REND. SEM. MAT. UNIV. PADOVA, Vol. 118 (2007)

Modular Permutations on $\mathbb{Z}$.

FRANCESCO DEL CASTILLO (*)

ABSTRACT - In this paper the group $\mathcal{M}$ of permutations σ of $\mathbb{Z}$ for which an integer $n = n(\sigma) > 0$ exists such that $(z + n)\sigma = z\sigma + n$ for every $z \in \mathbb{Z}$ is studied. $\mathcal{M}$ is countably infinite locally (abelian-by-finite) and contains all finitely generated (abelian-by-finite) groups as subgroups. The commutator subgroup $\mathcal{M}'$ is an infinite simple group and the quotient group $\mathcal{M}/\mathcal{M}'$ is isomorphic to $\mathbb{Z}$. Finally, all abelian groups that can be represented as modular permutation groups are determined: these are countable abelian groups whose quotient over the torsion subgroup is free.

1. Definitions and first results.

Let σ be a permutation of the set $\mathbb{Z}$ of the integers: we say that $n \in \mathbb{N} \setminus 0$ is a *module* for σ if

$$(z + n)\sigma = z\sigma + n,$$

for every $z \in \mathbb{Z}$ or, equivalently, if σ commutes with the translation τ_n and in this case we say that σ is *modular*. If it exists, such a n is not unique, since any multiple of it is still a module. The set of all modular permutations is a group, denoted by $\mathcal{M}$. For $\sigma \in \mathcal{M}$, we denote by $\mathrm{mod}\,(\sigma)$ the smallest module for σ. Then n is a module for σ if and only if $\mathrm{mod}\,(\sigma)$ divides n. M_n is the subgroup of $\mathcal{M}$ whose elements are the permutations for which n is a module. A modular permutation $\sigma \in \mathrm{M}_n$ preserves the n-congruence relation, i.e. $z_1 \equiv z_2 (\mathrm{mod}\, n)$ if and only if $z_1\sigma \equiv z_2\sigma (\mathrm{mod}\, n)$. Thus, a modular permutation $\sigma \in \mathrm{M}_n$ induces a permutation $\overline{\sigma_n}$ of the n cosets of $\mathbb{Z}/n\mathbb{Z}$. This fact allow us to write, for every $z \in \mathbb{Z}$,

$$z\sigma = (q_{z,n} + a_{[z]_n})n + ([z]_n)\overline{\sigma_n} \tag{1.1}$$

(*) Indirizzo dell'A.: Dipartimento di Matematica "Ulisse Dini", Università degli Studi di Firenze, Viale Morgagni, 67a, 50134 Firenze.

E-mail: delcastillo@math.unifi.it

where $q_{z,n}$, $[z]_n$ are resp. the quotient and the remainder of the (euclidean) division of z by n and $a_{[z]_n}$ is an integer depending only on $[z]_n$. With a slight abuse we adopt the same notation for both the remainder and the classes of n-congruence and will let $\overline{\sigma}_n$ act on both these objects; for this reason we will choose the set $\{0,\dots,n-1\}$ as support for the symmetric group S_n in place of the more usual $\{1,\dots,n\}$. Conversely we can associate to each $\rho \in \mathrm{S}_n$ a permutation $\widetilde{\rho} \in \mathrm{M}_n$ just by setting $a_{[z]_n} \equiv 0$ in the 1.1: $z\widetilde{\rho} = q_{z,n}n + ([z]_n)\rho$. Thus, for every $n \geq 1$, two homomorphism are defined

$$\begin{array}{cc} l_n : \mathrm{S}_n \to \mathrm{M}_n & f_n : \mathrm{M}_n \to \mathrm{S}_n \\ \rho \mapsto \widetilde{\rho} & \sigma \mapsto \overline{\sigma_n} \end{array}$$

such that $l_n f_n = 1$. f_n is therefore surjective and l_n determines an isomorphic copy $\widetilde{\mathrm{S}_n}$ of S_n in $\mathcal{M}$. Let Δ_n be the kernel of f_n: a permutation $\lambda \in \Delta_n$ can be written, according to 1.1, as

$$z\lambda = z + a_{[z]n}n.$$

The features of λ (which fixes each n-congruence class and acts "inside" each of them as a translation by $a_{[z]_n}$) suggest us to introduce a special class of modular permutations: for $n \geq 1$ and $I \subseteq \{0,\dots,n-1\}$ the permutation $\lambda_{n,I}$ defined, for $z \in \mathbb{Z}$, by

$$z\lambda_{n,I} = \begin{cases} z+n & \text{if } z \equiv i \pmod{n} \text{ for some } i \in I \\ z & \text{otherwise} \end{cases}$$

is called *modular translation*. In case $I = \{i\}$ we just write $\lambda_{n,i}$ and $\lambda_{n,i}$ is called an *elementary modular translation* (shortened *EMT*). It is clear that $\lambda_{n,I} = \prod_{i \in I} \lambda_{n,i}$ and $\mathrm{mod}\,(\lambda_{n,i}) = n$. It is pure routine to check that $\Delta_n = \langle \lambda_{n,i} \mid i = 0,\dots,n-1 \rangle$ and that Δ_n is a free abelian group of rank n for which the $\lambda_{n,i}$ form a basis.

