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

5- Friday September 9, 2011.

Definition 5.1: If $(G_i, *_i, e_i), i \in I$, is a family of groups indexed by a non-empty set I, then the product $G = \prod_{i\in I} G_i$ has a structure of group, called the *direct product*, where the operation $*$ is defined by $a * b = \{a_i *_i b_i, i \in I\}$ for $a = \{a_i, i \in I\}$, $b = \{b_i, i \in I\}$.[1]

Remark 5.2: Of course, the structure described is that of a group, since $*$ is obviously associative, the identity element is $e = \{e_i, i \in I\}$, and the inverse of $a = \{a_i, i \in I\}$ is $a^{-1} = \{a_i^{-1}, i \in I\}$. The direct product is Abelian if and only if G_i is Abelian for all $i \in I$.[2]

If for each $i \in I$, the coordinate a_i has a finite order m_i in G_i, then if I is finite a has a finite order equal to the least common multiple of all the m_i, but if I is infinite this "least common multiple" could be infinite.

Lemma 5.3: If $m_1, \ldots, m_k$ are pairwise relatively prime, then $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ is isomorphic to $\mathbb{Z}_n$ with $n = m_1 \cdots m_k$.
Proof: The mapping which to $a \in \mathbb{Z}$ associates $(a_1, \ldots, a_k)$, where a_i is (the equivalence class of) the remainder in the division of a by m_i for $i = 1, \ldots, k$ is an homomorphism, and since two integers differing from a multiple of n have the same image, it defines an homomorphism from $\mathbb{Z}_n$ into $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$; by the Chinese remainder theorem, this homomorphism is a bijection, so that it is an isomorphism.[3]

Remark 5.4: Comparing the orders of elements gives a simple way to show that two groups are not isomorphic.

$\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ both have 4 elements, but they are not isomorphic: $\mathbb{Z}_4$ has 1 element of order 2 (which is 2) and 2 elements of order 4 (which are 1 and 3); $\mathbb{Z}_2 \times \mathbb{Z}_2$ has 3 elements of order 2 (which are $(0,1)$, $(1,0)$, and $(1,1)$) and 0 element of order 4.

Similarly, $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ all have 8 elements, but no two of these groups are isomorphic: $\mathbb{Z}_8$ has 1 element of order 2 (which is 4), 2 elements of order 4 (which are 2 and 6), and 4 elements of order 8 (which are 1, 3, 5, and 7); $\mathbb{Z}_2 \times \mathbb{Z}_4$ has 3 elements of order 2 (which are $(0,2)$, $(1,0)$, and $(1,2)$), 4 elements of order 4 (which are $(0,1)$, $(0,3)$, $(1,1)$, and $(1,3)$), and 0 element of order 8; $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has 7 elements of order 2 (which are all the elements different from the identity $(0,0,0)$), 0 element of order 4, and 0 element of order 8.

There are two non-Abelian groups of order 8, the *dihedral group* D_4, and the *quaternion group* Q_8,[4] which are not isomorphic (and not isomorphic to any of the three Abelian groups of order 8, of course).

D_4 is the group of symmetries of a square,[5] and it has 5 elements of order 2 (which are the four mirror symmetries, and R_{180}, the rotation of 180 degrees), 2 elements of order 4 (which are R_{90} and R_{270}, the rotations of 90 degrees and of 270 degrees), and 0 element of order 8.

$Q_8 = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$, with $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ and $\mathbf{i}\,\mathbf{j}\,\mathbf{k} = -1$,[6] and it has 1 element of order 2 (which is -1), 6 elements of order 4 (which are $\pm\mathbf{i}$, $\pm\mathbf{j}$, and $\pm\mathbf{k}$), and 0 element of order 8.

[1] In the case of rings, the direct product has a structure of rings, where the product is done coordinate by coordinate, but the product of two rings is never an integral domain, since $(0,1)\cdot(1,0) = (0,0)$; in particular, a product of fields is not a field.

[2] We shall see later in the course that in some cases one can put on $G_1 \times G_2$ another group structure, called a semi-direct product, and this semi-direct group can be non-Abelian even with G_1 and G_2 Abelian.

[3] If a bijection f from G_1 into G_2 is an homomorphism (with respect to group structures on G_1 and G_2), then the inverse f^{-1} is an homomorphism from G_2 into G_1: indeed, if $a, b \in G_2$, then $a = f(\alpha), b = f(\beta)$ for $\alpha = f^{-1}(a), \beta = f^{-1}(b) \in G_1$, and since $f(\alpha\,\beta) = f(\alpha)\,f(\beta) = a\,b$ one has $f^{-1}(a\,b) = \alpha\,\beta = f^{-1}(a)\,f^{-1}(b)$, showing that f^{-1} is an homomorphism.

