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

10- Wednesday September 21, 2011.

Definition 10.1: If N and H are two groups, a *semi-direct product* of N and H is a group denoted $G = N \times_\psi H$ obtained by choosing an homomorphism ψ of H into $Aut(N)$, the group of automorphisms of N, and defining on the product $N \times H$ the operation $\star_\psi$ by $(n_1, h_1) \star_\psi (n_2, h_2) = \big(n_1\psi_{h_1}(n_2), h_1h_2\big)$, where one writes ψ_h for $\psi(h)$.

Lemma 10.2: With the notation of Definition 10.2, G is a group, with identity $e = (e_N, e_H)$, and the inverse of (n, h) is $(\psi_{h^{-1}}(n^{-1}), h^{-1})$.

$\widetilde{N} = \{(n, e_H) \mid n \in N\}$ is a normal subgroup of G isomorphic to N, $\widetilde{H} = \{(e_N, h) \mid h \in H\}$ is a subgroup of G isomorphic to H, and one has $\widetilde{N} \cap \widetilde{H} = \{e\}$. Moreover, there exists an homomorphism χ from G into $\widetilde{H}$, which when restricted to $\widetilde{H}$ is the identity, and whose kernel is $\widetilde{N}$, namely $\chi : (n, h) \mapsto (e_N, h)$.

This group is non-Abelian, except if ψ is the trivial homomorphism (with kernel H), in which case the group is the usual product of groups, which is Abelian if and only if both N and H are Abelian.

Proof: The operation $\star_\psi$ is associative: $\big((n_1, h_1) \star_\psi (n_2, h_2)\big) \star_\psi (n_3, h_3) = (n_1\psi_{h_1}(n_2), h_1h_2) \star_\psi (n_3, h_3) = (n_1\psi_{h_1}(n_2)\, \psi_{h_1h_2}(n_3), h_1h_2h_3)$, and then $(n_1, h_1) \star_\psi \big((n_2, h_2) \star_\psi (n_3, h_3)\big) = (n_1, h_1) \star_\psi (n_2\psi_{h_2}(n_3), h_2h_3) = \big(n_1\psi_{h_1}\big(n_2\psi_{h_2}(n_3)\big), h_1h_2h_3\big)$, which are equal because $\psi_{h_1}\big(n_2\psi_{h_2}(n_3)\big) = \psi_{h_1}(n_2)\, \psi_{h_1}\big(\psi_{h_2}(n_3)\big)$ since $\psi_{h_1} \in Aut(N)$, and because $\psi_{h_1} \circ \psi_{h_2} = \psi_{h_1h_2}$ since ψ is an homomorphism. The identity is (e_N, e_H), since $(e_N, e_H) \star_\psi (n, h) = (e_N\psi_{e_H}(n), h)$ and $(n, h) \star_\psi (e_N, e_H) = (n\, \psi_h(e_N), h)$, which are equal to (n, h) because $\psi_{e_H} = id_N$ and $\psi_h(e_N) = e_N$ for all $h \in H$. The inverse of (n, h) is $(\psi_{h^{-1}}(n^{-1}), h^{-1})$, since $(n, h) \star_\psi (\psi_{h^{-1}}(n^{-1}), h^{-1}) = \big(n\, \psi_h\big(\psi_{h^{-1}}(n^{-1})\big), e_H\big)$ and $(\psi_{h^{-1}}(n^{-1}), h^{-1}) \star_\psi (n, h) = \big(\psi_{h^{-1}}(n^{-1})\, \psi_{h^{-1}}(n), e_H\big)$, which are equal to (e_N, e_H) because $\psi_h \circ \psi_{h^{-1}} = \psi_{e_H} = id_N$ and $\psi_{h^{-1}}(n^{-1})\, \psi_{h^{-1}}(n) = \psi_{h^{-1}}(e_N) = e_N$ for all $h \in H$.

$\widetilde{N}$ is a subgroup of G isomorphic to N because $(n_1, e_H) \star_\psi (n_2, e_H) = (n_1n_2, e_H)$ for all $n_1, n_2 \in N$. It is a normal subgroup because for all $n' \in N$ and all $(n, h) \in G$ one has $(n, h) \star_\psi (n', e_N) = (n'', e_N) \star_\psi (n, h)$ with $n'' = n\, \psi_h(n')\, n^{-1}$ (since $n\, \psi_h(n') = n''n = n''\psi_{e_N}(n)$).

