Groups

preliminary version September 7, 2009

This is not meant as a systematic account of elementary facts about groups, those are assumed known, and in any case to be found in the course compendium, but is meant as a complement.

Groups come in basically three flavours, finite groups, countable groups and continuous groups. Examples of all three will figure in the course, especially of the first and last.

There is a notion of an abstract group and a concrete one, the latter is usually referred to as a representation. A representation is usually given by an action of a group. A group G is said to act on a set X by associating to every $x \in X$ an element $gx \in X$. The action should be compatible with the group structure this means the 'associative' law $g(hx) = (gh)x$.

The set $gx : g \in G$ is refered to as the orbit of x. Any action of a group on a set X effects a partion of the set given by the orbits. An action is said to be transitive, if X itself is an orbit.

(Any action on X defines an action on $X \times X$ by $g(x, y) = (gx, gy)$. The original action can be recaptured by looking at the restriction to the diagonal $\Delta = \{(x, x)\}$. The action is said to be doubly transitive, if $X \setminus \Delta$ is an orbit. I.e. for any pairs $(x_1, x_2), (y_1, y_2)$ with $x_1 \neq x - 2, y_1 \neq y_2$ there is a g such $gx_1 = y_1, gx_2 = y_2$).

The stabilizer of an element is the subgroup S_x defined by $\{g : gx = x\}$. The number of elements in an orbit is given by the index of S_x in G, i.e. $|G|/|S_x|$.

If X is a finite set we speak of G as a sub-group of permutations. If X is an infinite set with some structure, say a vector space, we want the functions $x \to gx$ to respect that structure. In particular we have representations of groups as linear transformations on some vector space. Those are actually the most important and fruitful of all the concrete presentations and we will return to them later in the course.

Every finite group can be thought of as a subgroup of a finite permutation group. Simply let G cat on itself by left multiplication. A more important action is given by conjugation. $g \mapsto (x \to gxg^{-1})$. In particular a group can act on itself by conjugation. Each element can then be thought of an automorphism of the group (the action respects the special structure on G, namely its group structure). The stabilizer of every element $x \in G$ is then all the elements that commute with x. In particular the number of elements in a conjugacy class is given by the index of the stabilizer.

If G is a finite group and H is a subgroup then the order of H always divide the order of G, the quotient is referred to as the index of the sub-group. We can think of H and its left cosets aH. Those make up a partition of the elements of the group under the equivalence relation $a \sim b$ iff there is an $h \in H$ such that $a = hb$. The properties of a group makes sure that this is indeed an equivalence relations, and equivalence classes are given by the cosets. The crucial observation is that all the cosets have the same number of elements. Thus the order of H divides that of G, and the index is given by the number of cosets. The cosets form a set on which

G operates transitively, the stabilizer to H is H itself while the stabilizer of aH is the conjugate aHa^{-1}. The cosets form a set (denoted by G/H, but not in general a group.

The following conditions are equivalent.

(i) every left coset is a right coset i.e. $\forall a \exists b$ such that $aH = Hb$

(ii) $\forall a \quad aH = Ha$

(iii) $\forall a \quad aHa^{-1} = H$ i.e. H is normal.

Sketch of proof: (ii) (iii) obvious as well as (ii) (i) for the other just put $h = 1$ and we get $b \in aH$.

Now because of this property we can define a multiplication
$(aH)(bH) = a(Hb)H = a(bH)H = abH$

In general a subgroup is not normal, unless of course the group is abelian. If H and K are two subgroups then HK i.e. all elements of type $hk, h \in H, k \in K$s not in general a subgroup. However if K is contained in the so called normalizer of H i.e. $kHk^{-1} = H \forall k$ then $kh = h^k k$ for some unique $h^k \in K$. The map $h \to h^k$ is actually an automorphism of H and we can define a multiplication because $h_1k_1h_2k_2 = h_1h_2^{k_1}k_1k_2$ and we see that the set HK satisfies all the conditions for a subgroup.

Inspired by this example we may define what is called a semi-direct product. More precisely given two groups H, K and with a homomorphism $K \to Aut(H)$ where the homomorphism corresponding to k is denoted by $h \mapsto h^k$ we will write down a group composition on the product $H \times K$ as follows.

$$(h_1, k_1)(h_2, k_2) = (h_1h_2^{k_1}, k_1k_2)$$

It is a good exercise to check that this really defines a group structure making $H = H \times (1)$ into a normal subgroup. Note also that we have a direct product if and only if the map $K \to Aut(H)$ is trivial.

Now in general the group HK is not a semi-direct product, it is so iff we have that $H \cap K = (1)$. In this case we have indeed $|HK| = |H||K|$. In general the representation hk is not unique, but we have of course a group homomorphism $H \times K \to HK$ given in the obvious way $(h, k) \mapsto hk$.

