Structure of groups of special sizes

Summary:

Let p denote a prime number. Then (i) $|G| = p \Rightarrow G \cong \mathbf{Z}_p$; (ii) $|G| = p^2 \Rightarrow G$ is Abelian, so $G \cong \mathbf{Z}_{p^2}$ or $\mathbf{Z}_p \times \mathbf{Z}_p$; (iii) If $p > 2$, then $|G| = 2p \Rightarrow G \cong \mathbf{Z}_{2p}$ or D_p.

Let $g(n)$ denote the number of groups of size n. Then $g(p) = 1$ if p is a prime and

n	1	4	6	8	9	10	12	14	15	16
$g(n)$	1	2	2	5	2	2	5	2	1	14

The 5 groups of 8 elements are $\mathbf{Z}_8$; $\mathbf{Z}_4 \times \mathbf{Z}_2$; $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$; D_4; and Q.

The 5 groups of 12 elements are $\mathbf{Z}_4 \times \mathbf{Z}_3$; $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3$; D_6; A_4, and one more group.

Please note, that there is only one group of size 15, though 15 is not a prime.

Proofs of some special cases:

(A) $|G| = p$: It was a consequence of Lagrange's Theorem (see there) that G is cyclic, hence $G \cong \mathbf{Z}_p$.

(B) $|G| = 4$: We show that $G \cong \mathbf{Z}_4$ or K (the Klein group). Consider the orders of the elements. If some element has order 4, then G is cyclic. Otherwise every element has order 2 except the identity (as $o(g) \mid |G|$). Let the three non-identity elements be a, b, and c, which element will be (say) ab? If $ab = e = a^2$, then multiplying both sides by a from the left, we obtain $b = a$, a contradiction. We arrive at a contradiction similarly also if $ab = a$ or $ab = b$. Hence $ab = c$. So the product of any two distinct non-identity elements is the third one. These conditions yield $G \cong K$.

(C) $|G| = 2p$ where $p > 2$ is a prime. If G is cyclic, then $G \cong \mathbf{Z}_{2p}$. We show that a non-cyclic G is isomorphic to D_p. The orders of the non-identity elements are non-trivial divisors of $2p$, i.e. 2 and p. It can be shown, that if a prime q divides the size of a group, then there must be an element of order q (Cauchy's Theorem, this is not necessarily true for composite q, see Problem 117). Let $o(r) = p$, $o(t) = 2$. Then $t^j r^k$, $0 \le j \le 1, 0 \le k \le p-1$ are all distinct, hence they are all elements of G. Also, $t^2 = r^k = e$. To complete the characterization of G as D_p we have to verify $rt = tr^{-1}$. Clearly, (*) $rt = tr^s$ for some $0 \le s \le p-1$. We rewrite (*) as $t^{-1}rt = r^s$, and conjugate it again by t:

$$r = t^{-1}(t^{-1}rt)t = t^{-1}r^s t = (t^{-1}rt)(t^{-1}rt)\dots(t^{-1}rt) = (r^s)^s = r^{s^2}.$$

Thus $p = o(r) \mid s^2 - 1$, and since p is a prime, this implies $s = 1$ or $s = p-1$. In the first case $rt = tr$, so $(rt)^m = r^m t^m$, which easily yields $o(rt) = 2p$. This would mean that G is cyclic, hence $s = p-1$, so (*) gives $rt = tr^{p-1} = tr^{-1}$ as claimed.

Permutation groups are subgroups of S_n.

Cayley's Theorem: Every group of size n is isomorphic to a subgroup of S_n (hence every group can be considered as a permutation group).

Proof: Consider S_n as all permutations of the group $G = \{e = g_1, g_2, \dots, g_n\}$ and define $\varphi : G \to S_n$ by $g \mapsto \begin{pmatrix} g_i \\ gg_i \end{pmatrix}$, i.e. we assign to every $g \in G$ the permutation of G onto itself which multiplies every $g_i \in G$ by the given g from the left. This multiplication is one-to-one indeed, as $gg_i = gg_j \Rightarrow g_i = g_j$. We show that φ is an injective homomorphism, hence $G \cong \operatorname{Im}\varphi \le S_n$.

We first verify $\varphi(g)\varphi(h) = \varphi(gh)$, i.e.

$$\begin{pmatrix} g_i \\ gg_i \end{pmatrix} \begin{pmatrix} g_i \\ hg_i \end{pmatrix} = \begin{pmatrix} g_i \\ (gh)g_i \end{pmatrix}. \tag{1}$$

The left hand side in (1) means that we multiply every element g_i first by h, and then by g from the left, so we obtain $g(hg_i)$. Due to associativity in G this is equal to the multiplication of g_i by gh which is just the right hand side of (1).

Injectivity is equivalent to $\operatorname{Ker}\varphi = e_G$, i.e. $\begin{pmatrix} g_i \\ gg_i \end{pmatrix}$ is the identity iff $g = e$ which is obvious.

Permutation groups and the solvability of algebraic equations — a tale

An important fact is that for $n \geq 5$, A_n has only trivial normal subgroups. This is the key of the fact that there exists no general formula for solving algebraic equations of degree greater than four.

We make a very vague illustration how permutations and equations are related.

To solve an equation of degree 1 we need just the field operations. For degree 2 we have the quadratic formula which involves one square root, too. For degree 3 the so-called Cardano formula works which requires also taking a square root and a cube root. For degree 4 we take a square root, a cube root, and two more square roots.

We can write the following chains for S_n:

$$\{e\} \lhd S_2; \quad \{e\} \lhd A_3 \lhd S_3; \quad \{e\} \lhd \mathbf{Z}_2 \lhd K \lhd A_4 \lhd S_4$$

where $K = \{e, (12)(34), (13)(24), (14)(23)\}$ and (e.g.) $\mathbf{Z}_2 = \{e, (12)(34)\}$. In these chains every subgroup is normal in the next subgroup (verify it!), but not necessarily in the entire group, and the size of each factor group is a prime. These primes correspond to the exponents of roots in the formulas for solving the equations. The relation is that we can assign to an equation of degree n certain permutations of its n zeros (among the complex numbers).

For $n \geq 5$ we have only the chain $\{e\} \lhd A_n \lhd S_n$, and here the size $n!/2$ of the first factor group is not a prime, and this is the reason that there is no formula for solving equations of degree ≥ 5.

Simple groups — another tale

A G group is *simple* if its only normal subgroups are the trivial ones. E.g. A_n is simple for $n \geq 5$, as mentioned above. The simple groups play a central role in describing the structure of groups. As a result of the work of many hundreds of outstanding mathematicians for more than 100 years, all finite simple groups have been found and their complete list and description was summarized in the Atlas of Finite Simple Groups in 1985. This list contains 17 infinite sequences (such as A_n for $n \geq 5$) and 26 sporadic groups. The largest sporadic group is the *Monster* having about $8 \cdot 10^{53}$ elements which is a far bigger number than the number of atoms in the Earth. The Monster can be interpreted as the group of certain rotations of the 196883 dimensional space, and this is the smallest possible dimension for this purpose. The characterization of the finite simple groups is called the ten-thousand-page-proof referring to the (underestimated) total length of the papers providing the result. The first major breakthrough was the proof that the size of a finite simple group cannot be an odd composite number, these (very concisely written) 250 pages filled the complete volume of a journal in 1963.