Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

1068

Number Theory Noordwijkerhout 1983

Proceedings of the Journées Arithmétiques
held at Noordwijkerhout, The Netherlands
July 11-15, 1983

Edited by H. Jager

Springer-Verlag
Berlin Heidelberg New York Tokyo 1984

HEURISTICS ON CLASS GROUPS OF NUMBER FIELDS

by

H. COHEN and H. W. LENSTRA, Jr.

-:-:-:-

§ 1. - Motivations

The motivation for this work came from the desire to understand heuristically (since proofs seem out of reach at present) a number of experimental observations about class groups of number fields, and in particular imaginary and real quadratic fields. In turn the heuristic explanations that we obtain may help to find the way towards a proof.

Three of these observations are as follows :

A/ The odd part of the class group of an imaginary quadratic field seems to be quite rarely non cyclic.

B/ If p is a small odd prime, the proportion of imaginary quadratic fields whose class number is divisible by p seems to be significantly greater than $1/p$ (for instance 43 % for $p=3$, 23.5 % for $p=5$).

C/ It seems that a definite non zero proportion of real quadratic fields of prime discriminant (close to 76 %) has class number 1, although it is not even known whether there are infinitely many.

The main idea, due to the second author, is that the scarcity of noncyclic groups can be attributed to the fact that they have many automorphisms. This naturally leads to the heuristic assumption that isomorphism classes G of abelian groups should be weighted with a weight proportional to $1/\#\,\mathrm{Aut}\,G$. This is a very natural and common weighting factor, and it is the purpose of this paper to show that the assumption above, plus another one to take into account the units, is sufficient to

give very satisfactory heuristic answers of quantitative type to most natural questions about class groups. For example we find that the class number of an imaginary quadratic field should be divisible by 3 with probability close to 43.987 %, and that the proportion of real quadratic fields with class number one (having prime discriminant) should be close to 75.446 %.

To distinguish clearly between theorem and conjectural statements, this paper can be considered as having two parts. In the first part (§ 2 to § 7) we give theorems about finite modules over certain Dedekind domains. The second part (§ 8 to § 10) explains in detail the heuristic assumptions that we make, and gives a large sample of conjectures which follow from these heuristic assumptions using the theory developed in the first part.

§ 2. - Notations

In what follows, A will be the ring of integers of a number field. It will be seen that more general Dedekind domains can be used, and also direct products of such, but for simplicity we will assume that A is as above. The special case $A = \mathbb{Z}$ is of particular importance. We denote by $\mathcal{P}$ the set of non zero prime ideals of A, and if $\mathfrak{p} \in \mathcal{P}$, the norm of $\mathfrak{p}$ is by definition $N\mathfrak{p} = \#(A/\mathfrak{p})$. The letter $\mathfrak{p}$ will be used only for elements of $\mathcal{P}$.

. If G_1 and G_2 are A-modules, we write $G_1 \leq G_2$ to mean that G_1 is a submodule of G_2.

. If $\mathfrak{p} \in \mathcal{P}$ and G is a finite A-module, then we write $r_{\mathfrak{p}}(G)$ for the $\mathfrak{p}$-rank of G, i.e. the dimension of $G/\mathfrak{p}G$ as an $A/\mathfrak{p}$-vector space.

. k will be a non negative integer or ∞. If $k \neq \infty$ and G is a finite A-module, $s_k(G)$ (or $s_k^A(G)$ when the ring A must be specified) will be the number of surjective A-homomorphisms from A^k to G.

. If G is a finite A-module we define the k-weight $w_k(G)$ of G, and the weight w(G) of G as follows :

$$w_k(G) = s_k(G)\,(\#\,G)^{-k}\,(\#\,\mathrm{Aut}\,G)^{-1}$$

$$w(G) = w_\infty(G) = (\#\,\mathrm{Aut}\,G)^{-1}$$

where $\mathrm{Aut}\,G = \mathrm{Aut}_A G$ is the group of A-automorphisms of G.

. For $\mathfrak{p} \in \mathcal{P}$ we set $\eta_k(\mathfrak{p}) = \prod_{1 \leq i \leq k} (1 - N\mathfrak{p}^{-i})$, $\eta_\infty(\mathfrak{p}) = \prod_{1 \leq i} (1 - N\mathfrak{p}^{-i})$.

. If $0 \leq b \leq a$ with a, b integers we define

$$\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]_{\mathfrak{p}} = \eta_a(\mathfrak{p}) / (\eta_{a-b}(\mathfrak{p})\ \eta_b(\mathfrak{b}))$$

and if $a \geq 0$ but $b < 0$ or $b > a$, we set $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]_{\mathfrak{p}} = 0$.

. Let $\zeta_A(s)$ be the Dedekind zeta function of the ring A. Then we set

$$C_k = \varkappa \prod_{2 \leq i \leq k} \zeta_A(i) \quad , \quad C_\infty = \varkappa \prod_{2 \leq i} \zeta_A(i)$$

where $\varkappa = \varkappa_A$ is the residue at $s = 1$ of the function $\zeta_A(s)$ (see also section 7).

. We will need the well known notion which generalises to finite A-modules G the notion of cardinality for finite $\mathbb{Z}$-modules. This has several names in the literature (1^{st} Fitting ideal [10], 0^{th} determinantial ideal [2] for example). We will call it the A-cardinal of G, and write $\chi_A(G)$ or $\chi(G)$ as in [12]. It is an ideal of A which can be defined as follows: every finite A-module G can be written in a non canonical way

$$G = \bigoplus_i A/\mathfrak{a}_i \qquad (\mathfrak{a}_i \text{ ideals in } A).$$

Then we set $\chi_A(G) = \prod_i \mathfrak{a}_i$, and this <u>is</u> canonical and does not depend on the decomposition. In the case $A = \mathbb{Z}$, $\chi_{\mathbb{Z}}(G) = n\mathbb{Z}$ where $n = \# G$. In the general case, $\# G = N(\chi_A(G))$.

. We shall use the notations

$\sum_{G(\mathfrak{a})}$ as an abbreviation for $\sum$ G up to A-isomorphism, $\chi_A(G) = \mathfrak{a}$

$\sum_{G(\mathfrak{a}),\, \varphi_u}$ as an abbreviation for $\sum$ G up to A-isomorphism, $\chi_A(G) = \mathfrak{a}$, $\varphi \in \mathrm{Hom}_A(A^u, G)$.

. We define the k-<u>weight</u> $w_k(\mathfrak{a})$ of an integral ideal $\mathfrak{a}$ as follows:

$$w_k(\mathfrak{a}) = \sum_{G(\mathfrak{a})} w_k(G)$$

and we set $w(\mathfrak{a}) = w_\infty(\mathfrak{a})$.

. The letter u will be used to denote a non negative integer, and it will be in our applications the A-rank of a certain group of units (see section 8).

§ 3. - Fundamental properties of the functions $w_k(G)$ and $w_k(\mathfrak{a})$

We first show :

PROPOSITION 3.1. - Let J be a projective A-module of rank k and G a finite A-module. Set $\chi_A(G) = \mathfrak{a}$

i) The number of surjective A-homomorphisms from J to G is equal to $s_k(G)$

ii) $s_k(G) = (N\mathfrak{a})^k \prod_{\mathfrak{p}\mid\mathfrak{a}} \eta_k(\mathfrak{p}) / \eta_{k-r_{\mathfrak{p}}(G)}(\mathfrak{p})$

$w_k(G) = \left(\prod_{\mathfrak{p}\mid\mathfrak{a}} \eta_k(\mathfrak{p}) / \eta_{k-r_{\mathfrak{p}}(G)}(\mathfrak{p}) \right) (\# \operatorname{Aut} G)^{-1}$

iii) $\# \{ H \leq J : J/H \simeq G \} = (N\mathfrak{a})^k \, w_k(G)$

iv) $\lim_{k \to +\infty} w_k(G) = w(G)$.

Proof. - i) By inverting all the prime ideals which are not in $\mathfrak{a}$, one easily sees that G is unchanged and A becomes a semilocal Dedekind ring and in particular is a principal ideal ring. In that case i) is trivial since $J \simeq A^k$ as an A-module.

ii) It is easy to check that $s_k(G) = \prod_{\mathfrak{p}\mid\mathfrak{a}} s_k(G_{\mathfrak{p}})$ where $G_{\mathfrak{p}}$ is the $\mathfrak{p}$-component of G (note that $G_{\mathfrak{p}}$ is non trivial if and only if $\mathfrak{p} \mid \mathfrak{a}$). Hence we may assume that G is a $\mathfrak{p}$-group. Then we know (e.g. see [1], § 3, prop. 11) that if $\varphi \in \operatorname{Hom}_A(A^k, G)$, φ is surjective if and only if $\overline{\varphi}$ is surjective, where $\overline{\varphi} \in \operatorname{Hom}_{A/\mathfrak{p}}((A/\mathfrak{p})^k, G/\mathfrak{p}\,G)$ is obtained by reduction mod. $\mathfrak{p}$. Hence it follows that :

$$s_k^A(G) = s_k^{A/\mathfrak{p}}(G/\mathfrak{p}\,G) \, \# \{ \varphi \in \operatorname{Hom}_A(A^k, G) / \overline{\varphi} = 0 \} .$$

If we set $r = r_{\mathfrak{p}}(G)$, then $s_k^{A/\mathfrak{p}}(G/\mathfrak{p}\,G)$ is equal to the number of $k \times r$ matrices of rank r over $A/\mathfrak{p}$, i.e. to the number of $A/\mathfrak{p}$-linearly independent r-tuples $(v_1, \ldots, v_r)$, where $v_i \in (A/\mathfrak{p})^k$. Since a vector space of dimension i over $A/\mathfrak{p}$ has $(N\mathfrak{p})^i$ elements, we obtain :

$$s_k^{A/\mathfrak{p}}(G/\mathfrak{p}\,G) = \prod_{0 \leq i < r} (N\mathfrak{p}^k - N\mathfrak{p}^i) = (N\mathfrak{p})^{kr} \, \eta_k(\mathfrak{p}) / \eta_{k-r}(\mathfrak{p}) .$$

On the other hand $\overline{\varphi} = 0 \Leftrightarrow \forall v \in A^k$, $\varphi(v) \in \mathfrak{p}\,G$, and so

$$\# \{ \varphi \in \operatorname{Hom}_A(A^k, G) / \overline{\varphi} = 0 \} = (\# \mathfrak{p}\,G)^k = \left(\frac{\# G}{\# G/\mathfrak{p}\,G} \right)^k = \frac{(N\mathfrak{a})^k}{(N\mathfrak{p})^{kr}}$$

and proposition 3.1 ii) follows.

iii) Follows from the fact that if M and N are two A-modules and $\varphi_1, \varphi_2 \in \mathrm{Hom}_A(M,N)$ are surjective then

$$\mathrm{Ker}\,\varphi_1 = \mathrm{Ker}\,\varphi_2 \Leftrightarrow \exists \sigma \in \mathrm{Aut}\,N \text{ such that } \varphi_2 = \sigma \circ \varphi_1 .$$

Finally iv) is a trivial consequence of ii).