Furthermore, M_n splits as the semidirect product $\Delta_n \times \widetilde{\mathrm{S}_n}$: if $x \in \mathrm{M}_n$, once taken $\sigma = x f_n l_n \in \widetilde{\mathrm{S}_n}$ one has immediately $x\sigma^{-1} \in \Delta_n$ and then $x = \lambda\sigma$, with $\lambda \in \Delta_n, \sigma \in \widetilde{\mathrm{S}_n}$ uniquely determined. To this particular factorization we will refer (unless otherwise stated) in the following when we say "$x = \lambda\sigma \in \mathrm{M}_n$". We also observe that this factorization means that $\mathcal{M}$ is locally (abelian-by-finite).

$\widetilde{\mathrm{S}_n}$ in its action by conjugation on Δ_n permutes the elements of the basis according to the natural action of S_n, namely one has $(\lambda_{n,i})^{\widetilde{\sigma}} = \lambda_{n,i\sigma}$; thus M_n is isomorphic to the permutational wreath product $\mathbb{Z}\ \overline{wr}_n\ \mathrm{S}_n$. This allows us to state the first of two theorems about groups that can be embedded in $\mathcal{M}$, which is somehow a converse of the local (abelian-by-finite) structure of $\mathcal{M}$.

THEOREM 1.1. *Let G be a finitely generated (abelian-by-finite) group. Then G can be embedded in $\mathcal{M}$.*

PROOF. Let $A \rightarrowtail G \twoheadrightarrow H$ be exact, with A abelian and H finite. A is the direct product $T \times F$ of its torsion subgroup T and a free abelian group of rank, say, k. Put $N = F_G$ the core of F in G; N is still free abelian of rank k. The index $|G : N|$ is finite and then $U = G/N$ is a finite group of order, say, n. According to the Kaluznin-Krasner theorem ([2], theorem 6.2.8.), G is isomorphic to a subgroup of $N \overline{wr}\ U \simeq \mathbb{Z}^k \overline{wr}\ U$. We now show how the latter can be embedded in $\mathcal{M}$. First we can embed the standard wreath product in the permutational wreath product (via the Cayley regular representation for finite groups) $\mathbb{Z}^k \overline{wr}_U \mathrm{S}_n$; now, $\mathbb{Z}^k \overline{wr}_U \mathrm{S}_n = (\mathbb{Z}^k)^n \rtimes \mathrm{S}_n \lesssim \mathbb{Z}^{kn} \rtimes \mathrm{S}_{kn}$, where, in the last embedding, S_n is identified with the subgroup of S_{kn} acting on the n blocks $\{ik, \ldots, ik + (k-1)\}$ of length k. The theorem is proved, since $\mathbb{Z}^{kn} \rtimes \mathrm{S}_{kn} \simeq \mathbb{Z} \overline{wr}_{kn} \mathrm{S}_{kn} \simeq \mathrm{M}_{kn}$. □

2. The commutator subgroup of $\mathcal{M}$.

In this section we show that $\mathcal{M}'$ is an infinite simple group (Theorem 2.8) and that the quotient group $\mathcal{M}/\mathcal{M}'$ is isomorphic to $\mathbb{Z}$ (theorem 2.5). For this purpose it is useful to have another way of writing the elements of $\mathcal{M}$ in terms of certain basic elements. Let Γ_n be the subgroup of M_n generated by the modular translations whose modules divide n,

$$\Gamma_n = \langle \lambda_{m,i} \mid m \text{ divides } n,\ i = 0, \ldots, m-1 \rangle$$

and let G_n be the image of Γ_n through the homomorphism f_n. Since the image of $\lambda_{m,i}$ is easily checked to be the cycle $(\,0 \quad m \quad \ldots \quad n-m\,)$ of length n/m in S_n, we have $G_n = \langle (\,0 \quad m \quad \ldots \quad n-m\,) \mid m \text{ divides } n \rangle$.

THEOREM 2.1. *For every $n \geq 2$, if $G_n = (\Gamma_n)f_n$, the following equality holds:*

$$G_n = \begin{cases} \mathrm{S}_n & \text{if } n \text{ is even and not a prime power} \\ \mathrm{A}_n & \text{if } n \text{ is odd and not a prime power} \\ \text{a } p\text{-Sylow subgroup of } \mathrm{S}_n & \text{if } n \text{ is a prime power} \end{cases}$$

In order to prove the theorem we recall a result due to Jordan ([4], Theorem 13.9):

THEOREM (Jordan, 1873). *Let p be a prime and G a primitive group of degree $n = p + k$ with $k \geq 3$. If G contains an element of degree and order p, then G is either alternating or symmetric.*

PROOF OF THEOREM 2.1. The first two cases (n not a prime power) can be proved via Jordan's theorem. Let $n = pqk$ with $p < q$ different primes and $k \in \mathbb{N}$. Since the cycle $(\,0 \quad qk \ldots \quad n - qk\,) \in G_n$ is an element of order and degree p, one just has to check that G_n is primitive. Let $\{0\} \neq \Delta$ be a block containing 0 and $\kappa = \lambda_{1,0} f_n = (\,0 \quad 1 \quad \ldots \quad n-1\,)$. Let u be the smallest non-zero element of Δ; since $0\kappa^u = u$, Δ contains the whole orbit of 0 under the action of κ^u and, since it is the smallest nonzero element, u must be a divisor of n and we must have $\Delta = \{0, u, \ldots, n-u\}$. If $u \neq 1$, consider a divisor v of n such that v is neither a multiple nor a divisor of u. If $\rho = \lambda_{v,0} f_n$, one has the contradiction $0\rho = v \notin \Delta$, $u\rho = u \in \Delta$: then we must have $u = 1$ and $\Delta = \{0, 1, \ldots, n-1\}$, i.e. G_n is primitive. Now, if n is odd the image of any $\lambda_{m,i}$ is a cycle of odd length and therefore it lies in A_n; otherwise, if n is even, G_n contains some odd permutation and must be the whole of S_n.