Now what is the kernel of this map? It consists of elements (h, k) such that $hk = 1$ i.e. elements of the form (h, h^{-1}) where $h \in H \cap K$. Thus in particular we have that $|HK| = |H||K|/|H \cap K|$.

So now let us look at the simplest and most basic forms of groups, namely the (finite) cyclic groups. A cyclic group of order n is a group generated by one element a such that the group is given by $1, a, \ldots a^n = 1$. It is usually denoted by Z_n and sometimes written additively $0, 1, 2a, \ldots na = 0$.

The following facts are elementary and characterize cyclic groups.

(i) They are generated by one element

(ii) Whenever $d|n$ where n is the order of the group, there is a unique subgroup of that order.

In particular we get that there is a nontrivial homomorphism between Z_n and Z_m iff $(n, m) \neq 1$

We also note that if the order of a group is a prime p the group has to be cyclic of order p.

Now what is the automorphism group of a cyclic group? An automorphism is uniquely determined by giving its value on a generator. A generator has to map to a generator. If a is a generator, when is a^k a generator? Clearly we should have $(k, n) = 1$. Thus the automorphism of a finite cycle group is given by the multiplicatiove group Z_n^* of all elements k relatively prime to n (and taken modulo n). In case $n = p$ a prime, this group is of order $p - 1$ and turns out to be cyclic.

To what extent can groups be built up from cyclic groups? In the case of finite abelian groups the answer is very easy, every abelian group is the direct product (or direct sum, as we usually think of abelian groups as additive) of a finite number of cyclic groups.

In the general case we would like to build up a given group G from cyclic groups. That is start with a cyclic subgroup Z choose then an element $a \notin Z$ but which normalizes Z and consider Za, then pick another element and continue, In this way we could construct the group by successively adjoining cyclic groups to a product with twists and quotients. Is this feasible? There is no problem taking one element at the time, but how do we make sure that the elements can be chosen to normalize the previous groups.

As a first step we will consider so called p-groups. A p group is a group whose order is a power of p. Note that trivially any subgroup or quotient of a p group is a p group, as is any semi-direct product of p-groups.

Now let a p-group act on a set. The basic observation to be made is that the cardinality of all the orbits are either one, or divisible by p, as those orbits are indices of sub-groups.

Let us now apply it to the conjugate action on itself. Such an action has always an orbit of cardinality one, namely the orbit of 1. More generally an orbit has only one element exactly when the element is part of the center, i.e. commutes with all elements. From this we conclude that the center in a p-group cannot just consist of one alone. Thus any p-group has a non-trivial normal subgroup (except of course when it is of prime order).

Now the further thing we want to know, is the existence of suitable cyclic subgroups. Of course there are plenty of such, each element generating one. The order of such a cyclic group is called the order of the element. The order of an element always divides the order of the group. The converse is not true, unless the group is cyclic.

We now want to prove the following. If the prime p divides the order of the group, there is an element of order p in the group.

This is trivially true for the trivial group, so let us proceed by induction. This means that we assume that the fact is true for all groups of order strictly less than a given G and we want to prove it for G as well.

If G is cyclic we actually know it by the observation above. So first assume that G is abelian. Pick a non-trivial element. It generates a cyclic subgroup$Z$. If p divide its order, we are done. If not we consider G/Z which we can for Z is automatically normal. The quotient has order divisible by p and is of strictly less order than G, by induction we can pick an element $a\mathfrak{g}/Z$ of order p. Pick an element b in its pre-image. It generates a cyclic subgroup of order divisible by p and we are done.

Now for the general case. The problem is that we cannot guarantee the existence of either normal subgroups or proper subgroups with orders divisible by p. If there would be no such subgroups, that would mean in particular that all the non-trivial conjugate classes would have cardinalities divisible by p, and thus in particular the center would be divisible by p. But the center being abelian we are done.

Thus we see that for p-groups we can actually build them up cyclic subgroups one at a time. More generally groups that can be so built up are called solvable groups. For all we know all groups maybe solvable.

We can now make some handy observations as corollaries of what we have just proved.

First any group of order p^2 is abelian. Such a group being a p-group it has a non-trivial center. Pick a central element x and an element y outside the cyclic group generated by x (if that would be the whole thing we would be done). Now the group of element commuting with y contains both x, y, thus it contains properly the subgroup generated by x and has to be the whole thing.

The case of groups of order p^3 is a bit more complicated and will be given as an exercise. the case of order p^4 is more complicated still, and with increasing value of the exponent, the complexity increases dramatically.

First any group of order pq (p, q) primes is either cyclic or non-commutative. In the second case exactly one of the cyclic subgroups is normal, and the group is a semi-direct product of the two cyclic groups.