PROPOSITION 3.2. - For $k_1, k_2 \neq \infty$ and G a finite A-module :

$$s_{k_1+k_2}(G) = \sum_{G_1 \leq G} s_{k_1}(G_1)\, s_{k_2}(G/G_1)\, (\#\, G_1)^{k_2} .$$

Proof. - Write $A^{k_1+k_2}$ as $A^{k_1} \times A^{k_2}$. It is clear that :

$$s_{k_1+k_2}(G) = \sum_{G_1 \leq G} \#\{\varphi \in \mathrm{Hom}_A(A^{k_1+k_2}, G) / \varphi \text{ surjective}, \varphi(A^{k_1}) = G_1\}$$

$$= \sum_{G_1 \leq G} \sum_{\substack{\varphi_1 \in \mathrm{Hom}(A^{k_1}, G_1) \\ \varphi_1 \text{ surjective}}} \#\{\varphi \in \mathrm{Hom}_A(A^{k_1+k_2}, G) / \varphi \text{ surjective}, \varphi|_{A^{k_1}} = \varphi_1\} .$$

It will thus suffice to prove the following lemma :

LEMMA 3.3. - If $\varphi_1 \in \mathrm{Hom}_A(A^{k_1}, G_1)$, φ_1 surjective, then

$$\#\{\varphi \in \mathrm{Hom}_A(A^{k_1+k_2}, G) / \varphi \text{ surjective}, \varphi|_{A^{k_1}} = \varphi_1\} = s_{k_2}(G/G_1)\,(\#\, G_1)^{k_2} .$$

Proof. - Put $E = \{\varphi \in \mathrm{Hom}_A(A^{k_1+k_2}, G) / \varphi \text{ surjective}, \varphi|_{A^{k_1}} = \varphi_1\}$ and $F = \{\overline{\varphi}_2 \in \mathrm{Hom}_A(A^{k_2}, G/G_1), \overline{\varphi}_2 \text{ surjective}\}$.
Then it is not difficult to check that the natural map obtained by restricting to A^{k_2} and then reducing mod. G_1 is indeed a map from E to F. Furthermore, by writing down explicitly a set of representatives in G of G/G_1, one can also easily see that every $\varphi_2 \in F$ has exactly $(\#\, G_1)^{k_2}$ preimages. Hence

$$\#\, E = \#\, F \,.\, (\#\, G_1)^{k_2} ,$$

thus proving lemma 3.3 and proposition 3.2.

COROLLARY 3.4. - If $k_1 \neq \infty$:

$$w_{k_1+k_2}(G) = (\#\,\mathrm{Aut}\,G)^{-1} \sum_{G_1 \leq G} (\#\, G/G_1)^{-k_1} (\#\,\mathrm{Aut}\,G_1)(\#\,\mathrm{Aut}\,G/G_1)\, w_{k_1}(G_1)\, w_{k_2}(G/G_1) .$$

Proof. - For $k_2 \neq \infty$ this is just a restatement of proposition 3.2, and the case $k_2 = \infty$ follows by letting $k_2 \to +\infty$ and using proposition 3.1, iv).

The following theorem, although not difficult to prove, will be very important in the sequel :

THEOREM 3.5. - Let K and C be finite A-modules. Then for all k :

$$\sum_{G \text{ up to A-isomorphism}} w_k(G) \, \# \{ G_1 \leq G : G_1 \simeq K \text{ and } G/G_1 \simeq C \} = w_k(K) \, w_k(C) \ .$$

Proof. - We consider only k finite since the case $k = \infty$ follows by making $k \to \infty$. We shall count the number of pairs (H, J) of A-modules such that $H \subset J \subset A^k$, $A^k/J \simeq C$, $J/H \simeq K$. Note that H and J are necessarily projective modules of rank k.

If we write $m = \# K$ and $n = \# K \, \# C$, then the number of J is $(n/m)^k w_k(C)$ (proposition 3.1 (iii)), while for a given J the number of H is equal to $m^k w_k(K)$ by the same proposition. Hence the number of pairs (H, J) as above is equal to $n^k w_k(K) \, w_k(C)$.

Now let H be fixed and set $G = A^k/H$. Then every submodule of G can be written uniquely in the form J/H for some J such that $H \subset J \subset A^k$, hence the number of J is equal to

$$\# \{ G_1 \leq G : G_1 \simeq K \text{ and } G/G_1 \simeq C \}$$

where we have set $G_1 = J/H$.

Finally, using again proposition 3.1, we see that for a given G the number of H such that $A^k/H \simeq G$ is equal to $n^k w_k(G)$, and Theorem 3.5 follows. (Note that $m = N(\chi_A(K))$, $(n/m) = N(\chi_A(C))$ and that if $0 \to G_1 \to G \to G/G_1 \to 0$ is an exact sequence then $\chi_A(G) = \chi_A(G_1) \, \chi_A(G/G_1)$.)

THEOREM 3.6. - Let $\mathfrak{a}$ be a non zero ideal of A

i) For any $k_2 \neq \infty$:

$$w_{k_1+k_2}(\mathfrak{a}) = \sum_{\mathfrak{b} \mid \mathfrak{a}} (N\mathfrak{b})^{-k_2} w_{k_1}(\mathfrak{b}) \, w_{k_2}(\mathfrak{a}\mathfrak{b}^{-1}) \ .$$

ii) For any k, $\sum_{\mathfrak{b} \mid \mathfrak{a}} w_k(\mathfrak{b}) = (N\mathfrak{a}) \, w_{k+1}(\mathfrak{a})$. In particular

$$\sum_{\mathfrak{b} \mid \mathfrak{a}} w(\mathfrak{b}) = (N\mathfrak{a}) \, w(\mathfrak{a}) \ .$$

Proof. - i) By corollary 3.4 we have, setting $b = \chi_A(G/G_1)$:

$$w_{k_1+k_2}(a) = \sum_{G(a)} w_{k_1+k_2}(G) = \sum_{b \mid a} (Nb)^{-k_1} \sum_{C(b)} (\# \text{ Aut } C)\, w_{k_2}(C) \times$$

$$\times \sum_{K(ab^{-1})} (\# \text{ Aut } K)\, w_{k_1}(K) \sum_{G(a)} w(G) \# \{G_1 \leq G : G_1 \simeq K \text{ and } G/G_1 \simeq C\}$$

so using Theorem 3.5 with $k = \infty$:

$$w_{k_1+k_2}(a) = \sum_{b \mid a} (Nb)^{-k_1} \sum_{C(b)} w_{k_2}(C) \sum_{K(ab^{-1})} w_{k_1}(K)$$

$$= \sum_{b \mid a} (Nb)^{-k_2} w_{k_2}(b)\, w_{k_1}(ab^{-1})$$

and (i) follows after interchanging k_1 and k_2 .

For (ii) we apply (i) with $k_1 = k$, $k_2 = 1$. Note that $s_1(G) \neq 0$ if and only if $G \simeq A/a$, where a is a non zero ideal of A , and $s_1(A/a) = \# (A/a)^* = \# \text{ Aut}(A/a)$.

Since $\chi_A(A/a) = a$ and that $A/a \simeq A/b$ if and only if $a = b$, it easy follows that

$$w_1(a) = 1/Na$$

and ii) follows.

This theorem is best expressed in terms of Dirichlet series as follows :

COROLLARY 3.7. - (i) Let $p \in \mathcal{P}$. Then for $\text{Re } s > -1$

$$\sum_{\alpha \geq 0} w_k(p^\alpha)(Np)^{-\alpha s} = \prod_{1 \leq j \leq k} (1 - Np^{-j-s})^{-1} .$$

(ii) If we set $\zeta_{k,A}(s) = \zeta_k(s) = \sum w_k(a)(Na)^{-s}$ for $\text{Re } s > 0$, then

$$\zeta_{k,A}(s) = \prod_{1 \leq j \leq k} \zeta_A(s+j)$$

where $\zeta_A(s)$ is the Dedekind zeta function of A .

Proof. - Clear by induction on k .

Note that theorem 3.6 (i) follows from the identity

$$\zeta_{k_1+k_2}(s) = \zeta_{k_1}(s+k_2)\, \zeta_{k_2}(s) .$$

COROLLARY 3.8. - For every $k \geq 1$:

$$w_k(\mathfrak{a}) = \frac{1}{N\mathfrak{a}} \prod_{\mathfrak{p}^\alpha \| \mathfrak{a}} \left[\begin{matrix} \alpha+k-1 \\ \alpha \end{matrix} \right]_{\mathfrak{p}} \qquad \text{and in particular}$$

$$w(\mathfrak{a}) = \frac{1}{N\mathfrak{a}} \prod_{\mathfrak{p}^\alpha \| \mathfrak{a}} (\eta_\alpha(\mathfrak{p}))^{-1} \quad . \quad (*)$$

(See section 2 for notations ; $\mathfrak{p}^\alpha \| \mathfrak{a}$ means that α is the exact exponent of $\mathfrak{p}$ in the prime ideal decomposition of $\mathfrak{a}$.)

Proof. - We use induction on k . For $k=1$, $w_1(\mathfrak{a}) = 1/N\mathfrak{a}$ as we have seen so the formula is true. Assume that it is true for some $k \geq 1$ and let us prove it for $k+1$. First note that both sides of the formula are multiplicative functions of $\mathfrak{a}$, hence it suffices to prove it for $\mathfrak{a} = \mathfrak{p}^\alpha$. Now by theorem 3.6 (ii) and our induction hypothesis :

$$w_{k+1}(\mathfrak{p}^\alpha) = (N\mathfrak{p})^{-\alpha} \sum_{0 \leq \beta \leq \alpha} (N\mathfrak{p})^{-\beta} \left[\begin{matrix} \beta+k-1 \\ \beta \end{matrix} \right]_{\mathfrak{p}} .$$

Now the following lemma is well known and straightforward to prove (it is the q-analogue of the formula

$$\binom{\beta+k}{k} = \binom{\beta+k-1}{k} + \binom{\beta+k-1}{k-1} \quad \text{for binomial coefficients, with } q = (N\mathfrak{p})^{-1}) :$$

LEMMA 3.9.- $$\left[\begin{matrix} \beta+k \\ k \end{matrix} \right]_{\mathfrak{p}} = \left[\begin{matrix} \beta+k-1 \\ k \end{matrix} \right]_{\mathfrak{p}} + (N\mathfrak{p})^{-\beta} \left[\begin{matrix} \beta+k-1 \\ k-1 \end{matrix} \right]_{\mathfrak{p}}$$

Hence

$$w_{k+1}(\mathfrak{p}^\alpha) = (N\mathfrak{p})^{-\alpha} \sum_{0 \leq \beta \leq \alpha} \left(\left[\begin{matrix} \beta+k \\ k \end{matrix} \right]_{\mathfrak{p}} - \left[\begin{matrix} \beta+k-1 \\ k \end{matrix} \right]_{\mathfrak{p}} \right) = (N\mathfrak{p})^{-\alpha} \left[\begin{matrix} \alpha+k \\ k \end{matrix} \right]_{\mathfrak{p}} = (N\mathfrak{p})^{-\alpha} \left[\begin{matrix} \alpha+k \\ \alpha \end{matrix} \right]_{\mathfrak{p}}$$

and so corollary 3.8 follows by induction and then letting $k \to \infty$ since $\lim_{k \to \infty} \left[\begin{matrix} \alpha+k-1 \\ \alpha \end{matrix} \right]_{\mathfrak{p}} = \eta_\alpha(\mathfrak{p})^{-1}$.

