Classification of Finite Rings of Order p^2

BENJAMIN FINE
Fairfield University
Fairfield, CT 06430

Most treatments of elementary abstract algebra include a discussion of finite groups and some work on their classification. However, very little is done with finite rings. For example most beginning texts state and prove the theorem that for p a prime the cyclic group of order p is the only group of order p up to isomorphism. Yet the equally striking and easily proved result that for a prime p there are only two rings of order p up to isomorphism is either not mentioned at all or relegated to the exercises.

The purpose of this note is to give a complete classification of all finite rings of order p^2 with p a prime. In particular, we show that up to isomorphism there are exactly 11 rings of order p^2. The techniques are elementary and grew out of a project given to an undergraduate abstract algebra course. We use a concept called a *ring presentation*, which is an excellent computational tool for dealing with finite rings. After explaining this concept, we state our main result, Theorem 2, which can be given as a large project to a good undergraduate class with guidance provided by the instructor.

1. Presentation If R is a finite ring then its additive group is a finite abelian group and is thus a direct product of cyclic groups. Suppose these have generators $g_1, \ldots, g_k$ of orders $m_1, \ldots, m_k$. Then the ring structure is determined by the k^2 products

$$g_i g_j = \sum_{t=1}^{k} c_{ij}^t g_t \quad \text{with } c_{ij}^t \in \mathbf{Z}_{m_t} \tag{1}$$

and thus by the k^3 structure constants c_{ij}^t. We introduce a convenient notation, motivated by group theory, for giving the structure of a finite ring. A *presentation* for a finite ring R consists of a set of generators $g_1, \ldots, g_k$ of the additive group of R together with *relations*. The relations are of two types:

(i) $m_i g_i = 0$ for $i = 1, \ldots, k$ indicating the additive order of g_i, and

(ii) $g_i g_j = \sum_{t=1}^{k} c_{ij}^t g_t$ with $c_{ij}^t \in \mathbf{Z}_{m_t}$

for $i = 1, \ldots, k$; $j = 1, \ldots, k$; $t = 1, \ldots, k$.

If the ring R has the presentation above we write

$$R = \left\langle g_1, \ldots, g_k;\ m_i g_i = 0 \text{ for } i = 1, \ldots, k,\ g_i g_j = \sum_{i=1}^{k} c_{ij}^t g_i \right\rangle.$$

For example the ring $\mathbf{Z}_2 + \mathbf{Z}_2 = \langle a, b;\ 2a = 2b = 0,\ a^2 = a,\ b^2 = b,\ ab = ba = 0 \rangle$, while the finite field of order 4 is $\langle a, b;\ 2a = 2b = 0,\ a^2 = a,\ ab = b,\ b^2 = a + b \rangle$. Notice that if the additive group is cyclic with generator g, the ring structure is completely determined by g^2. Therefore the ring $\mathbf{Z}_4 = \langle a;\ 4a = 0,\ a^2 = a \rangle$.

Finally if a relation follows by applying the ring properties to other relations, we delete it. For example suppose that a ring R is generated by a and b having prime

additive orders p and q. If $a^2 = 0$ and $b^2 = 0$ it follows that $ab = 0$ and $ba = 0$, so these relations are deleted. To see this last fact notice that if $ab = ta + ub$ then $a^2b = 0 = ta^2 + uab = uta + u^2b$. Since a, b constitute an additive basis it follows that $u^2 \equiv 0 \pmod{q}$ and since q is a prime we must then also have $u \equiv 0 \pmod{q}$. Similarly, by calculating ab^2 we deduce that $t \equiv 0 \pmod{p}$.

2. Cyclic additive groups We first present a result that characterizes rings with cyclic additive groups. This appeared in [2].

