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

3- Friday September 2, 2011.

The basic algebraic structures depend upon the number of operations used. With one *binary operation* satisfying some properties, a natural structure is that of a *group*, and with two binary operations (addition and multiplication) satisfying some properties a natural structure is that of a *ring*, with a particular case of a *field*. With addition and a second operation external, a natural structure is that of a *vector space* over a field F or a *module* over a ring R, depending upon the *scalars* belonging to F or R.

Between sets, one uses arbitrary *mappings*, but when one restricts attention to sets which have a particular algebraic structure,[1] one considers mappings which are adapted to the *category* of sets considered, *homomorphisms* in the case of *groups*, *rings*, or *fields*, *linear mappings* in the case of *vector spaces*, for example. In general, these particular mappings are called *morphisms*, and one uses a list of (Greek) prefixes which give information about them: an *injective* (one-to-one) mapping is called a *monomorphism*, a *surjective* (onto) mapping is called an *epimorphism*, a *bijective* (injective and surjective) mapping is called an *isomorphism*; a mapping from a set into itself is called an *endomorphism*, and an isomorphism of a set onto itself is called an *automorphism*.

If two sets with some algebraic structures are proved to be isomorphic, it means that by changing the names of elements and the names of the operations they are somewhat the same, and sometimes such a result is not so obvious and one needs a mathematician's mind for discovering it. Of course, it is part of the mathematician's job to observe similarities between situations, and to go from the general case to the particular examples, and out of a few examples to imagine a general situation.

Parables are like general theorems, and they can be transmitted by people who do not necessarily understand all the various applications of the teaching: if after stating a general theorem one gives an example, weaker students may only understand the example while stronger students foresee that the theorem applies to many situations. Since the gospels say that the disciples of Jesus often asked for examples,[2] it suggests that they did not understand what the teaching they received was about.[3]

Definition 3.1: A binary operation $*$ on a set X is *associative* if for all $a, b, c \in X$ one has $a * (b * c) = (a * b) * c$, so that one may write $a * b * c$ without ambiguity.

A binary operation $*$ on a set X is *commutative* if for all $a, b \in X$ one has $a * b = b * a$.

A binary operation $*$ on a set X has an *identity* e if for all $a \in X$ one has $a * e = e * a = a$.

For a binary operation $*$ on a set X which has an identity e, one says that an element a has an *inverse* a^{-1} if $a^{-1} * a = a * a^{-1} = e$.

Remark 3.2: An identity is unique: if both e_1 and e_2 are identities, then $e_1 * e_2$ is equal to e_1 because e_2 is an identity, and it is equal to e_2 because e_1 is an identity. Actually, once one has written a proof, it is useful to check what one has really used and what more general statements one can deduce: here, one may define an *identity on the left* e_ℓ if for all $a \in X$ one has $e_\ell * a = a$, and an *identity on the right* e_r if for all $b \in X$ one has $b * e_r = b$; then, if both e_ℓ and e_r exist, one considers $e_\ell * e_r$ and one deduces that $e_\ell = e_r$.

[1] Or non-algebraic, like *topological spaces*, where one restricts attention to *continuous mappings*.

[2] Jesus of Nazareth, Jewish religious teacher, 7 BCE–30 CE (or 2 BCE–36 CE). He is believed by Christians to be the (unique) son of God, and the messiah whom Jews were waiting for, hence its title Christ, which comes from the Greek Christos. Of course, I consider that he was only human, and I often refer to him as the Teacher. According to the gospels, he practiced meditation past the point where one can do miracles, but without using that power for a personal advantage. He was executed by the Romans, probably because some of his followers believed him to be the messiah whom Jews were waiting for, and whom they expected to put an end to the Roman occupation of Palestine.

[3] I deduce that Jesus of Nazareth existed, because the evangelists did not perceive that by repeating the stories they showed that the disciples were not so bright, hence they were not bright enough themselves for inventing such a character as Jesus: the only person who seems to have taught in parables before is the Buddha, and the story of Jesus of Nazareth does not resemble that of the Buddha.

