G^*\).

(b) Since \(G^p \subset W\), \(G_2 = [G, S] \not\subset W\) and so there is a \(t \in G\) with \([t, S] \not\subset W\). Then \(t \not\in S\) and the map \(k: G \to G^*/W\) with \(k(x) = [t, x]\) is an epimorphism as in part (a) of the proof. The subgroup \(T = \text{Ker}(k)\) is maximal in \(G\) and different from \(S\). Using \(T = \langle t \rangle (T \cap S)\) we deduce that \(T_2 \leq W\), so \(S^* T^* = W\) by (a).

(c) As in the proof of (b) there is an element \(u \in G\) so that \([u, S] \not\subset W\). The homomorphism \(k: G \to G^*/W\) defined by \(k(x) = [u, x]\), is then surjective on \(S\) already. So there is an element \(s \in S\) with \([u, s] \equiv u^{-2} \mod W\). Let \(t = su\). We then have \(t^2 \equiv s^2 u^2 [u, s] \equiv 1 \mod W\) by (1) and because \(G_3 \leq W\). The modified homomorphism \(\tilde{k}: G \to G^*/W\) with \(\tilde{k}(x) = [t, x]\) now furnishes the required maximal subgroup \(T = \text{Ker}(\tilde{k})\) of \(G\). Indeed, for \(y \in S\) we have \([t, y] = [s, y] [s, y], u [u, y] \equiv [u, y] \mod S_2\), hence \(\tilde{k}\) and \(k\) coincide on \(S\), \(t \not\in S\), and \(\tilde{k}\) is surjective. It remains to verify that \(T^2 \subset W\). Write \(v \in T = v = t^u y\) with \(y \in T \cap S\). Then \(v^2 \equiv t^u y^2 [y, t^a] \equiv [t, y^{-a}] \equiv 1 \mod W\).

(d) The assignment \(x \mapsto x^p\) induces an epimorphism \(G \to G^*/S^* G_2\) whose kernel contains \(S\). To prove the second statement, let \(p = 2\) and consider the five term cohomology sequence associated with the group extension \(1 \to S \to G \to \overline{G} \to 1\) where \(\overline{G} = G/S\), together with the respective cup product homomorphisms \(\cup_G\) and \(\cup_{\overline{G}}:\)

\[
\begin{array}{ccccccc}
H^1(G) & \overset{r}{\longrightarrow} & H^1(S) & \longrightarrow & H^2(\overline{G}) & \longrightarrow & H^2(G) \\
\cup_{\overline{G}} \uparrow \downarrow & & & & & & \uparrow \cup_G \\
H^1(\overline{G}) \otimes \mathbb{Z}/2 & \longrightarrow & H^1(G) \otimes \mathbb{Z}/2 \\
\end{array}
\]

Since \(H^2(\overline{G}) = \mathbb{Z}/(2)\) and \(\cup_{\overline{G}}\) is an isomorphism, we see that \(g \cup_G g = 0\) if and only if the restriction \(r\) is not surjective which in turn is equivalent to \(G^* \neq S^* G_2\). □

PROPOSITION 2. Using the notation of Proposition 1, there is an exact sequence induced by the differential

\[0 \to K_S \to A_S \xrightarrow{d} H^1(G^*/S) \to 0,\]

where \(K_S = H^1(G/S)\) if \(p\) is odd, and \(K_S = 0\) if \(p = 2\).

PROOF. We begin by constructing the homomorphism \(d: A_S \to H^1(G^*)\). If \(f \in A_S\), then there is a continuous map \(d_f: G \to \mathbb{Z}/(p)\) such that

\[(2) \quad f(x) g(y) = d_f(x) + d_f(y) - d_f(xy) \quad \text{for all } x, y \in G.\]
It follows that $d_f$ is multiplicative on $S$ as well as on $\text{Ker}(f)$. So, in particular, the restricted map $d_f |_{G^*}$ lies in $H^1(G^*)$. If $\tilde{d}_f$ is another map satisfying (2), then $d_f - \tilde{d}_f$ is in $H^1(G)$ and hence vanishes on $G^*$. We can thus define the map $d$ by setting $d(f) = d_f |_{G^*}$. By the linearity of (2), $d$ is a homomorphism.