Proving the case of n a prime power is a matter of counting elements. We recall that the order of a p-Sylow subgroup of S_{p^k} is p^r, where $r = 1 + p + \cdots + p^{k-1}$. We then proceed by induction on $k \in \mathbb{N}$. Let $P_k = G_{p^k}$. The case $k = 1$ is trivial. Suppose now that P_k is a p-Sylow subgroup of S_{p^k} and consider $P_{k+1} \leq \mathrm{S}_{p^{k+1}}$. Denote again by P_k the image of P_k via the usual embedding of S_{p^k} in the pointwise stabilizer of the set $\{p^k, p^k + 1, \ldots, p^{k+1} - 1\}$ in $\mathrm{S}_{p^{k+1}}$, let $\kappa = \lambda_{1,0} f_{p^{k+1}}$ and $\gamma \in \mathrm{S}_{p^{k+1}}$ be a permutation such that, for $0 \leq z \leq p^k - 1$, $z\gamma = pz$. Let $P_k^0 = (P_k)^\gamma$; then

$$P_k^0 = \langle ((\lambda_{p^j,0}) f_{p^k})^\gamma \mid 0 \leq j < k \rangle = \langle (\lambda_{p^j,0}) f_{p^{k+1}} \mid 0 < j < k+1 \rangle$$

and P_k^0 has support $\{0, p, 2p, \ldots, p^{k+1} - p\}$. For $0 < i \leq p-1$, let $P_k^i = (P_k^0)^{\kappa^i}$. The P_k^i's are subgroups of P_{k+1} and have pairwise disjoint supports. Thus they generate their direct product $P = \langle (\lambda_{p^j,i}) f_{p^{k+1}} \mid 0 < j < k+1,\ 0 \leq i \leq p-1 \rangle$, whose order is $|P_k^0|^p = p^{(p+\cdots+p^k)}$. Furthermore, $\kappa \notin P$ and $(P_k^i)^{\kappa^p} = P_k^i$.

Let now $\alpha = (\lambda_{p,0}) f_{p^{k+1}}$ and $\beta = \alpha\kappa$. We have $1 \neq \beta \in P_{k+1} \setminus P$, $\beta^p = 1$ and β normalizes P. Thus, $\langle P, \beta \rangle = P \rtimes \langle \beta \rangle$ and $\langle P, \beta \rangle$ has order $p^{(1+p+\cdots+p^k)}$, i.e. it is a p-Sylow subgroup of $\mathrm{S}_{p^{k+1}}$. Finally, since β acts on P essentially in the same way as κ, we get $P \rtimes \langle \beta \rangle = \langle P_k^0, \kappa \rangle = \langle (\lambda_{p^j,0}) f_{p^{k+1}} \mid 0 \leq j < k+1 \rangle = P_{k+1}$. □

COROLLARY 2.2. *If n is even and not a prime power, then $\Gamma_n = \mathrm{M}_n$.*

PROOF. Let $x \in \mathrm{M}_n$. Since the restriction of f_n to Γ_n is surjective one can take $\gamma \in \Gamma_n$ such that $\gamma f_n = x f_n$, and then $x = \gamma\delta$ for some $\delta \in \Delta_n \leq \Gamma_n$ and therefore $x \in \Gamma_n$. □

COROLLARY 2.3. *$\mathcal{M}$ is generated by the modular translations.*

Thus, if $x \in \mathcal{M}$, besides the factorization $x = \lambda\sigma$ in some M_n, we also have $x = \prod \lambda_i^{a_i}$ with the λ_i's elementary modular translations and the a_i's integers. The latter expression is not unique but will be useful in this section as well as in the next one.

Consider the application $\Psi_n : \mathcal{M} \to \mathbb{Z}$ defined, for $x \in \mathcal{M}$, by $x\Psi_n = \sum_{i=0}^{n-1} (zx - z)$. Ψ_n is the sum of the shiftings of the first n integers under the action of x; the restriction ψ_n of Ψ_n to M_n is a homomorphism, as a direct check shows: let $x, y \in \mathrm{M}_n$, then

$$(xy)\psi_n = \sum_{z=0}^{n-1} ((zx)y - z) = \sum_{z=0}^{n-1} ((zx)y - zx) + \sum_{z=0}^{n-1} (zx - z) =$$

$$= \sum_{z=0}^{n-1} [(a_{[z]_n} n + z\overline{x})y - (a_{[z]} n + z\overline{x})] + x\psi_n = \sum_{z=0}^{n-1} (zy - z) + x\psi_n = y\psi_n + x\psi_n.$$

Furthermore, $\widetilde{\mathrm{S}_n} \leq \ker(\psi_n)$ and $\lambda_{n,i}\psi_n = n$. Thus n divides $x\psi_n$ for every $x \in \mathrm{M}_n$.