If $*$ is associative, such an inverse is unique. More generally, one says that a has a *left inverse* α if $\alpha * a = e$, and that it has a *right inverse* β if $a * \beta = e$, and then if $*$ is associative and both α and β exist, one has $\alpha = \alpha * e = \alpha * a * \beta = e * \beta = \beta$.

Definition 3.3: A *group* $(G, *, e)$ is a set G equipped with an associative binary operation $*$ with identity $e \in G$ and such that each $a \in G$ has an inverse. An *Abelian group* is a group for which the operation is commutative, and in this case one uses $+$ for the operation, 0 for the identity, and $-a$ for a^{-1}.

A *monoid* $(M, *, e)$ is a set M equipped with an associative binary operation $*$ with identity $e \in M$.

A *semigroup* $(S, *)$ is a set S equipped with an associative binary operation $*$. It has the *cancellation property* if $a * b = a * c$ implies $b = c$ and if $a * b = c * b$ implies $a = c$.[4]

Remark 3.4: When one uses a multiplicative notation, it is common not to write a symbol for the operation, i.e. instead of writing $a \cdot b$, or $a * b$, or $a \star b$, for example, one writes $a\,b$, and then one has $(a\,b)^{-1} = b^{-1}a^{-1}$ (since $b^{-1}a^{-1}a\,b = b^{-1}e\,b = b^{-1}b = e$ and $a\,b\,b^{-1}a^{-1} = a\,e\,a^{-1} = a\,a^{-1} = e$).

One writes 0 for the identity if the operation is $+$, only used for a commutative operation, and in multiplicative notation one also writes 1 for the identity.

There are actually two mappings involved for a group, the operation $*$ which is a (surjective) mapping of $G \times G$ onto G and the inverse mapping $a \mapsto a^{-1}$ which is a bijection of G onto G.

By an abuse of language, one says a group G, so that which binary operation is considered and which is the identity must be clear, but in situations where one feels that there could be some confusion, it is better to give different names to the various operations which appear in a formula, of course.

Although $\mathbb{N}$ with addition is not a group, there is a natural symmetrization which embeds it into the additive *Abelian group* $\mathbb{Z}$ (since addition is *commutative*), and it is surprising that inventing zero took so long, and it seems that the Arab mathematicians learned it from the Indian mathematicians before it was introduced in Europe.[5] Inventing zero and negative numbers should have been obvious for merchants, who would understand their financial situation as the amount of cash a (or the value of the merchandise) they have and the amount b they borrowed, and consider their wealth to be a pair (a, b) with a different symbol to use for a if they are broke, or for b if they have reimbursed all their debts, but it may have been difficult to imagine an ideal world where one can borrow without interest so that the wealth of (a, b) is the same as that of $(a + c, b + c)$ after borrowing a positive amount c, so that there is a natural equivalence relation behind the definition of $a - b$ even though b may be $\geq a$, and this is formalized as Lemma 3.5.

Recall that an *equivalence relation* on a set X is a binary relation $\mathcal{R}$ which is *reflexive* (i.e. $a\,\mathcal{R}\,a$ for all $a \in X$), *symmetric* (i.e. $a\,\mathcal{R}\,b$ implies $b\,\mathcal{R}\,a$) and *transitive* (i.e. $a\,\mathcal{R}\,b$ and $b\,\mathcal{R}\,c$ imply $a\,\mathcal{R}\,c$), so that one can define the *equivalence class* of a as $\overline{a} = \{b \mid a\,\mathcal{R}\,b\}$, observe that two equivalence classes are either equal or disjoint, and define the *quotient set* $X/\mathcal{R}$ whose elements are the equivalence classes, with a natural *projection* π from X onto $X/\mathcal{R}$ which to each a associates its equivalence class $\overline{a}$. One then observes that if f is a mapping from X into Y which has the property that $a\,\mathcal{R}\,b$ implies $f(a) = f(b)$, then f factorizes as $f = \overline{f} \circ \pi$ for a mapping $\overline{f}$ from $X/\mathcal{R}$ into Y (defined by $\overline{f}(\overline{a}) = f(b)$ for any $b \in \overline{a}$).