Proof: Let $H \equiv Z_p$ and $K \equiv Z_q$ and assume that both are normal. We first note that $H \cap K = (1)$ the only thing we will need in addition to the normality. Then let $a \in H, b \in K$ and consider the commutator $aba^{-1}b^{-1}$ we have

$$H \ni a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1} \in K$$

thus $aba^{-1}b^{-1} = 1$ i.e. $ab = ba$. Thus the subgroup generated by HK is the direct product $H \times K$. In particular if H, K commutative, so is HK.

Now assume that H is thrown around by conjugation of the elements of K. Either all the conjugates are equal or distinct. In the latter case they will spread out to $1 + q(p-1)$ elements, then there is only $q - 1$ left which along with 1 have to make up K. Thus the latter is normal. Finally if K is a normal group then the conjugations $x \mapsto axa^{-1}$ make up automorphisms of K. Thus the group is determined by the homomorphism $H \to Aut(K)$ In our case it means a map $Z_p \to Z_q^* \equiv Z_{q-1}$. In order to get a non-trivial map (leading to a non-commutative group, we need that $p|q-1$. Note that in this case the map is unique, so in particular all the non-commutative examples are isomorphic.)

As a special case we note that for prime $p > 2$ there are two kinds of groups of order $2p$, the cyclic ones Z_{2p} and also the dihedral D_{2p} corresponding to Z_p being a normal subgroup and the involution given by $x \mapsto x^{-1}$.

Now we can strengthen this to the following classical theorem of Sylow. Let p^n be the highest power of p divisble in the order of a group G. then

(i) G contains a subgroup H of order p^n, a so called Sylow p-group

(ii) All Sylow p-groups are conjugate, in particular isomorphic

(iii) Given any p-group P, it is contained in some Sylow group.

(iv) The number of Sylow groups is of the form $1 + kp$.

Proof: Let us proceed by induction to prove (1). If G contains a subgroup H whose index is prime to p, then H satisfies the induction hypothesis. If not this would mean that all conjugacy classes, except those associated to elements in the center, would have a number of elements divisible by p, hence in particular there would be a center of order divisible by p. By induction we can assume that the center contains a Sylowgroup P as does G/P (P normal as being central). The pullback of a Sylow group of G/P gives one of G.

Let S be a Sylow p-group of G and Q a given p-group. Q acts on the set G/S whose cardinality is prime to p by left translations. All the orbits have cardinalities divisible by p, except the singletons. The latter must hence exist. Let aP be one such. We have that for each $x \in Q$ that $xaP = aP$ i.e. $a^{-1}xa \in P$ or $Q \subset aPa^{-1}$. This shows (iii). If Q is another Sylow p-group it shows (ii).

Special families of groups

The Symmetric group

The symmetric group on n elements consists of all the permutations of the same. It is thus a group with $n!$ elements. Any permutation π can be written as a product of disjoint cycles, simply by considering the orbits of the cyclic group generated by π. Each cycle of length k corresponds to a cyclic permutation of k elements, leaving the other fixed. Disjoint cycles commute. the cycle structure of a permutation is the collection of the lengths of its cycles. This corresponds to a partition of n. The basic fact is that cycle structures are invariant under conjugation, and conversely any two permutations with the same cycle structure are conjugate. This is easy to see on the level of cycles, as a cycle $(x, y, \dots z)$ is transformed into the cycle $(gx, gy \dots gz)$. Given the same cycle structure, we can by rearranging the order of the commuting cycles, effect a permutation conjugating one to the other.

It can be instructive to write down the conjugacy classes of S_n for low n, by listing the partitions. It is also relatively easy to compute the number ofelements in each conjugacy class, by keeping in mind that there are $(k-1)!$ possible ways of cyclically permuting k elements.

We have (note that $1+1+\dots+1$ always denotes the identity, keeping all elements fixed)

$S_2(Z_2) : 2(1), 1+1(1)$

$S_3(D_6) : 3(2)2+1(3)1+1+1(1)$

$S_4 : 4(6)3+1(8)2+2(3)2+1+1(6)1+1+1+1(1)$

$S_5 : 5(24)4+1(30)3+2(20)3+1+1(20)2+2+1(15)2+1+1+1(10)1+1+1+1+1(1)$

The sign $s(\pi)(=\pm 1)$ of a permutation is given by the transformation

$$\prod_{i<j}(x_i - x_j) = s(\pi)\prod_{i<j}(x_{\pi(i)} - x_{\pi(j)})$$

and called even or odd accordingly. (Whenever $\pi(j) < pi(i)$ for $i < j$ we say that we have a transposition, a permutation is even if it has an even number of transpositions). The map $S_n \rightarrow Z_2(= (S_2)$ given by the sign is a homomorphism, (i.e. the product of two odd permutations is an even permutation etc). The kernel of this morphism defines a normal subgroup A_n of index two called the alternating group. Its order is obviously $n!/2 = 3 \times 4 \dots n$. Note that the subgroups of S_n are pof two types, those that are bisected by A_n and those which are entirely contained in A_n.

