GROUPS OF ORDER p^2

KEITH CONRAD

For each prime p there is one group of order p up to isomorphism, namely the cyclic group $\mathbf{Z}/(p)$. For groups of order p^2 there are at least two possibilities: $\mathbf{Z}/(p^2)$ and $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$. These are not isomorphic since the first group is cyclic and the second is not (every non-identity element in it has order p). We will show that every group of order p^2 is isomorphic to one of those two groups. This result is due to Netto [2, pp. 148–149].[1] and we will largely follow Netto's proof, which doesn't involve anything other than careful work with products, conjugates, and orders of elements. The key point is to show first that all groups of order p^2 are abelian. After that, it is not hard to classify the possible groups that can occur. At the end we'll revisit Netto's argument to see how it can be simplified using cosets.

Theorem 1. *For prime p, every group of order p^2 is abelian.*

Proof. Let G be a group of order p^2. If G is cyclic then it is abelian, so we can suppose G is not cyclic. Pick $x \in G - \{e\}$, and since $G \neq \langle x \rangle$ (otherwise G would be cyclic) we can pick $y \in G - \langle x \rangle$. Since the order of each element of G divides p^2 and no element of G has order p^2, each non-identity element of G must have order p. Thus x and y each have order p. Since $\langle x \rangle$ and $\langle y \rangle$ are subgroups of G with prime order p and they are different subgroups (the first does not contain y and the second does), their intersection is trivial: $\langle x \rangle \cap \langle y \rangle = \{e\}$.

In the list of products $\{x^i y^j : 0 \leq i, j \leq p-1\}$ we will show there are no duplicates. If $x^i y^j = x^{i'} y^{j'}$ then $x^{-i'+i} = y^{j'-j}$, which belongs to $\langle x \rangle \cap \langle y \rangle$, so $x^{-i'+i} = e$ and $y^{j'-j} = e$. Since x and y have order p, $i' \equiv i \bmod p$ and $j' \equiv j \bmod p$. The exponents are in $\{0, 1, \ldots, p-1\}$, so being congruent mod p forces equality: $i' = i$ and $j' = j$. Thus the number of different elements of G in $\{x^i y^j : 0 \leq i, j \leq p-1\}$ is p^2, which matches $|G|$, so $G = \{x^i y^j : 0 \leq i, j \leq p-1\}$.

Now consider the product yx. It has to be some $x^{i_1} y^{j_1}$. Similarly, $y^2 x, \ldots, y^{p-1} x$ all have a similar form:

$$yx = x^{i_1} y^{i_1}, \quad y^2 x = x^{i_2} y^{i_2}, \quad \ldots, \quad y^{p-1} x = x^{i_{p-1}} y^{i_{p-1}},$$

where $0 \leq i_k, j_k \leq p-1$. Each i_k is not 0, since otherwise $y^k x = y^{i_k}$, so $x = y^{i_k - k} \in \langle y \rangle$, but $\langle x \rangle$ and $\langle y \rangle$ intersect trivially.

Claim: there are $m, n \not\equiv 0 \bmod p$ such that $x y^m x^{-1} = y^n$.

Case 1: Two of the products among $yx, y^2 x, \ldots, y^{p-1} x$ have the same power of x when written as $x^i y^j$.

This implies there are $k \neq k'$ in $\{1, \ldots, p-1\}$ such that $y^k x = x^i y^{j_k}$ and $y^{k'} x = x^i y^{j_{k'}}$ for a common i. Then $j_k \neq j_{k'}$ in $\{0, \ldots, p-1\}$ (otherwise $y^k x = y^{k'} x$, so $k \equiv k' \bmod p$, but k and k' are distinct in $\{1, \ldots, p-1\}$). Solving for x^i in both equations, we get

$$y^k x y^{-j_k} = x^i = y^{k'} x y^{-j_{k'}},$$

[1] The special case $p = 2$ was treated earlier by Cayley [1, pp. 43-44].

so $y^{k-k'}x = xy^{j_k-j_{k'}}$, or equivalently $xy^{j_k-j_{k'}}x^{-1} = y^{k-k'}$. The exponents on y on both sides are nonzero mod p since each is a difference of unequal numbers in $\{0,\dots,p-1\}$.

Case 2: All of the products among $yx, y^2x, \dots, y^{p-1}x$ have different powers of x when written as x^iy^j.

This means one of these p terms has $i = 1$: $y^kx = xy^j$ for some k in $\{1,\dots,p-1\}$ and some j. Rewrite that equation as $xy^jx^{-1} = y^k$. We have $j \not\equiv 0 \bmod p$, since otherwise $y^k = xex^{-1} = e$, but that is not true since y has order p and k is not divisible by p.