(*) In the case $A = \mathbb{Z}$, this last formula was proved by a completely different method by P. Hall [8].

§ 4. - Some consequences of theorems 3.5 and 3.6

In this section we collect a number of almost direct consequences of theorems 3.5 and 3.6 which will be useful to us later on.

PROPOSITION 4.1. - Let $\mathfrak{a}$; $\mathfrak{b}$ be (non zero) ideals of A , such that $\mathfrak{b} | \mathfrak{a}$, and K a finite A-module such that $\mathfrak{b} = \chi_A(K)$. Then for all k :

(i) $\sum_{G(\mathfrak{a})} w_k(G) \# \{ G_1 \leq G : G_1 \simeq K \} = w_k(\mathfrak{a}\mathfrak{b}^{-1})\, w_k(K)$

(ii) $\sum_{G(\mathfrak{a})} w_k(G) \# \{ G_1 \leq G : G/G_1 \simeq K \} = w_k(\mathfrak{a}\mathfrak{b}^{-1})\, w_k(K)$

(iii) $\sum_{G(\mathfrak{a})} w_k(G) \# \{ G_1 \leq G : \chi_A(G_1) = \mathfrak{b} \} = w_k(\mathfrak{a}\mathfrak{b}^{-1})\, w_k(\mathfrak{b})$.

Proof. - Clear from theorem 3.5 by summing over suitable isomorphism classes.

We now want to generalize theorems 3.5 and its consequences to the case where G is replaced by $G/\mathrm{Im}\,\varphi$, where $\varphi \in \mathrm{Hom}_A(A^u, G)$. For this we need a new definition :

DEFINITION 4.2. - For u, k arbitrary and $\mathfrak{a}$ non zero ideal, we set :

$$w_{k,u}(\mathfrak{a}) = \sum_{G(\mathfrak{a})} w_k(G)\, w_u(G) \,\#\, \mathrm{Aut}\, G \quad \text{and} \quad \zeta_{k,u}(s) = \sum_{\mathfrak{a}} \frac{w_{k,u}(\mathfrak{a})}{(N\mathfrak{a})^s} .$$

Note that $w_{k,u} = w_{u,k}$ and that $w_{\infty,u} = w_u$, and similarly for $\zeta_{k,u}$.
The first result that we need is the following :

PROPOSITION 4.3. - Let $\mathfrak{a}$, $\mathfrak{b}$ be (non zero) ideals of A with $\mathfrak{b} | \mathfrak{a}$, and K a finite A-module such that $\chi_A(K) = \mathfrak{b}$. Then

$$\sum_{G(\mathfrak{a})} w_k(G) \# \{ \varphi \in \mathrm{Hom}_A(A^u, G) : G/\mathrm{Im}\,\varphi \simeq K \} = (N(\mathfrak{a}\mathfrak{b}^{-1}))^u\, w_{k,u}(\mathfrak{a}\mathfrak{b}^{-1})\, w_k(K) .$$

Proof. - The left hand side clearly equals

$$\sum_{L(\mathfrak{a}\mathfrak{b}^{-1})} s_u(L) \sum_{G(\mathfrak{a})} w_k(G) \# \{ G_1 \leq G : G_1 \simeq L \text{ and } G/G_1 \simeq K \}$$

$$= \sum_{L(\mathfrak{a}\mathfrak{b}^{-1})} (N(\mathfrak{a}\mathfrak{b}^{-1}))^u \,\#\, \mathrm{Aut}\, L\; w_u(L)\, w_k(L)\, w_k(K) \quad \text{by theorem 3.5}$$

$$= (N(\mathfrak{a}\mathfrak{b}^{-1}))^u\, w_{k,u}(\mathfrak{a}\mathfrak{b}^{-1})\, w_k(K) , \quad \text{and the proposition is proved.}$$

COROLLARY 4.4. - Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be (non zero) ideals of A with $\mathfrak{b}\mathfrak{c} \mid \mathfrak{a}$ and K, C finite A-modules such that $\chi_A(K) = \mathfrak{b}$, $\chi_A(C) = \mathfrak{c}$. Then

$$\sum_{G(\mathfrak{a}), \varphi_u} w_k(G) \# \{ G_1 \leq G/\mathrm{Im}\,\varphi : G_1 \simeq K \text{ and } (G/\mathrm{Im}\,\varphi)/G_1 \simeq C \}$$
$$= N(\mathfrak{a}\mathfrak{b}^{-1}\mathfrak{c}^{-1})^u \, w_{k,u}(\mathfrak{a}\mathfrak{b}^{-1}\mathfrak{c}^{-1}) \, w_k(C) \, w_k(K).$$

Proof. - The left hand side clearly equals

$$\sum_{L(\mathfrak{b}\mathfrak{c})} \# \{ G_1 \leq L : G_1 \simeq K \text{ and } L/G_1 \simeq C \} \sum_{G(\mathfrak{a})} w_k(G) \# \{ \varphi \in \mathrm{Hom}(A^u, G) : (G/\mathrm{Im}\,\varphi) \simeq L \}$$
$$= \sum_{L(\mathfrak{b}\mathfrak{c})} \# \{ G_1 \leq L : G_1 \simeq K \text{ and } L/G_1 \simeq C \} N(\mathfrak{a}\mathfrak{b}^{-1}\mathfrak{c}^{-1})^u \, w_{k,u}(\mathfrak{a}\mathfrak{b}^{-1}\mathfrak{c}^{-1}) \, w_k(L)$$

by proposition 4.3, and the result follows from theorem 3.5.

PROPOSITION 4.5. - Let $\mathfrak{a}, \mathfrak{b}$ be (non zero) ideals of A with $\mathfrak{b} \mid \mathfrak{a}$, and K a finite A-module such that $\chi_A(K) = \mathfrak{b}$. Then :

(i) $\displaystyle\sum_{G(\mathfrak{a}), \varphi_u} w_k(G) \# \{ G_1 \leq G/\mathrm{Im}\,\varphi : G_1 \simeq K \} = N(\mathfrak{a}\mathfrak{b}^{-1})^u \, w_k(\mathfrak{a}\mathfrak{b}^{-1}) \, w_k(K)$

(ii) $\displaystyle\sum_{G(\mathfrak{a}), \varphi_u} w_k(G) \# \{ G_1 \leq G/\mathrm{Im}\,\varphi : (G/\mathrm{Im}\,\varphi)/G_1 \simeq K \} = N(\mathfrak{a}\mathfrak{b}^{-1})^u \, w_k(\mathfrak{a}\mathfrak{b}^{-1}) \, w_k(K)$

(iii) $\displaystyle\sum_{G(\mathfrak{a}), \varphi_u} w_k(G) \# \{ G_1 \leq G/\mathrm{Im}\,\varphi : \chi_A(G_1) = \mathfrak{b} \} = N(\mathfrak{a}\mathfrak{b}^{-1})^u \, w_k(\mathfrak{a}\mathfrak{b}^{-1}) \, w_k(\mathfrak{b})$.

THEOREM 4.6. - We have for $\mathrm{Re}\, s > 0$:

$$\zeta_{k,u}(s) = \sum_{\mathfrak{a}} \frac{w_{k,u}(\mathfrak{a})}{(N\mathfrak{a})^s} = \frac{\zeta_k(s)}{\zeta_k(s+u)} = \frac{\zeta_k(s)\,\zeta_u(s)}{\zeta_{k+u}(s)} = \prod_{1 \leq j \leq k} \frac{\zeta_A(s+j)}{\zeta_A(u+s+j)} \quad .$$

Proofs. - We prove proposition 4.5 (i) and theorem 4.6 simultaneously.

If we sum the formula in corollary 4.4 over $C(\mathfrak{c})$ and then over all $\mathfrak{c} \mid \mathfrak{a}\mathfrak{b}^{-1}$, it is clear that we obtain :

$$\sum_{G(\mathfrak{a}), \varphi_u} w_k(G) \# \{ G_1 \leq G/\mathrm{Im}\,\varphi : G_1 \simeq K \} = f(\mathfrak{a}\mathfrak{b}^{-1}) \, w_k(K)$$

where $\displaystyle f(\mathfrak{a}) = \sum_{\mathfrak{c} \mid \mathfrak{a}} N(\mathfrak{a}\mathfrak{c}^{-1})^u \, w_{k,u}(\mathfrak{a}\mathfrak{c}^{-1}) \, w_k(\mathfrak{c})$.

Now the important point is that $f(\mathfrak{a}\mathfrak{b}^{-1})$ depends only on the ideal $\mathfrak{a}\mathfrak{b}^{-1}$. Hence if we take $K = \{0\}$ the trivial A-module, we have $w_k(K) = 1$ and $\chi_A(K) = \mathfrak{b} = A$ hence :

$$f(\mathfrak{a}) = \sum_{G(\mathfrak{a}), \varphi_u} w_k(G) = (N\mathfrak{a})^u \, w_k(\mathfrak{a}), \quad \text{so} \quad f(\mathfrak{a}\mathfrak{b}^{-1}) = N(\mathfrak{a}\mathfrak{b}^{-1})^u \, w_k(\mathfrak{a}\mathfrak{b}^{-1})$$

and proposition 4.5 (i) follows.

Now we have just proven the identity

$$f(\mathfrak{a}) = \sum_{\mathfrak{c} \mid \mathfrak{a}} N(\mathfrak{a}\mathfrak{c}^{-1})^u \, w_{k,u}(\mathfrak{a}\mathfrak{c}^{-1}) \, w_k(\mathfrak{c}) = (N\mathfrak{a})^u w_k(\mathfrak{a}) \ .$$

In terms of Dirichlet series, this gives :

$$\zeta_{k,u}(s-u) \ \zeta_k(s) = \zeta_k(s-u) \ ,$$

and theorem 4.6 follows immediately.

