Groups of Order 2p Which Are Isomorphic to Unit Groups of Finite Rings

Takao SUMIYAMA

有限環の単数群に同型なる位数2pの群について

隅　山　孝　夫

Let p be an odd prime. We will classify groups of order 2p which are isomorphic to unit groups of finite rings.

Throughout the present paper, R will represent an associative ring with 1, and R^* the unit group of R. We denote by C_n the cyclic group of order n. When $p=2^n-1$ (n is a positive integer) is a prime, p is called a Mersenne prime. When p and 2p +1 are both primes, p is called a Sophie Germain prime. The present objective is to prove the following theorem.

Theorem. If G is a finite group of order 2p (p is an odd prime) and isomorphic to the unit group of a finite ring R, then there holds one of the following :
(i) $G\cong S_3$ (the symmetric group on 3 symbols).
(ii) $G\cong C_2\times C_p$, where p is a Mersenne prime.
(iii) $G\cong C_2\times C_p$, where p is a Sophie Germain prime.
(iv) $G\cong C_2\times C_p$, where 2p+1 is a power of 3.

Conversely, if a finite group G satisfies one of (i) ~(iv), then there exists a finite ring R such that $G\cong R^*$.

Proof. First we consider the case p=3. Every group of order $2\cdot 3=6$ is isomorphic to S_3 or $C_2\times C_3$. Obviously, S_3 is isomorphic to the unit group of 2×2 matrix ring over GF (2), and $C_2\times C_3\cong$ (GF (3) $\oplus$ GF $(2^2))^*$. Note that p=3 is a Mersenne prime and a Sophie Germain prime, as well.

Now, let us assume $p\geqq 5$. By [1, Theorem 6.1], G is Abelian. Hence $G\cong C_2\times C_p$, so we have only to show that p satisfies one of (ii)~(iv). Let J be the Jacobson radical of R. As 1+J is a subgroup of R^*, there are four cases :

(A) $|J|=1$, (B) $|J|=2$, (C) $|J|=p$, (D) $|J|=2p$.

Case (A). In this case, J=0, i.e. R is semisinple. As R^* is Abelian, by Wedderburn-Artin theorem, R is a direct sum of finite fields.

$$R=GF(p_1^{r_1})\oplus GF(p_2^{r_2})\oplus\cdots\cdots\oplus GF\ (p_n^{r_n}).$$

Then $2p=|R^*|=(p_1^{r_1}-1)(p_2^{r_2}-1)\cdots\cdots(p_n^{r_n}-1)$.
Without loss of generality, we may assume that either $p_1^{r_1}-1=p$, $p_2^{r_2}-1=2$, and $p_i^{r_i}-1=1 (3\leqq i\leqq n)$, or $p_1^{r_1}-1=2p$ and $p_i^{r_i}-1=1 (2\leqq i\leqq n)$.

If $p_1^{r_1}-1=p$, then $p_1^{r_1}=p+1$ is an even number, and so $p+1=2^{r_1}$, that is, p is a Mersenne prime.

If $p_1^{r_1}-1=2p$ and $r_1\geqq 2$, then $2p=(p_1-1)(p_1^{r_1-1}+\cdots\cdots+p_1+1)$. As p_1-1 is a multiple of 2 and $p_1^{r_1-1}+\cdots\cdots+p_1+1\geqq 4$, it follows that $p_1-1=2$. Hence 2p+1 is a power of 3.

If $p_1-1=2p$, then p is a Sophie Germain prime.

In general,

(1) $R=R_1\oplus R_2\oplus\cdots\cdots\oplus R_n$,

where each $|R_i|=p_i^{r_i} (1\leqq i\leqq n)$ and $p_1, p_2,\cdots\cdots, p_n$ are distinct primes. Then

(2) $J=J_1\oplus J_2\oplus\cdots\cdots\oplus J_n$,

where each J_i is the Jacobson radical of R_i. So

(3) $R/J=R_1/J_1\oplus R_2/J_2\oplus\cdots\cdots\oplus R_n/J_n$.

Note that each $|J_i|$ is a power of p_i.

Case (B). By (2), we may assume that $|J_1|=2$ and $J_i=0$ $(2\leqq i\leqq n)$. Then

$$p=|(R/J)^*|=|(R_1/J_1)^*|\cdot|R_2^*|\cdots\cdots|R_n^*|.$$

Therefore we may assume further that either $|(R_1/J_1)^*|=1$, $|R_2^*|=p$, $|R_i^*|=1$ $(3\leqq i\leqq n)$, or $|(R_1/J_1)^*|=p$, $|R_i^*|=1$ $(2\leqq i\leqq n)$. But in the same way as before, we can see that p is a Mersenne prime in either case.

Next, we will show that the cases (C) and (D) are impossible for $p\geqq 5$.

Let us suppose $|J|=p$. By (2), we may assume that $|J_1|=p$, $J_i=0$ $(2\leqq i\leqq n)$. Then by (3), we get

$$2=|(R/J)^*|=|(R_1/J_1)^*|\cdot|R_2^*|\cdots\cdots|R_n^*|.$$

If $|(R_1/J_1)^*|=1$, then $R_1/J_1=GF(2)\oplus\cdots\cdots\oplus GF(2)$. Then $|R_1|$ is a power of 2, which contradicts $|J_1|=p$. So $|(R_1/J_1)^*|=2$. Then $R_1/J_1=GF(3)$, which contradicts $p\geqq 5$.

On the other hand , if $|J|=2p$, then we may suppose that $|J_1|=p$, $|J_2|=2$, $J_i=0$ $(3\leqq i\leqq n)$. As $|(R/J)^*|=1$, $R/J=GF(2)\oplus\cdots\cdots\oplus GF(2)$. So $|R|$ is a power of 2, which contradicts $|J_1|=p$.

Q.E.D.

As an application of the theorem in group rings, we readily obtain

Corollary. Let R be a finite ring, and G a finite group of order 2p (p is an odd prime). If G satisfies none of (i) ～ (iv), then G is a proper subgroup of $R[G]^*$.

In conclusion, we write down some primes of type (ii)～(iv).

primes of type (ii) : 3, 7, 31, 127, 2047, 8191, ……
primes of type (iii) : 3, 5, 11, 23, 29, 41, 53, ……
primes of type (iv) : 13, 1093, 797161, ……

Whether there are infinitely many Mersenne primes, whether there are infinitely mamy Sophie Germain primes, and whether there are infinitely many primes of type (iv), are unsolved problems for the present.

Reference

〔1〕 T.Sumiyama, Unit groups of finite rings, Thesis, Okayama University, 1977.

(Received January 16, 1983)