Can. J. Math., Vol. XXX, No. 1, 1978, pp. 161–163

A NOTE ON SUBNORMAL SUBGROUPS OF DIVISION ALGEBRAS

GARY R. GREENFIELD

Let D be a division algebra and let D^* denote the multiplicative group of nonzero elements of D. In [**3**] Herstein and Scott asked whether any subnormal subgroup of D^* must be normal in D^*. Our purpose here is to show that division algebras over certain p-local fields do not satisfy such a "subnormal property".

Definition. We say a division algebra D satisfies the *subnormal property* if whenever $H \lhd G$ and $G \lhd D^*$ then $H \lhd D^*$.

Let K be a p-local field, and for convenience assume p is an odd prime, $p > 3$. Let D be a K-division ring (a division algebra central over K) of index $n > 1$. Our goal is to prove D does not satisfy the subnormal property.

If $|\bar{K}| = q$, then D contains a unique unramified extension $L = K(\epsilon)$ where ϵ is a primitive $q^n - 1$st root of unity. D is a cyclic crossed product $D \cong (L, \sigma, \lambda)$ where λ is a fixed prime element of K and $\langle \sigma \rangle \cong \mathrm{Gal}(L/K)$. The rings of integers of K, L, D will be denoted O_K, O_L, O_D, their unique maximal ideals by P_K, P_L, P_D and their groups of units by U_K, U_L, and U_D. We note that $O_K/P_K \cong GF(q)$ while $O_L/P_L \cong O_D/P_D \cong GF(q^n)$. This fact plays an important role in the sequel.

Let N be the reduced norm of D^* and let $|\ |$ be any nontrivial valuation of K. Then N induces a valuation on D^* via $|\alpha|_D = |N(\alpha)|^{1/n}$. The kernel G_0 of the homomorphism N is the normal subgroup of D^* consisting of those elements of reduced norm one. By [**4**, Lemma 5] $G_0 \subset U_D$. Set $U_D{}^0 = U_D$ and for any integer $j \geqq 1$ define $U_D{}^j = \{\alpha \in U_D | \alpha \equiv 1 \bmod P_D{}^j\}$. For any integer $r \geqq 0$ we define, as in [**4**], the "congruence subgroups" of G_0 by setting

$$H_r = \{\alpha \in G_0 | \alpha \equiv 1 \bmod P_D{}^r\}, \text{ and}$$

$$G_r = \{\alpha \in G_0 | \alpha \equiv \beta \bmod P_D{}^r \text{ for some } \beta \in U_K\}.$$

Clearly, H_r, G_r are subgroups of G_0 and, as is evident from the definition, $H_r, G_r \lhd G_0$. We shall be interested in these subgroups principally when $n \nmid r$.

Assume $n \nmid r$. For $\alpha \in U_K U_D{}^r$ write $\alpha \equiv a + b\pi^r \bmod P_D{}^{r+1}$ where $a \in U_K$, $b \in O_L$, and π is a generator for P_D. Define

$$\rho_r : U_K U_D{}^r \rightarrow O_D/P_D$$

Received November 24, 1976.

via $\rho_r(\alpha) = a^{-1}b + P_D$. One checks ρ_r is a well-defined (additive) homomorphism. Since ρ_r restricted to H_r (respectively G_r) is surjective [**4**, Lemma 6] and has kernel H_{r+1} (respectively G_{r+1}) we have:

LEMMA 1. $H_{r+1} \lhd H_r, G_{r+1} \lhd G_r$, *and* $G_r/G_{r+1} \cong H_r/H_{r+1} \cong O_D/P_D \cong GF(q^n)$.

Viewing $GF(q^n)$ as an additive abelian group, it is isomorphic to a direct sum of n copies of $GF(q)$. Let G be the preimage under ρ_r restricted to H_r of one such copy. Then by the Correspondence Theorem for group homomorphisms it follows that $H_{r+1} \subset G \subset H_r$ where the inclusions are proper and $G \lhd H_r$.

LEMMA 2. $H_r, G_r \lhd D^*$.

Proof. If $r = 0$, then $G_0 = H_0$ and we know $G_0 \lhd D^*$. For $r \geqq 1$ we prove that $G_r \lhd D^*$ as the proof for H_r is identical. Let $\alpha \in G_r$ so $\alpha \equiv \beta \bmod P_D{}^r$ for some $\beta \in U_K$. Thus $\alpha - \beta \in P_D{}^r$. If $r = 1$, then since $P_D = \{\eta \in D \mid |\eta|_D < 1\}$ and N is invariant under conjugation it follows that $\gamma(\alpha - \beta)\gamma^{-1} \in P_D$ for any $\gamma \in D^*$. Then by induction on r one obtains $\gamma(\alpha - \beta)\gamma^{-1} \in P_D{}^r$ for any $\gamma \in D^*$. So $\gamma\alpha\gamma^{-1} - \beta \in P_D{}^r$ and the result follows.

Definition. A subgroup M of G_0 is of *level* s if $M \subset G_s$ but $M \not\subset G_{s+1}$.

