p-group

Not to be confused with n-group (category theory).

In mathematical group theory, given a prime number p, a ***p*-group** is a group in which each element has a power of p as its order. That is, for each element g of a p-group, there exists a nonnegative integer n such that the product of p^n copies of g, and not less, is equal to the identity element. The orders of different elements may be different powers of p. Such groups are also called ***p*-primary** or simply **primary**.

A finite group is a p-group if and only if its order (the number of its elements) is a power of p. Given a finite group G, the Sylow theorems guarantee for every prime power p^n that divides the order of G the existence of a subgroup of G of order p^n.

The remainder of this article deals with finite p-groups. For an example of an infinite abelian p-group, see Prüfer group, and for an example of an infinite simple p-group, see Tarski monster group.

1 Properties

Every p-group is periodic since by definition every element has finite order.

1.1 Non-trivial center

One of the first standard results using the class equation is that the center of a non-trivial finite p-group cannot be the trivial subgroup.[1]

This forms the basis for many inductive methods in p-groups.

For instance, the normalizer N of a proper subgroup H of a finite p-group G properly contains H, because for any counterexample with $H=N$, the center Z is contained in N, and so also in H, but then there is a smaller example H/Z whose normalizer in G/Z is $N/Z=H/Z$, creating an infinite descent. As a corollary, every finite p-group is nilpotent.

In another direction, every normal subgroup of a finite p-group intersects the center nontrivially as may be proved by considering the elements of N which are fixed when G acts on N by conjugation. Since every central subgroup is normal, it follows that every minimal normal subgroup of a finite p-group is central and has order p. Indeed, the socle of a finite p-group is the subgroup of the center consisting of the central elements of order p.

If G is a p-group, then so is G/Z, and so it too has a non-trivial center. The preimage in G of the center of G/Z is called the second center and these groups begin the upper central series. Generalizing the earlier comments about the socle, a finite p-group with order p^n contains normal subgroups of order p^i with $0 \leq i \leq n$, and any normal subgroup of order p^i is contained in the ith center Zi. If a normal subgroup is not contained in Zi, then its intersection with Zi_{+1} has size at least p^{i+1}.

1.2 Automorphisms

The automorphism groups of p-groups are well studied. Just as every finite p-group has a nontrivial center so that the inner automorphism group is a proper quotient of the group, every finite p-group has a nontrivial outer automorphism group. Every automorphism of G induces an automorphism on $G/\Phi(G)$, where $\Phi(G)$ is the Frattini subgroup of G. The quotient $G/\Phi(G)$ is an elementary abelian group and its automorphism group is a general linear group, so very well understood. The map from the automorphism group of G into this general linear group has been studied by Burnside, who showed that the kernel of this map is a p-group.

2 Examples

p-groups of the same order are not necessarily isomorphic; for example, the cyclic group C_4 and the Klein four-group V_4 are both 2-groups of order 4, but they are not isomorphic.

Nor need a p-group be abelian; the dihedral group Dih_4 of order 8 is a non-abelian 2-group. However, every group of order p^2 is abelian.[note 1]

The dihedral groups are both very similar to and very dissimilar from the quaternion groups and the semidihedral groups. Together the dihedral, semidihedral, and quaternion groups form the 2-groups of maximal class, that is those groups of order 2^{n+1} and nilpotency class n.

2.1 Iterated wreath products

The iterated wreath products of cyclic groups of order p are very important examples of p-groups. Denote the cyclic group of order p as $W(1)$, and the wreath product of $W(n)$ with $W(1)$ as $W(n+1)$. Then $W(n)$ is the Sylow p-subgroup of the symmetric group $\mathrm{Sym}(p^n)$. Maximal p-subgroups of the general linear group $\mathrm{GL}(n,\mathbf{Q})$ are direct products of various $W(n)$. It has order p^k where $k = (p^n - 1)/(p - 1)$. It has nilpotency class p^{n-1}, and its lower central series, upper central series, lower exponent-p central series, and upper exponent-p central series are equal. It is generated by its elements of order p, but its exponent is p^n. The second such group, $W(2)$, is also a p-group of maximal class, since it has order p^{p+1} and nilpotency class p, but is not a regular p-group. Since groups of order p^p are always regular groups, it is also a minimal such example.