PROPOSITION 2.4. *The application Ψ defined, for $x \in \mathcal{M}$, by $x\Psi = \lim_{i\to\infty} \frac{x\Psi_i}{i}$ is well defined and, if $x \in \mathrm{M}_n$, $x\Psi = \frac{x\psi_n}{n}$. In particular Ψ is a surjective homomorphism of $\mathcal{M}$ onto $\mathbb{Z}$.*

PROOF. Let x be an element of M_n and write $i = qn + [i]$ (division of i by n). We have

$$\begin{aligned} x\Psi &= \lim_{i\to\infty} \frac{1}{i} \left(\sum_{z=0}^{qn-1} (zx - z) + \sum_{z=qn}^{i-1} (zx - z) \right) = \\ &= \lim_{i\to\infty} \frac{1}{i} \left(q(x\psi_n) + \sum_{z=0}^{[i]-1} (zx - z) \right) = \\ &= \lim_{i\to\infty} \frac{q(z\psi_n)}{qn + [i]} + \lim_{i\to\infty} \frac{\sum_{z=0}^{[i]-1} (zx - z)}{i}. \end{aligned} \tag{2.1}$$

If $z\psi_n = kn$ the first limit of the last member of the (2.1) is k, while the second one equals 0, since $\left| \sum_{z=0}^{[i]-1} (zx - z) \right| \leq \sum_{z=0}^{n-1} |zx - z|$ (an i-independent constant). □

What can be observed in the last proposition is that, if $x = \prod_{i=1}^{n} \lambda_i^{a_i}$ is a factorization of x in terms of EMT's, since $\lambda_i \Psi = 1$, then $x\Psi = \sum_{i=1}^{n} a_i$. Thus, although the EMT's that occur in the factorization of x are not uniquely determined, the sum of the a_i's is indeed unique. In a certain sense the EMT's play a role in $\mathcal{M}$ similar to that of transpositions in finite symmetric groups and one can also regard the value of Ψ at x as a sort of "signature". However the usefulness of EMT's is clear in the following results.

THEOREM 2.5. *$\mathcal{M}' = \ker \Psi$ and then $\mathcal{M}/\mathcal{M}' \simeq \mathbb{Z}$.*

PROOF. The inclusion $\mathcal{M}' \leq \ker \Psi$ is obvious since Ψ has an abelian image. In order to prove the opposite inclusion, we note that, if $x = \sum_{i=1}^{k} \lambda_i^{a_i} \in \ker \Psi$ with the λ_i EMT's, since $\sum a_i = 0$, we can suppose, up to multiplication by an element of $\mathcal{M}'$, $a_i = (-1)^i$ and k even (say $k = 2r$). Thus it suffices to show that, for every $n, m \in \mathbb{N}$ and every possible i, j, $\lambda_{n,i}^{-1} \lambda_{m,j} \in \mathcal{M}'$.

Suppose then that $x = \lambda_{n,i}^{-1} \lambda_{m,j}$. If $n = m = 1$ there is nothing to prove. If $n = m \geq 2$, let $\sigma \in \mathrm{S}_n$ be such that $i\sigma = j$. Then one has $\lambda_{n,i}^{-1} \lambda_{n,j} = \lambda_{n,i}^{-1} (\lambda_{n,i})^{\tilde{\sigma}} = [\lambda_{n,i}, \widetilde{\sigma}] \in [\Delta_n, \widetilde{\mathrm{S}_n}] \leq \mathrm{M}_n'$. We also note that $[\Delta_n, \widetilde{\mathrm{S}_n}] = \ker \Psi \cap \Delta_n$ (since for $\delta \in \Delta_n, \widetilde{\sigma} \in \widetilde{\mathrm{S}_n}$, clearly $(\delta^{-1} \widetilde{\sigma}^{-1} \delta \widetilde{\sigma}) \Psi = 0$).

Finally, if $n \neq m$, let $s = 2 \cdot \text{l.c.m.}(n, m)$ and consider $\lambda_{n,i}$ and $\lambda_{m,j}$ as elements of M_s: both $\lambda_{n,i} f_s$ and $\lambda_{m,j} f_s$ are odd permutation of S_s, and then $\lambda_{n,i}^{-1} \lambda_{m,j} \in \widetilde{\mathrm{A}_s} \Delta_s \leq \mathrm{M}_s' \Delta_s$. Thus $\lambda_{n,i}^{-1} \lambda_{m,j} \in (\mathrm{M}_s' \Delta_s) \cap \ker \Psi = \mathrm{M}_s' (\Delta_s \cap \ker \Psi) = \mathrm{M}_s' [\Delta_s, \widetilde{\mathrm{S}_s}] \leq \mathrm{M}_s'$. □

In order to obtain information about the commutator subgroup $\mathcal{M}'$ we need to better understand the structure of the groups M_n. From now on we assume $n \geq 5$ and set $\mathrm{K}_n = \ker \Psi \cap \mathrm{M}_n$. Just by simple observations, as applying the isomorphism and the correspondence theorems, it is easy to verify the following facts:

- $\Delta_n \cap \mathrm{K}_n = [\Delta_n, \widetilde{\mathrm{S}_n}] = [\Delta_n, \mathrm{M}_n]$ is a free abelian group of rank $n - 1$ with basis $\{\lambda_{n,0}^{-1} \lambda_{n,i} \mid i = 1, \ldots, n - 1\}$;
- $\mathrm{K}_n = [\Delta_n, \mathrm{M}_n] \rtimes \widetilde{\mathrm{S}_n}$;
- if $\Theta_n = \Delta_n \rtimes \widetilde{\mathrm{A}_n}$, $\mathrm{M}_n' \leq \Theta_n$;
- $\mathrm{M}_n' = [\Delta_n, \mathrm{M}_n] \rtimes \widetilde{\mathrm{A}_n} \lneq \mathrm{K}_n$.

