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

7- Wednesday September 14, 2011.

Remark 7.1: When one has an equivalence relation $\mathcal{R}$ on a set X, it defines a partition of X into equivalence classes and a quotient set $X/\mathcal{R}$ whose elements are the equivalence classes, and there is a natural (surjective) *projection* π from X onto $X/\mathcal{R}$ which to $x \in X$ associates its equivalence class $\pi(x) = \{y \in X \mid y\,\mathcal{R}\,x\}$. If a mapping f from X into a set Y has the property that $x\,\mathcal{R}\,y$ implies $f(x) = f(y)$, then it defines a mapping $\overline{f}$ from $X/\mathcal{R}$ into Y defined by $\overline{f}\big(\pi(x)\big) = f(x)$ for all $x \in X$,[1] and one has $f = \overline{f} \circ \pi$.

If G is a group, what kind of equivalence relation $\mathcal{R}$ can one put on G so that the quotient set $G/\mathcal{R}$ is a group and π is an homomorphism? The kernel of π should be a normal subgroup, and since $x\,\mathcal{R}\,y$ means $\pi(x) = \pi(y)$, or equivalently $\pi(x\,y^{-1}) = e$, i.e. $x\,y^{-1} \in N$, the equivalence class of x is the coset $N\,y$, which by the normality of N is equal to $y\,N$.

Said otherwise, suppose that H is a subgroup of G and one wonders if one can define an operation on cosets $x\,H$ by deciding that for making the product of $a\,H$ by $b\,H$, one picks an element $x \in a\,H$, an element $y \in b\,H$ and the product is the coset containing $x\,y$: it only makes sense if this coset is independent of the choice of x and y, and since a particular choice is $x = a, y = b$, one must be sure that $x = a\,h_1, y = b\,h_2$ implies $x\,y = a\,b\,h_3$ (with $h_1, h_2, h_3 \in H$, as suggested by the choice of notation, but the quantifiers are 'for all h_1, h_2 there exists h_3')); since $a\,h_1\,b\,h_2 = a\,b\,h_3$ is equivalent to $h_1 b = b\,h_3 h_2^{-1}$, it means that $b\,H = H\,b$, and because b is arbitrary, H must be a normal subgroup of G.

Definition 7.2: If G is a group and N is a normal subgroup of G, one denotes G/N the *quotient group* defined by the operation $(a\,N)\,(b\,N) = (a\,b)\,N$.

Lemma 7.3: (first isomorphism theorem for groups) If ψ is an homomorphism of a group G_1 into a group G_2, then $\psi(G_1)$ is subgroup of G_2 which is isomorphic to $G_1/\psi^{-1}(\{e\})$.
Proof: It was shown before that $\psi(G_1)$ is a subgroup of G_2 (and it follows from $\psi(a)\,\psi(b) = \psi(a\,b)$), and that $\psi^{-1}(e)$ is a normal subgroup of G_2, so that since $\psi(a) = \psi(b)$ whenever $\pi(a) = \pi(b)$ there is a factorization $\psi = \overline{\psi} \circ \pi$, where $\overline{\psi}$ is an homomorphism from $G_1/\psi^{-1}(e)$ into G_2, which is injective (since its kernel is the identity of the quotient group), and it becomes surjective if one considers it as an homomorphism from $G_1/\psi^{-1}(e)$ onto $\psi(G_1)$, so that it then is a bijection, hence an isomorphism between these two groups.

Remark 7.4: The same approach works for a *ring* R (even without imposing the existence of an identity for multiplication, which one then denotes 1),[2] which is an Abelian group (with operation noted $+$, identity noted 0, and inverse noted $-$) with an associative multiplication written without a symbol, which is distributive with respect to addition on both sides, i.e. $a\,(b + c) = a\,b + a\,c$ and $(a + b)\,c = a\,c + b\,c$ for all $a, b, c \in R$. One then defines an *ideal* J as any subgroup of R which has the property that for all $r \in R$ and all $j \in J$, both $r\,j$ and $j\,r$ belong to J.[3]

One then defines a *ring-homomorphism* ψ from a ring R_1 into a ring R_2 as a mapping satisfying $f(a+b) = f(a) + f(b)$ and $f(a\,b) = f(a)\,f(b)$ for all $a, b \in R_1$, so that it is an homomorphism of groups, and the kernel of f is $f^{-1}(\{0\}) = \{a \in R_1 \mid f(a) = 0\}$, which is a subgroup of R (automatically normal since R is Abelian), but the kernel is actually an ideal of R_1 since $f(j) = 0$ implies $f(r\,j) = f(r)\,f(j) = 0$ and $f(j\,r) = f(j)\,f(r) = 0$ for all $r \in R_1$.

