21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc Tartar, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

11- Friday September 23, 2011.

Lemma 11.1: (second isomorphism theorem)[1] If $H \leq G$, and $N \triangleleft G$, then,

a) $H\,N = N\,H \leq G$,

b) $N \cap H \triangleleft H$, and $H\,N/N \simeq H/(N \cap H)$.

Proof: a) That N is a normal subgroup of G means $g\,N = N\,g$ for all $g \in G$, so that $h\,N = N\,h$ for all $h \in H$, which implies $H\,N = N\,H$, and this implies that it is a subgroup of G.

b) Let π be the projection of G onto G/N, which is a (surjective) homomorphism, and restrict it to H, so that the kernel of $\pi|_H$ is $N \cap H$, which is then a normal subgroup of H. By the first homomorphism theorem, $H/(N \cap H)$ is isomorphic to the image of H by $\pi|_H$, which is the set of cosets $h\,N$ for $h \in H$, i.e. the quotient of $H\,N$ by N (and N is a normal subgroup of $H\,N$ since $N \leq H\,N \leq G$).

Remark 11.2: More generally if $H, N \leq G$ and $H \leq N_G(N)$, one replaces G by the normalizer $N_G(N)$, and a) holds with $H\,N = N\,H \leq N_G(N)$ and b) is unchanged.

If $N \leq H \leq G$, then $H\,N = N\,H = H$, so that a) is true, and if one adds $N \triangleleft G$, then $N \triangleleft H$, which is the first part of b), and the second part is obvious since both sides are H/N.

If $H \leq N \leq G$, then $H\,N = N\,H = N$, so that a) is true, and one does not need to add $N \triangleleft G$, for having b) since $N \cap H$ being H is a normal subgroup of H, and the second part is obvious since both sides are $\{e\}$ as quotient of a group by itself.

Lemma 11.3: Let $K, L \leq G$ be such $K \cap L = \{e\}$. Then, each $g \in K\,L$ can be written in a unique way as $g = k\,\ell$ with $k \in K, \ell \in L$.

If $K \cap L \neq \{e\}$, with K and L finite, then $|K\,L| = \frac{|K|\,|L|}{|K \cap L|}$.

Proof: By definition, each $g \in K\,L$ can be written as $g = k\,\ell$ for some $k \in K$ and $\ell \in L$, so that only uniqueness must be proved. If $k_1\ell_1 = k_2\ell_2$, one deduces that $k_2^{-1}k_1 = \ell_2\ell_1^{-1}$, which then belongs to both K and L, and must be e, but $k_2^{-1}k_1 = e$ means $k_1 = k_2$, and $\ell_2\ell_1^{-1} = e$ means $\ell_1 = \ell_2$.

$K\,L$ is the union of the cosets $k\,L$ for $k \in K$. One has $k_1L = k_2L$ if and only if $k_2^{-1}k_1 \in L$, so that it belongs to $K \cap L$; for each $k_1 \in K$, there are exactly $|K \cap L|$ elements $k_2 \in K$ giving the same coset as k_1, so that there are $\frac{|K|}{|K \cap L|}$ distinct cosets, and each coset has size $|L|$, hence the size of $K\,L$.

Lemma 11.4: Let $G = K \times L$ for groups K and L, and let $K_1 = K \times \{e\} \simeq K$ and $L_1 = \{e\} \times L \simeq L$. Then, $K_1, L_1 \triangleleft G$, $G = K_1L_1 = L_1K_1$, with $K_1 \cap L_1 = \{e\}$.

Conversely, if $K, L \triangleleft G$ for a group G, with $K \cap L = \{e\}$ and $G = K\,L$, then elements from K and L commute (so that $G = L\,K$) and $G \simeq K \times L$ via the homomorphism $g = k\,\ell \mapsto (k, \ell)$.

Proof: The kernel of the projection π_1 of G onto K is L_1, and the kernel of the projection π_2 of G onto L is K_1, so that K_1 and L_1 are normal subgroups of G (since π_1 and π_2 are homomorphisms). Then $g = (k, \ell) = (k, e) \cdot (e, \ell) \in K_1L_1$ and $g = (e, \ell) \cdot (k, e) \in L_1K_1$. Finally, $g = (k, \ell) \in K_1$ means $\ell = e$, and $g \in L_1$ means $k = e$, so that $g \in K_1 \cap L_1$ means $g = (e, e) = e$ (which means $(e_K, e_L) = e_G$, of course).

