On unit groups of finite local rings

Takao Sumiyama*

* Aichi Institute of Technology

ON UNIT GROUPS OF FINITE LOCAL RINGS

TAKAO SUMIYAMA

Throughout the present paper, \( R \) will represent a (not necessarily commutative) finite local ring with radical \( M \). Let \( K \) be the residue field \( R/M \), and \( R^* \) the unit group of \( R \). Let \( |K| = p^r (p \text{ a prime}), |R| = p^{nr}, |M| = p^{(n-1)r} \), and \( p^k (k \leq n) \) the characteristic of \( R \). Let \( Z_{p^k} = Z/p^kZ \) be the prime subring of \( R \). The \( r \)-dimensional Galois extension \( GR(p^{kr}, p^k) \) of \( Z_{p^k} \) is called a Galois ring (see [3]). By [5, Theorem 8 (i)], \( R \) contains a subring isomorphic to \( GR(p^{kr}, p^k) \), which will be called a maximal Galois subring of \( R \).

In the proof of [6, Theorem], the author showed that \( R^* \) contains an element \( u \) such that (i) its multiplicative order is \( p^r - 1 \) (and hence \( \bar{u} \) is a generator of \( K^* \)) and (ii) \( Z_{p^r}[u] \) is a maximal Galois subring of \( R \). Then \( R^* \) is a semidirect product of \( \langle u \rangle \) with \( 1+M \). Given \( v \in \langle u \rangle \), we define \( \phi_v \in \text{Aut}(1+M) \) by \( \phi_v(x) = v^{-1}xv \ (x \in 1+M) \). A map \( f : \langle u \rangle \to 1+M \) is called a crossed homomorphism if \( f(ab) = \phi_a(f(b))f(a) \) for any \( a, b \in \langle u \rangle \). The set of all crossed homomorphisms of \( \langle u \rangle \) to \( 1+M \) will be denoted by \( Z^1 = Z^1(\langle u \rangle, 1+M) \) (cf. [2, pp. 104—106]). For each \( x \in 1+M \), the map \( f_x : \langle u \rangle \to 1+M \) defined by \( f_x(a) = \phi_a(x)x^{-1} \) is a crossed homomorphism. Such a crossed homomorphism is called principal, and the set of all principal crossed homomorphisms is denoted by \( B^1 = B^1(\langle u \rangle, 1+M) \). In case \( M \) is commutative, \( Z^1 \) and \( B^1 \) are Abelian groups and \( H^1 = Z^1/B^1 \) is the first cohomology group of \( \langle u \rangle \) over \( 1+M \). Given \( v \in \langle u \rangle \), we define \( N_v : 1+M \to 1+M \) by

\[
N_v(x) = (vx)^{p^r-1} = v^{-1}(p^r-1)(vx)^{p^r-1} = \phi_{p^r-1}(x) \cdots \phi_v(x) \phi_v(x)x.
\]

Note that if \( M \) is commutative then \( N_v \) is a group homomorphism. We set \( D = \{ x \in 1+M \mid N_v(x) = 1 \} \).

The purpose of this paper is to prove the following theorems.

**Theorem 1.**

1. \( |Z^1| = |D| \).
2. \( |B^1| \) coincides with the number of maximal Galois subrings of \( R \).
3. If \( M \) is commutative then \( H^1 = 0 \).

**Theorem 2.**

1. The number of solutions of \( X^{p^r-1} = 1 \) in \( R \) is...
Mathematical Journal of Okayama University, Vol. 23 [1981], Iss. 2, Art. 13

T. SUMIYAMA

$(p^r-1)s$ with a positive integer $s$.

(2) The following are equivalent:
   1) The number of solutions of $X^{p^r-1} = 1$ in $R$ is $p^r-1$, namely the set of solutions of $X^{p-1} = 1$ in $R$ coincides with $<u>$. 
   2) $R^* = <u> \times (1+M)$. 
   3) $R^*$ is a nilpotent group. 
   4) $R$ has a unique maximal Galois subring. 
   5) $|B_\downarrow| = 1$. 
   6) $[a.x] \in M^2$ for all $a \in R^*$ and $x \in M$. 

(3) The number of solutions of $X^{p-1} = 1$ in $R$ is $p-1$, namely the set of solutions of $X^{p^r-1} = 1$ in $R$ coincides with the subgroup of $<u>$ generated by the $\left(\frac{p^r-1}{p-1}\right)$-th power of $u$ contained in $Z_{p^r}$.