Being a normal subgroup it is a union of conjugate classes. A cycle is even iff it is of odd length. Thus the condition of a cycle structure to correspond to an even permutation is that it is a partition with an even number of even summands. Thus we get

$A_2(1) : 1 + 1(1)$
$A_3(Z_3) : 3(2)1 + 1 + 1(1)$
$A_4 : 3 + 1(8)2 + 2(3)1 + 1 + 1 + 1(1)$
$A_5 : 5(24)3 + 1 + 1(20)2 + 2 + 1(15)1 + 1 + 1 + 1 + 1(1)$

Note that a conjugacy class may split up when considered in the smaller group. There is a split up exacly when the group of elements in S_n commuting with a given element in the group is entirely contained in A_n. Given a 5-cycle, the only elements commuting with it are powers of the cycle, thus all even. In the remaining cases it is easy to find a transposition commuting with the type. Thus in A_5 we have five conjugacy classes of orders $12, 12, 20, 15, 1$. Every normal subgroup has to be a union of such, containing the identity. There is no way of achieving this and get a sum that divides 60. Hence A_5 is simple, i.e. containing no non-trivial normal subgroups. A_5 is the simplest example of such a group. In general A_n with $n \geq 5$ are simple.

Möbius transformations on finite fields.

Given the 2×2 matrix with non-vanishing determinant. They form a group under multiplication. If the coefficients are complex numbers or real numbers, we get continous groups, but the definition makes sense for any kind of field, in particular finite fields.

The finite fields are classified, but let us restrict ourselves at first to the simple fields $Z_p(= F_p)$ for p prime. We consider numbers modulo p but also using multiplication as well as addition. Then it is well-known that any non=trivial element has a multiplicative inverse. The simplest field is the prime field F_2 with just two elements $\{0, 1\}$. It is easy to list the elements of $GL(2, F_2)$, they are

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Thus we have a group of six elements, and it is easy to see that it must be S_3 by classification. It is easy to identify the three involutions as those with trace zero, and by exclusion the elements of order three. But how can we see directly that it is the permutation group? The elements of F_2^2 are given by $(0, 0)$ and three elements outside namely $(1, 0), (1, 1), (0, 1)$ those being permuted by the linear transformations.

Note that only six of the sixteen possible matrices are non-singular. This can be interpreted as follows. Write down a 2×2 matrix with random integers. What is the probability that its determinant will be even? According to this analysis $10/16 = 0.625$

Now we may first compute the number of elements in the group $GL(2, F_p)$. the first row of the matrix can be any non-sero vector, thus $p^2 - 1$ choices, the second should be chosen linearly independent from the first, thus this leaves $p^2 - p$ choices. Thus the result is $p(p-1)^2(p+1)$ thus in particular for $p = 3$ we get order 48.

In order to investigate those groups it is necessary to do some linear algebra over finite fields. Recall that two linear transformations are conjugate, i.e. similar, iff they have the same characteristic polynomials. (This is only roughly true, one needs to consider the case with multiple roots a bit more closely, the exact statement being that the minimal polynomial is the invariant we are looking for.) In our case the situation is as follows

minimal *polynomial*	# *ofcases*	# *cardinality*	*matrix*
$(x - \lambda)$	$p - 1$	1	$\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$
$(x - \lambda)^2$	$p - 1$	$(p-1)(p+1)$	$\begin{pmatrix}\lambda & 0\\ 1 & \lambda\end{pmatrix}$
$x^2 + ax + b$ $a^2 - 4b = \square \neq 0$	$\frac{(p-1)(p-2)}{2}$	$p(p + 1)$	$\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}$ $\lambda \neq \mu$
$x^2 + ax + b$ $0 \neq a^2 - 4b \neq \square$	$\frac{(p-1)(p+2)}{2}$	$p(p - 1)$	$\begin{pmatrix}\lambda & 0\\ 0 & \lambda^p\end{pmatrix}$ $\lambda \in F_{p^2}$

Some explanations may be necessary: The second degree polynomials come in two types, depending on whether they are irreducible or not over F_p. To check that one needs to look at the discriminant $a^2 - 4b$ whether it is a square or not. (In the case of $p = 2$ completing the square is no longer possible, and another approach is needed). By F_{p^2} is meant a quadratic extension of F_p.

