Math. J. Okayama Univ. 26 (1984), 169—173

NONEXISTENCE OF CERTAIN FINITE RINGS

TAKAO SUMIYAMA

Throughout the present paper, R will represent an associative ring with 1, and R^* the unit group of R. If R^* is of odd order then [3, Theorem] shows that R^* is an abelian group. The purpose of this paper is to prove the following related results.

Theorem 1. *There exists no finite ring whose unit group is a non-abelian Z-group of order not divisible by* 3.

Theorem 2. *Let p and q be distinct primes not smaller than* 5. *Then there exists no finite ring whose radical is commutative and whose unit group is non-abelian and of order $2p^iq^j$ $(i \geq 1, 1 \geq j \geq 0)$.*

In advance of proving our theorems, we state the following remark.

Remark 1. Let G be a Z-group (every Sylow subgroup of G be cyclic). Then G is a meta-cyclic group generated by elements x and y with the following relations:

$$x^n = 1 = y^m \text{ and } x^{-1}yx = y^r$$

where $(r-1, m) = (n, m) = 1$, $r^n \equiv 1 \pmod{m}$ (see [5, Proposition 2. 12.11, p.106]). Conversely, if n, m and r are positive integers such that $(r-1, m) = (n, m) = 1$, $r^n \equiv 1 \pmod{m}$ and $nm \not\equiv 0 \pmod{3}$, then the group defined by the above relations is a non-abelian Z-group whose order is not divisible by 3, provided $r > 1$.

Proof of Theorem 1. Assume that the assertion is false, and choose an example R with the minimal order. First, we claim that R is indecomposable. In fact, if $R = R_1 \oplus R_2$ then $R^* \simeq R_1^* \times R_2^*$, so the minimality of R implies that R is indecomposable. Hence the additive group of R is primary and $|R|$ is a power of a prime p. Let J be the radical of R. As R^* is solvable (see Remark 1), [2, Theorem 1] shows that R/J is a direct sum of finite fields and/or 2×2 matrix rings over GF(2) or GF(3). As $|R^*|$ is not divisible by 3, neither $|\mathrm{GL}(2,2)| = 6$ nor $|\mathrm{GL}(2,3)| = 48$ can be a divisor of $|R^*|$, and therefore $R/J = \mathrm{GF}(p^{e_1}) \oplus \cdots \oplus \mathrm{GF}(p^{e_r})$. Since R^* is a Z-group, Schur-Zassenhaus theorem [5, Theorem 2.10.4, p.83] shows

that R^* is a semi-direct product of a normal cyclic p-Sylow subgroup $1+J=\langle u\rangle$ by a cyclic p'-group $\langle a\rangle \simeq (R/J)^*$. If $p=2$, then the order of the automorphism $\tilde{a}$ of $\langle u\rangle$ induced by the inner automorphism effected by a is odd. On the other hand, the order of the automorphism group of $\langle u\rangle$ is a power of 2. Hence $\tilde{a}=1$ and R^* is the direct product of $1+J$ and $\langle a\rangle$, which contradicts that R^* is non-abelian. Thus p has to be odd. If $r>1$, then $a^{(p-1)s}=1$ and the order of $\langle a\rangle$ is $(p-1)^r s$, where $s=\prod_{i=1}^{r}((p^{e_i}-1)/(p-1))$. This contradiction tells us that $r=1$. Assume that $J^2\neq 0$. Then $(R/J^2)^*$ is abelian and generates R/J^2. Thus R/J^2 is commutative, and [4, Lemma 1] proves that R^* is nilpotent, and hence cyclic. This contradiction shows that $J^2=0$, and therefore J is a vector space over $R/J=\mathrm{GF}(p^{e_1})$ (and $pJ=0$). Setting $u=1+v$ with some $v\in J$, we get $|J|=p$, and so $e_1=1$. Noting that $R=\boldsymbol{Z}1+\boldsymbol{Z}v$, we see that R is commutative. But this is a contradiction.

Corollary 1. *There exists no finite ring whose unit group is a non-abelian group of square free order not divisible by* 3.