$\widetilde{H}$ is a subgroup of G isomorphic to H because $(e_N, h_1) \star_\psi (e_N, h_2) = (e_N, h_1h_2)$ for all $h_1, h_2 \in H$.

Since $\chi\big((n, h)\big) = (e_N, h)$ for all $n \in N, h \in H$, and the second components in the operation $\star_\psi$ use the product in H, χ is an homomorphism, and it is the identity if one restricts it to $\widetilde{H}$ since it consists of using $n = e_N$, and its kernel is the set of (n, h) with $h = e_H$, i.e. $\widetilde{N}$.

If $N \times_\psi H$ is Abelian, then using $n_1 = n_2 = e_N$ shows that H is Abelian, and then one must have $n_1\psi_{h_1}(n_2) = n_2\psi_{h_2}(n_1)$ for all $h_1, h_2 \in H, n_1, n_2 \in N$; using $h_1 = h_2 = e_H$ shows that N is Abelian, and then using $h_1 = e_H$ gives $n_1n_2 = n_2\psi_{h_2}(n_1)$, i.e. $n_1 = \psi_{h_2}(n_1)$ for all $h_2 \in H, n_1 \in N$, or $\psi_{h_2} = id_N$ for all $h_2 \in H$, so that ψ is the trivial homomorphism of H into $Aut(N)$.

Remark 10.3: Since a semi-direct product uses an homomorphism ψ from H into $Aut(N)$, it is useful to know if a non-trivial ψ exists, since a trivial ψ gives the direct product.

For example, if $H = \mathbb{Z}_p$ for a prime p, a nontrivial ψ exists if and only if there exists an element of order p in $Aut(N)$, and in the case where N is finite, it is equivalent to p dividing the order of $Aut(N)$, by Cauchy's theorem.

One has seen that $Aut(\mathbb{Z}_n)$ is isomorphic to $\mathbb{Z}_n^*$, which has order $\varphi(n)$, so that for $p = 2$ it is always possible if $n \geq 3$ (since 1 and 2 are the only values n for which $\varphi(n)$ is odd), and we shall see below that $\mathbb{Z}_n \times_\psi \mathbb{Z}_2$ is isomorphic to the dihedral group D_n. Actually, there is a non-trivial homomorphism from $\mathbb{Z}_2$ into $Aut(N)$ for any Abelian group N, since there is a natural element of order 2 in $Aut(N)$, which is inversion inv, i.e. $n \mapsto inv(n) = n^{-1}$;[1] because $inv \circ inv = id_N$, there is then an homomorphism ψ of $\mathbb{Z}_2$ in $Aut(N)$, given by $\psi(0) = id_N$ and $\psi(1) = inv$, hence one can then construct the non-Abelian group $N \star_{inv} \mathbb{Z}_2$, which has twice the number of elements of N if N is finite.

Lemma 10.4: If $p < q$ are (distinct) primes, and $q \neq 1 \pmod p$, every group G of order $p\,q$ is isomorphic to $\mathbb{Z}_{p\,q}$, but if $q = 1 \pmod p$, there exists a non-Abelian group G of order $p\,q$ of the form $\mathbb{Z}_q \times_\psi \mathbb{Z}_p$.

[1] For a non-Abelian group G, the mapping $g \mapsto g^{-1}$ is not an homomorphism, which would require the inverse of $a\,b$ to be $a^{-1}b^{-1}$, and it is not the case for at least one pair $a, b \in G$.

Proof: By Sylow's theorem, as seen for the case of $|G| = 15$, there is one (normal) Sylow q-subgroup H_q isomorphic to $\mathbb{Z}_q$, and if $q \neq 1 \pmod p$ there is one (normal) Sylow p-subgroup H_p isomorphic to $\mathbb{Z}_p$, so that G is isomorphic to $H_p \times H_q \simeq \mathbb{Z}_{p\,q}$, but if $q = 1 \pmod p$ there is the possibility that there are q Sylow p-subgroup $K_1, \ldots, K_q$ (isomorphic to $\mathbb{Z}_p$), and indeed such a non-Abelian group can be constructed in the form $\mathbb{Z}_q \times_\psi \mathbb{Z}_p$ for a non-trivial homomorphism ψ from $\mathbb{Z}_p$ into $Aut(\mathbb{Z}_q)$, since $Aut(\mathbb{Z}_q)$ has order $q-1$, which is a multiple of p.