Lemma 3.5: Let S be a (non-empty) semigroup with commutative operation $*$ having the cancellation property.

The relation $\mathcal{R}$ defined on $S \times S$ by '$(a, b)\,\mathcal{R}\,(c, d)$ means $a * d = b * c$' is an equivalence relation.

The operation $\star$ defined on $S \times S$ by $(a_1, b_1) \star (a_2, b_2) = (a_1 * a_2, b_1 * b_2)$ is compatible with $\mathcal{R}$ and induces on the quotient $G = S \times S/\mathcal{R}$ a binary operation $\overline{\star}$, which gives G an Abelian group structure, with

[4] One may define cancellation properties on the left or on the right, of course.

[5] In his *Ecclesiastical History of the English People*, written in 731, Bede popularized the dating system with AD (Anno Domini) invented in 525 by Dionysius the Humble for replacing the Diocletian years, and he invented the dating system with BC (Before Christ), without a year zero, so that the year preceding 1AD is 1BC. Since it is silly to confuse numbering systems with religious questions, it is better to use CE (Common Era) instead of AD, and BCE (Before Common Era) instead of BC. Confusing astronomical questions with religious ones should also be avoided, and the astronomical corrections introduced in 1582 for starting the Gregorian calendar were difficult to accept for some Protestant countries, and England switched to it in 1752, or for Greek Orthodox countries, and Greece switched to it in 1923, Russia having done it just after its "October revolution" in 1917, which for us occurred in November.

the identity 0 being the equivalence class of (s,s) for any $s \in S$, and the inverse of the equivalence class of (a,b) being the equivalence class of (b,a).

S is embedded into G by the mapping j with $j(a)$ being the equivalence class of $(a*s,s)$ for all $s \in S$, and one has $j(a*b) = j(a)\,\overline{\star}\,j(b)$ for all $a,b \in S$.

Proof: $\mathcal{R}$ is reflexive since $(a,b)\,\mathcal{R}\,(a,b)$ means $a*b = b*a$ and $*$ is assumed commutative. $\mathcal{R}$ is symmetric since $(c,d)\,\mathcal{R}\,(a,b)$ means $c*b = d*a$, which is the same as $a*d = b*c$ by commutativity. $\mathcal{R}$ is transitive since $(a_1,b_1)\,\mathcal{R}\,(a_2,b_2)$ and $(a_2,b_2)\,\mathcal{R}\,(a_3,b_3)$ mean $a_1*b_2 = b_1*a_2$ and $a_2*b_3 = b_2*a_3$, so that $a_1*b_2*b_3 = b_1*a_2*b_3 = b_1*b_2*a_3$, hence $b_2*a_1*b_3 = b_2*b_1*a_3$ by commutativity, which implies $a_1*b_3 = b_1*a_3$ by the cancellation property.

One needs to show that if $(a_1,b_1)\,\mathcal{R}\,(c_1,d_1)$ and $(a_2,b_2)\,\mathcal{R}\,(c_2,d_2)$ then $(a_1*a_2, b_1*b_2)\,\mathcal{R}\,(c_1*c_2, d_1*d_2)$; indeed, one has $a_1*d_1 = b_1*c_1$ and $a_2*d_2 = b_2*c_2$, so that using commutativity $(a_1*a_2)*(d_1*d_2) = (a_2*d_2)*(a_1*d_1) = (b_2*c_2)*(b_1*c_1) = (b_1*b_2)*(c_1*c_2)$. This shows that $\star$ implies an operation $\overline{\star}$ on the quotient. Associativity of $*$ implies associativity of $\star$, which implies associativity of $\overline{\star}$, and commutativity of $*$ implies commutativity of $\star$, which implies commutativity of $\overline{\star}$, of course. Since all (s,s) are equivalent, its equivalence class 0 is the identity of $\overline{\star}$ if $(a,b)\star(s,s)$ is equivalent to (a,b) for all (a,b), which follows from the cancellation property. Then, $(a,b)\star(b,a) = (a+b, a+b)$ by commutativity.