Theorem 3. Let $m$ be the number of solutions of $X^{p^r-1} = 1$ in $R$. If $r \geq 2$, then

$$|Z_\downarrow| + p^r - 2 \leq m \leq |Z_\downarrow| + p - 1 + p^{(n-1)r} (p^r - p - 1).$$

Theorem 4. Let $(p^r-1)s$ be the number of solutions of $X^{p^r-1} = 1$ in $R$. Let $T = \{v \in <u>| N_v(x) = 1 \text{ implies } x = 1\}$, and $t = |T|$.

(1) If $M$ is commutative, then $s + t$ is a multiple of $p$.

(2) If $M^2 = 0$ and $k = 1$, then $s + t$ is a multiple of $p^r$.

Proof of Theorem 1. (1) Let $f : <u> \rightarrow 1 + M$ be a crossed homomorphism. Since $f$ is completely determined by $f(u)$ and $1 = f(1) = f(u^{p^r-1}) = N_u(f(u))$, the number of all crossed homomorphisms coincides with $|D|$. 

(2) Let $f_x, f_y \in B_\downarrow$. If $f_x = f_y$, then $f_x(u) = f_y(u)$, which implies that $y^{-1}xu = uy^{-1}x$. So, each principal crossed homomorphism corresponds to a left coset of $1 + N$ in $1 + M$, where $N = \{z \in M | zu = uz\}$. Thus $|B_\downarrow| = |1 + M|/|1 + N| = |M : N|$. As was noted in [6], $|M : N|$ is the number of maximal Galois subrings of $R$.

(3) Consider $\Phi : D \rightarrow B_\downarrow$ defined by $\Phi(x) = f_x$. We shall show that $\Phi$ is injective. If $f_x = f_y$ ($x, y \in D$), then $z = x^{-1}y \in 1 + N$, and hence $1 = N_y(y) = N_y(x)z^{p^r-1} = x^{p^r-1}$. This means that $z = 1$, namely $x = y$. Thus, this together with (1) implies $Z_\downarrow = B_\downarrow$.

Proof of Theorem 2. (1) This is immediate by a theorem of Frobenius [1, Theorem 9.1.2].

(2) Obviously, 3) $\iff$ 2) $\implies$ 1).

http://escholarship.lib.okayama-u.ac.jp/mjou/vol23/iss2/13
ON UNIT GROUPS OF FINITE LOCAL RINGS

1) $\implies$ 2). By [1, Theorem 9.4.1], $\langle u \rangle$ is a normal subgroup of $R^*$, and therefore $R^* = \langle u \rangle \times (1 + M)$.

3) $\iff$ 4). See [6, Remark].

4) $\iff$ 5). By Theorem 1 (2).

6) $\implies$ 3). By [4, Lemma 1].

2) $\implies$ 6). Let $a = v(1 + y)$ ($v \in \langle u \rangle, y \in M$). Then $[a, x] = [v(1 + y), 1 + x] = v[y, x] \in M^2$.

3) By [5, Theorem 6], $X^{p-1} = 1$ has $p-1$ solutions in $Z_{p^a}$. So, we show that there are at most $p-1$ solutions in $R$. Let $a = vx$ ($v \in \langle u \rangle, x \in 1 + M$) be an element of $R^*$ such that $a^{p-1} = 1$. Then, the canonical image of $v$ in $K$ is contained in the prime field of $K$, and so $v = iy$ with some multiple $i$ of 1 and $y \in 1 + M$. Since

$$v^{-(p-1)} = v^{-(p-1)}(vx)^{p-1} = \phi_{v^{p-1}}(x) \cdots \phi_{v^{(p-1)/2}}(x)x$$

is in $\langle u \rangle \cap (1 + M) = 1$, we obtain

$$y^{p-1} = y^{p-1} \phi_{v^{p-1}}(x) \cdots \phi_{v^{(p-1)/2}}(x)x = (yx)^{p-1},$$

whence it follows that $y = yx$. Hence $x = 1$ and $a = v$. This completes the proof.