The proofs of (ii) and (iii) in proposition 4.5 are now trivial and left to the reader.

§ 5. - Some u-probabilistics and u-averages

In the beginning of this section, f will be a complex-valued function defined on isomorphism classes of finite A-modules.

DEFINITION 5.1. - We set

$$w_k(f;\mathfrak{a}) = \sum_{G(\mathfrak{a})} w_k(G) \, f(G) \ , \qquad \zeta_k(f;s) = \sum_{\mathfrak{a}} w_k(f;\mathfrak{a}) \, (N\mathfrak{a})^{-s}$$

and we define the (k,u)-average $M_{k,u}(f)$ of f as follows :

$$M_{k,u}(f) = \lim_{x \to \infty} \frac{\sum_{N\mathfrak{a} \leq x} (N\mathfrak{a})^{-u} \sum_{G(\mathfrak{a}), \varphi_u} f(G/\mathrm{Im}\,\varphi) \, w_k(G)}{\sum_{N\mathfrak{a} \leq x} (N\mathfrak{a})^{-u} \sum_{G(\mathfrak{a}), \varphi_u} w_k(G)} \ .$$

If $k = \infty$ we will simply speak of u-average of f and write $M_u(f)$ instead of $M_{\infty,u}(f)$.

Remarks. - 1) The (k,u)-average of f may not exist if the expression after the lim does not tend to a limit when $x \to \infty$.

2) The denominator in the definition of $M_{k,u}(f)$ is equal to

$$\sum_{N\mathfrak{a} \leq x} w_k(\mathfrak{a})$$

but we have written it in the above manner to make it clear that we are dealing with an average (i.e. the (k,u)-average of a function which is constant is that constant).

3) When f is the characteristic function of a property P (i.e. $f = 1$ if P is true, $f = 0$ if P is false) we will speak of (k,u)-probability or u-probability of P instead of (k,u)-average or u-average of f.

4) If $u = 0$ and $k = \infty$ we will speak of the average of f, or the probability of P. It should be noted that this is only a finitely additive measure, hence the word

probability should be taken to mean exactly that in our context.

The aim of this section is to show how, in many cases, one can easily compute (k,u) -averages and probabilities.

The most direct way is by using the following Tauberian theorem :

LEMMA 5.2. - *If* $D(s) = \sum_{\mathfrak{a}} c(\mathfrak{a}) (N\mathfrak{a})^{-s}$ *converges for* $\operatorname{Re} s > 0$ *and if* $D(s) - C/s$ *can be analytically continued for* $\operatorname{Re} s \geq 0$ *then if the* $c(\mathfrak{a})$ *are non negative we have*

$$\sum_{N\mathfrak{a} \leq x} c(\mathfrak{a}) \sim C \operatorname{Log} x \quad \text{as} \quad x \to +\infty .$$

Note that this follows from a classical Tauberian theorem (see e.g. [15]) by writing

$$\sum_{\mathfrak{a}} c(\mathfrak{a}) N\mathfrak{a}^{-s} = \sum_{n \geq 1} n \Big(\sum_{N\mathfrak{a}=n} c(\mathfrak{a}) \Big) n^{-s-1}$$

and then using partial summation.

Applying this to $w_k(\mathfrak{a}) = c(\mathfrak{a})$ and using corollary 3.7 we obtain

LEMMA 5.3. -

$$\sum_{N\mathfrak{a} \leq x} w_k(\mathfrak{a}) \sim C_k \operatorname{Log} x \qquad (x \to +\infty)$$

(see notations for C_k).

In fact one can obtain a more precise estimate, but this asymptotic equality will be sufficient for us since we only want a limit.

PROPOSITION 5.4. - *Write*

$$\zeta_k(f ; s+u)\ \zeta_k(s) / \zeta_k(s+u) = \sum_{\mathfrak{a}} a_{k,u}(f ; \mathfrak{a}) (N\mathfrak{a})^{-s} .$$

Then

$$M_{k,u}(f) = \lim_{x \to \infty} \frac{\sum_{N\mathfrak{a} \leq x} a_{k,u}(f ; \mathfrak{a})}{C_k \operatorname{Log} x} .$$

Proof. - We have

$$\sum_{G(\mathfrak{a}),\, \varphi_u} f(G/\operatorname{Im}\varphi)\ w_k(G) = \sum_{\mathfrak{b} \mid \mathfrak{a}} \sum_{L(\mathfrak{b})} f(L) \sum_{G(\mathfrak{a})} w_k(G) \# \{ \varphi \in \operatorname{Hom}(A^u, G) : G/\operatorname{Im}\varphi \simeq L \}$$

$$= \sum_{\mathfrak{b} \mid \mathfrak{a}} \sum_{L(\mathfrak{b})} f(L)\, N(\mathfrak{a}\mathfrak{b}^{-1})^u\, w_{k,u}(\mathfrak{a}\mathfrak{b}^{-1})\, w_k(L)$$

by proposition 4.3

$$= \sum_{\mathfrak{b} \mid \mathfrak{a}} N(\mathfrak{a}\mathfrak{b}^{-1})^u\, w_{k,u}(\mathfrak{a}\mathfrak{b}^{-1})\, w_k(f ; \mathfrak{b}) .$$

Hence

$$\sum_{\mathfrak{a}} (N\mathfrak{a})^{-s-u} \sum_{G(\mathfrak{a}),\varphi_u} f(G/\mathrm{Im}\,\varphi)\, w_k(G) = \zeta_{k,u}(s)\ \zeta_k(f\,;\, s+u)$$

$$= \zeta_k(s)\ \zeta_k(f\,;\, s+u)/\zeta_k(s+u) = \sum_{\mathfrak{a}} a_{k,u}(f;\mathfrak{a})(N\mathfrak{a})^{-s}$$

where we have used theorem 4.6. Hence

$$\sum_{N\mathfrak{a}\le x} (N\mathfrak{a})^{-u} \sum_{G(\mathfrak{a}),\varphi_u} f(G/\mathrm{Im}\,\varphi)\, w_k(G) = \sum_{N\mathfrak{a}\le x} a_{k,u}(f\,;\,\mathfrak{a})$$

and the proposition follows from remark 2 and lemma 5.3.

COROLLARY 5.5. - Assume that f is a non-negative valued function on the set of is isomorphism classes of finite A-modules. Assume further that $\zeta_k(f\,;\,s)$ converges for $\mathrm{Re}\ s>0$ and that $\zeta_k(f\,;\,s) - C/s$ can be analytically continued to $\mathrm{Re}\ s\ge 0$. Then :

For $u\neq 0$, $M_{k,u}(f) = \zeta_k(f\,;\,u)\ C_u/C_{u+k} = \zeta_k(f\,;\,u)/\zeta_k(u)$

For $u=0$, $M_{k,0}(f) = C/C_k = \lim_{s\to 0} (\zeta_k(f\,;\,s)/\zeta_k(s))$.

Proof. - From proposition 5.4 it is clear that $\sum_{\mathfrak{a}} a_{k,u}(f\,;\,\mathfrak{a})\, N\mathfrak{a}^{-s}$ converges for $\mathrm{Re}\ s>0$ and is asymptotic to $(\zeta_k(f\,;\,u)/\zeta_k(u))\times C_k/s$ if $u>0$ and to C/s if $u=0$.

Since $\zeta_k(u) = C_{u+k}/C_u$ the corollary follows from proposition 5.4 and our Tauberian lemma 5.2.

For our applications, we need to be able to restrict our attention to A-modules having only certain $\mathfrak{p}$-components. More precisely, in what follows we let $\mathcal{P}_1\subset\mathcal{P}$ and we call an A-module G a $\mathcal{P}_1$-A-module if $G = G_{\mathcal{P}_1}$, with an evident notation ($G_{\mathcal{P}_1} = \oplus_{\mathfrak{p}\in\mathcal{P}_1} G_{\mathfrak{p}}$). Then in a straightforward way one can define the notion of (k,u)-average of a function f restricted to $\mathcal{P}_1$-A-modules. The following proposition is easy and left to the reader :

PROPOSITION 5.6. - The (k,u)-average of a function f restricted to $\mathcal{P}_1$-A-modules is the same as the (k,u)-average of the function $f\circ\mathcal{P}_1$ defined by

$$f\circ\mathcal{P}_1(G) = f(G_{\mathcal{P}_1}) .$$

Essentially this proposition says that the $\mathfrak{p}$-components of a finite A-module behave independently.

The last information we need about $\mathcal{P}_1$-A-modules is the following :

PROPOSITION 5.7. - With the notations of proposition 5.6, we have :

$$w_k(f \circ \mathcal{P}_1 ; \mathfrak{a}) = w_k(f ; \mathfrak{a}_1)\, w_k(\mathfrak{a}_2)$$

where $\mathfrak{a}_1$ is the $\mathcal{P}_1$-part of $\mathfrak{a}$, and $\mathfrak{a}_2 = \mathfrak{a}\,\mathfrak{a}_1^{-1}$, and consequently

$$\zeta_k(f \circ \mathcal{P}_1 ; s) = \Big(\sum_{\substack{\mathfrak{a} \\ \mathfrak{p} \mid \mathfrak{a} \Rightarrow \mathfrak{p} \in \mathcal{P}_1}} w_k(f;\mathfrak{a}) (N\mathfrak{a})^{-s} \Big) \prod_{\mathfrak{p} \notin \mathcal{P}_1} \prod_{1 \le j \le k} (1-(N\mathfrak{p})^{-j-s})^{-1} .$$

Proof. - Set $\mathcal{P}_2 = \mathcal{P} - \mathcal{P}_1$. Then we clearly have $\mathfrak{a} = \mathfrak{a}_1 \mathfrak{a}_2$ with $\mathfrak{a}_i$ being the $\mathcal{P}_i$-part of $\mathfrak{a}$, and

$$w_k(f \circ \mathcal{P}_1 ; \mathfrak{a}) = \sum_{G(\mathfrak{a})} w_k(G)\, f(G_{\mathcal{P}_1}) = \sum_{G_1(\mathfrak{a}_1)} f(G_1)\, w_k(G_1) \sum_{G_2(\mathfrak{a}_2)} w_k(G_2)$$

and the first formula follows. The second one is a formal consequence of the definition of $\zeta_k(f ; s)$ and of corollary 3.7.

We can now give examples of u-probabilities and u-averages. For simplicity we assume $k = \infty$, but of course all the results can be obtained also for finite k. The proofs, being in general straightforward applications of the results of this section, will be omitted or only sketched.

It should be recalled at this point that all the constants like C_∞, $\eta_\infty(\mathfrak{p})$ etc... that have been introduced earlier, are relative to the domain A and should more properly be written C_∞^A, $\eta_\infty^A(\mathfrak{p})$, etc... .