LEMMA 2.6. *For $n \geq 5$, $\mathrm{M}_n'' = \mathrm{M}_n'$.*

PROOF. $[\Delta_n, \mathrm{M}_n] \leq \mathrm{M}_n''$: it suffices to show that every generator $\lambda_{n,0}^{-1}\lambda_{n,i}$ of $[\Delta_n, \mathrm{M}_n]$ belongs to M_n''. If $0 \neq j \neq i$ one can take $\sigma \in \mathrm{A}_n$ such that $j\sigma = j$ and $0\sigma = i$. With this choices one has at once $\lambda_{n,0}^{-1}\lambda_{n,i} = [\lambda_{n,0}\lambda_{n,j}^{-1}, \widetilde{\sigma}] \in [[\Delta_m, \mathrm{M}_n], [\widetilde{\mathrm{S}_n}, \widetilde{\mathrm{S}_n}]] \leq \mathrm{M}_n''$. Even more trivially $\widetilde{\mathrm{A}_n} = [\widetilde{\mathrm{A}_n}, \widetilde{\mathrm{A}_n}] \leq \mathrm{M}_n''$ and putting things together gives $\mathrm{M}_n' = [\Delta_n, \mathrm{M}_n] \rtimes \widetilde{\mathrm{A}_n} \leq \mathrm{M}_n''$. □

LEMMA 2.7. *For $n \geq 5$, let H be a normal proper subgroup of M_n'. Then $H \leq [\Delta_n, \mathrm{M}_n]$. In particular H is abelian.*

PROOF. Suppose $H \trianglelefteq \mathrm{M}_n'$ and $H \not\leq [\Delta_n, \mathrm{M}_n]$. Since $\mathrm{M}_n'/[\Delta_n, \mathrm{M}_n]$ is simple, we have $H[\Delta_n, \mathrm{M}_n] = \mathrm{M}_n'$ and consequently

$$\frac{\mathrm{M}_n'}{H} = \frac{H[\Delta_n, \mathrm{M}_n]}{H} \simeq \frac{[\Delta_n, \mathrm{M}_n]}{H \cap [\Delta_n, \mathrm{M}_n]}.$$

Thus in particular M_n'/H is abelian and $H \geq \mathrm{M}_n'' = \mathrm{M}_n'$. Thus, $H = \mathrm{M}_n'$. □

The above results are enough to prove that $\mathcal{M}'$ is simple.

THEOREM 2.8. *$\mathcal{M}'$ is a simple group.*

PROOF. Let $1 \neq N$ be a normal subgroup of $\mathcal{M}'$ and set, for every $n \geq 5$, $N_n = N \cap \mathrm{M}_n'$. N_n is normal in M_n' and then must coincide with M_n' or be abelian and contained in $[\Delta_n, \mathrm{M}_n]$. We now show that the latter cannot always be the case. Suppose that, for every $n \geq 5$, $N_n \leq [\Delta_n, \mathrm{M}_n]$. Let $m \geq 5$ be a fixed integer and take $x = \prod_{i=0}^{m-1} \lambda_{m,i}^{a_i} \in N_m$. If $k > 0$, x is also contained in N_{km} and then one also has $x = \prod_{i=0}^{km-1} \lambda_{km,i}^{b_i}$. This means that, given $z \in \mathbb{Z}$, x "fixes" z or "moves" it by a multiple of km, no matter how a large $k > 0$ one chooses. This necessarily implies that $x = 1$ and then $N = 1$, which contradicts the initial assumption $N \neq 1$. Then for some $m \geq 5$ $N_m = \mathrm{M}_m'$ and, for every $k > 0$, one has $N_{km} = \mathrm{M}_{km}'$, as $N_m \leq N_{km}$ implies that N_{km} is not abelian. This conclude the proof since $N = \bigcup_{k \geq 0} N_{km} = \bigcup_{k \geq 0} \mathrm{M}_{km}' = \mathcal{M}'$.

3. Abelian subgroups of $\mathcal{M}$.

Theorem 1.1 describes a large class of groups that can be embedded in $\mathcal{M}$. In this section we focus our attention to abelian groups and will com-

pletely determine those abelian groups that can be represented as subgroups of $\mathcal{M}$.

We denote by F_n the free abelian group of rank n ($\leq \aleph_0$). Given a sequence (possibly infinite) $\mathcal{P}$ of prime numbers, $C_{\mathcal{P}}$ is the group $\underset{p\in\mathcal{P}}{\mathrm{Dir}} C_p$ and $C_{\mathcal{P}}^{\infty}$ is the group $\underset{p\in\mathcal{P}}{\mathrm{Dir}} C_{p^\infty}$.

