ON p-REGULAR EXTENSIONS OF LOCAL FIELDS[1]

WALTER FEIT

1. Let K be a complete field with respect to a discreet valuation,[2] and suppose that the residue class field of K is finite and has characteristic p. A group which is finite and whose order is not divisible by p is said to be p-regular. A normal extension of K whose Galois group is p-regular will be called a p-regular extension of K. The object of this paper is to characterize those groups which are Galois groups of p-regular extensions of K, and to give a criterion for deciding how many p-regular extensions of K have a given group as Galois group.

It will be necessary to make use of a result closely related to a theorem of Iwasawa [**2**, Theorem 2, p. 463].

THEOREM 1. *Let K be a complete field with respect to a discreet valuation whose residue class field is finite and contains $q=p^f$ elements. Let $H(q)$ denote the group generated by two elements x, y which satisfy the relation $y^{-1}xy=x^q$, and no other that does not follow from this one. Then there is a one to one correspondence between normal subgroups N of $H(q)$ with the property that $H(q)/N$ is p-regular, and p-regular extensions L of K. The correspondence is such that N corresponds to L if and only if $H(q)/N$ is the Galois group of L over K.*

Since a p-regular extension is obviously tamely ramified, this is an immediate consequence of [**2**, Theorem 2], in the case that K is a p-adic number field. An argument essentially the same as that given in [**2**] can be used to prove the theorem above in its more general form.

Šafarevič has proved an analogous result for p-extensions in the case that K is a p-adic number field which does not contain the pth roots of unity (see [**3**]). There is one remarkable difference between the two results. The group $H(q)$ in the above theorem depends only on the number q of elements in the residue class field and is independent of the degree n_0 of K over the field K_0 of p-adic rationals. The analogous group constructed in [**3**] for p extensions depends on n_0 but is independent[3] of q. Šafarevič uses his result to show that if

Received by the editors November 10, 1958.

[1] This research was supported by the United States Army, contract No. DA-30-115-ORD-976.

[2] Throughout this paper the term valuation is used in the sense of [**1**], i.e. one dimensional valuation.

[3] The group is the free group on n_0 generators.

G, $\bar{G}$ are Galois groups of p-extensions of K (where K is a p-adic number field not containing the pth roots of unity), and $\bar{G}$ is the homomorphic image of G under a fixed homomorphism, then for any normal extension of K with Galois group $\bar{G}$ there exists a normal extension of K with Galois group G such that the given homomorphism of G onto $\bar{G}$ is the natural homomorphism of Galois theory. This last statement is no longer true if G, $\bar{G}$ are p-regular groups, even if K is a p-adic number field. A counter example is given below.

2. For integers a, b, c let $N(a, b, c)$ be the subgroup of $H(q)$ defined by: $N(a, b, c) \cap \{x\} = \{x^a\}$, $N(a, b, c) = \{x^a, y^b x^c\}$. We will be interested in considering ordered triples of integers a, b, c satisfying the conditions

$$(*) \qquad 0 \leqq c < a,\ 0 < b,\ (b, q) = 1,\ c(q-1) \equiv q^b - 1 \equiv 0 \pmod{a}.$$

Lemma. *If a, b, c are integers satisfying (*), then $N(a, b, c)$ is a normal subgroup of $H(q)$ whose index in $H(q)$ is ab. Conversely if N is a normal subgroup of $H(q)$ with the property that $H(q)/N$ is p-regular, then there exists a triple of integers a, b, c satisfying (*) such that $N = N(a, b, c)$. Furthermore if a', b', c' is another triple of integers satisfying (*), then $N(a, b, c) = N(a', b', c')$ if and only if $a = a'$, $b = b'$, $c = c'$.*

Proof. Obviously xx^ax^{-1}, $y^{-1}x^ay$ are in $N(a, b, c)$. Suppose that a, b, c is a triple of integers satisfying condition (*), then the relations $xy^bx^cx^{-1} = y^bx^cx^{q^b-1}$ and $y^{-1}y^bx^cy = y^bx^{cq} = y^bx^cx^{c(q-1)}$ imply that $xN(a, b, c)x^{-1}$ and $y^{-1}N(a, b, c)y$ are both contained in $N(a, b, c)$. The defining relation of $H(q)$ can be used to show that for any non-negative integer k, $(y^bx^c)^k = y^{kb}x^{c\{1+q^b+\cdots+q^{b(k-1)}\}}$.

The conditions (*) imply that

$$c\{1 + q^b + \cdots + q^{b(k-1)}\} \equiv kc \pmod{a},$$

hence $(y^bx^c)^a = y^{ab}x^{ma}$ for some integer m. Therefore y^{ab} is in $N(a, b, c)$. For any z in $N(a, b, c)$, $z_1 = y^{ab}zy^{-ab}$ and $z_2 = x^{-a}zx^a$ both lie in $N(a, b, c)$, hence $yzy^{-1} = y^{-(ab-1)}z_1y^{ab-1}$ and $x^{-1}zx = x^{a-1}z_2x^{-(a-1)}$ are in $N(a, b, c)$. Consequently $N(a, b, c)$ is a normal subgroup of $H(q)$. The index of $N(a, b, c)$ in $H(q)$ equals $[H(q) : N(a, b, c)\{x\}][N(a, b, c)\{x\} : N(a, b, c)] = ab$.