Now we could do some linear algebra. Observe that if A has distinct eigenvalues, it will have a basis of eigen-vectors. The condition on B that $AB = BA$ is that it respects those eigenspaces. (If $Ae = \lambda e$ then $ABe = BAe = \lambda Be$ thus Be is an eigenvector with the same eigenvalue.) Thus B can be built up from the powers of A. On the simple 2-dimensional case it means that $B = \lambda I + \mu A$. Because $A^2 = \mathrm{Tr}(A) - det(A)I$ elements of this form are closed under multiplication. We have thus identified the maximal abelian subgroups in $GL(2, F_p)$. The condition that $\lambda I + \mu A$ belongs to the group is that $0 \neq \det(\lambda I + \mu A) = \mu^2(\frac{\lambda}{\mu} I + A) = \lambda^2 + \lambda\mu\mathrm{Tr}(A) + \mu^2 \det(A)$. Two cases can now occur, either the characteristic equation of A has no roots, i.e. it is irreducible. Then $(0, 0)$ is the only exception, and the elements $\lambda I + \mu A$ actually form a field (the quadratic extension of the characteristic equation) and its non-sero elements form a cyclic group of order $p^2 - 1$. In the other case we have critical values for (λ, μ) in fact they form two lines in F_p^2 and hence the group has $p^2 - 2p + 1 = (p - 1)^2$ elements and in fact will be equal to a sum of two cyclic groups of order $p - 1$. (If A_1, A_2 are singular matrices corresponding to the two different eigenvectors, then any element can be written as a linear combination of those. Furthermore $A_1 A_2 = 0$ and by multiplying them with suitable scalar factors we may arrange that $A_1^2 = A_1, A_2^2 = A_2$). Thus if we consider the conjugacy class corresponding to an element with reducible characteristic equation, its cardinality will be $p(p - 1)^2(p + 1)/(p - 1)^2 = p(p + 1)$ while for the irreducible case we will have $p(p - 1)^2(p + 1)/(p^2 - 1) = p(p - 1)$.

We can of course go one step further. What are the normalizers to those maximal abelian subgroups? If we have an element that does not commute, it must be one which switches eigenspaces. Thus if $A = \begin{pmatrix} a & 0\\ 0 & b\end{pmatrix}$ the normalizer needs to be of the form $\begin{pmatrix} 0 & c\\ d & 0\end{pmatrix}$. Squares of such normalizers are also diagonal matrices, thus the normalizer will form a subgroup in which the maximal abelian sits as a subgroup of index two.

A good exercise for the reader at this stage would be to identify the Sylow 2-groups of the group $GL(2, F_5)$ which has 480 elements.

Matrices such as λI obviously make up a subgroup (in fact a cyclic one) contained in the center (and in fact make up the center). The quotient is refered to as $PGL(2, F_p)$ it has $p(p - 1)(p + 1)$ elements. It is refered to as the group of Moebius transformations (or broken linear), and is usually written as

$$z \mapsto \frac{az+b}{cz+d}$$

Note that $\begin{pmatrix} a\lambda & b\lambda \\ c\lambda & d\lambda \end{pmatrix}$ give the same transformation as $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. In this form it is well-known from elementary studies of one complex variable, but it makes sense for coefficients in any field. In the complex case it is thought of operating on the Riemann sphere, i.e. $\mathbb{C}$ with a point ∞ added at infinity. Thus the expression also has a value even when the denominator vanishes, and the value of ∞ is the obvious one (a/c). This can be made more rigorous by the following considerations. Consider $K^2 \setminus \{0\}$ for any field K. By KP^1 we will mean all the lines in the space. Those are defined by any point (p,q) in $K^2 \setminus \{0\}$ and two different points (p,q) and (p',q') define the same line iff $p = \lambda p', q = \lambda q'$. Which simply means that we have $\frac{p}{q} = \frac{p'}{q'}$ for the fractions giving the slope. Now if $q \neq 0$ we can parametrize all the lines, except the horizontal (the infinity). Now consider linear maps

$$(p,q) \mapsto (ap+bq, cp+dq)$$

By dehomogenizing (i.e. dividing by q) we get

$$\frac{p}{q} \mapsto \frac{a\frac{p}{q}+b}{c\frac{p}{q}+d}$$

and we have recaptured the original broken linear expression.

Thus $PGL(2,F_p)$ acts naturally on the projective line $F_pP^1 = F_p \cup \{\infty\}$. This action is triply transitive, given any distinct points a,b,c the Moebius transformation

$$z \mapsto \frac{b-c}{b-a}\frac{z-a}{z-c}$$

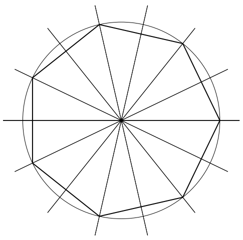
maps them to $0,1,\infty$ respectively. Also, this is the unique Moebius transformation with this property, which explains the count of $p(p-1)(p+1)$ of the order of the group.