PROPOSITION 3. *The subnormal property does not hold for D.*

Proof. We first show our G (as constructed above) is of level r. Since $H_r \subset G_r$ it suffices to show $G \not\subset G_{r+1}$. If not, G is contained in the kernel of ρ_r restricted to G_r and in H_r. Thus G is contained in the kernel of ρ_r restricted to H_r. But the latter is H_{r+1} so $G \subset H_{r+1}$ contrary to assumption. Now suppose D satisfies the subnormal property. Then since $G \lhd H_r$ and $H_r \lhd D^*$ we must have $G \lhd D^*$. In particular, $G \lhd G_0$. But by [**4**, Theorem 15] we must have $H_r \subset G \subset G_r$, a contradiction. Thus $G \ntriangleleft D^*$.

We conclude with an example to show that the subnormal property holds for the case $p = \infty$. Here the only possible division algebra is the real quaternions.

Example. The subnormal property holds for U_R, the division ring of real quaternions.

Proof. We first determine the normal subgroups of $U_R{}^*$. Let G_0 be the kernel of the usual sum of squares norm of $U_R{}^*$, i.e., the quaternions of norm one. Suppose H is a finite subgroup of $U_R{}^*$, with H not contained in the center, $Z(U_R)$. Note that this implies $|H| > 2$ and $H \subset G_0$. If $\alpha \in H, \alpha \notin Z(U_R)$ then [**2**, Theorem 1] α has an infinite number of distinct conjugates, say $\{\gamma_j\alpha\gamma_j{}^{-1}\}$, in U_R. Then $\{\delta_j\alpha\delta_j{}^{-1}\}$ where $\delta_j = \gamma_j/(N(\gamma_j))^{1/2}$ is an infinite number of distinct conjugates in G_0. This shows $H \ntriangleleft U_R{}^*$ and $H \ntriangleleft G_0$. Now, G_0 modulo its center, $\langle -1 \rangle$, is isomorphic to the special orthogonal group SO_3 [**5**, p. 115] which is simple [**1**, Theorems 4.8 and 4.9, p. 163 and 165]. Thus a composition series for G_0 is $\{SO_3, C_2\}$. Suppose $H \lhd G_0$ is an infinite group. If $-1 \in H$, H contains the kernel of $\rho : G_0 \rightarrow SO_3$ so $H = G_0$. If $-1 \notin H$, then the cosets of H in G_0 must be H and $-H$. But then either $i \in H$ or $-i \in H$ so in either case the square $-1 \in H$, a contradiction. This shows the only proper normal subgroups of G_0 are $\langle 1 \rangle$ and $\langle -1 \rangle$.

Claim. $G \lhd U_R^*$ if and only if $G \subset Z(U_R)$ or $G \supset G_0$.

Proof. Clearly if either condition is satisfied $G \lhd U_R^*$. Suppose $G \lhd U_R^*$. Then $G \cap G_0 \lhd G_0$. If $G \cap G_0 = G_0$ then $G \supset G_0$ as required. If $G \cap G_0 = \langle 1 \rangle$ then for fixed $\alpha \in G$ and any $\beta \in G_0$, $\alpha(\beta\alpha^{-1}\beta^{-1}) \in G \cap G_0$ so $\alpha\beta = \beta\alpha$. Thus α commutes with G_0 and hence with U_R, so $\alpha \in Z(U_R)$. Finally if $G \cap G_0 = \langle -1 \rangle$ and there exists $\alpha \in G$, $\alpha \notin Z(U_R)$ choose distinct conjugates $\beta_j\alpha\beta_j^{-1}$, $1 \leqq j \leqq 3$ of α in U_R. Then since $(\beta_j\alpha\beta_j^{-1})\alpha^{-1} \in G \cap G_0$ we have, without loss of generality, $\beta_1\alpha\beta_1^{-1}\alpha^{-1} = \beta_2\alpha\beta_2^{-1}\alpha^{-1}$ and so $\beta_1\alpha\beta_1^{-1} = \beta_2\alpha\beta_2^{-1}$, a contradiction. Thus in this case we must also have $G \subset Z(U_R)$.

Assume $H \lhd G$ and $G \lhd U_R^*$. Then we know either $G \subset Z(U_R)$ or $G \supset G_0$. If $G \subset Z(U_R)$ then $H \subset Z(U_R)$ so $H \lhd U_R^*$. If $G \supset G_0$ and $H \supset G_0$ then $H \lhd U_R^*$ so we need only consider the case where $G \supset G_0$ and $H \cap G_0 \neq G_0$. Then $H \cap G_0 \lhd G_0$ so $H \cap G_0 = \langle -1 \rangle$ or $\langle 1 \rangle$ and the proof of the above claim shows $H \subset Z(U_R)$ so $H \lhd U_R^*$.

References

1. E. Artin, *Geometric algebra* (Interscience Publishers Inc., New York, 1957).

2. I. N. Herstein, *Conjugates in division rings*, Proc. Amer. Math. Soc. *2* (1956), 1021–1022.

3. I. N. Herstein and W. R. Scott, *Subnormal subgroups of division rings*, Can. J. Math. *15* (1963), 80–83.

4. C. Riehm, *The norm 1 group of p-adic division algebra*, Amer. J. Math. *92* (1970), 499–523.

5. N. E. Steenrod, *The topology of fibre bundles* (Princeton University Press, Princeton, 1951).

Wayne State University,
Detroit, Michigan