For $g \in \mathcal{M}$ we consider the equation $x^k = g$ and, if a solution exists, we call it a *k-root* of g. It is clear that mod (g) divides mod (x). Suppose now that x is a k-root of g and $g = \lambda\sigma, x = \delta\tau \in \mathrm{M}_n$; one has $g = x^k = \delta'\tau^k$ for some $\delta' \in \Delta_n$ and in particular $\tau^k = \sigma$, i.e. τ is a k-root of σ: in a certain sense this allows us to subordinate the existence of roots in $\mathcal{M}$ to the existence of roots in finite symmetric groups, for which the following result holds ([3]):

PROPOSITION 3.1. *$\sigma \in \mathrm{S_n}$ has a k-root if and only if for every positive integer l, the number of l-cycles in the canonical decomposition of σ is a multiple of $\{k\}_l$.*

In the statement of the above proposition $\{k\}_l$ denotes the part of k which shares prime divisors with l, i.e. if Π is the set of prime divisors of l, $\{k\}_l$ is the Π-part of k.

If an element $g = \lambda\sigma \in \mathrm{M}_n$ admits a k-root x, it is not necessary that x lies in M_n: anyway, both g and x will be in some M_m, with m a multiple of n. For this reason it is useful to know how to factorize g in the group M_m for multiples m of n.

LEMMA 3.2. *Let $n \in \mathbb{N}$, $i \in \{0, 1 \ldots, n-1\}$ and $k \geq 0$. Then the following equalities hold:*

$$\lambda_{n,i} = \lambda_{kn,i+(k-1)n}(i \quad i+n \quad \ldots \quad i+(k-1)n),$$

$$\lambda_{n,i}^{-1} = \lambda_{kn,i}^{-1}(i \quad i+n \quad \ldots \quad i+(k-1)n)^{-1}.$$

Thus, if a is a positive integer,

$$\lambda_{n,i}^{a} = \lambda_{kn,i+(k-1)n}\lambda_{kn,i+(k-2)n}\cdots\lambda_{kn,i+(k-a)n}(i \quad i+n \quad \ldots \quad i+(k-1)n^a$$

$$\lambda_{n,i}^{-a} = \lambda_{kn,i+n}^{-1}\lambda_{kn,i+2n}^{-1}\cdots\lambda_{kn,i+an}^{-1}(i \quad i+n \quad \ldots \quad i+(k-1)n^{-a}.$$

For $g = \lambda\sigma \in \mathrm{M}_n$ with $\lambda = \prod_{i=0}^{n-1} \lambda_{n,i}^{a_i}$ we put $\varepsilon(g) = \sum_{i=0}^{n-1} |a_i|$. We have the following technical result:

LEMMA 3.3. *Let $g = \lambda\sigma \in \mathrm{M}_n$, $m \in \mathbb{N}$. Then $\varepsilon(g^m) \leq m\varepsilon(g)$.*

PROOF. If $\lambda = \prod_{i=0}^{n-1} \lambda_{n,i}^{a_i}$, one has $g^m = \lambda\lambda^{\sigma^{-1}}\lambda^{\sigma^{-m+1}}\sigma^m$ and $\lambda^{\sigma^{-j}} = \prod_{i=0}^{n-1} \lambda_{n,i}^{a_{i\sigma^j}}$. Thus,

$$\varepsilon(g^m) = \sum_{i=0}^{n-1} \left| \sum_{j=0}^{m-1} a_{i\sigma^j} \right| \leq \sum_{i,j} |a_{i\sigma^j}| = m \sum_{i=0}^{n-1} |a_i| = m\varepsilon(g). \qquad \square$$

PROPOSITION 3.4. *Let $g = \lambda\sigma \in \mathrm{M}_n$ be an element of infinite order. Then, for every $k > \varepsilon(g)$, the equation $x^k = g$ admits no solution in $\mathcal{M}$.*

PROOF. As usual set $\lambda = \prod_{i=0}^{n-1} \lambda_{n,i}^{a_i}$. We consider first the case $g \in \Delta_n$, i.e. $\sigma = 1$, and proceed by way of contradiction. Put $a = \sum_i |a_i| = \varepsilon(g)$ and suppose that, for some $k > a$, an element $x \in \mathcal{M}$ exists such that $x^k = \lambda$. We can regard x as an element of some M_{tn} with t large enough so that $t > |a_i|$ for every i and, if $a_i \neq 0$, ka_i divides t. For such a choice of t we have $g = \delta\tau \in \mathrm{M}_{tn}$, with $\tau = \left(\prod_{i=0}^{n-1} \tau_i^{a_i} \right)$ and the τ_i's are disjoint "t-cycles" in $\widetilde{\mathrm{S}_{tn}}$. Furthermore, when $a_i \neq 0$, $\tau_i^{a_i}$ is the product of $|a_i|$ nontrivial cycles of length $t/|a_i|$ (and in particular $\tau \neq 1$). Let $\zeta_i (= \zeta_{t,i})$ be the number of cycles of length $t/|a_i|$ in the decomposition of τ: we have $\zeta_i \leq \sum_{i=0}^{n-1} |a_i| = a$ for every i, and this inequality holds for every choice of t with the desired properties.

Now, if $x = \eta\upsilon \in \mathrm{M}_{tn}$, we have $\upsilon^k = \tau$, i.e. τ admits a k-root in $\widetilde{\mathrm{S}_{tn}}$ and, according to Proposition 3.1, for $a_i \neq 0$, $k = \{k\}_{t/|a_i|}$ divides $\zeta_i \leq a$, which contradicts the initial assumption $k > a$.