We show next that $\text{Ker}(d) \subset H^1(G/S)$. Assume $d(f) = 0$, i.e., $d_f(G^*) = 0$. Since $d_f |_{S} \in H^1(S)$, there is then a map $c \in H^1(G)$ such that $c |_{S} = d_f |_{S}$. The modified map $\tilde{d}_f = d_f - c$ satisfies (2) and vanishes on $S$. So we may assume that $d_f(S) = 0$. We want to show that $f(S) = 0$. To this end, pick some $s \in S$ and let $z \in G$ be such that $g(z) = 1 \in \mathbb{Z}/(p)$. Then, by (2), $f(s) = d_f(z) - d_f(sz)$ and also $d_f(sz) = d_f(zs^p) = d_f(z)$. Hence $f(s) = 0$.

If $p$ is odd, then the formula $g(x)g(y) = \frac{1}{2}(g(xy)^2 - g(x)^2 - g(y)^2)$ shows that $d(g) = 0$. Hence $\text{Ker}(d) = H^1(G/S)$ in this case.

Let $p = 2$. If $g \cup g \neq 0$, then $H^1(G/S) \cap A_S = 0$ and so $\text{Ker}(d) = 0$ by the above. If $g \cup g = 0$, then (2) implies that $g(x) = g(x^2) = d_g(x^2)$ for all $x \in G$. But $G^* = (G^2)$ in this case (by (1)), hence $d(g) \neq 0$ and $\text{Ker}(d) = 0$.

To see that $d$ actually lands in $H^1(G^*/S)$, let $f \in A_S \setminus \text{Ker}(f)$ and put $T = \text{Ker}(f)$. Then $d_f(S^*T^*) = 0$. If $T \neq S$, then $\tilde{S} \leq S^*T^*$ by (a) of the Lemma. If $T = S$, then $p = 2$ and we may assume $f = g$. Thus $g \cup g = 0$ and (2) implies that $d_g(xy) = d_g(yx)$ for all $x, y \in G$. Since $d_g |_{S}$ is a homomorphism, it follows that $d_g([s, x]) = d_g(s^{-1}) + d_g(s^2) = 0$ for all $s \in S$, $x \in G$. Hence $d_g(G^2) = 0$ and, in particular,

$$(3) \quad d_g(\tilde{S}) = 0.$$

To show that $d(A_S) = H^1(G^*/\tilde{S})$, we deal with odd $p$ first. Let $0 \neq \varphi \in H^1(G^*)$ be such that $\varphi(\tilde{S}) = 0$. We want to produce an $f \in H^1(G)$ such that $f \cup g = 0$ and $d(f) = \varphi$. Let $z \in G$ be such that $g(z) = 1$ and define $f$ by $f(x) = \varphi([z, x])$. Then $f \in H^1(G)$ because $G_2 \leq \tilde{S}$. Let $\theta = \sigma_\pi$ where $\pi: G \rightarrow G/S$ is the natural map and $\sigma: G/S = \langle \tilde{z} \rangle \rightarrow G$ is the section defined by $\sigma(\tilde{z}^i) = z^i$ for $i = 1, \ldots, p - 1$. Since $G/S$ is $p$-elementary, we may assume that $\varphi$ is actually in $H^1(S)$, and can thus define a continuous map $c: G \rightarrow \mathbb{Z}/(p)$ by setting $c(x) = \varphi(\theta(x)^{-1}x)$. Then $c(xs) = c(x) + \varphi(s)$ for all $x \in G$, $s \in S$. So $c |_{G^*} = \varphi$. We want to show that $f(x)g(y) = c(x) + c(y) - c(xy)$ for all $x, y \in G$. Write $x = z^ir$ and $y = z^js$ where $0 \leq i, j \leq p - 1$ and $r, s \in S$. Then $f(x)g(y) = jf(x)$ and

$$c(x) + c(y) - c(xy) = \varphi(r) + \varphi(s) - c(z^irz^j) - \varphi(s) = \varphi(r) - c(z^irz^j).$$

Write $i + j = ap + m$ with $0 \leq m \leq p - 1$. Then $z^irz^j = z^mz^{mp}[r, z^i]$ and, since $\varphi(z^p) = 0$, $c(z^irz^j) = \varphi(r) + \varphi([r, z^i]) = \varphi(r) - jf(r)$ which is what we need because $f(r) = f(x)$.