In particular we see that $PGL(2,F_3)$ acts triply transitively on four elements, thus it has to be the symmetric group S_4.

We also note that we have a natural homomorphism det : $GL(2,F_p) \to F_p^*$. Itgiven by the determinant. The kernel of index $p-1$ is denoted by $SL(2,F_p)$ it is a normal subgroup and has likewise $p(p-1)(p+1)$ elements. (Note for $p=2$ all the groups we have defined coincide.). Finally we can combine the two operations and consider $PSL(2,F_p)$ by dividing out by $\pm I$. If $p>2$ we then get a group of $\frac{p(p-1)(p+1)}{2}$ elements. If $p=3$ we get A_4 and if $p=5$ we get A_5. In general for $p \geq 5$ the groups $PSL(2,F_p)$ are simple.

Linear representations

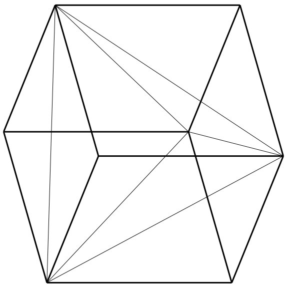
The group $\mathbb{C}^*$ under multiplication is a simple example of a non-compact continous group. A subgroup is given by the complex numbers λ on the unit-circle. This group is the simplest example of a compact continuos group, and is isomorphic to S^1, the group of the circle. Clearly $\mathbb{C}^* \equiv R_{>0} \times S^1$, where the first factor is the positive real numbers under multiplication. The simple circle group S^1 can be thought of as $\mathbb{R}/\mathbb{Z}$ groups under addition, and the isomorphism is given by the exponential map $t \to e^{2\pi i t}$. The subgroup $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is isomorphic to the cyclic group Z_n, and each element $\lambda_n^k = e^{2\pi i \frac{k}{n}}$ is an n-th root of unity. They form a regular n-gon on the unit-circle and multiplication by λ_n^k are given by rotations keeping the regular n-gon invariant. In addition to that we have reflections, those can be represented by complex conjugation followed by a rotation.



In the figure to the left we look at the particular case $n = 7$. Note how the polygon is split up into 14 triangles, the number of elements of the dihedral group D_{14}. Those triangles are being permuted by the action of the group, and each group element can be identified with a particular triangle, once we have fixed one as a reference. Thus in a sense we have a visual picture of the group.

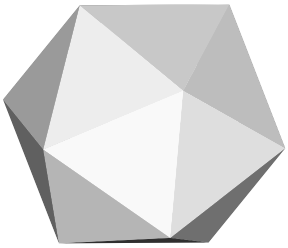
The group A_4 can be represented by rotations in 3-space leaving a regular tetrahedron invariant. A rotation in 3-space is given by fixing an axis. There are four axi of a tetrahedron, each of them giving rise to rotations $2\pi/3$. There are also three normals to three pairs of skew-lines. through which we can do roations of π. In total I have presented $1 + 4 \times 2 + 3 = 12$ operations. Those form a group, actually isomorphic to A_4, even permutations of the four vertices. It is called the tetrahedral group

Likewise we have a representation of the group S_4 by rotations in space leaving a regular cube, or by duality, a regular octahedron invariant. We have first three axi going through the midpoints of opposite faces. This gives rise to rotations of order four. We have four long diagonals by which the eight vertices are paired off. This gives rise to 3-fold symmetries, and finally we have six lines going through the midpoints of opposite edges, giving rise to involutions, by rotating halfway. Thus the count gives $1 + 3 \times 3 + 4 \times 2 + 6 = 24$. This group isomorphic to S_4 is referred to as the octahedral group.



The two groups are related because we can inscribe a regular tetrahedron in a cube in two different ways by suitably chosing four of the eight vertices (see the figure on the left for one of the cases, note that the edges of the tetrahedron are paired off with the faces of the cube, and the faces of the tetrahedron are paired off with the remaining vertices, which form the so called dual tetrahedron). The subgroup of even permutations keep the tetrahedra invariant, while odd permutations permute the two.

In fact we can consider all orthogonal matrices with integer coefficients. As the squares of the coefficients add up to 1 the only possibilities are $0, \pm 1$ with only one non-zero coefficient in each row and column. Thus we are taling about permutation matrices, except that we allow different signs. The count will be easy, there are 6 permutation matrices, and for each we have a choice of 2^3 different sign patterns. This makes 48. Now half of those will have determinant -1 and correspond to reflections in planes, the other half will consist of the rotations we have discussed above.