To conclude the proof, suppose $\sigma \neq 1$ and let m be the order of σ. Thus $g^m \in \Delta_n$. If x is a k-root of g one also has $x^{km} = g^m$ and then $km \leq \varepsilon(g^m) \leq m\varepsilon(g)$ and thus, $k \leq \varepsilon(g)$. $\square$

As a consequence of the previous proposition we can easily describe the structure of a torsion-free abelian subgroup of $\mathcal{M}$.

THEOREM 3.5. *Let G be a torsion-free abelian subgroup of $\mathcal{M}$. Then G is free.*

PROOF. By Proposition 3.4 every $g \in G$ admits k-roots only for a finite number of indexes k. Since G is torsion-free the equation $x^k = g$ admits at most one solution in G. Then every element of G admits only a finite number of roots and this is enough to conclude that G is free. $\square$

Examples of free abelian subgroups of $\mathcal{M}$ we have found so far are the Δ_n's, of finite rank n. A natural question is to ask whether $\mathcal{M}$ has a free abelian subgroup of infinite rank and such a question can be answered positively. Such a subgroup can be defined as the union of an ascending chain of free abelian subgroups of $\mathcal{M}$: let $m \geq 2$ be a fixed integer, set $x_0 = 0$ and $G_0 = \langle \lambda_{m,0} \rangle$; for $i \geq 1$ let x_i be such that

$$\begin{cases} 0 \leq x_i \leq 2^i m - 1 \\ x_i \not\equiv x_j \pmod{2^j m}, \text{ for every } j < i \end{cases}.$$

If we define $G_i = \langle \lambda_{2^j m, x_j} \mid j = 0, \dots, i \rangle$, the group $G = \bigcup_{i \in \mathbb{N}} G_i$ is free abelian of infinite countable rank, i.e. $G \simeq \mathrm{F}_{\aleph_0}$. Further, if one "removes" the generator $\lambda_{m,0}$ from the generating set of G, a group H is generated which is still isomorphic to $\mathrm{F}_{\aleph_0}$ and whose support is disjoint from the set $m\mathbb{Z}$.

We turn our attention to torsion subgroups of $\mathcal{M}$. We have already seen that $\mathcal{M}$ contains every finite group as a subgroup (Theorem 1.1) and a natural embedding one can think of is the regular representation in some $\widetilde{\mathrm{S}_n}$. If we adopt an argument similar to that we have used above for the free abelian group G of infinite rank, we can easily embed in $\mathcal{M}$ direct products of countably many finite cyclic groups. Let $\mathcal{P} = (p_1, p_2, \dots)$ be a sequence of prime numbers; for every prime p_i we can find a modular permutation of order p_i in such a way that these permutations have pairwise disjoint supports Σ_i. Let $n > p_1$ and consider $\widetilde{\tau_1} \in \widetilde{\mathrm{S}_n}$ where $\tau_1 = (\, 0 \quad 1 \quad \dots \quad p-1 \,) \in \mathrm{S}_n$. For $i \geq 2$ consider:

- $a_1, \dots, a_{p_i}$ the smallest positive integers not contained in $\bigcup_{j=1}^{i-1} \Sigma_i$;
- k_i the smallest positive integer such that $2^{k_i} n > a_{p_i}$;
- $\tau_i = (\, a_1 \quad a_2 \quad \dots \quad a_{p_i} \,) \in \mathrm{S}_{2^{k_i} n}$.

Then $\widetilde{\tau_i} \in \widetilde{\mathrm{S}_{2^{k_i} n}}$ is an element of $\mathcal{M}$ of order p_i and the $\widetilde{\tau_i}$'s generate a subgroup of $\mathcal{M}$ isomorphic to $C_{\mathcal{P}}$. With small changes to the argument, as restricting the domain where to choose the integers a_i, one can constrain the support of the generated subgroup in any infinite subset of $\mathbb{Z}$ with some modular feature, for example the set $m\mathbb{Z}$ mentioned above. It is therefore clear that $\mathcal{M}$ contains some subgroup isomorphic to $\mathrm{F}_{\aleph_0} \times C_{\mathcal{P}}$, for every countable sequence $\mathcal{P}$ of prime numbers.

One can go further and consider a single g image (under the homomorphism l_n) of a cycle of prime length p in the symmetric group S_n. As an element in $\widetilde{\mathrm{S}_{pn}}$, g is the image of a permutation $x \in \mathrm{S}_{pn}$ which is the product of p cycles of length p: x clearly admits a p-root x_1 in S_{pn} and x_1 is a cycle of

length p^2. Thus, g admits a p-root $g_1 = \widetilde{x_1}$ in $\widetilde{\mathrm{S}_{pn}}$. One can iterate the argument and find, for every $i \in \mathbb{N}$, an element $g_i \in \widetilde{\mathrm{S}_{p^i n}}$ such that $g_i^p = g_{i-1}$: g and the g_i's generate a subgroup of $\mathcal{M}$ isomorphic to the Prüfer p-group C_{p^∞}. By applying this argument to each of the $\widetilde{\tau_i}$'s above, one can build a subgroup of $\mathcal{M}$ isomorphic to $C_{\mathcal{P}}^{\infty}$ and, again, one can confine the support of the group into the set $m\mathbb{Z}$. Since any abelian torsion group can be embedded in a direct product of Prüfer p-groups, one has immediately the following results.

