Notes for 28 March (Thursday)

1 The road so far...

1. Defined normal subgroups and quotient groups.
2. Stated that A_4 does not have a subgroup of order 6 (and hence the converse to Lagrange's theorem is false).

2 Back to abstract groups...again

Indeed, A_4 consists of e, cyclic decomposition of two cycles (4 of them forming a subgroup $V \equiv K_4$), and the 8 three cycles. Suppose $H \subset A_4$ is of size 6 and $H' = H \cap V$. By Lagrange's theorem, $|H'| = 1$ or 2. If it is 1, then $(h, v) \to h.v$ is $1-1$ but then G would have at least 24 elements. So $|H'| = 2$ and H is made of e, an element v made of two cycles, and 4 three cycles. Since $[G : H] = 2$, H is a normal subgroup. Let $v = (ij)kl$ and $t = (ijk)$. Then $tvt^{-1} = (jkil) \neq (ij)(kl)$ but H is normal in G and H' has size 2.

The following partial converse does hold (which is generalised greatly to Sylow's theorem).

Theorem 1. *If G is a finite Abelian group of size n and p is a prime divisor of n, then G has an element of order p.*

Proof. In Childs' book. □

Now we state and prove an important isomorphism theorem (the "first isomorphism theorem").

Theorem 2. *If $f : G \to H$ is a group homomorphism with kernel K, then K is a normal subgroup such that quotient group G/K is isomorphic to its image.*

Proof. Firstly, the kernel is a subgroup. Indeed, if $x, y \in K$, then $f(y^{-1}) = (f(y))^{-1} = e$ and $f(xy) = f(x)f(y) = e$. Secondly, K is a normal subgroup. Indeed, if $y \in K$, then $f(xyx^{-1}) = f(x)f(y)f(x^{-1}) = f(x)f(x^{-1})) = e$ and hence $xKx^{-1} = K \;\forall\; x \in K$ (why does equality hold instead of being a subset?). Thirdly, f induces group homomorphism $\bar{f} : G/K \to H$ as $\bar{f}(xK) := f(x)$. This is well-defined ($f(xk) = f(x)f(k) = f(x) \;\forall\; k \in K$) and a homomorphism $\bar{f}(xK)\bar{f}(yK) = f(x)f(y) = f(xy) = \bar{f}(xyK)$. Also, it is $1-1$. Indeed, if $\bar{f}(x_1K) = \bar{f}(x_2K)$, then $f(x_1) = f(x_2)$ and hence $x_1 = x_2k$. Thus $x_1K = x_2K$. □

An example of an application of the first isomorphism theorem is there in Childs' book.

3 Quadratic reciprocity

Recall that one of the aims of number theory is to solve Diophantine equations. Unfortunately, it can be proven that there is no algorithm that decides whether a given such equation has a solution or not. Nonetheless, one can try to look at special cases, especially the equation reduced modulo m.

So far we looked at linear equations, Pythagorean triples, and Pythagorean primes. An obvious next step is to solve quadratic equations in one variable. A simpler question is, given m can we solve $x^2 \equiv_m a$ in $\mathbb{Z}_m$? Such an a is called a quadratic residue modulo m.