EIN HEURISTISCHES STUDIUM

DER KLASSENGRUPPEN

von H. Cohen und J. Martinet,
in Bordeaux

=-=-=-=

Dieser Vortrag beruht auf einer Arbeit, die jetzt nicht ganz geschrieben ist ([5]). Numerische Ergebnisse für die Körper vom Grade ≤ 4 kann man jedoch in [4] finden. Diese Arbeit ist eine Verallgemeinerung der vorherigen Arbeit von Cohen and Lenstra (Journées arithmétiques de Noordwijkerhout, [3]).

Das Ziel dieses Vortrags ist Vermutungen für die Mittelwerte verschiedener Funktionen, die über die Klassengruppen der Zahlkörper erklärt sind, auszudrücken.

Es handelt sich immer um Ereignisse, die zufällig aussehen. Wenn K zum Beispiel die imaginären Zahlkörper durchläuft, ist die Teilbarkeit durch 2 der Klassenzahl von K nicht zufällig : wegen des Primzahlsatzes ist diese Klassenzahl fast immer gerade ! Wir glauben aber, daß die Teilbarkeit der Klassenzahl durch eine ungerade Primzahl zufällig ist, und ein Wert der Wahrscheinlichkeit dieser Teilbarkeit wurde in [3] vermutet : Man findet

$1-\prod_{k\geq 1}(1-p^{-k})$ (ungefähr 44 % für $p = 3$, 24 % für $p = 5$, usw. ; siehe [4]).

Gliederung des Beitrags.

I - Die Grundideen (nach [3]).
II - Die Verallgemeinerung.
III - Einige Beispiele, die die Vermutungen belegen.
IV - Numerische Ergebnisse für die p-Komponenten.

I - Die folgenden Tatsachen sind wohlbekannt :

- Wenn K die quadratischen Zahlkörper (imaginär oder reell) mit einer p-komponente der Klassengruppe der Ordnung p^2 $(p>2)$ durchläuft, ist selten diese p-Komponente nicht zyklisch.
- Die p-Komponente (und auch die Klassenzahl selbst) ist viel größer im imaginären Falle als im reellen Falle.
- Die Klassengruppen können vielleicht nicht alle Strukturen besitzen, wenn es eine Wirkung einer Galoischen Gruppe gibt.
- Die Ordnung der p-Komponente ist manchmal nicht zufällig (siehe oben).

In [3] haben die beiden Autoren die folgenden Annahmen gemacht, auf deren Grund die Vermutungen angestellt wurden :

A1 - Die Abelschen Gruppen G müssen mit dem Gewicht $\frac{1}{|\mathrm{Aut}(G)|}$ gezählt werden. ($|A|$ ist stets die Ordnung der Gruppe A).

A2 - Weil der Rang der Einheitengruppe eines reellen quadratichen Zahlkörpers K gleich eins ist, sind im reellen Falle die Ergebnisse für Cl_K gleich den Ergebnissen, die wir für $Cl_K/\langle x\rangle$ im imaginären Falle gefunden haben, wobei x ein zufälliges Element von Cl_K ist.

A3 - Wenn K zyklisch vom ungeraden Primzahlgrade ℓ ist, muß man Cl_K als Modul über den Ring $\mathbf{Z}[\zeta_\ell]$ betrachten, wobei ζ_ℓ eine Einheitswurzel der Ordnung ℓ ist. Dann muß man $\mathrm{Aut}_{\mathbf{Z}[\zeta_\ell]}(Cl_K)$ statt $\mathrm{Aut}_{\mathbf{Z}}(Cl_K)$ betrachten, und die Einheitengruppe ist nun vom Rang 1.

A4 - Man darf nicht die Klassengruppe Cl_K selbst betrachten, sondern eine Untergruppe Cl_K^S von Cl_K, wobei S eine endliche Menge von Primzahlen ist (die "schlechte Primzahlen") und Cl_K^S ist das Produkt der p-Komponenten von Cl_K mit $p \in S$. (Für K/Q zyklisch vom Primzahlgrade ℓ ist $S = \{\ell\}$.)