2.2 Generalized dihedral groups

When $p = 2$ and $n = 2$, $W(n)$ is the dihedral group of order 8, so in some sense $W(n)$ provides an analogue for the dihedral group for all primes p when $n = 2$. However, for higher n the analogy becomes strained. There is a different family of examples that more closely mimics the dihedral groups of order 2^n, but that requires a bit more setup. Let ζ denote a primitive pth root of unity in the complex numbers, let $\mathbf{Z}[\zeta]$ be the ring of cyclotomic integers generated by it, and let P be the prime ideal generated by $1-\zeta$. Let G be a cyclic group of order p generated by an element z. Form the semidirect product $E(p)$ of $\mathbf{Z}[\zeta]$ and G where z acts as multiplication by ζ. The powers P^n are normal subgroups of $E(p)$, and the example groups are $E(p,n) = E(p)/P^n$. $E(p,n)$ has order p^{n+1} and nilpotency class n, so is a p-group of maximal class. When $p = 2$, $E(2,n)$ is the dihedral group of order 2^n. When p is odd, both $W(2)$ and $E(p,p)$ are irregular groups of maximal class and order p^{p+1}, but are not isomorphic.

2.3 Unitriangular matrix groups

The Sylow subgroups of general linear groups are another fundamental family of examples. Let V be a vector space of dimension n with basis $\{ e_1, e_2, \ldots, en \}$ and define Vi to be the vector space generated by $\{ ei, ei_{+1}, \ldots, en \}$ for $1 \le i \le n$, and define $Vi = 0$ when $i > n$. For each $1 \le m \le n$, the set of invertible linear transformations of V which take each Vi to $Vi_{+}m$ form a subgroup of $\mathrm{Aut}(V)$ denoted Um. If V is a vector space over $\mathbf{Z}/p\mathbf{Z}$, then U_1 is a Sylow p-subgroup of $\mathrm{Aut}(V) = \mathrm{GL}(n, p)$, and the terms of its lower central series are just the Um. In terms of matrices, Um are those upper triangular matrices with 1s one the diagonal and 0s on the first $m-1$ superdiagonals. The group U_1 has order $p^{n\cdot(n-1)/2}$, nilpotency class n, and exponent p^k where k is the least integer at least as large as the base p logarithm of n.

3 Classification

The groups of order p^n for $0 \le n \le 4$ were classified early in the history of group theory,[2] and modern work has extended these classifications to groups whose order divides p^7, though the sheer number of families of such groups grows so quickly that further classifications along these lines are judged difficult for the human mind to comprehend.[3] For example, Marshall Hall Jr. and James K. Senior classified groups of order 2^n for $n \le 6$ in 1964.[4]

Rather than classify the groups by order, Philip Hall proposed using a notion of isoclinism of groups which gathered finite p-groups into families based on large quotient and subgroups.[5]

An entirely different method classifies finite p-groups by their **coclass**, that is, the difference between their composition length and their nilpotency class. The so-called **coclass conjectures** described the set of all finite p-groups of fixed coclass as perturbations of finitely many pro-p groups. The coclass conjectures were proven in the 1980s using techniques related to Lie algebras and powerful p-groups.[6] The final proofs of the **coclass theorems** are due to A. Shalev and independently to C. R. Leedham-Green, both in 1994. They admit a classification of finite p-groups in directed coclass graphs consisting of only finitely many coclass trees whose (infinitely many) members are characterized by finitely many parametrized presentations.

Every group of order p^5 is metabelian.[7]

3.1 Up to p^3

The trivial group is the only group of order one, and the cyclic group Cp is the only group of order p. There are exactly two groups of order p^2, both abelian, namely Cp^2 and $Cp \times Cp$. For example, the cyclic group C_4 and the Klein four-group V_4 which is $C_2 \times C_2$ are both 2-groups of order 4.

There are three abelian groups of order p^3, namely Cp^3, $Cp^2 \times Cp$, and $Cp \times Cp \times Cp$. There are also two non-abelian groups.