Example 5.8. - Let $\alpha \in \mathbb{R}$. Then for $u > \alpha$ the u-average of $(\# G)^\alpha$ is equal to

$$M_u((\# G)^\alpha) = (C_u / C_\infty) \prod_{j \ge 1} \zeta_A(j + u - \alpha) .$$

In particular, if $u \ge 2$ the u-average of $\# G$ is $\zeta_A(u)$.

Example 5.9. - (i) Let L be a $\mathcal{P}_1$-group with $\# L = \ell$. Then the u-probability that the $\mathcal{P}_1$-part of an A-module be isomorphic to L is equal to :

$$\ell^{-u} (\# \mathrm{Aut}\ L)^{-1} \prod_{\mathfrak{p} \in \mathcal{P}_1} (\eta_\infty(\mathfrak{p}) / \eta_u(\mathfrak{p})) .$$

(ii) Assume that $\mathfrak{p} \mid \mathfrak{a} \Rightarrow \mathfrak{p} \in \mathcal{P}_1$. Then the u-probability that the $\mathcal{P}_1$-part of a group has A-cardinality equal to $\mathfrak{a}$ is equal to

$$(N\mathfrak{a})^{-u}\, w(\mathfrak{a}) \prod_{\mathfrak{p} \in \mathcal{P}_1} (\eta_\infty(\mathfrak{p}) / \eta_u(\mathfrak{p})) .$$

Example 5.10. - The u-probability that $G_{\mathfrak{p}} \neq 0$ is equal to

$$1 - \eta_{\infty}(\mathfrak{p}) / \eta_{u}(\mathfrak{p}) .$$

Example 5.11. - The u-probability that the $\mathcal{P}_1$-part of an A-module G is A-cyclic (i.e. $G_{\mathcal{P}_1} \simeq A/\mathfrak{a}$) is equal to

$$\prod_{\mathfrak{p} \in \mathcal{P}_1} \frac{1 - (N\mathfrak{p})^{-1} + (N\mathfrak{p})^{-u-2}}{(1-(N\mathfrak{p})^{-u-1})(1-(N\mathfrak{p})^{-1})} \frac{\eta_{\infty}(\mathfrak{p})}{\eta_{u}(\mathfrak{p})} .$$

In particular for $u = 0$ and $\mathcal{P}_1 = \mathcal{P}$ this is equal to

$$\varkappa_A \, \zeta_A(2) \, \zeta_A(3) / (\zeta_A(6) \, C_{\infty}^{A})$$

(recall that $\varkappa_A$ is the residue at $s = 1$ of $\zeta_A(s)$).

Example 5.12. - Let $\mathfrak{a}$ be an ideal. The u-average of the number of element x in a finite A-module whose annihilator is $\mathfrak{a}$ equals $(N\mathfrak{a})^{-u}$.

For example if $A = \mathbb{Z}$, the u-average of the number of elements of order $a \geq 1$ in an abelian group is a^{-u}.

Proof. - Simply note that the number of $x \in G$ such that $\mathrm{Ann}\, x = \mathfrak{a}$ is equal to

$$\varphi(\mathfrak{a}) \, \# \{ G_1 \leq G : G_1 \simeq A/\mathfrak{a} \}$$

where $\varphi(\mathfrak{a}) = \# (A/\mathfrak{a})^{*}$.

Example 5.13. - Call an A-module G elementary if for all $\mathfrak{p}$, $G_{\mathfrak{p}} \simeq (A/\mathfrak{p})^{k_{\mathfrak{p}}}$ for some $k_{\mathfrak{p}} \geq 0$, i.e. if no $A/\mathfrak{p}^{\alpha}$ occur in $G_{\mathfrak{p}}$ with $\alpha > 1$. Then :

(i) The 0-probability that a finite A-module is elementary equals

$$\Big(\prod_{\substack{k \not\equiv 1, 4 \pmod 5 \\ k \geq 2}} \zeta_A(k) \Big)^{-1}$$

(ii) The 1-probability that a finite A-module is elementary equals

$$\Big(\prod_{\substack{k \not\equiv 2, 3 \pmod 5 \\ k \geq 2}} \zeta_A(k) \Big)^{-1} .$$

(Example 5.13, (i) was suggested to us by D. Zagier.)

Proof. - Straightforward, using the easily proven fact that $\# \mathrm{Aut}\, (A/\mathfrak{p})^{m} = (N\mathfrak{p})^{m^2} \eta_m(\mathfrak{p})$ and the two identities of Rogers-Ramanujan.

§ 6. - u-probabilities and u-averages involving $\mathfrak{p}$-ranks

In this section we show how to obtain information on the distribution of $\mathfrak{p}$-ranks of finite A-modules, where $\mathfrak{p} \in \mathcal{P}$ is fixed. The first theorem is as follows :

THEOREM 6.1. - Let $\mathfrak{a}$ be an ideal of A , $\alpha = v_{\mathfrak{p}}(\mathfrak{a})$ and r a non negative integer such that $r \leq \alpha$ (otherwise the theorem is empty). Then :

$$\text{(i)} \quad \sum_{\substack{G(\mathfrak{a}) \\ r_{\mathfrak{p}}(G) = r}} w_k(G) = w_k(\mathfrak{a}) (N\mathfrak{p})^{-r^2+r} \begin{bmatrix} k \\ r \end{bmatrix}_{\mathfrak{p}} \begin{bmatrix} \alpha-1 \\ r-1 \end{bmatrix}_{\mathfrak{p}} / \begin{bmatrix} \alpha+k-1 \\ \alpha \end{bmatrix}_{\mathfrak{p}}$$

and in particular

$$\sum_{\substack{G(\mathfrak{a}) \\ r_{\mathfrak{p}}(G) = r}} w(G) = w(\mathfrak{a}) (N\mathfrak{p})^{-r^2+r} \begin{bmatrix} \alpha-1 \\ r-1 \end{bmatrix}_{\mathfrak{p}} \eta_{\alpha}(\mathfrak{p}) / \eta_r(\mathfrak{p})$$

$$\text{(ii)} \quad \sum_{\substack{G \text{ up to isomorphism} \\ G \ \mathfrak{p}\text{-A-module} \\ r_{\mathfrak{p}}(G) = r}} w_k(G) (\# G)^{-s} = \begin{bmatrix} k \\ r \end{bmatrix}_{\mathfrak{p}} (N\mathfrak{p})^{-r(r+s)} \prod_{1 \leq j \leq r} (1-(N\mathfrak{p})^{-j-s})^{-1} \quad \text{for Re } s > -1$$

and in particular if $k \geq r$:

$$\sum_{\text{same}} w_k(G) = \frac{(N\mathfrak{p})^{-r^2}}{(\eta_r(\mathfrak{p}))^2} \frac{\eta_k(\mathfrak{p})}{\eta_{k-r}(\mathfrak{p})} .$$

Proof. - (i) Write $\mathfrak{a} = \mathfrak{p}^{\alpha} \mathfrak{b}$ with $\mathfrak{p} \nmid \mathfrak{b}$. Then

$$\sum_{\substack{G(\mathfrak{a}) \\ r_{\mathfrak{p}}(G) = r}} w_k(G) = \sum_{G_1(\mathfrak{b})} w_k(G_1) \sum_{\substack{G_2(\mathfrak{p}^{\alpha}) \\ r_{\mathfrak{p}}(G_2) = r}} w_k(G_2)$$

$$= w_k(\mathfrak{b}) \sum_{\substack{G(\mathfrak{p}^{\alpha}) \\ r_{\mathfrak{p}}(G) = r}} (\# \text{ Aut } G)^{-1} \eta_k(\mathfrak{p}) / \eta_{k-r}(\mathfrak{p}) \quad \text{by proposition 3.1.}$$

Now it is easy to see that every $\mathfrak{p}$-A-module G of rank r is of the form $G = A^r/H$, and by proposition 3.1 the number of such H for a given G (with $\chi_A(G) = \mathfrak{p}^{\alpha}$) is equal to

$$((N\mathfrak{p})^{\alpha r} / \# \text{ Aut } G) \ \eta_r(\mathfrak{p}) .$$

Furthermore, given H, the conditions $\chi_A(A^r/H) = \mathfrak{p}^\alpha$ and $r_\mathfrak{p}(A^r/H) = r$ are equivalent to the conditions

$$H \subset \mathfrak{p}^r \quad \text{and} \quad \chi_A(\mathfrak{p}^r/H) = \mathfrak{p}^{\alpha-r} .$$

(Use the multiplicativity of χ_A on the exact sequence $0 \to \mathfrak{p}^r/H \to A^r/H \to (A/\mathfrak{p})^r \to 0$.) We obtain :

LEMMA 6.2.- With the above notations :

$$\sum_{\substack{G(\mathfrak{a}) \\ r_\mathfrak{p}(G) = r}} w_k(G) = \frac{w_k(\mathfrak{b})}{(N\mathfrak{p})^{\alpha r}} \begin{bmatrix} k \\ r \end{bmatrix}_\mathfrak{p} \sum_{\substack{H \subset \mathfrak{p}^r \\ \chi_A(\mathfrak{p}^r/H) = \mathfrak{p}^{\alpha-r}}} 1 .$$

Now by proposition 6.1 applied to $J = \mathfrak{p}^r$ (hence "k" = r) this last sum is equal to

$$(N\mathfrak{p})^{r(\alpha-r)}\, w_r(\mathfrak{p}^{\alpha-r}) = (N\mathfrak{p})^{(r-1)(\alpha-1)} \begin{bmatrix} \alpha-1 \\ \alpha-r \end{bmatrix}_\mathfrak{p} \qquad \text{(corollary 3.8)}$$

and theorem 6.1 (i) follows, using the fact that

$$w_k(\mathfrak{b}) = w_k(\mathfrak{a})(N\mathfrak{p})^\alpha / \begin{bmatrix} \alpha+k-1 \\ \alpha \end{bmatrix}_\mathfrak{p} .$$

The rest of the assertions in the theorem follow easily from (i) and lemma 6.2.