Since $(a*s,s)\,\mathcal{R}\,(a*t,t)$ by commutativity, it follows that $j(a)$ is well defined, and then $j(a*b)$ is the equivalence class of $\big((a*b)*(s*t),(s*t)\big) = (a*s,s)\star(b*t,t)$, i.e. $j(a)\overline{\star}j(b)$.

Example 3.6: If S is the positive integers ($\mathbb{N}^\times = \mathbb{N}\setminus\{0\}$) with addition, then G is (isomorphic) to $\mathbb{Z}$.

If S is the positive integers with multiplication, then G is (isomorphic) to the multiplicative group $\mathbb{Q}_+$, the positive rationals.

If $S = \mathbb{Z}^* = \mathbb{Z}\setminus\{0\}$ with multiplication, then G is (isomorphic) to the multiplicative group $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$, the non-zero rationals.[6]

Definition 3.7: If $(G_1,*_1,e_1)$ and $(G_2,*_2,e_2)$ are two groups and f is a mapping from G_1 into G_2,[7] then f is an *homomorphism* if $f(a\,*_1\,b) = f(a)\,*_2\,f(b)$ for all $a,b \in G_1$.

The *kernel* of an homomorphism f is the inverse image of $\{e_2\}$,[8] i.e. $f^{-1}(\{e_2\}) = \{a \in G_1 \mid f(a) = e_2\}$.

The groups G_1 and G_2 are said to be *isomorphic* if there exists an isomorphism from G_1 onto G_2 (whose inverse is then an isomorphism from G_2 onto G_1), and one then writes $G_1 \simeq G_2$.

Lemma 3.8: If f is an homomorphism from G_1 into G_2, then $f(e_1) = e_2$ and $f(a^{-1}) = \big(f(a)\big)^{-1}$ for all $a \in G_1$.

Proof: For $a \in G_1$, one has $a = a\,e_1$, so that $f(a) = f(a)\,f(e_1)$ and (by multiplying on the left by the inverse of $f(a)$) $e_2 = f(e_1)$. Then one has $a\,a^{-1} = e_1$, so that $f(a)\,f(a^{-1}) = e_2$ and (by multiplying on the left by the inverse of $f(a)$) $f(a^{-1}) = \big(f(a)\big)^{-1}$.

Remark 3.9: If S is an Abelian group, the symmetrization process of Lemma 3.5 produces an Abelian group G which is isomorphic to S, with j being an isomorphism from S onto G.

Example 3.10: The *logarithm*, introduced by NAPIER,[9] is defined by $\log(a) = \int_1^a \frac{dx}{x}$ for $a \in \mathbb{R}_+$, which

---

[6] For a ring R, one denotes R^* the multiplicative group of units, i.e. of elements of R which have an inverse for multiplication. For an integral domain D (i.e. a commutative ring without zero-divisors) and $S = D\setminus\{0\}$ with multiplication one obtains $F^* = F\setminus\{0\}$ where F is the field of fractions of D.

[7] By an abuse of language, one usually says that f is a mapping from a group G_1 into a group G_2, and that it is an homomorphism if ..., and I shall write in this way in the sequel.