Proof of Theorem 2. Assume that the assertion is false, and choose an example R with the minimal order. In view of [3, Theorem], we can easily see that R is indecomposable and $|R|$ is a power of a prime. According to [7, Theorem 4.6], R^* contains a normal subgroup A of order p^iq^j, and hence is solvable. Now, let J be the radical of R. Since $|R^*|$ is not divisible by 3, [2, Theorem 1] shows that R/J is a direct sum of finite fields. Since R^* is non-abelian, J has to be non-zero. Evidently, $|J|$ divides both $|R|$ and $2p^iq^j$, and so we may consider the following cases: (1) $|J|=2$, (2) $|J|=p^k\ (i\geq k\geq 1)$, (3) $|J|=q$.

Case (1). Since $R^*/(1+J)\simeq (R/J)^*$ is an abelian group of order p^iq^j and $|1+J|=2$, R^* is the direct product of $1+J$ and the abelian group A. But this is a contradiction.

Case (2). Since $|R|$ is a power of p, we have $R/J=\mathrm{GF}(p^{e_1})\oplus\cdots\oplus\mathrm{GF}(p^{e_r})$ and $2p^{i-k}q^j=(p^{e_1}-1)\cdots(p^{e_r}-1)$. Since each $p^{e_\lambda}-1$ is even and not divisible by p, we have $r=1$ and $k=i$. If $e_1>1$ then $2q^j=p^{e_1}-1=(p-1)(p^{e_1-1}+\cdots+p+1)$ and $p-1=2t$ with some $t\geq 2$. But this is impossible, for $j\leq 1$. Hence $e_1=1$, namely $R/J=\mathrm{GF}(p)$. Now, by [6, Corollary], R^* is the direct product of a cyclic group of order $p-1$ and the abelian group $1+J$, which is a contradiction.

Case (3). In the same way as in Case (2), we can easily see that $R/J = \mathrm{GF}(q^{e_1})$. Since $J^2 = 0$, J is a vector space over $\mathrm{GF}(q^{e_1})$, and hence $e_1 = 1$. Thus, R is commutative, which is a contradiction.

From the proof of Theorem 2, we can easily see the following

Corollary 2. *Let p and q be distinct primes not smaller than 5.*

(1) *There exists no finite ring whose unit group is non-abelian and of order $2p^i$ $(i \geq 1)$.*

(2) *There exists no finite ring whose unit group is non-abelian and of order $2p^iq$ $(2 \geq i \geq 1)$.*

Corollary 3. *Let p be a prime not smaller than 7. Then there exists no finite ring whose unit group is non-abelian and of order $4p^i$ $(i \geq 1)$.*

Proof. Assume that the assertion is false, and choose an example R with the minimal order. In view of [3, Theorem] and Corollary 2, we can easily see that R is indecomposable and $|R|$ is a power of a prime. Let J be the radical of R. Since R^* is solvable by Burnside theorem and $|R^*|$ is not divisible by 3, [2, Theorem 1] shows that R/J is a direct sum of finite fields. Noting that R^* is non-abelian, we see that $J \neq 0$. Since $|J|$ divides both $|R|$ and $4p^i$, we may consider the following cases : (1) $|J| = 4$, (2) $|J| = 2$, (3) $|J| = p^k$ $(i \geq k \geq 1)$.

Case (1). Let A be a p-Sylow subgroup of R^*. Then $A \simeq (R/J)^*$ is abelian and R^* is a semi-direct product of $1+J$ by A. Since $1+J$ is either a cyclic group of order 4 or the direct product of two cyclic groups of order 2, the order of the automorphism group of $1+J$ is either 2 or 6. Recalling here that $|A| = p^i$ $(p \geq 7)$, we can easily see that R^* is the direct product of A and $1+J$, which is a contradiction.

Case (2). Since $(R/J)^*$ is abelian and every automorphism of $1+J$ is trivial, R^* is commutative, a contradiction.

Case (3). Since R/J is commutative, we have $4p^{i-k} = (p^{e_1}-1)\cdots(p^{e_r}-1)$ for some positive integers $e_1, \ldots, e_r$. But each $p^{e_\lambda}-1$ is not divisible by p, so $4 = (p^{e_1}-1)\cdots(p^{e_r}-1)$. This is impossible, too, for $p \geq 7$.