From the claim, raise both sides of $xy^mx^{-1} = y^n$ to the ℓ-th power for $\ell \in \mathbf{Z}$, getting $(xy^mx^{-1})^\ell = y^{n\ell}$, so $xy^{m\ell}x^{-1} = y^{n\ell}$. Use for ℓ a multiplicative inverse of m mod p (this can be done since p is prime and $m \not\equiv 0 \bmod p$), so $y^{m\ell} = y^1 = y$ and thus $xyx^{-1} = y^N$ where $N = n\ell$. In words, this says the conjugate of y by x is y^N. Let's conjugate y by x^2:

$$x^2yx^{-2} = x(xyx^{-1})x^{-1} = xy^Nx^{-1} = (xyx^{-1})^N = (y^N)^N = y^{N^2}.$$

By similar reasoning and induction, $x^ryx^{-r} = y^{N^r}$ for all $r \geq 1$. Taking $r = p$, so $x^r = e$, we get $y = y^{N^p}$. Since y has order p, the exponents are congruent mod p: $1 \equiv N^p \bmod p$. By Fermat's little theorem we have $N^p \equiv N \bmod p$, so $1 \equiv N \bmod p$, and that means $y^N = y^1 = y$, so $xyx^{-1} = y^N = y$, or equivalently $xy = yx$: x and y commute.

Since every element of G has the form x^iy^j and x and y commute, all powers of x commute with all powers of y and thus all elements of G commute with each other:

$$(x^iy^j)(x^{i'}y^{j'}) = x^i(y^jx^{i'})y^{j'} = x^i(x^{i'}y^j)y^{j'} = (x^ix^{i'})(y^jy^{j'}) = x^{i+i'}y^{j+j'}. \tag{1}$$

This last expression is unchanged if we swap i with i' and j with j', so x^iy^j and $x^{i'}y^{j'}$ commute. □

Theorem 2. *For prime p, there are two groups of order p^2 up to isomorphism: $\mathbf{Z}/(p^2)$ and $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$.*

Proof. All cyclic groups of the same order are isomorphic, so it suffices to show every noncyclic group G of order p^2 is isomorphic to $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$.

By Theorem 1, G is abelian and contains elements x and y of order p such that every element of G has a unique representation as x^iy^j where $i, j \in \{0,\dots,p-1\}$. The exponents in x^iy^j only matter mod p since x and y have order p, so we can define $f\colon \mathbf{Z}/(p)\times\mathbf{Z}/(p) \to G$ by $f(i \bmod p, j \bmod p) = x^iy^j$. By the unique representation of elements of G in the form x^iy^j, f is a bijection. Since x and y commute, f is a homomorphism by (1):

$$f(i \bmod p, j \bmod p)f(i' \bmod p, j' \bmod p) = (x^iy^j)(x^{i'}y^{j'}) = x^{i+i'}y^{j+j'},$$

which is $f(i + i' \bmod p, j + j' \bmod p)$. A bijective homomorphism is an isomorphism: $G \cong \mathbf{Z}/(p) \times \mathbf{Z}/(p)$. □

In the proof of Theorem 1, an overarching logic to the succession of steps may be hard to make out. We will "modernize" the claim in that proof saying $xy^mx^{-1} = y^n$ for some integers m and n that are nonzero mod p by using cosets.

Set $H = \langle y\rangle$. Since $\langle x\rangle$ and $\langle y\rangle$ intersect trivially, no power of x is in H except for the identity, so the left H-cosets $H, xH, x^2H, \dots, x^{p-1}H$ are mutually disjoint (they have different powers of x as representatives).

The right H-coset Hx is disjoint from H (x is not in H and different right H-cosets are disjoint), so $Hx \subset \bigcup_{i=1}^{p-1} x^iH$. Since Hx has size p and the union contains $p-1$ cosets x^iH,

at least two elements from Hx have to lie in a common x^iH.[2] Write this as $y^jx \in x^iH$ and $y^kx \in x^iH$ where j and k are different integers in $\{0, \ldots, p-1\}$. Thus

$$y^jx = x^iy^{j'}, \quad y^kx = x^iy^{k'},$$

so $j' \not\equiv k' \bmod p$ (why?) and that implies

$$y^jxy^{-j'} = x^i = y^kxy^{-k'} \Longrightarrow y^{j-k}x = xy^{j'-k'} \Longrightarrow xy^{j'-k'}x^{-1} = y^{j-k}.$$

Since j and k are incongruent mod p, as are j' and k', we get $xy^mx^{-1} = y^n$ where $m = j' - k' \not\equiv 0 \bmod p$ and $n = j - k \not\equiv 0 \mod p$, and this completes the proof of the claim in the proof of Theorem 1.

References

[1] A. Cayley, "On the Theory of Groups, as Depending on the Symbolic Equation $\theta^n = 1$," *Philos. Mag.* **7** (1854), 40–47. Also pp. 123–130 of *The Collected Papers of Arthur Cayley,* Vol. II, Cambridge Univ. Press, 1889.

[2] E. Netto, *The Theory of Substitutions and its Applications to Algebra*, Register Publ. Co., Ann Arbor, 1892. Online at https://archive.org/details/theoryofsubstitu00nett/page/148.

[2] This is closely related to the pigeonhole principle: a function from an a-element set to a b-element set where $a > b$ must send at least two elements to the same value.