[8] If f is a mapping from a set X into a set Y, one associates a (push forward) mapping $f_>$ from $\mathcal{P}(X)$ into $\mathcal{P}(Y)$ defined by $f_>(A) = \{f(a) \mid a \in A\}$ for all $A \subset X$, and a (pull backward) mapping $f^<$ from $\mathcal{P}(Y)$ into $\mathcal{P}(X)$ defined by $f^<(B) = \{a \in X \mid f(a) \in B\}$ for all $B \subset Y$. This good notation was introduced by my colleagues Walter NOLL and Juan SCHÄFFER, who improved on a notation f_* and f^* from a book by MAC LANE and Garrett BIRKHOFF, but these notations are not common and almost everyone in mathematics writes $f(A)$ for $\{f(a) \mid a \in A\}$, and $f^{-1}(B)$ for $\{a \in X \mid f(a) \in B\}$, although it may be a little confusing in some cases.

[9] John NAPIER, Scottish mathematician, 1550–1617. He invented a form of logarithms in 1614, and

requires defining a so-called Riemann integral (since the function $x \mapsto \frac{1}{x}$ is continuous on $\mathbb{R}_+$),[10] whose intuition was clear to many a long time before, since ARCHIMEDES is credited for computing the area below a parabola,[11] without even having an equation for the parabola since the invention of analytic geometry (i.e. the introduction of algebraic notation in geometry) is attributed to DESCARTES;[12] the result ARCHIMEDES was the most proud of was that the surface area of a sphere of radius R is equal to the lateral area of a tangent cylinder of radius R and height $2R$, and he had asked that his tomb show a sphere and a cylinder, and when Cicero was named governor of Sicily,[13] this information permitted him to find the tomb (without the help of the people of Syracuse, who had forgotten where it was). By a simple change of variable, one proves that $\log(a\,b) = \log(a) + \log(b)$ for $a, b \in \mathbb{R}_+$, and this shows that the logarithm is an homomorphism from the multiplicative (Abelian) group $\mathbb{R}_+$ into the additive (Abelian) group $\mathbb{R}$, and it is actually an isomorphism, whose inverse is the *exponential*.

However, the multiplicative (Abelian) group $\mathbb{Q}_+$ is not isomorphic to the additive (Abelian) group $\mathbb{Q}$, because in $\mathbb{Q}$ the equation $x + x = a$ has a solution for all $a \in \mathbb{Q}$, while in $\mathbb{Q}_+$ the equation $x^2 = a$ only has a solution if $a = \frac{m^2}{n^2}$ for m, n positive integers (and relatively prime).

Besides $\mathbb{Z}$, there is a natural family of finite Abelian groups, the group $\mathbb{Z}_n$ of integers modulo n (and $\mathbb{Z}_n$ has n elements), introduced by GAUSS for reasons from number theory.[14]

Looking for finite groups, one has to consider the group of permutations of n objects (with $n \geq 2$), which is the *symmetric group* S_n (which has $n!$ elements), and only S_2 is Abelian and isomorphic to $\mathbb{Z}_2$.

Some particular non-Abelian groups are found by considering the groups of symmetries of various regular objects, like that of a regular polygon with n sides (with $n \geq 3$), which is the *dihedral group* D_n (which has $2n$ elements), and it reduces to the Abelian group $\mathbb{Z}_n$ if one restricts attention to symmetries conserving the orientation (i.e. if one rejects *mirror symmetries*), so that $\mathbb{Z}_n$ is isomorphic to the *group of rotations* by angles which are multiples of $\frac{2\pi}{n}$, or to the multiplicative group of nth roots of unity in $\mathbb{C}$; D_3 is actually isomorphic to S_3. The group of symmetries of a rhombus which is not a square or that of a rectangle which is not a square is $\mathbb{Z}_2 \times \mathbb{Z}_2$, called the *Klein four-group* V,[15] which is not isomorphic to $\mathbb{Z}_4$, while $\mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_6$, and we shall see the relation with the *Chinese remainder theorem*.

One non-Abelian group of order 8 is the *quaternion group* Q_8, which has some relation with the *quaternions* introduced by HAMILTON.[16]

We shall have to understand questions of product of groups, of quotient of groups, and other ways to construct new groups, and in what ways problems of groups appear in questions from outside mathematics.

Additional footnotes: BEDE,[17] Garrett BIRKHOFF,[18] .../...