THEOREM 1. *The number of rings R, up to isomorphism, with cyclic additive group C_m is given by the number of divisors of m. In particular, for each divisor d of m there is a ring $R_d = \langle g;\ mg = 0,\ g^2 = dg \rangle$ where g is an additive generator of C_m. For different d's these rings are nonisomorphic.*

Proof. Let R be a ring with additive group C_m and let g be an additive generator of C_m. Suppose $g^2 = ng$. If $(m, n) = 1$ then n has an inverse k modulo m so that $nk \equiv 1 \pmod{m}$. Let $g_1 = kg$. Since k is a unit in $\mathbf{Z}_m$, g_1 is also an additive generator. Now $g_1^2 = (kg)^2 = k^2g^2 = k^2(ng) = k(kng) = kg = g_1$. So the homomorphism from R to $\mathbf{Z}_m$ defined by $g_1 \to 1$ is an isomorphism. Therefore in this case $R = R_1$ is isomorphic to $\mathbf{Z}_m$.

Suppose $g^2 = 0$. Then all the multiplication is trivial and in this case $R = R_m$ is isomorphic to the ring with additive group C_m and trivial multiplication. These two possibilities correspond to the divisors 1 and m of m.

Now let d be a proper divisor of m with $m = kd$ and suppose $g^2 = kg$. Observe that kg generates a unique additive cyclic subgroup of order d. The generators of this subgroup are $(jk)g$ where $j = 0, 1, \ldots, d-1$ and $(j, d) = 1$. We show that for any $j = 0, 1, \ldots, d-1$ and $(j, d) = 1$, R is isomorphic to $\langle g_1;\ mg_1 = 0,\ g_1^2 = (jk)g_1 \rangle$ for some generator g_1 of C_m. To do so, we show that there is an n with $(m, n) = 1$ such that if $g_1 = ng$ then $g_1^2 = (jk)g_1$. Since $(n, m) = 1$, g_1 is then an additive generator and the map $g \to g_1$ gives the desired isomorphism.

Suppose $g_1 = ng$ with n to be determined. Then $g_1^2 = n^2g^2 = (n^2k)g$. If this is to equal $(jk)g_1 = (jkn)g$ we are led to the congruence:

$$kn^2 \equiv jkn \pmod{m}, \text{ with } n \text{ the variable.} \tag{1}$$

Assuming n is to be a unit mod m, we get

$$kn \equiv jk \pmod{m}. \tag{2}$$

The solutions modulo m are $n = j + td$ with $t = 0, 1, \ldots, k-1$. Since $(j, d) = 1$, by Dirichlet's theorem there exists a solution such that $j + td$ is prime to m. This solution n of (2) is then a unit mod m and gives the indicated n.

Thus the rings with additive groups C_m and generator g such that $g^2 = (jk)g$ with $kd = m$ and $(j, d) = 1$ all fall in one isomorphism class.

Notice further that if $g^2 = kg$ and $(j, d) \neq 1$, then for any solution to (1) or (2) we would have $(j + td, m) \neq 1$ and therefore there is no unit solution. This implies that there exists no additive generator g_1 such that $g_1^2 = (jk)g_1$ and thus no isomorphism. Therefore the rings whose presentations are given in terms of divisors of m of different additive orders are precisely the isomorphism classes. This completes the proof of the theorem.

We immediately have the following corollaries classifying rings of prime order and rings of order pq where p and q are distinct primes. For an abelian group G we let $G(0)$ denote the ring with additive group G and trivial multiplication.

COROLLARY 1. *If p is a prime there are, up to isomorphism, exactly two rings of order p, namely $\mathbf{Z}_p$ and $C_p(0)$.*

COROLLARY 2. *If p and q are distinct primes there are, up to isomorphism, exactly four rings of order pq. These are $\mathbf{Z}_{pq}$, $C_{pq}(0)$, $C_p(0) + \mathbf{Z}_q$, and $\mathbf{Z}_p + C_q(0)$.*

More generally if n is a square-free positive integer and R is a ring of order n, then the additive group of R must be cyclic. The following corollary follows immediately.

COROLLARY 3. *If $n = p_1 \dots p_k$ is a square-free positive integer with k distinct prime divisors then there are, up to isomorphism, exactly 2^k rings of order n.*

3. Rings of order p^2 We now give our main result. Notice that if a ring has order p^2 then its additive group is either C_{p^2} or $C_p \times C_p$.