Über diese Tatsachen konnten Cohen und Lenstra den u-Mittelwert einer positiven Funktion, die über die Isomorphismenklassen von endlichen Moduln erklärt wurde, definieren (u ist eine positive ganze Zahl, nähmlich der kommende Einheitenrang ; es handelt sich um Moduln über $\mathbf{Z}$ oder über $\mathbf{Z}[\zeta_\ell]$). Est wird immer vorausgesetzt, daß die Grenzwerte in $[0, +\infty]$ existieren. In den Anwendungen beschränkt man sich auf Moduln, deren Ordnungen durch die schlechte Primzahlen nicht teilbar sind.

1.1. DEFINITION. Der **u-Mittelwert** von f ist

$$M_u(f)= \lim_{x\to\infty} \frac{N_{u,x}(f)}{N_{u,x}(1)}, \text{ wobei der Zähler}$$

$$N_{u,x}(f)= \sum_{|G|\leq x} |G|^{-u} \sum_{\psi\in \mathrm{Hom}(P,G)} \frac{f(G/\mathrm{Im}\psi)}{|\mathrm{Aut}(G)|} \quad \text{ist.}$$

(P ist ein projectiver Modul vom Rang u ; der Zähler hängt von u (nicht von P) ab.)

Mit dieser Definition können wir die grundheuristische Hypothese schreiben.

1.2. DEFINITION. Für f wie oben sei es

$$M(f) = \lim_{x\to\infty} \frac{\sum_{|d_K|\leq x} f(CL_K^S)}{\sum_{|d_K|\leq x} 1}$$

Hier durchlaüft K die zyklischen Körper mit vorgegebenem Grade ℓ und vorgegebener Zerlegung der reellen Bewertungen falls $\ell=2$.

1.3. Grundheuristische Annahme. Der Grenzwert existiert, und es gilt $M(f)=M_u(f)$, wobei u der Rang der Einheitengruppe ist.

Um die Grenzwerte zu errechnen soll man Dirichletsche Reihen betrachten. Dieses wird im allgeweinen Falle am Ende des 2.§ getan.

II - In diesem Abschnitt betrachten wir Galoissche Erweiterungen K/K_0, wobei der Zahlkörper K_0 (bis auf Isomorphismus) und die Zerlegung der unendlichen Bewertungen von K_0 in K (genauer : die unendlischen Frobeniussubstitutionen bis auf Konjugation) vorgeschrieben sind. Es sei **e** ein Idempotent des Zentrums von $\mathbb{Q}[\Gamma]$.

2.1. DEFINITION. Eine Primzahl p heißt ***gut*** (sonst ***schlecht***) wenn $e \in \mathbb{Z}_p[\Gamma]$ und $e\mathbb{Z}_p[\Gamma]$ eine Maximalordnung in $\mathbb{Q}_p[\Gamma]$ ist. Die Menge der schlechten Primzahlen wird durch **S** bezeichnet werden.

Diese Definition erlaubt uns die Gruppen eCl_K^S zu betrachten. Sie sind Moduln über die Maximalordnung $\mathfrak{M} = e\mathbb{Z}[S^{-1}][\Gamma]$ von $\mathbb{Z}[S^{-1}]$ in $e\mathbb{Q}[\Gamma]$. Es sei χ der zu e gehörende Charakter, $\chi_1, \chi_2,\dots\chi_r$ seine unreduzierbaren Komponente und $e_1, e_2,\dots,e_r$ die zu $\chi_1, \chi_2,\dots,\chi_r$ gehörenden Idempotente. Für die halbeinfache Algebra $e\mathbb{Q}[\Gamma]$ und die Maximalordnung $\mathfrak{M}$ gelten die direkten Zerlegungen $e\mathbb{Q}[\Gamma] = \prod_i e_i\mathbb{Q}[\Gamma]$ und $\mathfrak{M} = \prod_i e_i\mathfrak{M}$, und jeder $\mathfrak{M}$-Modul M läßt sich in der Form $\oplus_i e_iM$ zerlegen.