---

suggested an improvement into the actual form to BRIGGS, who published his tables of logarithms in 1617, with whole credit to NAPIER, who had just died.

[10] Georg Friedrich Bernhard RIEMANN, German mathematician, 1826–1866. He worked at Georg-August-Universität, Göttingen, Germany. The Riemann ζ function is named after him, although EULER had studied it in his thesis. Riemannian manifolds and Riemannian geometry are named after him, as well as Riemann surfaces for functions of a complex variable, and Riemann invariants for conservation laws in continuum mechanics.

[11] ARCHIMEDES, Greek mathematician, 287 BCE–212 BCE. He worked in Siracusa (Syracuse), then a Greek colony, now in Italy.

[12] René DESCARTES, French mathematician and philosopher, 1596–1650. Université de Paris 5 is named after him. The terms Cartesian coordinates and Cartesian products are derived from his name (written in Latin as CARTESIUS, possibly DES CARTES in French).

[13] Marcus TULLIUS Cicero, Roman orator and politician, 106 BCE–43 BCE.

[14] And also for questions of calendar, I believe.

[15] Felix Christian KLEIN, German mathematician, 1849–1925. He worked at Georg-August-Universität, Göttingen, Germany.

[16] Sir William Rowan HAMILTON, Irish mathematician, 1805–1865. He worked in Dublin, Ireland.

[17] (The venerable) BEDE, English monk and historian, 673–735. He popularized the new dating system with AD (Anno Domini) in his *Ecclesiastical History of the English People*, and invented the dating system with BC (Before Christ), so that there is no year zero in the calendar.

[18] Garrett BIRKHOFF, American mathematician, 1911–1996. He worked at Harvard University, Cambridge,

BRIGGS,[19] Buddha,[20] DIOCLETIAN,[21] DIONYSIUS the Humble,[22] Gregory XIII,[23] GRESHAM,[24] JULIUS Caesar,[25] MAC LANE,[26] Walter NOLL,[27] Juan SCHÄFFER.[28]

MA.

[19] Henry BRIGGS, English mathematician, 1561–1630. He worked at Gresham college, London, and then in Oxford, England, holding the first Savilian chair of geometry(1619–1630). He was the first to publish a table of logarithms, following the suggestions of NAPIER.

[20] Siddhartha Gautama, Indian religious teacher, 563 BCE–483 BCE. Buddhists follow his teachings, and consider that he was the historical Buddha for our era.

[21] Gaius Aurelius Valerius DIOCLETIANUS (DIOCLES), Roman military and political leader, 244–311. He was Roman emperor from 284 to 305.

[22] DIONYSIUS the Humble (DIONYSIUS Exiguus), Greek Orthodox monk, 470–540. He invented a new system of numbering years to replace the Diocletian years, with AD (Anno Domini), thus starting the Christianized version of the Julian calendar.

[23] Gregory XIII (Ugo BONCOMPAGNI), Italian Pope, 1502–1585. He was elected Pope in 1572. The Gregorian calendar is named after him.

[24] Sir Thomas GRESHAM, English merchant and financier, 1519–1579. He left the money used for founding Gresham College in London, England, in 1597.

[25] Gaius JULIUS Caesar, Roman military and political leader, 100 BCE–44 BCE. The qualifier Caesar for the Roman emperors (which transformed into Kayser in Germany, and Czar in Russia) comes from his cognomen, and the Julian calendar also refers to him.

[26] Saunders MAC LANE, American mathematician, 1909–2005. He worked at Harvard, Cambridge, MA and at University of Chicago, Chicago, IL.

[27] Walter NOLL, German-born mathematician, born in 1925. He works at CMU (Carnegie Mellon University), Pittsburgh, PA, where he has been my colleague since I moved there, in 1987.

[28] Juan Jorge SCHÄFFER, Austrian-born mathematician, born in 1930. He works at CMU (Carnegie Mellon University), Pittsburgh, PA, where he has been my colleague since I moved there, in 1987.