PROPOSITION 3.6. *$\mathcal{M}$ contains every countable abelian torsion group as a subgroup.*

PROPOSITION 3.7. *Let $\mathcal{P}$ be a countable sequence of prime numbers and $A_{\mathcal{P}} = \mathrm{F}_{\aleph_0} \times C_{\mathcal{P}}^{\infty}$. Then $A_{\mathcal{P}}$ is isomorphic to a subgroup of $\mathcal{M}$.*

Proposition 3.7 individuates a large class of abelian groups that can be embedded in $\mathcal{M}$: the $A_{\mathcal{P}}$'s and their subgroups. We now show that all abelian subgroups of $\mathcal{M}$ belong to that class. Suppose A is an abelian subgroup of $\mathcal{M}$, let T be its (maximal) torsion subgroup and consider the quotient group A/T. Let $1 \neq aT \in A/T$ (in particular a is of infinite order in A) and suppose xT is a k-root of aT in A/T: for some $\tau \in T$, $x^k\tau = a$. If $|\tau| = n$, $x^{kn} = a^n$ and, according to Theorem 3.4, $kn \leq \varepsilon(a^n) \leq n\varepsilon(a)$ and then $k \leq \varepsilon(a)$. As a consequence, every element of A/T admits only a finite number of roots and then A/T is free abelian. T is therefore a direct factor of A and A is isomorphic to a subgroup of some $A_{\mathcal{P}}$ as defined in Proposition 3.7. What we have seen so far proves the following theorem.

THEOREM 3.8. *Let A be a countable abelian group and T be its torsion subgroup: A can be represented as a subgroup of $\mathcal{M}$ if and only if A/T is free abelian.*

Since we have showed (theorem 2.8) that the commutator subgroup $\mathcal{M}'$ of $\mathcal{M}$ is simple, a natural question could arise, whether it is possible to restate the last and theorem 1.1 with $\mathcal{M}'$ in place of $\mathcal{M}$.

For theorem 3.8 it is easily seen that it is just a matter of embedding $\mathrm{F}_{\aleph_0}$ in $\mathcal{M}'$, since any embedding of $C_{\mathcal{P}}^{\infty}$ already lies there. Such an embedding can be simply achieved by modifying the group $G = \bigcup_{i \in \mathbb{N}} G_i$ constructed before: one considers $\widetilde{G_i} = \langle (\lambda_{2m,x_1})^{-1} \lambda_{2^j m, x_j} \mid j = 2, \ldots, i \rangle \leq \mathrm{M}'_n$ and $\widetilde{G} = \bigcup_{i \geq 2} \widetilde{G_i} \leq \mathcal{M}'$ which is still isomorphic to $\mathrm{F}_{\aleph_0}$ with support disjoint from $m\mathbb{Z}$.

For theorem 1.1 the same is not as immediate as for theorem 3.8, but still possible. The homomorphism $f : \Delta_n \to \Delta_{2n}$, defined by $(\lambda_{n,i})f = \lambda_{2n,i}(\lambda_{2n,i+n})^{-1}$, is injective and commutes with every automorphism of $\widetilde{\mathrm{S}_n}$; furthermore, $(\Delta_n)f \leq [\Delta_{2n}, \widetilde{\mathrm{S}_{2n}}] = \Delta_{2n} \cap \ker(\Psi) = \Delta_{2n} \cap \mathcal{M}'$. Thus, it is possible to embed $\mathrm{M}_n = \Delta_n \rtimes \widetilde{\mathrm{S}_n}$ into $[\Delta_{2n}, \widetilde{\mathrm{S}_{2n}}] \rtimes \widetilde{\mathrm{S}_{2n}} \leq \mathcal{M}'$ and conclude that every finitely generated abelian-by-finite group can be embedded in $\mathcal{M}'$ (this also shows that every finitely generated (abelian-by-finite) group can be embedded into the commutator subgroup of a finitely generated (abelian-by-finite) group).

FINAL REMARK. Just before this work was submitted, a paper by M. R. Dixon, M. J. Evans and H. Smith appeared ([1]) in which the existence of a locally (abelian-by-finite) simple group that is not locally finite is established; the authors construct such a group by means of a direct limit involving wreath products of direct products of infinite cyclic groups by finite alternating groups, which are in some way basic "bricks" not too dissimilar to the ones of the group $\mathcal{M}$ of modular permutations. However, our work was originally intended with the main purpose of obtaining a better understanding of the group $\mathcal{M}$, whose definition sounds quite natural and reasonable, even though almost no traces were found in the literature.

REFERENCES

[1] M. R. DIXON - M. J. EVANS - H. SMITH, *Embedding groups in locally (soluble-by-finite) simple groups*, Journal of Group Theory **9** (2006), pp. 383–395.

[2] M. I. KARGAPOLOV - JU. I. MERZLJAKOV, *Fundamentals of the Theory of Groups*, Graduate Texts in Mathematics, vol. **62**, Springer (1979).

[3] N. POUYANNE, *On the number of permutations admitting an m-th root*, The Electronic Journal of Combinatorics **9** (2002).

[4] H. WIELANDT, *Permutationsgruppe*, Math. Inst. Univ. Tübingen (1955). [Translated in english: *Finite Permutation Groups*, Academic Press, New York (1964). Reprinted in *Mathematische Werke*, Walter de Gruyter, Berlin, Vol. **1** (1994), pp. 119–198.]

Manoscritto pervenuto in redazione il 10 luglio 2006