Queen Mary
University of London

MTHM024/MTH714U **Group Theory**

Notes 0 **Autumn 2011**

Sylow's proof

A complete proof of Sylow's Theorems can be found on page 19 of the revision notes. Below is Sylow's original proof of the first part of his theorem, the existence of Sylow subgroups. He wrote it in the language of double cosets; I have translated it into group actions.

Recall that a Sylow p-subgroup of a finite group G is a subgroup whose order is a power of p and whose index is coprime to p.

Theorem 1 *For any prime p, every finite group has a Sylow p-subgroup.*

Proof We proceed in four steps. The first is the "big idea".

Step 1 If G is a subgroup of a group H, and H has a Sylow p-subgroup, then G has a Sylow p-subgroup.

For let P be a Sylow p-subgroup of H, and consider the action of H on the coset space $\cos(P,H)$ by right multiplication. The number of cosets is coprime to p, and the stabiliser of any coset has p-power order.

Now restrict the action to G. There must be an orbit Δ whose size is coprime to p, since if all orbits sizes were divisible by p then the total number of cosets would be divisible by p. The stabiliser of a point of Δ (in G) has p-power order, since it is a subgroup of the stabiliser in H. So this stabiliser is a Sylow p-subgroup.

Step 2 A finite group G of order n is isomorphic to a subgroup of the symmetric group S_n.

This is *Cayley's Theorem*. Consider the action of G on the coset space $\cos(G,1)$: this action is faithful (since the stabiliser of any point is trivial), and so it is an embedding of G in S_n.

Step 3 There is an embedding of S_n in the general linear group $\mathrm{GL}(n,F)$ of invertible $n \times n$ matrices over any field F.

The embedding maps any permutation g to the *permutation matrix* $P(g)$, whose i,j entry is given by

$$P(g)_{ij} = \begin{cases} 1, & \text{if } ig = j, \\ 0, & \text{otherwise.} \end{cases}$$

Step 4 Let F be the field of integers mod p, where p is prime. Then $\mathrm{GL}(n,F)$ has a Sylow p-subgroup.

To see this, we first compute the order of $\mathrm{GL}(n,p)$ to be

$$(p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}) = p^{1+2+\cdots+(n-1)}M,$$

where M is not divisible by p. Now the upper unitriangular matrices (with 1 on the diagonal, arbitrary elements above, and 0 below) has order $p^{1+2+\cdots+(n-1)}$, so is a Sylow p-subgroup.

Putting the four parts together proves the theorem.

Remark It is possible to save a step by showing directly that the symmetric group S_n possesses a Sylow p-subgroup; but this is a bit more complicated.