Canad. Math. Bull. Vol. **14** (3), 1971

TOTALLY REAL SUBFIELDS OF p-ADIC FIELDS HAVING THE SYMMETRIC GROUP AS GALOIS GROUP

BY
HOWARD KLEIMAN

I. **Introduction.** In this paper, an elementary proof is given of the following proposition:

THEOREM 1. *If Q_p is an arbitrary field of p-adic numbers, then it contains normal subfields L_n $(2 \le n \le p)$ which have symmetric groups S_n as their respective Galois groups over Q, the field of rational numbers. Furthermore, each L_n may be chosen to be totally real.*

Theorem 1 is contained in my Ph.D. dissertation at the University of London. I would like to express my deep appreciation to Professor A. Fröhlich for his advice and encouragement throughout that venture.

II. **Preliminaries.** In order to prove Theorem 1, I shall need the following two theorems by Perron [1] and Weisner [2] as lemmas which I now state without proof:

LEMMA 1 (Perron). *Let $k_1, k_2, \ldots, k_n$ be n integers, and $p_1, p_2, \ldots, p_{n-1}$ be $n-1$ distinct rational prime integers such that for $v = 1, 2, \ldots, n-2$, the v numbers*

$$p_1k_1, p_1p_2k_2, \ldots, p_1p_2\ldots p_vk_v$$

are incongruent modulo p_{v+1} and relatively prime to p_{v+1}. Furthermore, suppose none of $p_1, \ldots, p_{n-1}$ divides k_n. Then if

$$f(x) = x(x-p_1k_1)(x-p_1p_2k_2)\ldots(x-p_1p_2\ldots p_{n-1}k_{n-1})+p_1p_2\ldots p_{n-1}k_n,$$

$f(x)$ has the symmetric group over Q.

LEMMA 2 (Weisner). *Let*

$$f(x) = ax(x-a_1)\ldots(x-a_{n-1}) \pm k$$

where $a, k, a_1, \ldots, a_{n-1}$ are positive and the a_j's are distinct. If the inequalities

$$2nk < aa_1a_2\ldots a_{n-1}$$
$$2nk < aa_j \prod_{\substack{i=1 \\ i \ne j}} |a_j - a_i| \quad (j = 1, 2, \ldots, n-1)$$

are satisfied, the roots of $f(x)$ are all real and lie within the intervals

$$[-\tfrac{1}{2}, \tfrac{1}{2}], \quad [a_j - \tfrac{1}{2}, a_j + \tfrac{1}{2}] \quad (j = 1, 2, \ldots, n-1).$$

Proof of Theorem 1. We must first consider the solution of the linear diophantine equation

$$ax = by + c. \tag{1}$$

A necessary and sufficient condition for a solution in integers x and y is that if d is the greatest common divisor of a and b, then d divides c. Thus, given distinct rational primes $p_1, \ldots, p_n, p$ where $|p_j| > p \geq n$, we can find nonzero integers $k_1, k_2, \ldots, k_{n-1}, m_1, m_2, \ldots, m_{n-1}$ such that

$$(p_1 p_2 \ldots p_j)k_j = (p_{j+1} p_{j+2} \ldots p_n p)m_j + j \tag{2}$$

where j ranges from 1 through $n-1$. Furthermore, let $k_n = p$. Then the conditions of Lemma 1 on $f(x)$ are met. Since $f(x)$ splits separably into linear factors modulo p, by Hensel's lemma the splitting field of $f(x)$ over Q is contained in Q_p. In each solution (k_j, m_j) of (2), we can choose k_j positive and arbitrarily large. By Lemma 2, $f(x)$ can therefore be chosen to have roots which are real and distinct, yielding the second portion of the theorem.

References

1. O. Perron, *Algebra*, de Gruyter, Berlin, **2** (1951), p. 220.

2. L. Weisner, *Irreducibility of polynomials of degree n which assume the same value n times*, Bull. Amer. Math. Soc. **41** (1935), 238–252.

Queensborough Community College,
Bayside, New York