Because K is a normal subgroup of G, one has $g\,K = K\,g$ for all $g \in G$, so that $\ell\,K = K\,\ell$ for all $\ell \in L$, which implies $L\,K = K\,L$, which is G. In particular, for $k \in K$ one has $\ell\,k = k_1\,\ell$ for some $k_1 \in K$, but also, because L is a normal subgroup of G, one has $\ell\,k = k\,\ell_1$ for some $\ell_1 \in L$; then, $k_1\,\ell = k\,\ell_1$ implies $k_1 = k$ and $\ell_1 = \ell$ by the uniqueness (resulting from $K\mathcal{L} = \{]\}$), so that k and ℓ commute. The mapping ψ from G into $K \times L$ such that $g = k\,\ell$ gives $\psi(g) = (k, \ell)$ is well defined, because k and ℓ are uniquely defined; ψ is an homomorphism, since if $g' = k'\ell'$, one has $g\,g' = (k\,\ell)\,(k'\ell') = (k\,k')\,(\ell\,\ell')$ (because ℓ and k' commute), so that $\psi(g\,g') = (k\,k', \ell\,\ell') = (k, \ell)\,(k', \ell') = \psi(g)\,\psi(g')$. Of course, ψ is bijective because for every $(k, \ell) \in K \times L$, there is exactly one g with $\psi(g) = (k, \ell)$, which is $g = k\,\ell$.

Theorem 11.5: (Sylow's theorems) Let p be a prime dividing $|G|$ and such that $|G| = p^n a$ (with $n \geq 1$) and p does not divide a. Then, every subgroup of G whose order is a power of p is included in a Sylow

[1] It is also called the diamond isomorphism theorem.

p-subgroup, all Sylow p-subgroups are conjugate, and their number is congruent to 1 modulo p, and divides $|G|$, so that it divides a.

Proof: a) Let Σ be the family of p-subgroups of G, which by Cauchy's theorem is not empty. Let Ω be the elements of Σ which are maximal for inclusion; because $|\Sigma| < \infty$, every element of Σ is included in an element of Ω. If G acts on subgroups by conjugation, then G acts on Σ (since conjugate subgroups have the same order), and G acts on Ω (since conjugation preserves inclusion).

b) If $P \in \Omega$, one considers the P-action on Ω (i.e. for $Q \in \Omega$ the orbit is made of the $g\,Q\,g^{-1}$ for $g \in P$), and one shows that P is the only fixed point of this action. Indeed, if $Q \in \Omega$ is fixed by P it means that $P \leq N_G(Q)$, so that $P\,Q \leq G$. By Lagrange's theorem, $|P \cap Q|$ is a power of p (so that $P \cap Q \in \Sigma$), and by the formula for the size of a product ($|P\,Q| = \frac{|P|\,|Q|}{|P \cap Q|}$) $P\,Q \in \Sigma$, but since $P\,Q$ contains both P and Q (since $e \in P \cap Q$), one has $P = P\,Q = Q$ by maximality of P and of Q.

c) All elements of Ω are conjugate. If it was not true, there would exist $P \in \Omega$ having orbit A, and $Q \in \Omega$ having orbit B, with A and B disjoint. Then in the P-action on A and on B, P is the only fixed point, and all the other orbits have a size dividing $|P|$, i.e. a power of p, so that $|A|$ is congruent to 1 and $|B|$ is congruent to 0 modulo p; using then the Q-action on A and on B gives a contradiction, that $|A|$ is congruent to 0 and $|B|$ is congruent to 1 modulo p.

d) If $P \in \Omega$, then by c) its orbit is Ω and $|\Omega|$ is congruent to 1 modulo p, but the size of the orbit divides $|G|$, so that it divides a.

e) Any Sylow-p subgroup is necessarily maximal, and belongs to Ω; conversely, one needs to show that every $H \in \Omega$ must be a Sylow-p subgroup. By d) the orbit of H is Ω and its size b is congruent to 1 modulo p and divides a, but it is also the index of $N_G(H)$ in G, so that the order of $N_G(H)$ is $p^n c$ with $b\,c = a$. If H was not a Sylow-p subgroup, its order would be p^m for $1 \leq m < n$, and the order of $N_G(H)$ being $p^n c$, the quotient space $N_G(H)/H$ (defined since $H \triangleleft N_G(H)$) would have order $p^{n-m}c$ which is a multiple of p, hence by Cauchy's theorem it would have a subgroup K order p; if π denotes the projection of $N_G(H)$ onto $N_G(H)/H$ the subgroup $\pi^{-1}(K)$ of $N_G(H) \leq G$ would have order a power of p and would contain H strictly, contradicting the maximality of H.

Remark 11.6: G has a unique Sylow-p subgroup if and only if it has a normal Sylow-p subgroup, and in this case the subgroup is characteristic. Indeed, the conjugates of the Sylow p-subgroup H are all the Sylow-p subgroups, i.e. they are equal to H, i.e. H is normal, and conversely. Then, if $\psi \in Aut(G)$ it must map H to a subgroup of the same size, and there is only H.