Finally the most exciting thing being the isomorphism group of the icosahedron, or alternatively its dual, the dodecahedron. The count for the icosahedron gives ten axi corresponding to 3-fold symmetry, 6 axi giving 5-fold and finally 15 giving involutions. This adds up to $1+10\times2+6\times4+15 = 60$. This group is not surprisingly called the Icosahedral group.

Infinite countable groups

The simplest infinite group is the cyclic group $\mathbb{Z}$ under addition. All the finite cyclic groups are quotients of it. In fact those are the only quotients. It can be thought of as a free group of one generator, and every group generated by just one member (that is a cyclic group) will be a quotient of it. Its subgroups are all of the form $n\mathbb{Z}$ for some n.

Similarly we can think of the free group F^2 on two elements formed by all the words built on the letters a, b, a^{-1}, b^{-1} with the convention that when whenever aa^{-1} are adjacent (and similarly for b, b^{-1}, they will be cancelled. The empty word is the identity. Typical words are $aba, a^2ba^3b^{-2}$. We can also think of the group as the free product $(Z * Z)$ of two copies of $\mathbb{Z}$. There is an obvious notion of length, i.e. the two words above have lengths $3, 8$ respectively. Length is obviously sub-additive, the concotation of two words such as $aba, a^{-1}b$ leads to cancellation. As cancellations come in pairs we note that words of even lengths are closed under multiplication (and taking of inverses) and thus make up a subgroup G of index four, the quotient F^2/G is isomorphic to $Z_2 \times Z_2$ generated by the images of a, b. Every group that is generated by two elements is a quotient of F^2. The kernel is known as the subgroup of relations. F^2 is a huge group, it contains within itself other free groups such as $F^3, F^4 \dots$ in fact by considering the elements $X_n = a^n b^n, X_n^{-1}, n \geq 1$ we see that any 'legal' product (i.e. we never allow $X_n X_n^{-1}$) of those can never cancel out and become the identity, and thus the free group of a countable infinite number of generators can be represented as a subgroup of F^2.

If we introduce the relations $a^2 = b^2 = 1$ i.e. we consider the free product $Z_2 * Z_2$ we can give a very explicit description of it. Let us now use the additive notation so 0 will denote the identity. Set $1 = ab$ to be the generator of the additive cyclic group $\mathbb{Z}$ (thus not an additive identity). We then get $a1 = a^2b = b$. As $(ab)(ba) = 0$ we should have $ba = -1$. Now set $n = (ab)(ab)\dots(ab)$ (n-times). We then get $an = a(ab)(ab)\dots(ab) = (ba)(ba)\dots(ba)b = (n-1)(-1)b$ from which we conclude $an = (-n)a$. Thus a operates on $\mathbb{Z}$ by taking the (additive) inverse. Any element can be written as either n or an and the addition rule is easily written down. (Note that if we only consider legal words, they divide into those starting with a and those starting with b, the former can be thought of as the positive ones, and the latter as the negative.) What we have here is the infinite dihedral group. All the elements an are involutions. And all the finite dihedral groups are quotients of this infinite. In particular any group that is generated by two involutions has to be dihedral. Either (ab) has finite order $((ab)^n = 1)$ and we then have D_{2n} (Dividing out by the subgroup $n\mathbb{Z}$.) or it has infinite order, and then we simply have our $D_{2\infty}(= Z_2 * Z_2)$

Continuous groups

We are now considering the case of a mixing of strcutures, namely topology being made compatible with the group structure. The notion is that of a topological group, meaning that the group G is a topological space and that the map $M : G \times G \to G$ defined by $M(x,y) = xy^{-1}$ is continuous. A natural condition on the topology is that it is Hausdorff, which implies that each point is closed. Conversely if the identity is closed, then so is verey point because of translation. And by taking the inverse we see that the diagonal is closed, which is an equivalent condition of Hausdorff. Furthermore homomorphisms between topological groups are of course assumed to be continuous. Thus normal subgroups are always closed. An open subgroup has all of its cosets open, hence the complement is open, so the group is automatically closed. The quotient of such a group will necessarily be discrete, i.e. every subset is open ((and closed).

We have already encountered some topological groups such as $\mathbb{C}^*, \mathbb{R}^*$ and S^1 the latter being a compact version of the cyclic groups, and as we have already noted containing all finite cyclic groups as subgroups. (In fact the union of all finite subgroups make up a countable subgroup isomorphic to $\mathbb{Q}/\mathbb{Z}$ the group of all roots of unity. (An alternative description is that of points on the unit corcle corresponding to angles given by rational degrees.) We will return to this later.

Now given S^1 we can consider arbitrary products of if $S^1 \times \dots S^1$ so called tori. In addition to S^1 there will be another sphere which is a group, namely S^3. Just as the group structure on S^1 is induced by multiplication by complex numbers, that on S^3 is induced by the quaternions. It is a non-commutative group.