For $p \ne 2$, one is a semi-direct product of $Cp \times Cp$ with Cp, and the other is a semi-direct product of Cp^2 with Cp. The first one can be described in other terms as group $\mathrm{UT}(3,p)$ of unitriangular matrices over finite field with p elements, also called the Heisenberg group mod p.

For $p = 2$, both the semi-direct products mentioned above are isomorphic to the dihedral group Dih_4 of order 8. The other non-abelian group of order 8 is the quaternion group Q_8.

4 Prevalence

4.1 Among groups

The number of isomorphism classes of groups of order p^n grows as $p^{\frac{2}{27}n^3+O(n^{8/3})}$, and these are dominated by the classes that are two-step nilpotent.[8] Because of this rapid growth, there is a folklore conjecture asserting that almost all finite groups are 2-groups: the fraction of isomorphism classes of 2-groups among isomorphism classes of groups of order at most *n* is thought to tend to 1 as *n* tends to infinity. For instance, of the 49 910 529 484 different groups of order at most 2000, 49 487 365 422, or just over 99%, are 2-groups of order 1024.[9]

4.2 Within a group

Every finite group whose order is divisible by *p* contains a subgroup which is a non-trivial *p*-group, namely a cyclic group of order *p* generated by an element of order *p* obtained from Cauchy's theorem. In fact, it contains a *p*-group of maximal possible order: if $|G| = n = p^k m$ where *p* does not divide *m*, then *G* has a subgroup *P* of order p^k, called a Sylow *p*-subgroup. This subgroup need not be unique, but any subgroups of this order are conjugate, and any *p*-subgroup of *G* is contained in a Sylow *p*-subgroup. This and other properties are proved in the Sylow theorems.

5 Application to structure of a group

p-groups are fundamental tools in understanding the structure of groups and in the classification of finite simple groups. *p*-groups arise both as subgroups and as quotient groups. As subgroups, for a given prime *p* one has the Sylow *p*-subgroups *P* (largest *p*-subgroup not unique but all conjugate) and the *p*-core $O_p(G)$ (the unique largest *normal* *p*-subgroup), and various others. As quotients, the largest *p*-group quotient is the quotient of *G* by the *p*-residual subgroup $O^p(G)$. These groups are related (for different primes), possess important properties such as the focal subgroup theorem, and allow one to determine many aspects of the structure of the group.

5.1 Local control

Much of the structure of a finite group is carried in the structure of its so-called **local subgroups**, the normalizers of non-identity *p*-subgroups.[10]

The large elementary abelian subgroups of a finite group exert control over the group that was used in the proof of the Feit–Thompson theorem. Certain central extensions of elementary abelian groups called extraspecial groups help describe the structure of groups as acting on symplectic vector spaces.

Brauer classified all groups whose Sylow 2-subgroups are the direct product of two cyclic groups of order 4, and Walter, Gorenstein, Bender, Suzuki, Glauberman, and others classified those simple groups whose Sylow 2-subgroups were abelian, dihedral, semidihedral, or quaternion.

6 See also

- Elementary group
- Prüfer rank
- Regular p-group

7 Footnotes

7.1 Notes

[1] To prove that a group of order p^2 is abelian, note that it is a *p*-group so has non-trivial center, so given a non-trivial element of the center *g,* this either generates the group (so *G* is cyclic, hence abelian: $G = C_{p^2}$), or it generates a subgroup of order *p,* so *g* and some element *h* not in its orbit generate *G,* (since the subgroup they generate must have order p^2) but they commute since *g* is central, so the group is abelian, and in fact $G = C_p \times C_p$.

7.2 Citations

[1] proof

[2] (Burnside 1897)

[3] (Leedham-Green & McKay 2002, p. 214)

[4] (Hall, Jr. & Senior 1964)

[5] (Hall 1940)

[6] (Leedham-Green & McKay 2002)

[7] "Every group of order p^5 is metabelian". Stack Exchange. 24 March 2012. Retrieved 7 January 2016.