To end the proof, let $p = 2$ and let $\varphi$ be as above. If $G_2 \notin \text{Ker}(\varphi)$, then, by (c) of the Lemma, $\text{Ker}(\varphi) = T^*S^*$ with some maximal $T \leq G$ different from $S$. So there is an element $z \in T$ such that $g(z) = 1$. Then $\varphi(z^2) = 0$ and we can proceed as above. If $G_2 \leq \text{Ker}(\varphi)$, then $\text{Ker}(\varphi) = S^*G_2$ and $g \cup g = 0$ by (d) of the Lemma. In this case, by (3), we have $d_g(\tilde{S}) = 0$. Since $d_g(G^*) \neq 0$, it follows that $d_g |_{G^*} = \varphi$. □
COROLLARY 1. Let $G$ be a pro-$p$ group and $f, g \in H^1(G)$ be linearly independent with $T = \text{Ker}(f)$, $S = \text{Ker}(g)$. Then $f \cup g = 0$ if and only if $S^*T^* \neq G^*$. Hence $f \cup g \neq 0$ if $G$ is abelian.

PROOF. $S \neq T$ by assumption. If $f \cup g = 0$, then, by Proposition 2, $\varphi = d(f) \neq 0$. Since $\varphi(S^*T^*) = 0$, we have that $S^*T^* \neq G^*$. Conversely, if this latter condition holds, then there is a nonzero $\varphi \in H^1(G^*)$ with $\varphi(S^*T^*) = 0$. If $p = 2$, then $G_2 \notin \text{Ker}(\varphi)$ by (a) of the Lemma. Define $\tilde{f} \in H^1(G)$ by $\tilde{f}(x) = \varphi([z, x])$ where $z \in T$ is such that $g(z) = 1$. Then $\tilde{f}(T) = 0$, so $\tilde{f} = af$ with some $a \in \mathbb{Z}/(p)$. By the proof of Proposition 2, we have $\tilde{f} \cup g = 0$ and $d(\tilde{f}) = \varphi \neq 0$. Hence $a \neq 0$ and $f \cup g = 0$. $\square$

COROLLARY 2. Let $G$ be a pro-$p$ group of finite rank with minimal pro-$p$ free presentation $1 \to R \to F \xrightarrow{\pi} G \to 0$. Let $S \leq G$ be a maximal subgroup and put $U = \pi^{-1}(S)$. Then $H^1(G/S)$ is contained in the radical of the cup product $H^1(G) \times H^1(G) \to H^2(G)$ if and only if $R \leq U^*(F^p)F^3$ if $p$ is odd, or $R \leq U^*F^3$ if $p = 2$.

PROOF. Define $\tilde{S}$ and $\tilde{U}$ as in Proposition 1. Then $\pi$ induces an epimorphism $\tilde{\pi}: F^*/\tilde{U} \to G^*/\tilde{S}$ whose kernel is $R\tilde{U}/\tilde{U}$. Therefore, $R \leq \tilde{U}$ if and only if the groups $F^*/\tilde{U}$ and $G^*/\tilde{S}$ are of the same rank. Let $n$ denote the rank of $G$ and $F$. Since $H^2(F) = 0$, Proposition 2 shows that the rank of $F^*/\tilde{U}$ is $n - 1$ if $p$ is odd and $n$ if $p = 2$. On the other hand, $H^1(G/S)$ is contained in the radical of the cup product for $G$ if and only if $\text{As} = H^1(G)$ which, by Proposition 2, is equivalent to $G^*/\tilde{S}$ having rank $n - 1$ if $p$ is odd and rank $n$ if $p = 2$. $\square$

PROOF OF PROPOSITION 1. We refer to the proof of Proposition 2. Let $z \in G$ be such that $g(z) = 1$. The map $s \mapsto [z, s]$ then induces a homomorphism $k: S/G^* \to G^*/\tilde{S}$ which does not depend on the choice of $z$. By the second part of the proof of Proposition 2, the following diagram is commutative:

$$
\begin{array}{ccc}
A_S & \xrightarrow{d} & H^1(G^*/\tilde{S}) \\
\downarrow & & \downarrow \tilde{k} \\
H^1(G) & \xrightarrow{r} & H^1(S/G^*)
\end{array}
$$

where $\tilde{k}$ is the dual of $k$ and $r$ is restriction. The snake lemma applied to this diagram enlarged by the appropriate kernels and cokernels now yields that $A_s = H^1(G/\tilde{S})$ if $p$ is odd, or if $p = 2$ and $S^*G_2 \neq G^*$, hence $H^1(G^*/S^*G_2) = H^1(G/S)$.