**Corollary.** If $r = 1$, then $R^* = \langle u \rangle \times (1 + M)$.

**Proof of Theorem 3.** If $a = vx$ ($v \in \langle u \rangle, x \in 1 + M$) is an element of $R^*$ such that $a^{p-1} = 1$, then $1 = (vx)^{p-1} = N_v(x)$. Hence, by Theorem 1 (1) we obtain

$$m = \sum_{v \in \langle u \rangle} |\{x \in 1 + M \mid N_v(x) = 1\}| \geq |D| + p^{r-2} = |Z_d| + p^{r-2}.$$ 

Now, let $w$ be the $\left(\frac{p^r-1}{p-1}\right)$-th power of $u$, and $v \in \langle w \rangle$. Then $N_v(x) = x^{p^r-1}$ by Theorem 2 (3). Hence,

$$m = |D| + \sum_{v \in \langle u \rangle} |\{x \in 1 + M \mid N_v(x) = 1\}| + \sum_{v \in \langle u \rangle \cup \langle w \rangle} |\{x \in 1 + M \mid N_v(x) = 1\}|$$

$$\leq |Z_d| + (p-1) + p^{(n-1)r} (p^r - 1 - (p-1))$$

$$= |Z_d| + p - 1 + p^{n-1} (p^r - p - 1).$$

**Proof of Theorem 4.** (1) For any $v \in \langle u \rangle$, the map $N_v$ is a group homomorphism, and $|\ker N_v|$ is a power of $p$, provided $v \in T$. Since

$$(p^r-1)s = \sum_{v \in \langle u \rangle} |\ker N_v| = t + \sum_{v \in T} |\ker N_v| = t + pl$$

with some non-negative integer $l$, we see that $s+t$ is a multiple of $p$. 

(2) Given $k_1, k_2, \ldots, k_n \in K$, we denote by $r_1\{k_1, k_2, \ldots, k_n\}$ the $n \times n$
matrix
\[
\begin{bmatrix}
k_1 & k_2 & \cdots & k_n \\
0 & 0 & \cdots & 0 \\
\vdots & & \ddots & \vdots \\
0 & 0 & \cdots & 0
\end{bmatrix}
\]

According to [5, Theorem 3], \( R \) may be regarded as the ring of all matrices of the form
\[
\text{diag}(c, \sigma_2(c), \cdots, \sigma_n(c)) + r_1\{0, d_2, \cdots, d_n\},
\]
where \( c, d_2, \cdots, d_n \) range over \( K \) and \( \sigma_2, \cdots, \sigma_n \) are fixed automorphisms of \( K \). Obviously, \( 1 + M \) consists of all matrices of the form
\[
1 + r_1\{0, d_2, \cdots, d_n\}.
\]

If \( b \) is a generating element of \( K^* \) then \( u = \text{diag}\{b, \sigma_2(b), \cdots, \sigma_n(b)\} \) is of order \( p^r - 1 \) and \( Z_p[u] \) is a maximal Galois subring of \( R \). Now, let \( v = \text{diag}(c, \sigma_2(c), \cdots, \sigma_n(c)) \) and \( x = 1 + r_1\{0, d_2, \cdots, d_n\} \). Then
\[
(vx)^{p^r-1} = 1 + r_1\{0, g_2, \cdots, g_n\},
\]
where
\[
g_i = c(\sum_{j=0}^{p^r-2} c^i \sigma_i(c)^{p^r-2-j})d_i = \begin{cases} 
0 & \text{if } c \neq \sigma_i(c) \\
-c^{p^r-1}d_i & \text{if } c = \sigma_i(c)
\end{cases}.
\]

Since \( v \) is in \( T \) if and only if \( c = \sigma_i(c) \) for all \( i \), we see that \( |\text{Ker } N_v| \) is a multiple of \( p^r \) for any \( v \in T \). Thus, \( (p^r - 1)s = t + p^r m' \) with some non-negative integer \( m' \), and therefore \( s + t \) is a multiple of \( p^r \).

**Example.** Let \( R = \left\{ \begin{pmatrix} c & d \\ 0 & c^d \end{pmatrix} \mid c, d \in GF(p^2) \right\} \). Then \( t = p - 1 \), and therefore the number of solutions of \( X^{p^r-1} = 1 \) in \( R \) is \( p - 1 + (p^2 - 1 - (p - 1))p^2 = p^4 - p^3 + p - 1 \).

**REFERENCES**


**AICHI INSTITUTE OF TECHNOLOGY**

*(Received July 31, 1980)*