Applying the techniques of section 5 we easily obtain :

THEOREM 6.3.- The u-probability that the $\mathfrak{p}$-rank of a finite A-module is r is equal to

$$(N\mathfrak{p})^{-r(r+u)}\, \eta_\infty(\mathfrak{p}) / (\eta_r(\mathfrak{p})\, \eta_{r+u}(\mathfrak{p})) .$$

The final result that we want about $\mathfrak{p}$-ranks is the one giving the u-average of $(N\mathfrak{p})^{r_\mathfrak{p}(G)}$ or more generally of $(N\mathfrak{p})^{\alpha r_\mathfrak{p}(G)}$ for $\alpha \geq 0$, α integral. This will follow from the following :

THEOREM 6.4.- Let $\alpha \geq 0$ be an integer, $\mathfrak{a}$ an ideal such that $\mathfrak{p}^\alpha \mid \mathfrak{a}$. Then :

$$(N\mathfrak{a})^{-u} \sum_{G(\mathfrak{a}), \varphi_u} w_k(G) \prod_{0 \leq i < \alpha} \left((N\mathfrak{p})^{r_\mathfrak{p}(G/\mathrm{Im}\,\varphi)} - (N\mathfrak{p})^i\right) =$$

$$= (N\mathfrak{p})^{-\alpha u}\, w_k(\mathfrak{a}\mathfrak{p}^{-\alpha})\, \eta_k(\mathfrak{p}) / \eta_{k-\alpha}(\mathfrak{p}) .$$

Proof. - We can deduce theorem 6.4 from theorem 6.1 using known q-identities. We shall use the converse approach, obtaining theorem 6.4 directly and deducing the q-identities.

We apply proposition 4.5 (i) to $K = (A/\mathfrak{p})^{\alpha}$. If G is a finite A-module, the number of submodules of G isomorphic to K is clearly equal to

$$(\#\,\mathrm{Aut}(A/\mathfrak{p})^{\alpha})^{-1}\,\#\{\varphi\in \mathrm{Hom}_A((A/\mathfrak{p})^{\alpha}, G),\ \varphi \text{ injective}\}\ .$$

Now if $G^{\mathfrak{p}}$ is the subgroup of G of elements annihilated by $\mathfrak{p}$, it is clear that

$$\#\{\varphi\in \mathrm{Hom}_A((A/\mathfrak{p})^{\alpha}, G),\ \varphi \text{ injective}\} = \#\{\varphi\in \mathrm{Hom}_A((A/\mathfrak{p})^{\alpha}, G^{\mathfrak{p}}),\ \varphi \text{ injective}\}$$
$$= \prod_{0\le i<\alpha} ((N\mathfrak{p})^{r_{\mathfrak{p}}(G)} - (N\mathfrak{p})^{i}) \quad \text{since } G^{\mathfrak{p}} \simeq (A/\mathfrak{p})^{r_{\mathfrak{p}}(G)}\ .$$

Hence proposition 4.5 (i) gives

$$\sum_{G(\mathfrak{a}),\,\varphi_u} w_k(G) \prod_{0\le i<\alpha} ((N\mathfrak{p})^{r_{\mathfrak{p}}(G/\mathrm{Im}\,\varphi)} - (N\mathfrak{p})^{i}) =$$
$$= \#\,\mathrm{Aut}\,(A/\mathfrak{p})^{\alpha}\ N(\mathfrak{a}\mathfrak{p}^{-\alpha})^{u}\ w_k(\mathfrak{a}\mathfrak{p}^{-\alpha})\ w_k((A/\mathfrak{p})^{\alpha})$$

and the theorem follows from proposition 3.1.

From the definition of $M_{k,u}$ we obtain immediately :

COROLLARY 6.5. - We have :

$$M_{k,u}\Big(\prod_{0\le i<\alpha} ((N\mathfrak{p})^{r_{\mathfrak{p}}(G)} - N\mathfrak{p}^{i})\Big) = (N\mathfrak{p})^{-\alpha u}\,\eta_k(\mathfrak{p})/\eta_{k-\alpha}(\mathfrak{p})\ .$$

Example 6.6. - The u-average of $(N\mathfrak{p})^{r_{\mathfrak{p}}(G)}$ is $1+(N\mathfrak{p})^{-u}$; the u-average of $(N\mathfrak{p})^{2r_{\mathfrak{p}}(G)}$ is $1+(N\mathfrak{p}+1)(N\mathfrak{p})^{-u}+(N\mathfrak{p})^{-2u}$.

As was mentioned earlier, one can easily obtain from the combination of preceding theorems some q-identities. We leave the proofs to the reader, noting that they can also be proved directly very simply :

COROLLARY 6.7. - Write $(q)_k = \prod_{1\le n\le k} (1-q^n)$. Then for $k\ge\alpha$:

$$\sum_{\alpha\le r\le k} \frac{q^{(r+u)(r-\alpha)}}{(q)_{r-\alpha}\,(q)_{k-r}\,(q)_{r+u}} = \frac{1}{(q)_{k-\alpha}\,(q)_{k+u}}\ .$$

In particular for $k \to \infty$:

$$\sum_{r \geq \alpha} \frac{q^{(r+u)(r-\alpha)}}{(q)_{r-\alpha}\,(q)_{r+u}} = \frac{1}{(q)_\infty}$$

and with $\alpha = u = 0$:

$$\sum_{r \geq 0} q^{r^2} / (q)_r^2 = 1 / (q)_\infty \quad .$$

§ 7. - An analytic digression : the function $\zeta_\infty(s)$

We study here the properties of the function $\zeta_\infty(s)$ as a meromorphic function. They will not be needed in the sequel, but may give some hints for the proofs of the conjectures that we will state in the next sections.

In what follows we assume that A is the ring of integers of a number field K of discriminant D, degree N over $\mathbb{Q}$, r_1 real places and $2r_2$ complex ones, with $r_1 + 2r_2 = N$. Then we recall that $\zeta_A(s)$ can be analytically continued to the whole complex plane with a single pole at $s = 1$, which is simple and with residue

$$\varkappa_A = 2^{r_1} (2\pi)^{r_2} h\, R / w \,|D|^{\frac{1}{2}} .$$

where as usual h is the class number, R the regulator and w the number of roots of unity in K. Furthermore if we set

$$\Lambda_A(s) = |D|^{s/2} (\pi^{-s/2}\, \Gamma(s/2))^{r_1} ((2\pi)^{-s}\, \Gamma(s))^{r_2}\, \zeta_A(s)$$

we have the functional equation

$$\Lambda_A(s) = \Lambda_A(1-s) \quad .$$

We want to study the function $\zeta_{\infty, A}(s) = \zeta_\infty(s)$ defined in corollary 3.7. We recall that

$$\zeta_\infty(s) = \overline{\prod_{j \geq 1}}\ \zeta_A(s+j) \ .$$

Note first that the Euler product is as follows :

$$\zeta_\infty(s) = \overline{\prod_{\mathfrak{p} \in \mathcal{P}}}\ \overline{\prod_{j \geq 1}}\ (1 - (N\mathfrak{p})^{-s-j})^{-1} \quad .$$

This is formally identical with the Euler product for the reciprocal of the Selberg zeta function $Z(s)$ (see e.g. [9]) where $\mathcal{P}$ denotes in that case the set of conjugacy classes of primitive hyperbolic matrices, and $N\mathfrak{p}$ is the norm of such a class. Helped by this analogy (which shouldn't be pushed too far since $Z(s)$ satisfies the

Riemann hypothesis while $\zeta_\infty(s)$ has its zeros spread out over the whole plane) we first note that $\zeta_\infty(s)$ is a meromorphic function of order 2 (more accurately, removing the poles, $(\sin \pi s)\, \zeta_\infty(s)$ is an entire function of order 2). This is easily proven and left to the reader.

Second, we can try to find a kind of functional equation for $\zeta_\infty(s)$, involving not only Γ-factors, but also Barnes' Γ_2-function, as for $Z(s)$ (see [16]). This is easily done as a consequence of the functional equation for $\zeta_A(s)$ itself. One such result is as follows :

THEOREM 7.1. - Set

$$W_\infty(s) = |D|^{-(s(s+1))/4} \left(\left(\Gamma\left(\frac{s}{2}\right)^{-1} \Gamma_2(s) \right)^{\frac{1}{2}} \pi^{s^2/4}\, 2^{(s-1)(s-2)/4} \right)^{r_1} \times$$
$$\times \left(\Gamma(s)^{-1} \Gamma_2(s) (2\pi)^{s(s+1)/2} \right)^{r_2} \zeta_\infty(s)$$

and

$$\Lambda_\infty(s) = W_\infty(s)\, W_\infty(-s)\, \frac{\sin^2 \pi s}{\pi^2 C_\infty^2} \ .$$

Then Λ_∞ is an entire function of order 2 which is even and periodic of period 1 , such that $\Lambda_\infty(n) = 1$ for $n \in \mathbb{Z}$.

Proof. - Simply note that $W_\infty(s) / W_\infty(s-1) = 1 / \Lambda_A(s)$ and hence the periodicity of Λ_∞ is trivially equivalent to the functional equation of Λ_A .

Remark. - It is an easy exercise to check that $\left(\Gamma\left(\frac{s}{2}\right)^{-1} \Gamma_2(s) \right)^{\frac{1}{2}}$ is a (single valued) meromorphic function on $\mathbb{C}$. We choose the square root so that it is positive for s positive.

Having a natural periodic function at hand, it is natural to plot it for real values of s , and this is what the first author did on a computer in the case of $A = \mathbb{Z}$, hence $D = 1$, $r_1 = 1$, $r_2 = 0$. The astounding (and impossible) result was that $\Lambda_\infty(s)$ seemed to be constant equal to 1 for all real s . Of course this is absurd since it would then have to be equal to 1 for all complex s , which is impossible since $\Lambda_\infty(s)$ vanishes at all the complex zeroes (and their integer translates) of the Riemann zeta function $\zeta_{\mathbb{Z}}(s)$.

This apparent paradox was resolved a few days later by computing the Weierstrass product of the function $\Lambda_\infty(s)$, which turns out to be particulary simple. The result is as follows (for any domain A) :

THEOREM 7.2. -

$$\Lambda_\infty(s) = \prod_{\mathrm{Im}\,\rho>0} \left(1 - \frac{\sin^2 \pi s}{\sin^2 \pi \rho}\right)$$

where the product is over the non trivial zeroes of $\zeta_A(s)$ with positive imaginary part.

The proof is left to the reader.

In the case $A = \mathbb{Z}$, we have the first zero $\rho_1 \simeq \frac{1}{2} + 14.134\,i$ hence $\sin^2 \pi \rho_1 \simeq \mathrm{ch}^2(\pi \times 14.134) \simeq \frac{1}{4} e^{2\pi \times 14.134} \simeq 9 \times 10^{37}$ and it is easy to deduce from this and known estimates on the zeroes ρ, that for s real, $|\Lambda_\infty(s) - 1| < 2.10^{-38}$. Hence one would need multiprecision arithmetic to at least 40 decimals to be able to detect that $\Lambda_\infty(s) \neq 1$!

§ 8. - The fundamental heuristic assumptions

We begin here the second part of this paper. Except if explicitly stated otherwise, it must be considered that all the statements made in this part are conjectural. These conjectures all derive essentially from one heuristic principle which we now explain.