Given a finite dimensional vector space V with scalars $K = \mathbb{R}, \mathbb{C}$ we can talk about $GL(V,K)$ the group of non-singular matrices. Those of determinant 1 make up a subgroup $SL(V,K)$. If we fix a non-singular quadratic form Q we have all the matrices preserving it, denoted the orthogonal group $O(K)$, which contains a subgroup $SO(K)$ of index two, consisting of those with determinant one. Now in the case $K = \mathbb{R}$ a non-singular quadratic form is determined by its index $a - b$ (with a positive squares and b negative squares and $a + b = n$ the rank. We thus talk about groups $S(a,b;\mathbb{R})$ which are compact iff $ab = 0$. $SO(2,\mathbb{R})$ is S^1 while $SO(3,\mathbb{R})$ is the group of orthogonal 3×3 matrices, given by identifying antipodal points on S^3. The group $SO(3,1,\mathbb{R})$ is called the Lorentz group and is important in relativity theory. In fact many of those groups defined by matrices are important in physics as they describe various symmetries and equivalently various invariants.

Finally we may return to the example $\mathbb{Q}/\mathbb{Z}$. By Q_p we can denote all rational numbers given by fractions whose denominators are powers of a prime p. They form an additive subgroup and $\mathbb{Q}$ is the direct sum of all the p-components $\mathbb{Q}_p$. Each such component contains all the cyclic subgroups of orders powers of p. In fact we have $p^n x = 0$ iff x can be written with a denominator p^n. Thus each number $x \in \mathbb{Q}_p$ has a unique expression as $\frac{a_1 p^{n-1} + a_2 p^{n-2} + \dots + a_n}{p^n}$ where the constant term $a_n \neq 0$. Thus each such number gives rise to a finite sequence $a_1, a_2 \cdots a_n, 0, 0, \dots$. What if you would allow infinite sequences? How should we add them? We have here a system $Z_p \subset Z_{p^2} \subset Z_{p^3} \subset \cdots$ where $\mathbb{Q}_p$ is simply the union. As it is a nested union, once an element belongs to one set, and will automatically belong to all the subsequent. We also have the notion of truncation. If $x \in Z_{n+1}$ we can drop its constant term, i.e. choose a appropriately as to make $x - \frac{a}{p^{n+1}} \in Z_n$.

Thus an element x can be thought of as an infinite sequence $x_1, x_2, x_3 \cdots$ where the truncation of x_{n+1} is x_n. The sequences we get are stable ones, i.e. for some n we have $x_n = x_{n+1} = x_{n+2} \cdots$. But what if we would allow infinite sequences? This would correspond to infinite sequences $\frac{a_1}{p} + \frac{a_2}{p^2} = \frac{a_3}{p^3} + \cdots$ which is nothing but a real number succesively approximated, not by what usually is done, negative powers of ten, but negative powers of an arbitrary prime p.

But now we can turns things around and look at infinite series like this $a_0 + a_1p + a - 2p^2 + a_3p^3 + \cdots$. How should we make sense of them? If the series are trubcated they obviously denote integers, but if we let them continue for ever? First what should we think of a_n as being. To have a unique representation we ned that $0 \leq a_i < p$, but then we can think of them as members of Z_p. Thus $a_0 \in Z_p$, while $a_0 + a_1p \in Z_{p^2}$. What we have here is a sequence of surjective homomorphisms $\cdots Z_{p^3} \rightarrow Z_{p^2} \rightarrow Z_p$ and an infinite sequence of elements $a_n \in Z_{p^n}$ such that $a_{n+1} \mapsto a_n$. Two sequences are said to be close if their initial parts agree up to a high order. This means that we have a topology on the integers $\mathbb{Z}$ such that two integers are close if the difference is divisible by a high power of p. One may formalize this by introducing a norm, i.e. a distance from 0 by $d_p(ap^n, 0) = p^{-n}$ where $(a,p) = 1$. This is the p-adic metric on $\mathbb{Z}$ and we are talking about its completion $\mathbb{Z}_p$ of p-adic integers. This is clearly an uncountable set. It is not a field, but it can easily be turned into a field, by considering Laurent expansions instead, or equivalently, allowing arbitrary powers of p in the denominators. The observation to make is that if $a_0 \neq 0$ then $a_0 + a_1p + \cdots$ is invertible. This follows from $1 + p + p^2 + p^3 + \cdots = \frac{1}{1-p}$ (multiply both sides with $(p-1)$) and the fact that if you add subsequent powers of $p(a + bp + \cdots)$ you will have no problems with convergence. Now you could do everything you have done before for $\mathbb{R}$ and $\mathbb{C}$ with those p-adic fields which are denoted by $\mathbb{Q}_p$.