Remark 2. If R is a finite local ring with maximal ideal M and $R/M = \mathrm{GF}(p^s)$, then R^* has a normal chain $R^* \supsetneq 1+M \supsetneq 1+M^2 \supsetneq \cdots \supsetneq 1+M^k = 1$, $R^*/(1+M)$ is a cyclic group of order p^s-1, and $(1+M^i)/(1+M^{i+1})$ is an elementary p-group, $k-1 \geq i \geq 1$ (see [1, Theorem 1]).

However, we can show that a group with the above structure need not be the unit group of a finite ring. Let $q \geq 5$ be a Sophie Germain prime (both q and $p = 2q+1$ be prime numbers). In Remark 1, consider the case $m = q$, $n = 2p$ and $r = q-1$. Then we obtain a non-abelian Z-group G of order $2pq$ with a normal subgroup H such that $|H| = p$ and G/H is a cyclic group of order $2q = p-1$. In view of Corollary 2 (2), G cannot be the unit group of a finite ring.

Remark 3. Let $p \geq 5$ be a Sophie Germain prime, and $q = 2p+1$. We consider the ring

$$R = \left|\begin{pmatrix} a & 0 \\ c & b \end{pmatrix}\right| a,\ b,\ c \in \mathrm{GF}(q)\}.$$

Then R^* is non-abelian and $|R^*| = (q-1)^2q = 4p^2q$. Thus, in Corollary 2 (2), we cannot replace $2p^iq$ by $4p^iq$.

Remark 4. For the present, it is unknown whether there are infinitely many Sophie Germain primes. The following is the table of all Sophie Germain primes less than 10000.

2	3	5	11	23	29	41	53	83	89
113	131	173	179	191	233	239	251	281	293
359	419	431	443	491	509	593	641	653	659
683	719	743	761	809	911	953	1013	1019	1031
1049	1103	1223	1229	1289	1409	1439	1451	1481	1499
1511	1559	1583	1601	1733	1811	1889	1901	1931	1973
2003	2039	2063	2069	2129	2141	2273	2339	2351	2393
2399	2459	2543	2549	2693	2699	2741	2753	2819	2903
2939	2963	2969	3023	3299	3329	3359	3389	3413	3449
3491	3539	3593	3623	3761	3779	3803	3821	3851	3863
3911	4019	4073	4211	4271	4349	4373	4391	4409	4481
4733	4793	4871	4919	4943	5003	5039	5051	5081	5171
5231	5279	5303	5333	5399	5441	5501	5639	5711	5741
5849	5903	6053	6101	6113	6131	6173	6263	6269	6323
6329	6449	6491	6521	6551	6563	6581	6761	6899	6983
7043	7079	7103	7121	7151	7193	7211	7349	7433	7541
7643	7649	7691	7823	7841	7883	7901	8069	8093	8111
8243	8273	8513	8663	8693	8741	8951	8969	9029	9059
9221	9293	9371	9419	9473	9479	9539	9629	9689	9791

In conclusion, the author would like to express his indebtedness and

gratitude to Prof. K. Motose for his helpful suggestions and valuable comments.

REFERENCES

[1] C. W. AYOUB : On finite primary rings and their groups of units, Compositio Math. 21 (1969), 247−252.
[2] P. B. BHATTACHARYA and S. K. JAIN : A note on the adjoint group of a ring, Arch. Math. 21 (1970), 366−368.
[3] S. DITOR : On the group of units of a ring, Amer. Math. Monthly 78 (1971), 522−523.
[4] K. MOTOSE and H. TOMINAGA : Group rings with nilpotent unit groups, Math. J. Okayama Univ. 14 (1969), 43−46.
[5] D. S. PASSMAN : Permutation Groups, Benjamin, New York−Amsterdam, 1968.
[6] T. SUMIYAMA : On unit groups of finite local rings, Math. J. Okayama Univ. 23 (1981), 195−198.
[7] H. WIELANDT : Finite Permutation Groups, Academic, New York−London, 1964.

AICHI INSTITUTE OF TECHNOLOGY

(Received December 15, 1983)