Let Γ be an abelian group of order N, and r_1, r_2 chosen such that $r_1 + 2r_2 = N$. Finally we let $A = A_\Gamma$ be the maximal order in the ring $\mathbb{Q}[\Gamma] / \sum_{g \in \Gamma} g$. It is well known that A_Γ is unique, and that it is a product of ring of integers of number fields.

Hence, as was mentioned at the beginning of section 2, the theory developed in part 1 is applicable to A.

Examples. - 1) If $\Gamma = \mathbb{Z}/N\mathbb{Z}$ with N prime, then $A_\Gamma = \mathbb{Z}[\sqrt[N]{1}]$, the ring of integers of the N^{th} cyclotomic field.

2) For $\Gamma = \mathbb{Z}/4\,\mathbb{Z}$ then $A_\Gamma = \mathbb{Z}[i] \times \mathbb{Z}$.

3) For $\Gamma = \mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/2\,\mathbb{Z}$ then $A_\Gamma = \mathbb{Z} * \mathbb{Z} \times \mathbb{Z}$.

We will write $\mathfrak{F}_{\Gamma, r_1, r_2}$ (or simply $\mathfrak{F}$ when there is no ambiguity on Γ, r_1, r_2) for the set of isomorphism classes of abelian extensions of $\mathbb{Q}$ with Galois group Γ, r_1 real places and $2r_2$ complex ones. Note that $\mathfrak{F}_{\Gamma, r_1, r_2} = \emptyset$ unless $r_1 = N$, $r_2 = 0$ (the totally real case) or $r_1 = 0$, $r_2 = N/2$ (the totally

complex case).

We assume the set of fields in $\mathfrak{F}$ ordered by the absolute value of the discriminant, and in the (rare) cases of equal discriminant, any ordering will do. If $K \in \mathfrak{F}$ and $\mathcal{H} = \mathcal{H}(K)$ is the prime to N part of the class group of K, it is easy to see that $\mathcal{H}$ is a finite A_Γ-module. Hence, if f is a function defined on isomorphism classes of finite A_Γ-modules (of order prime to N if necessary) we can define the average of f on the prime to N part of the class groups as the following limit, if it exists :

$$M(f) = \lim_{X \to \infty} \frac{\sum_{K \in \mathfrak{F},\ |D(K)| \leq X} f(\mathcal{H}(K))}{\sum_{K \in \mathfrak{F},\ |D(K)| \leq X} 1}$$

where $D(K)$ is the discriminant of K and $\mathcal{H}(K)$ is the prime to N part of the class group.

FUNDAMENTAL ASSUMPTIONS 8.1. - For all "reasonable" functions f (including probably non negative functions) we have :

(1) (Complex quadratic case) If $r_1 = 0$, $r_2 = 1$ then $M(f)$ is the 0-average of f restricted to A_Γ-modules of order prime to N. [Here in fact $A_\Gamma = \mathbb{Z}$, $N = 2$.]

(2) (Totally real case) If $r_1 = N$, $r_2 = 0$ then $M(f)$ is the 1-average of f restricted to A_Γ-modules of order prime to N.

For lack of experimental evidence, we do not make any assumptions in the totally complex case, except when $N = 2$. We hope to come back to this in another paper (see also section 10). Note also that in both cases, we take the u-average, where u is the A_Γ-rank of the groups of units.

In the next section we will give some consequences of these fundamental assumptions. In the rest of this section we would like to try to justify them.

The first assumption, for the complex quadratic case, is exactly the assumption mentioned in section 1, i.e. weighting isomorphism classes of abelian groups G with weight proportional to $1/\#\,\mathrm{Aut}\ G$. Since the number of group structures on a set with n elements which are isomorphic to G is $n!/\#\,\mathrm{Aut}\ G$, the assumption above, for a given n, boils down to giving equal weight to each group structure. However for different n it is difficult to compare. Hence it would

seem that one could define the 0-average of f as

$$M_0(f,\psi) = \lim_{x\to\infty} \frac{\sum_{n\le x} \psi(n) \sum_{G(n\mathbb{Z})} f(G)\, w(G)}{\sum_{n\le x} \psi(n) \sum_{G(n\mathbb{Z})} w(G)}$$

for some function ψ. Luckily, it turns out that for quite a wide class of functions ψ, including for instance the non zero polynomials, $M_0(f,\psi)$ is independent of ψ, whence the choice $\psi = 1$.

It is much more difficult to justify the second assumption. Let us assume $N = 2$ (i.e. the real quadratic case), the case of general N being a reasonable extrapolation from this case. Then it is well known that in terms of binary quadratic forms the class group can be obtained as follows : Consider the set of reduced binary quadratic forms having the right discriminant. This set is finite. In the imaginary quadratic case, composition of quadratic forms gives a group law on this set, and the group is exactly the class group. In the real quadratic case this is not true for several reasons which all boil down to the fact that the group of units is of rank 1 instead of 0. However in some sense which can be made precise, composition gives a group-like structure to this set, if we neglect a logarithmic number of reductions to be done. Furthermore this set breaks into cycles under the reduction operation, and in some sense one can interpret the principal cycle as being a "cyclic subgroup" ; finally the cycles do not have necessarily the same number of forms, but their length (in the sense of [11] or [13]) is the same, i.e. the regulator R. The number of these cycles being the class number, our heuristic assumption can be reformulated in the following way : the class group of a real quadratic field is of the form $G/\langle\sigma\rangle$, where G is a "random" group, weighted as usual with $1/\#\,\mathrm{Aut}\ G$, and σ is a random element in G (we denote by $\langle\sigma\rangle$ the cyclic subgroup of G generated by σ). The group G can then be thought of as the "group" of reduced quadratic forms, and $\langle\sigma\rangle$ as the principal cycle.

Another way of saying this is that we are trying to give a group theoretical interpretation of the trivial equality $h = hR/R$.

The "explanations" above have been put on more solid ground by the second author [11], and under this interpretation one should try to extend the techniques of the preceding sections to compact groups.

A very analogous situation was suggested to us by B. Gross. Let p be a fixed prime, and consider the set of <u>imaginary</u> quadratic fields K where p splits :

$p = \mathfrak{p}\bar{\mathfrak{p}}$. Then almost by definition $\mathcal{H}(O_K[1/\mathfrak{p}]) \simeq \mathcal{H}(O_K)/<\mathfrak{p}>$, where $O_K[1/\mathfrak{p}] = \{x \in K / \mathfrak{p}\, x \subset O_K\}$. This is exactly of the type $G/<\sigma>$, and G is weighted with $1/\#\,\mathrm{Aut}\, G$ if we assume assumption 1, and $\{\mathfrak{p}\}$ is random in $\mathcal{H}(O_K)$. Tables of such class groups reveal a striking similarity with tables of class groups of real quadratic fields.

§ 9. - Consequences of the heuristic assumptions

It must be again emphasized that all the results in this section are conjectural, except noted otherwise. No "proofs" are given since the conjectures are trivial consequences of the assumptions and the work done in the first part of the paper.

I. - Complex quadratic fields

Here $\mathcal{H}$ will denote the odd part of the class group, $h = \#\mathcal{H}$, $\mathcal{H}_p$ will be the p-part of $\mathcal{H}$, $r_p(\mathcal{H})$ will be the p-rank of $\mathcal{H}$, where p is always an odd prime.

All constants and zeta functions are relative to $A = \mathbb{Z}$.

(C 1) The probability that $\mathcal{H}$ is cyclic is equal to

$$\zeta(2)\,\zeta(3)/(3\,\zeta(6)\,C_\infty\,\eta_\infty(2)) \simeq 97.7575\ \%\ .$$

(C 2) The probability that p divides h is equal to

$$f(p) = 1 - \eta_\infty(p) = p^{-1} + p^{-2} - p^{-5} - p^{-7} + \ldots\ .$$

In particular

$$f(3) \simeq 43.987\ \%\ ;\quad f(5) \simeq 23.967\ \%\ ;\quad f(7) \simeq 16.320\ \%\ .$$

(C 3) The probability that $\mathcal{H}_3 \simeq \mathbb{Z}/9\,\mathbb{Z}$ is close to 9.335 %
" $\mathcal{H}_3 \simeq (\mathbb{Z}/3\mathbb{Z})^2$ " 1.167 %
" $\mathcal{H}_3 \simeq (\mathbb{Z}/3\,\mathbb{Z})^3$ " 0.005 %
" $\mathcal{H}_3 \simeq (\mathbb{Z}/3\,\mathbb{Z})^4$ " 2.3×10^{-8}
" $\mathcal{H}_5 \simeq \mathbb{Z}/25\,\mathbb{Z}$ " 3.802 %
" $\mathcal{H}_5 \simeq (\mathbb{Z}/5\,\mathbb{Z})^2$ " 0.158 %

(The exact formulas can easily be obtained from example 5.9 (i).).

(C 4) Let n be odd. The average number of elements of $\mathcal{H}$ of order exactly equal to n is 1.

(C 5) The probability that $r_p(\mathcal{H}) = r$ is equal to

$$p^{-r^2}\ \eta_\infty(p) \prod_{1 \le k \le r} (1 - p^{-k})^{-2}\ .$$

(C 6) The average of

$$\overline{\prod_{0\le i<\alpha}} \left(p^{r_p(\mathcal{K})} - p^i\right)$$

where α a fixed integer, is equal to 1 . In particular the average of $p^{r_p(\mathcal{K})}$ is equal to 2 and that of $p^{2r_p(\mathcal{K})}$ is equal to $p+3$.

It is a consequence of a theorem of Heilbronn-Davenport (see [5]) that the average of $3^{r_3(\mathcal{K})}$ is equal to 2 . Thus (C 6) is true for $\alpha = 1$, $p = 3$.

II. - Real quadratic fields

We keep the same notations as in the complex case. All the conjectural statements made in that case have an analog here. We give a few :

(C 7) The probability that p divides h is equal to

$$1 - \overline{\prod_{k\ge 2}} (1 - p^{-k}) = p^{-2} + p^{-3} + p^{-4} - p^{-7} - \dots \quad .$$

(C 8) Let n be odd. The average number of elements of $\mathcal{K}$ of order exactly equal to n is $1/n$.

(C 9) The probability that $r_p(\mathcal{K}) = r$ is equal to

$$p^{-r(r+1)}\, \eta_\infty(p) \overline{\prod_{1\le k\le r}} (1 - p^{-k})^{-1} \overline{\prod_{1\le k\le r+1}} (1 - p^{-k})^{-1} \quad .$$

(C 10) The average of

$$\overline{\prod_{0\le i<\alpha}} \left(p^{r_p(\mathcal{K})} - p^i\right)$$

where α is a fixed integer, is equal to $p^{-\alpha}$. In particular the average of $p^{r_p(\mathcal{K})}$ is equal to $1+p^{-1}$ and that of $p^{2r_p(\mathcal{K})}$ is equal to $2+p^{-1}+p^{-2}$.