THEOREM 2. *For any prime p there are, up to isomorphism, exactly 11 rings of order p^2. Specifically these are given by the following presentations:*

$$A = \langle a;\ p^2a = 0,\ a^2 = a \rangle = \mathbf{Z}_{p^2}$$

$$B = \langle a;\ p^2a = 0,\ a^2 = pa \rangle$$

$$C = \langle a;\ p^2a = 0,\ a^2 = 0 \rangle = C_{p^2}(0)$$

$$D = \langle a, b;\ pa = pb = 0,\ a^2 = a,\ b^2 = b,\ ab = ba = 0 \rangle = \mathbf{Z}_p + \mathbf{Z}_p$$

$$E = \langle a, b;\ pa = pb = 0,\ a^2 = a,\ b^2 = b,\ ab = a,\ ba = b \rangle$$

$$F = \langle a, b;\ pa = pb = 0,\ a^2 = a,\ b^2 = b,\ ab = b,\ ba = a \rangle$$

$$G = \langle a, b;\ pa = pb = 0,\ a^2 = 0,\ b^2 = b,\ ab = a,\ ba = a \rangle$$

$$H = \langle a, b;\ pa = pb = 0,\ a^2 = 0,\ b^2 = b,\ ab = ba = 0 \rangle = \mathbf{Z}_p + C_p(0)$$

$$I = \langle a, b;\ pa = pb = 0,\ a^2 = b,\ ab = 0 \rangle$$

$$J = \langle a, b;\ pa = pb = 0,\ a^2 = b^2 = 0 \rangle = C_p \times C_p(0)$$

$$K = GF(p^2) = \textit{finite field of order } p^2$$

$$= \begin{cases} \langle a, b;\ pa = pb = 0,\ a^2 = a,\ b^2 = ja,\ ab = b,\ ba = b \rangle \\ \qquad \textit{where } j \textit{ is not a square in } \mathbf{Z}_p, \quad \textit{if } p \neq 2. \\ \langle a, b;\ 2a = 2b = 0,\ a^2 = a,\ b^2 = a + b,\ ab = b,\ ba = b \rangle, \quad \textit{if } p = 2. \end{cases}$$

Proof. Let R be a ring of order p^2. Then the additive group is isomorphic to C_{p^2} or $C_p \times C_p$. If the additive group is C_{p^2} then from Theorem 1 there are three rings up to isomorphism whose presentations are given by:

$$A = \langle a;\ p^2a = 0,\ a^2 = a \rangle = \mathbf{Z}_{p^2}$$

$$B = \langle a;\ p^2a = 0,\ a^2 = pa \rangle$$

$$C = \langle a;\ p^2a = 0,\ a^2 = 0 \rangle = C_{p^2}(0).$$

We now concentrate on rings whose additive group is $C_p \times C_p$. In this case R is a vector space of dimension 2 over the finite field $\mathbf{Z}_p$. Therefore if a' and b' are additive generators of R and $a = xa' + yb'$, $b = wa' + zb'$, then a and b are also additive generators whenever $xw - zy \neq 0 \pmod{p}$.

To obtain the complete classification we show that given a set of additive generators a' and b' for R there exists a (possibly distinct) set of generators a and b such that R equals D, E, F, G, H, I, J, or K. At the same time we show that no two of these rings are isomorphic. This procedure involves an enumeration of cases involving a and b. These cases, in turn, break into two large groups. In the first R contains a set of additive generators a and b whose squares a^2 and b^2 are multiples of themselves—that is $a^2 = ma$ and $b^2 = nb$ with m, n in $\mathbf{Z}_p$. (m or n or both may be zero.) In the second set of cases R has no set of additive generators whose squares are multiples of themselves. We present part of the first set of cases in detail to illustrate the process and then sketch the remainder.

Suppose first that there exist generators a and b such that $a^2 = ma$, $b^2 = nb$, $m \not\equiv 0 \pmod{p}$, and $n \not\equiv 0 \pmod{p}$. Then a and b generate subrings of R isomorphic to $\mathbf{Z}_p$. Thus without loss of generality we may assume that $m = n = 1$ so that we have generators a and b with $a^2 = a$ and $b^2 = b$. Suppose then that $ab = ta + ub$. Then $a^2b = ab = ta^2 + uab = (t + ut)a + u^2b = ta + ub$. It follows that $u^2 \equiv u \pmod{p}$ so that $u \equiv 0 \pmod{p}$ or $u \equiv 1 \pmod{p}$.