[4] The relation with the division ring of quaternions (introduced by Hamilton) is described below.

[5] For $n \geq 3$, the dihedral group D_n is the group of symmetries of a regular polygon with n sides, and it has $2n$ elements; D_3 is isomorphic to the symmetry group S_3, of permutations of 3 objects. The symmetry group S_n of permutations of n objects has order $n!$.

[6] This implies $\mathbf{i}\,\mathbf{j} = \mathbf{k} = -\mathbf{j}\,\mathbf{i}$, $\mathbf{j}\,\mathbf{k} = \mathbf{i} = -\mathbf{k}\,\mathbf{j}$, $\mathbf{k}\,\mathbf{i} = \mathbf{j} = -\mathbf{i}\,\mathbf{k}$.

Remark 5.5: Comparing the subgroups and their inclusions gives another (less simple) way to show that two groups are not isomorphic.

$\mathbb{Z}_4$ has 1 subgroup H of order 2, with $\{0\} \le H \le \mathbb{Z}_4$; $\mathbb{Z}_2 \times \mathbb{Z}_2$ has 3 subgroups H_1, H_2, H_3 of order 2, with $\{0\} \le H_1, H_2, H_3 \le \mathbb{Z}_2 \times \mathbb{Z}_2$, and no relation of order between H_1, H_2, and H_3.

$\mathbb{Z}_8$ has 1 subgroup H of order 2, and 1 subgroup K of order 4, with $\{0\} \le H \le K \le \mathbb{Z}_8$.

$\mathbb{Z}_2 \times \mathbb{Z}_4$ has 3 subgroups or order 2, and 2 subgroups of order 4, so that there is (at least) one subgroup of order 2 which is not included in a subgroup of order 4, and the reason is that among the 3 elements of order 2 (which are $(0,2)$, $(1,0)$, and $(1,2)$), only 1 can be divided by 2 (i.e. $(0,2) = (0,1) + (0,1) = (0,3) + (0,3) = (1,1) + (1,1) = (1,3) + (1,3)$), and the subgroup $H_0 = \{(0,0),(0,2)\}$ is actually the intersection of the 2 subgroups K_1, K_2 of order 4 (with $K_1 = \{(0,0),(0,1),(0,2),(0,3)\}$ and $K_2 = \{(0,0),(1,1),(0,2),(1,3)\}$, which are isomorphic to $\mathbb{Z}_4$), and the other 2 subgroups H_1, H_2 of order 2 (with $H_1 = \{(0,0),(1,0)\}$ and $H_2 = \{(0,0),(1,2\})$ are not comparable, so that besides the relations $\{(0,0)\} \le H_0 \le K_1, K_2 \le \mathbb{Z}_2 \times \mathbb{Z}_4$ one has $\{(0,0)\} \le H_1, H_2 \le \mathbb{Z}_2 \times \mathbb{Z}_4$.

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has 7 subgroups $H_1, \ldots, H_7$ of order 2, 0 subgroup of order 4, and $\{(0,0)\} \le H_1, \ldots, H_7 \le \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

D_4 has 5 subgroups of order 2 (H_0 generated by R_{180}, and $H_1, \ldots, H_4$ generated by the 4 mirror symmetries), and 1 subgroup K of order 4 (generated by R_{90} or by R_{270}, and isomorphic to $\mathbb{Z}_4$), and one has $\{(0,0)\} \le H_0 \le K \le D_4$ and $\{(0,0)\} \le H_1, \ldots, H_4 \le D_4$.

Q_8 has 1 subgroup H of order 2 (which is $\{+1,-1\}$) and 3 subgroups I, J, K of order 4 (with $I = \{\pm 1, \pm \mathbf{i}\}$, $J = \{\pm 1, \pm \mathbf{j}\}$, and $K = \{\pm 1, \pm \mathbf{k}\}$, isomorphic to $\mathbb{Z}_4$), and one has $\{(0,0)\} \le H \le I, J, K \le Q_8$.

Remark 5.6: We shall see later a general structure property for finite Abelian groups, but for understanding about finite non-Abelian groups, we shall need some general tools, like Cauchy's theorem and its generalizations, the Sylow's theorems,[5] and learn about group actions.

Definition 5.7: If p is prime, and a is not a multiple of p, then a is a *quadratic residue modulo p* if there exists $x \in \mathbb{Z}$ with $x^2 = a \pmod{p}$, and it is a *quadratic non-residue modulo p* if there does not exist such an x. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is only defined for p prime and a not a multiple of p,[6] as $+1$ if a is a quadratic residue modulo p, and as -1 if a is a quadratic non-residue modulo p. One obviously has $\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)$ if $b = a \pmod{p}$, and $\left(\frac{a^2}{p}\right) = +1$ (for a not a multiple of p).