An equivalence relation $\mathcal{R}$ on a ring R is adapted to the ring structure if the quotient $R/\mathcal{R}$ is a ring and the projection π is a ring-homomorphism, so that the kernel of π (which is the inverse image of $\{0\}$) is an ideal J of R, and then $\pi(x) = \pi(y)$ means $\pi(x - y) = 0$, i.e. $y \in x + J$, but since $\pi(a\,b) = \pi(a)\,\pi(b)$ it means that $(a + j_1)\,(b + j_2) = a\,b + j_3$ (with $j_1, j_2, j_3 \in J$, as suggested by the choice of notation, but the

[1] For the definition to make sense, it is necessary that $\pi(x) = \pi(y)$ implies $f(x) = f(y)$, which is precisely the hypothesis made, since $\pi(x) = \pi(y)$ is equivalent to $x\,\mathcal{R}\,y$.

[2] Some authors call a *rng* (i.e. ring without the letter i) such a ring without an identity for multiplication.

[3] An ideal is also called a *two-sided ideal*, because one defines a *left ideal* as any subgroup $J \le R$ with the property that for all $r \in R$ and all $j \in J$, $r\,j \in J$, and a *right ideal* as any subgroup $J \le R$ with the property that for all $r \in R$ and all $j \in J$, $j\,r \in J$.

quantifiers are 'for all j_1, j_2 there exists j_3), so that by taking $j_1 = 0$ one finds that $a\, j_2 \in J$ and by taking $j_2 = 0$ one finds that $j_1 b \in J$, and since a, b are arbitrary in R and j_1, j_2 are arbitrary in J, one deduces that J is an ideal.

Said otherwise, suppose that H is a subgroup of R (for addition) and one wonders if one can define a multiplication on cosets $x + H$ by deciding that for making the product of $a + H$ by $b + H$, one picks an element $x \in a + H$, an element $y \in b + H$ and the product is the coset containing $x\, y$: it only makes sense if this coset is independent of the choice of x and y, and since a particular choice is $x = a, y = b$, one must be sure that $x = a + h_1, y = b + h_2$ implies $x\, y = a\, b + h_3$ (with $h_1, h_2, h_3 \in H$, as suggested by the choice of notation, but the quantifiers are 'for all h_1, h_2 there exists h_3')); the choice $h_1 = 0$ implies that $a\, h_2 \in H$ for all $a \in R$ and all $h_2 \in H$, and the choice $h_2 = 0$ implies that $h_1 b \in H$ for all $b \in R$ and all $h_1 \in H$, i.e. H is an ideal of R.

Definition 7.5: If R is a ring and J is an ideal of R, one denotes R/J the *quotient ring* defined by the addition $(a + J) + (b + J) = (a + b)\, J$ and the multiplication $(a + J)\,(b + J) = (a\, b)\, J$.

Lemma 7.6: (first isomorphism theorem for rings) If ψ is a ring-homomorphism of a ring R_1 into a ring R_2, then $\psi(R_1)$ is subring of R_2 which is ring-isomorphic to $R_1/\psi^{-1}(\{0\})$.
Proof: That $\psi(R_1)$ is a subring of R_2 follows from $\psi(a) + \psi(b) = \psi(a + b)$ and $\psi(a)\, \psi(b) = \psi(a\, b)$, and it was shown that $\psi^{-1}(\{0\})$ is an ideal of R_2, so that since $\psi(a) = \psi(b)$ whenever $\pi(a) = \pi(b)$ there is a factorization $\psi = \overline{\psi} \circ \pi$, where $\overline{\psi}$ is an homomorphism from $R_1/\psi^{-1}(\{0\})$ into R_2, which is injective (since its kernel is the 0 of the quotient ring), and it becomes surjective if one considers it as a ring-homomorphism from $R_1/\psi^{-1}(\{0\})$ onto $\psi(R_1)$, so that it then is a bijection, hence a ring-isomorphism between these two rings.