To prove the converse, let x^a be the smallest positive power of x in[4] N, hence $N \cap \{x\} = \{x^a\}$. Let b be the smallest positive integer with the property that $y^b\{x\} \cap N \neq 1$, then[5] $(b, q) = 1$. Finally let c

[4] Such an a exists as N is of finite index in $H(q)$.

[5] $(b, q) = 1$ as q is a power of p.

be the smallest non-negative integer such that $y^b x^c$ is in N. It is clear that $0 \leqq c < a$ and $N(a, b, c)$ is contained in N. Since N is normal in $H(q)$, $y^b x^c x^{q^b - 1} = x y^b x^c x^{-1}$ and $y^b x^c x^{c(q-1)} = y^{-1} y^b x^c y$ are in N, hence the choice of a, b, c implies that $c(q-1) \equiv q^b - 1 \equiv 0 \pmod a$. The index of N in $H(q)$ is $[H(q): N\{x\}][N\{x\}: N] = ab = [H(q): N(a, b, c)]$. Hence $N = N(a, b, c)$.

The "if" part of the last statement is trivial. Conversely suppose that $N = N(a, b, c) = N(a', b', c')$ and both triples of integers satisfy (*). As $N \cap \{x\} = \{x^a\} = \{x^{a'}\}$, $a = a'$: as $[H(q): N] = ab = ab'$, $b = b'$. It follows from the definition of N that $y^b x^c$, $y^b x^{c'}$ are both in N. Hence $x^{c-c'}$ is in N, consequently $c - c' \equiv 0 \pmod a$ and $-a < c - c' < a$, thus $c = c'$.

This lemma can be used in giving a criterion for deciding how many p-regular extensions of K there are with a given Galois group.

THEOREM 2. *For any triple of integers a, b, c let $G(a, b, c)$ denote the group of order ab generated by two elements x, y satisfying the relations $x^a = y^b x^c = 1$ and $y^{-1} x y = x^q$. Let K be a field satisfying the assumptions of Theorem 1. A finite group G is the Galois group of a p-regular extension of K if and only if G is isomorphic to a group of the form $G(a, b, c)$ for some triple of integers a, b, c satisfying (*). The number of p-regular extensions of K with Galois group G is equal to the number of triples a, b, c satisfying (*) such that G is isomorphic to $G(a, b, c)$.*

PROOF. For any triple a, b, c of integers satisfying (*), $H(q)/N(a, b, c)$ is isomorphic to $G(a, b, c)$. Thus Theorem 1 implies that there is a one to one correspondence between such subgroups $N(a, b, c)$ and p-regular extensions of K with Galois groups $G(a, b, c)$. The number of p-regular extensions of K with a given Galois group G is equal to the number of normal subgroups N of $H(q)$ with $H(q)/N$ isomorphic to G. By the lemma this number is precisely the number of triples a, b, c satisfying (*) for which G is isomorphic to $G(a, b, c)$.

As a final result here is the counter example mentioned at the end of §1. Let K be the field of 3-adic rationals, let $F = K(\pi, \xi)$, where $\pi^4 = 3$, and ξ is a primitive $(3^4 - 1)$th root of unity. It is easily seen that F is a normal extension of K with $[F: K] = 2^4$. Let G be the Galois group of F over K, then $G = \{x, y \mid x^4 = y^4 = 1, yxy^{-1} = x^{-1}\}$ where the automorphisms x, y are defined by $x(\xi) = \xi$, $x(\pi) = \pi\xi^{20}$ and $y(\xi) = \xi^3$, $y(\pi) = \pi$. For any group H let H'_m denote the subgroup generated by commutators and mth powers of elements in H. Then it is easily seen that $(G'_2)'_2 = \{1\}$, hence G is a homomorphic image of $H(3)/(H(3)'_2)'_2$. It is not hard to show that $[H(3): (H(3)'_2)'_2] = 2^4$.

Consequently Theorem 1 implies that F is the only extension of K whose Galois group is isomorphic to G.

Let $G_0 = \{x^2, y\}$ and $G_1 = \{x, y^2\}$ be subgroups of G, and let K_0, K_1 be their respective fixed fields. The group $\overline{G}$ of order 2 is isomorphic to the Galois groups of both K_0 and K_1 over K. If a given homomorphism of G onto $\overline{G}$ has a kernel consisting of G_0, then the possibility of realizing this homomorphism as the homomorphism of Galois groups, where $\overline{G}$ is the Galois group of K_1 over K is equivalent to showing that there is an automorphism of G which sends G_0 onto G_1, since F is the only extension whose Galois group in G. We now show no such automorphism exists. Since x^2 generates the commutator subgroup of G and this has order 2, any automorphism of G sends x^2 onto itself. This immediately shows that G_0 cannot be sent onto G_1 as x^2 is a square in G_1 but not in G_0.

References

1. E. Artin, *Algebraic numbers and algebraic functions* I, Lecture notes at Princeton University, 1950–1951.

2. K. Iwasawa, *On galois groups of local fields*, Trans. Amer. Math. Soc. vol. 80 (1955) pp. 448–469.

3. I. R. Šafarevič, *On p-extensions*, Amer. Math. Soc. Translations, vol. 4, 1956, pp. 59–73.

Cornell University