Remark 5.8: It seems natural to have wondered about solving equations of degree 2, but one should remember that thinking in terms of equations modulo n was initiated by GAUSS, so that the initial motivation of mathematicians was certainly different.

The formula $(a^2+b^2)\,(\alpha^2+\beta^2) = (a\,\alpha - b\,\beta)^2 + (a\,\beta + b\,\alpha)^2$ is now known as Brahmagupta's identity,[7] and it is related to complex numbers since it says that $|z_1 z_2|^2 = |z_1|^2 |z_2|^2$ for all $z_1, z_2 \in \mathbb{C}$. GIRARD conjectured that a positive integer is the sum of two squares if and only if its factorization has the primes of the form $4m+3$ at an even power,[8] and FERMAT claimed to have a proof (using his method of descent to show that every prime of the form $4m+1$ is the sum of two squares), but EULER was the first to publish a proof. If an odd prime p can be written as a^2+b^2, it implies (by multiplying by the inverse of a modulo p) that -1 is a quadratic residue modulo p, and the first step was to show that it is not true if p is of the form $4n+3$ (or $4n-1$), and it is true if p is of the form $4n+1$.

Theorem 5.9: (EULER) If p is an odd prime, then for a not a multiple of p one has $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \pmod{p}$, so that -1 is a quadratic residue modulo p if and only if $\frac{p-1}{2}$ is even, i.e. p has the form $4n+1$, and $\left(\frac{a\,b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for all a, b not multiples of p.

[5] Peter Ludwig Mejdell SYLOW, Norwegian mathematician, 1832–1918. After being a high school teacher in Fredrikshald (now Halden), he worked in Kristiania (now Oslo), Norway.

[6] Jsevenrm ACOBI has extended the definition of the Legendre symbol to $\left(\frac{a}{n}\right)$ with a and n non-zero integers; however, although $\left(\frac{a}{n}\right) = -1$ implies that there is no solution of $x^2 = a \pmod{n}$, one cannot conclude if n is not a prime and $\left(\frac{a}{n}\right) = +1$.

[7] BRAHMAGUPTA, Indian mathematician and astronomer, 598–670.

[8] Albert GIRARD, French mathematician, 1595–1632.

Proof: Since $p = 2m+1$, and $a^{2m} = 1 \pmod{p}$ by Fermat's theorem, it means that $a^m = \pm 1 \pmod{p}$, because $\mathbb{Z}_p$ is a field.[9] Every square $a = x^2$ (with $x \neq 0 \pmod{p}$) satisfies $a^m = 1 \pmod{p}$ since $(x^2)^m = x^{p-1} = 1 \pmod{p}$ by Fermat's theorem, and since $-x$ and x have the same square (and $-x \neq x \pmod{p}$ since p is odd) there are exactly m non-zero squares modulo p; because the polynomial equation $x^m = 1 \pmod{p}$ cannot have more than m distinct solutions since $\mathbb{Z}_p$ is a field,[10] one knows all of them and they are the quadratic residues modulo p which are those a satisfying $\left(\frac{a}{p}\right) = +1$, and the quadratic non-residues modulo p are those b satisfying $\left(\frac{b}{p}\right) = -1$. Applying to $a = -1$, one finds that $\left(\frac{-1}{p}\right) = +1$ if and only if $\frac{p-1}{2}$ is even. Then one has $\left(\frac{a\,b}{p}\right) = (a\,b)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}\,b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$, and since the Legendre symbol only take the values ±1 (and $p \neq 2$) one deduces that $\left(\frac{a\,b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$.

Remark 5.10: One then has a surprising result, that if $x^2 = a \pmod{p}$ has no solution x, and $y^2 = b \pmod{p}$ has no solution y, then there exists a solution z of $z^2 = a\,b \pmod{p}$, but the proof has given no algorithm for finding such a solution.

For going further, one needs to compute $\left(\frac{2}{p}\right)$ (by a lemma of GAUSS), and prove the law of quadratic reciprocity, which says that if p and q are distinct odd primes, then $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ if either p or q has the form $4n+1$, and that $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$ if both p and q have the form $4n+3$: it was conjectured by LEGENDRE and EULER could not prove it, but GAUSS published six different proofs (and two more were found in his papers after he died). However, one difficulty with computing Legendre symbols is that one needs to know the factorization into prime factors of the numbers which one uses.