Remark 10.5: Since $Aut(\mathbb{Z}_q)$ is isomorphic to $\mathbb{Z}_q^*$, and it was mentioned that $\mathbb{Z}_q^*$ is cyclic, it is isomorphic to $\mathbb{Z}_{q-1}$. For any n, it was shown that for any divisor d of n, $\mathbb{Z}_n$ has exactly one subgroup of order d (and $\varphi(d)$ elements of order d), so that if p divides $q-1$ there is exactly one subgroup of order p of $Aut(\mathbb{Z}_q)$, so that there is no choice for the image $\psi(\mathbb{Z}_p)$ if ψ is a non-trivial homomorphism from $\mathbb{Z}_p$ into $Aut(\mathbb{Z}_q)$, but there are as many different ψ than elements in $Aut(\mathbb{Z}_p)$, i.e. $p-1$.

For $p = 3, q = 7$, ψ must send 1 onto an element of order 3 in $\mathbb{Z}_7^*$, and these are the quadratic residues different from 1, i.e. 2 and 4: one semi-direct product then consists in putting on $\mathbb{Z}_7 \times \mathbb{Z}_3$ the operation $(n_1, h_1) \star (n_2, h_2) = (n_1 2^{h_1} n_2, h_1 h_2)$, and the other semi-direct product consists in putting on $\mathbb{Z}_7 \times \mathbb{Z}_3$ the operation $(n_1, h_1) \star (n_2, h_2) = (n_1 4^{h_1} n_2, h_1 h_2)$, where the first components are taken modulo 7 and the second components are taken modulo 3.

Example 10.6: The dihedral group D_n is the group of symmetries of a regular polygon with n sides, and such a polygon can considered as the set of nth root of unity in $\mathbb{C}$, i.e. if $\omega = e^{\frac{2 i \pi}{n}}$, the polygon is $\{1, \omega, \ldots, \omega^{n-1}\}$. If a denotes the multiplication by ω, i.e. a rotation of $\frac{2\pi}{n}$ and b is complex conjugation, then $D_n = \{e, a, \ldots, a^{n-1}, b, b\,a, \ldots, b\,a^{n-1}\}$.[2] Since $b\,a$ applied to $z \in \mathbb{C}$ gives $\overline{\omega\,z} = \overline{\omega}\,\overline{z}$, which is $a^{-1}b$ applied to z (since $\overline{\omega} = \frac{1}{\omega}$), one deduces that $b\,a = a^{-1}b$. Then, $b\,a^{k+1} = b\,a\,a^k = a^{-1}b\,a^k$, and one finds by induction that $b\,a^k = a^{-k}b$ for all non-negative integers k; if $k < 0$, then $k + m\,n \geq 0$ for some $m \in \mathbb{N}$, so that using $a^n = e$ one deduces that $b\,a^k = b\,a^{k+m\,n} = a^{-k-m\,n}b = a^{-k}b$.

In this example $a^n = b^2 = e$, so that $b^{-1} = b$, but without using this information one has $(b\,a^k)^{-1} = (a^{-k}b)^{-1}$ for all $k \in \mathbb{Z}$, i.e. $b^{-1}a^k = a^{-k}b^{-1}$, so that one may push b or b^{-1} to the right through any power of a and change the sign of the exponent of a; by induction, one deduces that $b^\ell a^k = a^{(-1)^\ell k} b^\ell$ for all $k, \ell \in \mathbb{Z}$; then $(a^\alpha b^\beta)\,(a^\gamma b^\delta) = a^\alpha (b^\beta\,a^\gamma)\,b^\delta = a^{\alpha+(-1)^\beta \gamma} b^{\beta+\delta}$, and in the case of D_n the sum of exponents for a is taken in $\mathbb{Z}_n$, and the sum of exponent of b is taken in $\mathbb{Z}_2$.

One recognizes here a semi-direct product with $\psi_h(a^\gamma) = a^{(-1)^\beta \gamma}$ for $h = b^\beta$, i.e. $\psi_h = inv^\beta$, so that it is an example of the procedure mentioned for $N \times_{inv} \mathbb{Z}_2$.

[2] From a geometrical point of view, if one wants to send 1 onto ω^k, either one keeps orientation and one uses a rotation of angle $\frac{2k\,\pi}{n}$, i.e. a^k, or one changes orientation, in which case one uses complex conjugation before using a rotation of angle $\frac{2k\,\pi}{n}$, i.e. $a^k b$.