Queen Mary
University of London

MTHM024/MTH714U **Group Theory**

Notes 2 **Autumn 2011**

2 How many groups?

The number of $n \times n$ arrays with entries chosen from a set of size n is n^{n^2}. So certainly this is an upper bound for the number of groups of order n.

In fact one can do much better, using two results from elementary group theory: the theorems of Lagrange and Cayley.

Theorem 2.1 *The number of groups of order n is at most $n^{n \log_2 n}$.*

Proof By Cayley's Theorem, every group of order n is isomorphic to a subgroup of the symmetric group S_n. So if we can find an upper bound for the number of such subgroups, this will certainly bound the number of groups up to isomorphism.

We use Lagrange's Theorem in the following way. We say that a set $\{g_1, \ldots, g_k\}$ of elements of a group G *generates* G if no proper subgroup of G contains all these elements. Equivalently, every element of G can be written as a product of these elements and their inverses.

Now we have the following:

Proposition 2.2 *A group of order n can be generated by a set of at most $\log_2 n$ elements.*

To see this, pick a non-identity element g_1 of G, and let G_1 be the subgroup generated by g_1. If $G_1 = G$, stop; otherwise choose an element $g_2 \notin G_1$, and let G_2 be the subgroup generated by g_1 and g_2. Continue in this way until we find $g_1, \ldots, g_k$ which generate G.

We claim that $|G_i| \geq 2^i$ for $i = 1, \ldots, k$. The proof is by induction on i. The assertion is clear for $i = 1$, since by assumption $|G_1| > 1$, so $|G_1| \geq 2$. Now suppose that $|G_i| \geq 2^i$. Now G_i is a subgroup of G_{i+1}, and so $|G_i|$ divides $|G_{i+1}|$, by Lagrange's Theorem; since $G_i \neq G_{i+1}$, we have that $|G_{i+1}| \geq 2|G_i| \geq 2^{i+1}$. So the assertion is proved by induction.

Finally, $n = |G| = |G_k| \geq 2^k$, so $k \leq \log_2 n$.

Thus, to specify a subgroup G of order n of S_n, we only have to pick $k = \lfloor \log_2 n \rfloor$ elements which generate G. There are at most $n!$ choices for each element, so the number of subgroups is at most

$$(n!)^k \leq (n^n)^{\log_2 n} = n^{n \log_2 n},$$

since clearly $n! \leq n^n$.

The revision notes contain a proof that there is a unique group of prime order. Here are proofs that the numbers of groups of orders 4, 6, 8 are 2, 2 and 5 respectively.

Order 4**:** Let G be an element of order 4. If G contains an element of order 4, then it is cyclic; otherwise all its elements apart from the identity have order 2. Let $G = \{1, x, y, z\}$. What is xy? By the cancellation laws, xy cannot be 1 (since $xx = 1$), or x, or y; so $xy = z$. Similarly the product of any two of x, y, z is the third, and the multiplication table is determined. So there is at most one type of non-cyclic group. But the group $C_2 \times C_2$ realises this case.

Order 6**:** Again suppose that there is no element of order 6, so that elements of G have orders 1, 2 and 3 only. All these orders actually appear [why?]. Let a have order 3 and b order 2. Then it is easy to see that $G = \{1, a, a^2, b, ab, a^2b\}$. We cannot have $ba = ab$, since then we would find that this element has order 6. All other possibilities for ba except $ba = a^2b$ are eliminated by the cancellation laws. So $ba = a^2b$, and then the multiplication table is determined. This case is realised by the symmetric group S_3.

Order 8**:** If there is an element of order 8, then G is cyclic; if no element has order greater than 2, then $G = C_2 \times C_2 \times C_2$ (this is a bit harder). So assume that a is an element of order 4, and let b be an element which is not a power of a. Then $G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$. This time we need to know which of these eight elements is b^2, and which is ba, in order to determine the group. We find that $b^2 = 1$ or $b^2 = a^2$, and that $ba = ab$ or $ba = a^3b$. There seem to be four different possibilities; but two of these turn out to be isomorphic (namely, the cases $b^2 = 1, ba = ab$ and $b^2 = a^2, ba = ab$). So there are three different groups of this form. All of them actually occur: they are $C_4 \times C_2$ and the dihedral and quaternion groups. These together with the two we already found make five altogether.