Remark 5.11: Using the *scalar product* (V,W) and the *cross product* $V \times W$ for vectors $V,W \in \mathbb{R}^3$,[11] HAMILTON wanted to define an associative multiplication which is distributive with respect to addition,[12] and he found a way with pairs of a scalar and a vector: it is natural to define addition as $(a,V)+(\alpha,W) = (a+\alpha, V+W)$, and his unusual multiplication is $(a,V)\cdot(\alpha,W) = (a\,\alpha-(V,W), a\,W+\alpha\,V+V\times W)$: distributivity with respect to addition is clear, and associativity follows easily from the formula for the double cross product, $V\times(W\times X) = (V,X)\,W-(V,W)\,X$. Using the notation $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$ for the canonical (orthonormal) basis of $\mathbb{R}^3$, and b,c,d for the components of a vector $V \in \mathbb{R}^3$, one then writes $\mathbb{H} = \{a+b\,\mathbf{i}+c\,\mathbf{j}+d\,\mathbf{k} \mid a,b,c,d \in \mathbb{R}\}$; an element $a+b\,\mathbf{i}+c\,\mathbf{j}+d\,\mathbf{k}$ is called a *quaternion*. One checks easily that $\mathbf{i}\cdot\mathbf{i} = \mathbf{j}\cdot\mathbf{j} = \mathbf{k}\cdot\mathbf{k} = -1$ and $\mathbf{i}\cdot\mathbf{j} = \mathbf{k} = -\mathbf{j}\cdot\mathbf{i}$, $\mathbf{j}\cdot\mathbf{k} = \mathbf{i} = -\mathbf{k}\cdot\mathbf{j}$, $\mathbf{k}\cdot\mathbf{i} = \mathbf{j} = -\mathbf{i}\cdot\mathbf{k}$. One writes $N\big((a,V)\big) = a^2+|V|^2$, or $N(a+b\,\mathbf{i}+c\,\mathbf{j}+d\,\mathbf{k}) = a^2+b^2+c^2+d^2$, called the *norm* of the quaternion,[13] and has $N\big((a,V)\cdot(\alpha,W)\big) = N\big((a,V)\big)\,N\big((\alpha,W)\big)$, i.e. $(a^2+b^2+c^2+d^2)\,(\alpha^2+\beta^2+\gamma^2+\delta^2) = (a\,\alpha-b\,\beta-c\,\gamma-d\,\delta)^2+(a\,\beta+b\,\alpha+c\,\delta-d\,\gamma)^2+(a\,\gamma-b\,\delta+c\,\alpha+d\,\beta)^2+(a\,\delta+b\,\gamma-c\,\beta+d\,\alpha)^2$, attributed to EULER, and it may have been known to BACHET, who conjectured that every positive integer is the sum of four squares; FERMAT claimed to have a proof, but LAGRANGE was the first to publish a proof. If $N\big((a,V)\big) \neq 0$, the multiplicative inverse of (a,V) is $\lambda\,(a,-V)$, with $\lambda\,N\big((a,V)\big) = 1$, so that $\mathbb{H}$ is a division ring.

The quaternion group Q_8 is then a subgroup of the multiplicative group $\mathbb{H}^* = \mathbb{H}\setminus\{(0,0)\}$, obtained by imposing $a \in \mathbb{Z}$ and $V \in \mathbb{Z}^3$, which gives a set stable by multiplication, and imposing $N\big((a,V)\big) = 1$, for the inverse to have also its components in $\mathbb{Z}$: then only one component a,b,c,d is non-zero, and equal to ±1.

Additional footnotes: JACOBI.[14]

[9] Since $z = a^m$ satisfies $z^2 = 1$, and $z^2-1 = (z-1)\,(z+1)$ can only be 0 if $z-1$ or $z+1$ is 0.

[10] For any commutative ring R, one notes $R[x]$ the polynomials with coefficients in R, and if $P(x)$ is such a polynomial of degree $n \geq 1$, and $a \in R$, one can perform the Euclidean division of $P(x)$ by $x-a$, which gives $P(x) = (x-a)\,Q(x)+P(a)$ with Q of degree $n-1$; one deduces that $P(a) = 0$ if and only if P is divisible par $x-a$. If R is an integral domain and $P(b) = 0$ for $b \neq a$, then $Q(b) = 0$, and one divides Q by $x-b$, and by induction on n there cannot exist more than n distinct roots of P.

[11] For $i = 1,2,3$, the component $(V\times W)_i$ is $\sum_{j,k}\varepsilon_{i,j,k}V_jW_k$, where ε is the *completely antisymmetric tensor*, such that $\varepsilon_{i,j,k} = 0$ if two indices coincide, and if they are distinct it is the signature of the permutation $(1,2,3) \mapsto (i,j,k)$, i.e. $\varepsilon_{1,2,3} = \varepsilon_{2,3,1} = \varepsilon_{3,1,2} = +1$, and $\varepsilon_{1,3,2} = \varepsilon_{2,1,3} = \varepsilon_{3,2,1} = -1$.

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

[13] In analysis, the norm would be the square root of $a^2+b^2+c^2+d^2$.

[14] Carl Gustav Jacob JACOBI, German mathematician, 1804–1851. He worked in Königsberg (then in Germany, now Kaliningrad, Russia) and Berlin, Germany.