Similarly by considering $ab^2 = ab$ we see that $t^2 \equiv t \pmod{p}$, hence either $t \equiv 0 \pmod{p}$ or $u \equiv 0 \pmod{p}$. This gives four possibilities for (t, u) namely $(0,0)$, $(1,0)$, $(0,1)$, or $(1,1)$.

If $(t, u) = (1,1)$ then $ab = a + b$. Then $a^2b = ab = a(a + b) = a^2 + ab = 2a + b \neq a + b = ab$. Therefore the case $t = 1$, $u = 1$ is impossible and so there are only three possibilities for (t, u); namely $(0,0)$, $(1,0)$, and $(0,1)$.

By a symmetrical argument if $ba = xa + yb$ there are three possibilities for (x, y) again; namely $(0,0)$, $(1,0)$, and $(0,1)$. Thus if $a^2 = a$ and $b^2 = b$ there are nine possibilities for ab and ba.

Case 1. $a^2 = a$, $b^2 = b$, $ab = 0$, $ba = 0$. In this case $R = D = \langle a, b : pa = pb = 0, a^2 = a, b^2 = b, ab = ba = 0 \rangle$, and so R is isomorphic to $\mathbf{Z}_p + \mathbf{Z}_p$ under the map $a \to (1,0), b \to (0,1)$.

Case 2. $R = \langle a, b : pa = pb = 0, a^2 = a, b^2 = b, ab = a, ba = a \rangle$. This is isomorphic to $\mathbf{Z}_p + \mathbf{Z}_p$, which we denoted D under the map $a \to (1,0), b \to (1,1)$.

Case 3. $R = \langle a, b : pa = pb = 0, a^2 = a, b^2 = b, ab = b, ba = b \rangle$. This case is symmetric to case 2 above and therefore this R is also isomorphic to $D = \mathbf{Z}_p + \mathbf{Z}_p$.

Case 4. $R = \langle a, b : pa = pb = 0, a^2 = a, b^2 = b, ab = a, ba = 0 \rangle$. In this case $aba = a^2 = a \neq 0$ since a is a generator. However $aba = a \cdot 0 = 0$ and so this case is impossible.

By the same arguments the following three cases are impossible.

Case 5. $R = \langle a, b : pa = pb = 0, a^2 = a, b^2 = b, ab = b, ba = 0 \rangle$.

Case 6. $R = \langle a, b : pa = pb = 0, a^2 = a, b^2 = b, ab = 0, ba = a \rangle$.

Case 7. $R = \langle a, b : pa = pb = 0, a^2 = a, b^2 = b, ab = 0, ba = b \rangle$.

We now consider

Case 8. $R = \langle a, b : pa = pb = 0, a^2 = a, b^2 = b, ab = a, ba = b \rangle$. This is a legitimate possibility in which R is not isomorphic to $\mathbf{Z}_p + \mathbf{Z}_p$ since R is noncommutative. We call this new ring E.

The final case is the following:

Case 9. $R = \langle a, b : pa = pb = 0, a^2 = a, b^2 = b, ab = b, ba = a \rangle$. This R is not isomorphic to $\mathbf{Z}_p + \mathbf{Z}_p$ since R is noncommutative. We claim that R is also not isomorphic to E. Call this ring F. We show that there are no elements in F that satisfy the relations of ring E. Let $A = ma + nb$ where at least one of m and n is