If $p = 2$ and $S^*G_2 = G^*$, then, in a way similar to the proof of (c) of the Lemma, an element $z \in G$ such that $g(z) = 1$ can be found which satisfies $z^2 \in \tilde{S}$. Let $k: G \to G^*/\tilde{S}$ be the homomorphism induced by $x \mapsto [z, x]$. Then the proof of Proposition 2 shows that

$$
\begin{array}{ccc}
A_S & \xrightarrow{d} & H^1(G^*/\tilde{S}) \\
\downarrow & & \downarrow k \\
H^1(G)
\end{array}
$$

is commutative. Hence $A_S = H^1(G/\tilde{S})$ in this case, too. $\square$
Remark. Let $p$ be an odd prime and $G$ a pro-$p$ group with a maximal subgroup $S$. By Proposition 2, the annihilator $A_S$ with respect to the cup product, of $H^1(G/S)$ in $H^1(G)$ is smallest possible, i.e., $A_S = H^1(G/S)$, exactly when $G^* = S_2(G^p)G_3$. Let (C) denote this condition if it holds for all maximal $S \leq G$. It is obviously satisfied if $G_2 \leq (G^p)$ in which case $G$ is called powerful in [2]. The converse holds if the rank $n_G$ of $G$ is $\leq 3$, but fails for $n_G = 4$.

Proof. (i) Let $G$ satisfy (C) and $n_G \leq 3$. We can assume that $G^p = 1$ and $G_3 = 1$ because $G$ satisfies (C) if and only if $G/(G^p)G_3$ does, and the same is true for powerfulness. So it remains to show that $G$ is abelian. We have $S_2 = G_2$ for all maximal $S \leq G$. This settles the case $n_G = 2$ because $S/S_2 \hookrightarrow G/G_2$ implies that $n_S = n_G - 1 = 1$, hence $S_2 = 1$. Now let $n_G = 3$, $G = \langle x_1, x_2, x_3 \rangle$, and assume that $G_2 \neq 1$. Then $G_2 = \mathbb{Z}/(p)$ by using some maximal subgroup as above. Let $G_2 = \langle [x_1, x_2] \rangle$, say. Then $[x_3, x_1] = [x_2, x_1]^a = [x_3^a, x_1]$ for some $a \in \mathbb{Z}$. Let $\tilde{x}_3 = x_3 x_2^{-a}$. Then $[\tilde{x}_3, x_1] = 1$ and $G = \langle x_1, x_2, \tilde{x}_3 \rangle$. The subgroup $S = (x_1, \tilde{x}_3)G_2$ is maximal because $G = \langle x_2 \rangle S$, but $S_2 = 1$.

(ii) Let $G = \langle x_1, x_2, x_3, x_4 \rangle$ satisfy the relations $G^p = 1$, $G_3 = 1$, $\langle (x_1, x_2), (x_3, x_4) \rangle = 1$, and $[x_1, x_2] = [x_3, x_4]$ ($\neq 1$). Then $G$ is not powerful. Since $G_2 = \mathbb{Z}/(p)$, condition (C) just means that $S_2 \neq 1$ for all maximal $S \leq G$. Assume there is an $S$ with $S_2 = 1$. Then $S = C_G(s)$, the centralizer of any $s \in S$ which is not in the center $Z(G)$. We have that $x_1 \notin S$ because otherwise, since $x_1 \notin Z(G)$, $x_3$ and $x_4$ would be in $S$ and would hence commute. Therefore, $G = \langle x_1 \rangle S$ and $x_2 = x_1^a s$ for some $a \in \mathbb{Z}$, $s \in S$. Then $s = x_1^{-a} x_2 \notin Z(G)$ because $[s, x_1] = [x_2, x_1]$. But $x_3, x_4 \in C_G(s) = S$ which is impossible. □


References

2. A. Lubotzky and A. Mann, Powerful $p$-groups, preprint.

Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802

Current address: Pennsylvania State University, Delaware County Campus, Media, Pennsylvania 19063