It is again a consequence of a theorem of Heilbronn-Davenport (see [5]) that the average of $3^{r_3(\mathcal{K})}$ is equal to $4/3$. Thus (C 10) is true for $\alpha = 1$, $p = 3$.

A number of results are uninteresting in the complex case (for example the analogue of (C 11) would say that the probability that $\mathcal{K} \simeq L$ is equal to 0 , which is true since the class number tends to infinity).

(C 11) If L is a group of odd order ℓ , the probability that $\mathcal{K}$ be isomorphic to L is equal to :

$$(2\ell\, C_\infty\, \eta_\infty(2)\, \#\,\mathrm{Aut}\, L)^{-1} \quad .$$

In particular, if $p(\ell)$ is the probability that $\#\mathcal{K} = \ell$, we have :

$$p(1) \simeq 75.446\,\% \ ; \ p(3) \simeq 12.574\,\%; \ p(5) \simeq 3.772\,\% \ ;$$

$$p(7) \simeq 1.796\,\% \ ; \ p(9) \simeq 1.572\,\% \ .$$

If we make the extra assumption that fields with prime discriminants behave like the others with respect to the odd part of the class group, then $p(\ell)$ is the probability that $h = \ell$ when one restricts to prime discriminants.

(C 12) (Suggested by C. Hooley) Call $h(p)$ the class number of $\mathbb{Q}(\sqrt{p})$. Then, when p is restricted to the primes congruent to 1 mod. 4, and $x \to \infty$:

a) The probability that $h(p) > x$ is asymptotic to $\frac{1}{2x}$;

b) $\sum_{p \leq x} h(p) \sim x/8$.

III. - Higher degree fields

We give two examples :

(C 13) For cyclic cubic extensions (i.e. $\Gamma = \mathbb{Z}/3\mathbb{Z}$, $r_1 = 3$, $r_2 = 0$, $A_\Gamma = \mathbb{Z}[\sqrt[3]{1}]$) the probability that the class number is divisible by 2 (or by 4, which is the same) is equal to

$$1 - \prod_{k \geq 2} (1 - 4^{-k}) \simeq 8.195\,\% \ .$$

(C 14) For totally real extensions of prime degree p (including $p = 2$) (here $\Gamma = \mathbb{Z}/p\mathbb{Z}$, $r_1 = p$, $r_2 = 0$, $A_\Gamma = \mathbb{Z}[\sqrt[p]{1}]$) the probability that the prime to p part of the class number is 1, is equal to

$$(1 - p^{-1}) / (\eta_\infty(p) \prod_{k \geq 2} \zeta_{\mathbb{Q}(\sqrt[p]{1})}(k))$$

where $\zeta_{\mathbb{Q}(\sqrt[p]{1})}(s)$ is the Dedekind zeta function of the cyclotomic field $\mathbb{Q}(\sqrt[p]{1})$.

One can easily check that the above probability tends to 1 as $p \to \infty$. This would imply that, at least for $\mathbb{Z}/p\mathbb{Z}$-extensions, the non triviality of the class group comes only from the p-part. In fact, if we assume that we can restrict to prime conductors (as we did in the real quadratic case) the probability above is the probability that $h = 1$, when restricted to prime conductor. Hence, contrary to popular opinions, the proportion of class number 1 fields would seem to increase (and tend to 1) among fields of prime conductor. Apparently this had already been predicted by C. L. Siegel. (We thank D. Shanks for this information). Tables

seem to agree with this : we have seen that the probability is 75.446 % in the real quadratic case, and it is close to 85.0 % in the cyclic cubic case, and both are close to the observed data ([14], [7]). We lack sufficient data in the cyclic quintic case.

§ 10. - Discussion of the conjectures. Further work

A) All the conjectures that we make are in close agreement with existing tables ([3], [4], [6], [7], [14]). Furthermore a conjecture like (C 5) helps to explain why class groups with high 3-rank (for instance) are difficult to find : to our knowledge, the record is 3-rank 5 , and we have $3^{-25} \simeq 10^{-12}$ while $3^{-36} \simeq 7.10^{-18}$. This can help to give an indication of the difficulty of finding 3 - rank 6 .

B) A very nice fact is that two particular cases of our conjectures ((C 6), $\alpha = 1$, $p = 3$ and (C 10), $\alpha = 1$, $p = 3$) are in fact theorems, due to Heilbronn-Davenport. Since all the conjectures are consequences of a single heuristic principle, this gives strong support for this principle, hence for the rest of the conjectures.

C) By a completely different heuristic method, C. Hooley has also conjectured (C 12). (Personal communication)

D) We can try to obtain statistical information on class groups of complex quadratic orders and not only on maximal orders. A priori, the only information available is the formula for the class number :

$$h(D f^2) = \Big[f \prod_{\substack{\ell \mid f \\ \ell \text{ prime}}} \Big(1 - \Big(\frac{D}{\ell}\Big)/\ell\Big) \Big] h(D)$$

where D is a fundamental discriminant.

With a naïve assumption of probabilistic independence, one can obtain from (C 2) the following conjecture :

(C' 2) The probability that p divides the class number of a complex quadratic order (p an odd prime) is equal to

$$f'(p) = 1 - (1 - p^{-3})\, \eta_\infty(p) \prod_{\substack{\ell \equiv \pm 1 \pmod p \\ \ell \text{ prime},\ \ell > 2}} (1 - (\ell - 1)/2\ell^3) \times \begin{cases} 1 & \text{if } p > 3 \\ 11/12 & \text{if } p = 3 \end{cases} .$$

This gives for example

$$f'(3) \simeq 52.4664\ \% \quad ; \quad f'(5) = 25.1301\ \% \quad ; \quad f'(7) = 16.9271\ \% \ ,$$

in reasonable agreement with the tables.

E) It is interesting to notice that in many cases, the observed probabilities or averages do not oscillate around the predicted value, but seem to have a generally monotonic behavior (taken in a very wide sense) towards the predicted limit. For example, the probability that $3|h$ is around 42.5 or 43 % instead of 43.987 % for discriminants less than 10^9 (private communication of C. P. Schnorr) while in the real quadratic case with prime discriminant the proportion of class number 1 seems to decrease very slowly, and is still around 77 % for $D = 10^7$ ([14]).

F) In the totally complex case $r_1 = 0$, $r_2 = N/2$, for which we have not given any assumptions except for $N = 2$, J. Martinet (private communication) has suggested the following : if K is such a field let K_0 be its maximal real subfield. Then the 0-average of f should be the average of f taken on the <u>relative</u> class group, i.e. classes $c \in \mathcal{K}$ such that $c\bar{c} = 1$ in $\mathcal{K}$, where $\bar{}$ denotes complex conjugation.

G) It would be very interesting to extend the above conjectures to non abelian Γ, and in fact more generally to non Galois extensions of $\mathbb{Q}$. The first case to consider, for which plenty of tables are available, is the case of non cyclic cubics, either with $r_1 = 1$, $r_2 = 1$, or totally real.

The behavior of the N-part, while certainly not random, should also be investigated.

H) In most of the conjectures, values of the function $\zeta_\infty(s)$ or of an Euler factor of that function occur (see typically (C 2), (C 11)). Since we believe these conjectures to be true at least in the complex quadratic case, we are led to believe that any <u>proof</u> of these conjectures <u>must</u> use analytic functions of order 2 like $\zeta_\infty(s)$, and in fact maybe $\zeta_\infty(s)$ itself.

A confirmation of this belief comes from the fact that the only cases where the conjectures have indeed been proved using existing mathematical tools (the Heilbronn-Davenport theorems) are also the only cases in which the result does not contain Euler factors or values of functions of order 2 (with the exception of C 12, but here the difficulty lies probably in dealing with the regulator). It would in fact be very interesting to know if the Heilbronn-Davenport results can be extended to proving C 6 or C 10 with $p = 3$ and $\alpha = 2$ or with $p = 5$ and $\alpha = 1$.

Acknowledgements

It is a pleasure for us to thank our friends and colleagues B. Gross, J. Martinet, D. Shanks, L. Washington, D. Zagier for valuable discussions during the preparation of this paper and D. Buell, C. P. Schnorr, D. Shanks and H. Williams for making available to us, or even computing for us, extensive tables which have not yet been published and which confirmed our conjectures.

-:-:-:-

REFERENCES

[1] N. BOURBAKI, Algèbre commutative, ch. 2.

[2] N. BOURBAKI, Algèbre commutative, ch. 7, § 4, ex. 10.

[3] D. A. BUELL, Class groups of quadratic fields, Math. Comp. 30 (1976), 610-623.

[4] D. A. BUELL, The expectation of good luck in factoring integers-some statistics on quadratic class numbers, technical report n° 83-006, Dep^t of Computer Science, Louisiana State University/Baton Rouge.

[5] H. DAVENPORT, H. HEILBRONN, On the density of discriminants of cubic fields II, Proc. Royal Soc., A 322 (1971), 405-420.

[6] M.-N. GRAS et G. GRAS, Nombre de classes des corps quadratiques réels $\mathbb{Q}(\sqrt{m})$, $m<10\,000$, Institut de Math. Pures, Grenoble (1971-72).

[7] M.-N. GRAS, Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$, J. reine und angew. Math. 277 (1975), 89-116.

[8] P. HALL, A partition formula connected with Abelian groups, Comment. Math. Helv. 11 (1938-39), 126-129.

[9] D. HEJHAL, The Selberg trace formula for PSL(2, $\mathbb{R}$) I, Springer Lecture notes 548 (1976) and II, Springer Lecture notes 1 001 (1983).

[10] I. KAPLANSKY, Commutative rings, Allyn and Bacon (1970), p. 146.

[11] H. W. LENSTRA, Jr., On the calculation of regulators and class numbers of quadratic fields, pp 123-150 in : J. V. Armitage (ed.), Journées Arithmétiques 1980, London Math. Soc. Lecture notes series 56, Cambridge University Press (1982).

[12] J.-P. SERRE, Corps locaux, Hermann (1966).

[13] D. SHANKS, The infrastructure of real quadratic fields and its applications, proc. 1972 number theory conference, Boulder (1972).

[14] D. SHANKS, H. WILLIAMS, in preparation.

[15] G. TENENBAUM, Cours de théorie analytique des nombres, Bordeaux (1980).

[16] M.-F. VIGNÉRAS, L'équation fonctionnelle de la fonction zêta de Selberg du groupe modulaire PSL(2, $\mathbb{Z}$), Astérisque 61 (1979), 235-249.

-:-:-:-

H. COHEN
L.A. au C.N.R.S. n° 226
Mathématiques et Informatique
Université de Bordeaux
351, cours de la Libération
33405 Talence Cedex (France)

H. W. LENSTRA, Jr.
Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam
(The Netherlands)