nonzero. Suppose $A^2 = A$. Using the relations in F, we have $(m^2 + mn)a + (n^2 + mn)b = ma + nb$. This implies that $m^2 + mn \equiv m \pmod{p}$ and $n^2 + mn \equiv n \pmod{p}$. If $m = 0$ then $n^2 = n$ and so $n = 1$. Similarly, if $n = 0$ then $m = 1$. If $m \neq 0$ then $m(n + m) = M$, and so $n + m = 1$. Therefore if $A^2 = A$ we must have $A = a$ or $A = b$ or $A = na + (1 - n)b$ for some $n \neq 0, 1$. Similarly, if B is independent from A, we must have either $B = a$ or $B = b$ or $B = xa + (1 - x)b$ for some $x \neq 0, 1$. In case $A = a$ and $B = b$, $AB = ab = b \neq A$, and so A and B do not satisfy the relations of E. Similarly in case $A = b$ and $B = a$. In case $A = a$ and $B = xa + (1 - x)b$ with $x \neq 0, 1$, $AB = a(xa + (1 - x)b) = xa^2 + (1 - x)ab = xa + (1 - x)b = B \neq A$, and so A and B do not satisfy the relations of E. The result is similar in case $A = b$ and $B = xa + (1 - x)b$, in case $B = a$ and $A = na + (1 - n)b$, and in case $B = b$ and $A = na + (1 - n)b$. Therefore the only case in which we could get the ring E is the one in which $A = na + (1 - n)b$ for some $n \neq 0, 1$ and $B = xa + (1 - x)b$ for some $x \neq 0, 1$. Suppose then that $AB = A$ as it would be in E. By computing we find that AB also equals B, and so $A = B$, which contradicts the fact that A and B are independent. Therefore F is not isomorphic to E. Thus F is another ring with additive group $C_p \times C_p$.

Cases 1 through 9 describe the possibilities in which $a^2 = a$ and $b^2 = b$ and give us three additional nonisomorphic rings D, E, and F.

We now sketch the remainder of the proof. The details are carried out as in the above cases—possible presentations for R are identified and then shown to either equal a ring that is isomorphic to one already on the list or to be a new nonisomorphic ring.

For instance, consider the situation in which R has a set of additive generators a and b with one of their squares zero and the other a multiple of itself. If $a^2 = 0$ and $b^2 = b$, two new nonisomorphic rings, G and H, are obtained:

$$G = \langle a, b;\ pa = pb = 0,\ a^2 = 0,\ b^2 = b,\ ab = a,\ ba = a \rangle$$
$$H = \langle a, b;\ pa = pb = 0,\ a^2 = 0,\ b^2 = b,\ ab = 0,\ ba = 0 \rangle.$$

G is commutative and H is isomorphic to $\mathbf{Z}_p + C_p(0)$.

In the final situation R has no set of two independent generators whose squares are both nonzero multiples of themselves. If R has a generator a with $a^2 = b$ and b independent from a, then an enumeration of cases leads to two new additional nonisomorphic rings, I and K:

$$I = \langle a, b;\ pa = pb = 0,\ a^2 = b,\ ab = 0 \rangle$$
$$K = \begin{cases} \langle a, b;\ pa = pb = 0,\ a^2 = a,\ ab = b,\ b^2 = ja \text{ for some } j \text{ in } \mathbf{Z}_p \rangle, & \text{if } p \neq 2. \\ \langle a, b;\ 2a = 2b = 0,\ a^2 = a,\ b^2 = a + b,\ ab = b,\ ba = b \rangle, & \text{if } p = 2. \end{cases}$$

In both cases K is precisely the finite field $GF(p^2)$.

If R has two generators both of whose squares are trivial, then the multiplication is trivial and so $R = C_p \times C_p(0) = J$.

We mention in closing that the group ring $\mathbf{Z}_p(C_2)$, which also has order p^2, is isomorphic to $\mathbf{Z}_p + \mathbf{Z}_p$. Identifying 1 in $\mathbf{Z}_p$ with the generator a and the group generator of C_2 with b shows that the group ring has the presentation $\langle a, b;\ pa = pb = 0,\ a^2 = a,\ b^2 = a,\ ab = b,\ ba = b \rangle$. The map $a \to (1, -1), b \to (1, -1)$ gives the desired isomorphism.

REFERENCES

1. J. A. Gallian, *Contemporary Abstract Algebra*, D. C. Heath and Company, Lexington, MA, 1990.
2. W. C. Waterhouse, Rings with cyclic additive group, *Amer. Math. Monthly* 71 (1964), 449–450.