[8] (Sims 1965)

[9] (Besche, Eick & O'Brien 2002)

[10] (Glauberman 1971)

8 References

- Besche, Hans Ulrich; Eick, Bettina; O'Brien, E. A. (2002), "A millennium project: constructing small groups", *International Journal of Algebra and Computation*, **12** (5): 623–644, doi:10.1142/S0218196702001115, MR 1935567

- Burnside, William (1897), *Theory of groups of finite order*, Cambridge University Press
- Glauberman, George (1971), "Global and local properties of finite groups", *Finite simple groups (Proc. Instructional Conf., Oxford, 1969)*, Boston, MA: Academic Press, pp. 1–64, MR 0352241
- Hall, Jr., Marshall; Senior, James K. (1964), *The Groups of Order 2^n ($n \le 6$)*, London: Macmillan, LCCN 64016861, MR 168631 — An exhaustive catalog of the 340 non-abelian groups of order dividing 64 with detailed tables of defining relations, constants, and lattice presentations of each group in the notation the text defines. "Of enduring value to those interested in finite groups" (from the preface).
- Hall, Philip (1940), "The classification of prime-power groups", *Journal für die reine und angewandte Mathematik*, **182** (182): 130–141, doi:10.1515/crll.1940.182.130, ISSN 0075-4102, MR 0003389
- Leedham-Green, C. R.; McKay, Susan (2002), *The structure of groups of prime power order*, London Mathematical Society Monographs. New Series, **27**, Oxford University Press, ISBN 978-0-19-853548-5, MR 1918951
- Sims, Charles (1965), "Enumerating p-groups", *Proc. London Math. Soc. (3)*, **15**: 151–166, doi:10.1112/plms/s3-15.1.151, MR 0169921

9 Further reading

- Berkovich, Yakov (2008), *Groups of Prime Power Order*, de Gruyter Expositions in Mathematics 46, Volume 1, Berlin: Walter de Gruyter GmbH, ISBN 978-3-1102-0418-6
- Berkovich, Yakov; Janko, Zvonimir (2008), *Groups of Prime Power Order*, de Gruyter Expositions in Mathematics 47, Volume 2, Berlin: Walter de Gruyter GmbH, ISBN 978-3-1102-0419-3
- Berkovich, Yakov; Janko, Zvonimir (2011-06-16), *Groups of Prime Power Order*, de Gruyter Expositions in Mathematics 56, Volume 3, Berlin: Walter de Gruyter GmbH, ISBN 978-3-1102-0717-0

10 External links

- Rowland, Todd and Weisstein, Eric W. "p-Group". *MathWorld*.

11 Text and image sources, contributors, and licenses

11.1 Text

- **P-group** *Source:* https://en.wikipedia.org/wiki/P-group?oldid=740935446 *Contributors:* AxelBoldt, Derek Ross, Zundark, Toby Bartels, Patrick, Chas zzz brown, Michael Hardy, TakuyaMurata, AugPi, Andres, Charles Matthews, Lowellian, MathMartin, Tea2min, Giftlite, Almit39, Goochelaar, Saccade, Marudubshinki, Graham87, Staecker, R.e.b., FlaBot, Margosbot~enwiki, Grubber, Dtrebbien, SmackBot, Nbarth, Tsca.bot, Mhym, Richard L. Peterson, J. Finkelstein, Dto, Ntsimp, Thijs!bot, Kilva, Headbomb, RobHar, Lawilkin, Fruits Monster, Idioma-bot, TXiKiBoT, Thehotelambush, JackSchmidt, Joelsims80, Tyrus 400, Legobot, Luckas-bot, Yobot, Citation bot, Citation bot 1, DrilBot, Jonesey95, Alexander Chervov, DanielConstantinMayer, ZéroBot, Wikfr, BG19bot, Teddyktchan, Bender the Bot and Anonymous: 23

11.2 Images

- **File:Cyclic_group.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/5/5f/Cyclic_group.svg *License:* CC BY-SA 3.0 *Contributors:*
- Cyclic_group.png *Original artist:*
- derivative work: Pbroks13 (talk)

11.3 Content license

- Creative Commons Attribution-Share Alike 3.0