Definition 7.7: If G is a group, then for $a, g \in G$, the *conjugate* of a by g is $a^g = g\, a\, g^{-1}$, and the *conjugate of a subgroup* H by g is $H^g = \{g\, h\, g^{-1} \mid h \in H\}$, which is a subgroup of G (and a subgroup H is normal if and only if $H^g = H$ for all $g \in G$).[4] The *conjugation by* g is the automorphism $\psi_g \in Aut(G)$ defined by $\psi_g(x) = g\, x\, g^{-1}$ for all $x \in G$. The *conjugacy class* of a is $\{a^g \mid g \in G\}$.

Remark 7.8: The fact that $\psi_g(x\, y) = g\, x\, y\, g^{-1} = g\, x\, g^{-1} g\, y\, g^{-1} = \psi_g(x)\, \psi_g(y)$ show that ψ_g is an homomorphism of G into G (i.e. an endomorphism), but $\psi_g\big(\psi_h(x)\big) = \psi_g(h\, x\, h^{-1}) = g\, h\, x\, h^{-1} g^{-1} = (g\, h)\, x\, (g\, h)^{-1} = \psi_{g\, h}(x)$ shows that $\psi_g \circ \psi_h = \psi_{g\, h}$, and in particular ψ_g is invertible with inverse $\psi_{g^{-1}}$ (since ψ_e is the identity mapping id_G on G), so that ψ_g is an isomorphism of G onto G (i.e. an automorphism). The set of automorphism of G, denoted $Aut(G)$, is a group for the operation of composition, whose identity is $e = id_G$, and the relation $\psi_g \circ \psi_h = \psi_{g\, h}$ for all $g, h \in G$ shows that the mapping $g \mapsto \psi_g$ is an homomorphism from G into $Aut(G)$.

If G is Abelian, then $\psi_g = id_G$ for all $g \in G$, all subgroups are normal, and each conjugacy class is reduced to one element.

Definition 7.9: One says that a subgroup $H \le G$ is *characteristic* in G, and one writes $H\, char\, G$, if (and only if) $\psi(H) = H$ for all $\psi \in Aut(G)$,[5] the group of automorphisms of G.

Remark 7.10: Being a characteristic subgroup is a stronger property than being a normal subgroup, since normality is $\psi_g(H) = H$ for all $g \in G$ (or simply $\psi_g(H) \subset H$ for all $g \in G$), where ψ_g is the automorphism of conjugation by g.

Lemma 7.11: $A\, char\, B\, char\, C$ implies $A\, char\, C$, and $A\, char\, B \triangleleft C$ implies $A \triangleleft C$.
Proof: In the first case, for $\varphi \in Aut(C)$ one has $\varphi(B) = B$, so that $\varphi\big|_B \in Aut(B)$, and then $\varphi(A) = \varphi\big|_B(A) = A$.

In the second case, for $c \in C$ one has $\varphi_c(B) = B$, so that $\varphi_c\big|_B \in Aut(B)$, and then $\varphi_c(A) = \varphi_c\big|_B(A) = A$.

Remark 7.12: In general $A \triangleleft B \triangleleft C$ does not imply $A \triangleleft C$.

---

[4] Since $\big(H^{g_1}\big)^{g_2} = H^{g_2 g_1}$ for all $g_1, g_2 \in G$, $K = H^g$ is equivalent to $H = K^{g^{-1}}$, and one deduces that H is normal if and only if $H^g \subset H$ for all $g \in G$.

[5] It is enough that $\psi(H) \subset H$ for all automorphisms of G, because ψ^{-1} being also an automorphism, one has $\psi^{-1}(H) \subset H$, and then applying ψ gives $H \subset \psi(H)$.

For example, let C be the dihedral group D_4 which has order 8, and is generated by a which has order 4 and b which has order 2, satisfying $b\,a = a^3 b$,[6] so that $b\,a^2 = a^3 b\,a = a^6 b = a^2 b$, and $b\,a^3 = a^2 b\,a = a^5 b = a\,b$. Since b commutes with a^2, $B = \{e, a^2, b, a^2 b\}$ is a subgroup of C, which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$,[7] and which is a normal subgroup of C, since B has index 2 in C. Since B is Abelian, $A = \{e, b\}$ is a normal subgroup of B. However, $a\,b\,a^{-1} = a\,b\,a^3 = a^2 b$, so that A is not stable by ψ_a, hence A is not a normal subgroup of C.

Example 7.13: $G = \mathbb{Z}_n$ is Abelian, so that $\psi_g = id_G$ for all $g \in G$, but $Aut(G)$ is not reduced to one element, and it actually has $\varphi(n)$ elements, and $Aut(G)$ is isomorphic to Z_n^*, the multiplicative group of units of the ring $\mathbb{Z}_n$. Indeed, if ψ is an automorphism of G, it sends any generator of $\mathbb{Z}_n$ to a generator of $\mathbb{Z}_n$, i.e. 1 is sent to an element $a \in \mathbb{Z}_n^*$, so that x is sent to $a\,x$ modulo n, and if another automorphism ψ' is the multiplication by $b \in \mathbb{Z}_n^*$, then the composition of ψ and ψ' is the multiplication by $a\,b$.

All the subgroups of $\mathbb{Z}_n$ are characteristic subgroups, since for every d dividing n there is exactly one subgroup of order d, and any automorphism must send this subgroup of order d on itself, so that it is a characteristic subgroup.

Example 7.14: $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ is Abelian, so that $\psi_g = id_G$ for all $g \in G$, but $Aut(G)$ is not reduced to one element, and it actually has 6 elements, and $Aut(G)$ is isomorphic to the symmetric group S_3. Indeed, if ψ is an automorphism, it sends any element of order 2 to an element of order 2, and there are 3 of them: $G = \{e, a, b, c\}$ with $a^2 = b^2 = c^2 = e$, $a\,b = b\,a = c$, $b\,c = c\,b = a$, and $c\,a = a\,c = b$; once $\psi(a)$ and $\psi(b)$ are chosen distinct among a, b, c, the image $\psi(c)$ is the third one, so that any permutation of a, b, c gives an automorphism of G.

There are 3 subgroups of order 2, which are normal since G is Abelian, but none of them is a characteristic subgroup, since they are permuted by the automorphisms.

Example 7.15: $G = \mathbb{Z}_2 \times \mathbb{Z}_4$ is Abelian, so that $\psi_g = id_G$ for all $g \in G$, but $Aut(G)$ is not reduced to one element. G has 4 elements of order 4 ($(0,1), (0,3), (1,1), (1,3)$), and 3 elements of order 2 ($(0,2), (1,0), (1,2)$) so that it has 2 subgroups of order 4 and 3 subgroups of order 2, but the intersection of the two subgroups of order 4 is a subgroup of order 2, generated by $(0,2)$, so that this subgroup is characteristic (among the elements or order 2, $(0,2)$ is the only one which is divisible by 2).

Since G is generated by 2 of the elements of order 4, like $a = (0,1)$ and $b = (1,1)$, so that the other elements of order 4 are $3a$ and $3b$, and the elements of order 2 are $2a = 2b$, $b - a$, and $b + a$. There are then 4 automorphisms, obtained by sending (a, b) on either (a, b), $(3a, b)$, $(a, 3b)$, or $(3a, 3b)$, and $Aut(G)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.[8]

---

[6] For example, a is the rotation of angle $\frac{\pi}{2}$ (like multiplication by i in $\mathbb{C}$), and b is a mirror symmetry (like complex conjugation in $\mathbb{C}$), so that $b\,a(z) = b(i\,z) = -i\bar{z} = a^3 b(z)$, hence $b\,a = a^3 b$.

[7] Since it is a subgroup, and a^2, b, and $a^2 b$ have order 2.

[8] These are given by mappings $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_4 \mapsto (\alpha\,x + \beta\,y, \gamma\,x + \delta\,y) \in \mathbb{Z}_2 \times \mathbb{Z}_4$ with the matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ given by $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}$, $\begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$.