2.2. DEFINITION. Es sei D_i der (bis auf Isomorphismus eindeutige bestimmte) Schiefkörper, für welche $e_i\mathbb{Q}[\Gamma]$ zu einer Algebra $M_{h_i}(D_i)$ isomorph ist. Der ***Rang*** eines projektiven $\mathfrak{M}$-Moduls P ist

$$u=(u_1,u_2,\dots,u_r) \text{ wobei } u_i = \frac{1}{h_i} \dim_{D_i} (\mathbb{Q}\otimes P) \text{ ist.}$$

Um die Definition 1.1. zu verallgemeinern betrachten wir nun nur die über die Isomorphismenklassen von $\mathfrak{M}$-Moduln erklärten Funktionen, die als Produkte von Funktionen über $e_i\mathfrak{M}$-moduln sich schreiben lassen.

2.3. DEFINITION. Es seien G ein endlicher $\mathfrak{M}$-Modul und $u=(u_1,\dots,u_r)$ der Rang eines projektiven $\mathfrak{M}$-Moduls P. Dann ist $|G|^u$ das Produkt $\prod |G_i|^{u_i}$.

Die Verallgemeinerung der Definition 1.1. ist nun leicht zu schreiben, und außerdem können wir auf eine einfache Algebra $A = e\mathbb{Q}[\Gamma]$ uns beschränken. Die Definition 1.2. lä t sich auch leicht mit $f(eCl_K^S)$ anstatt $f(Cl_K^S)$ verallgemeinern. Nur sollen wir den Einheitenrang u errechnen um die Definition 1.3 im allgemeinen Falle zu schreiben. Dieses wird mit Hilfe des Satzes von Herbrand getan.

2.4. SATZ VON HERBRAND. Für jede undendliche Primstelle v von K_0 sei Γ_v die Zerlegungsgruppe einer bestimmten Primstellen w von K über v (Γ_v ist bis auf Konjugation erklärt). Dann ist der Charakter des Γ-Moduls $\mathbb{Q}\otimes E_K$ gleich

$$\chi_E = -1+ \sum_v \mathrm{Ind}_{\Gamma_v}^{\Gamma} (1_{\Gamma_v}).$$

Dann gilt es $e_\chi Cl_L \simeq Cl_K \times Cl_K$, und $e_\chi Z_p[\Gamma] \simeq M_2(Z_p)$ für $p \neq 3$. So ist 3 die einzige schlechte Primzahl und für $p \neq 3$ teilt p die Ordnungen der Gruppen Cl_L und $Cl_K \times Cl_K$ mit gleicher Wahrscheinlichkeit. Nach 2.4. ist $u = 1$ für L total-reell und $u = 1/2$ sonst. Man findet für diese Wahrscheinlichkeiten

$$1 - \prod_{k\geq 3}(1-p^{-k}) \text{ im reellen Falle und}$$

$$1 - \prod_{k\geq 2}(1-p^{-k}) \text{ im imaginären Falle.}$$

Für $p \neq 2,3$ ist die letzte Formel gleich der Formel der reellen quadratischen Körper (siehe aber die Bemerkung 3.7).

III - Wir geben in diesem Abschnitt einige Beispiele, die zeigen, daß unsere Vermutungen stimmen. Wir schreiben $pr(p|h_K)$ für die Wahrscheinlichkeit, daß p $|Cl_K|$ teilt, usw...

3.1. Lange Tabellen existieren für quadratischen Körper, imaginär (besonders Buell, [1]) oder reell, für zyklische kubische Körper (Frau Gras, [7]), und für reine kubische Körper $\mathbb{Q}(\sqrt{p})$ mit $p \equiv -1$ modulo 3 (Williams, [9] ; diese Körper sind genau die reinen Körper, deren Klassenzahl durch 3 nicht teilbar sind). Diese Tabellen zeigen eine gute Übereinstimmung der Tatsachen mit den vermutungen.

3.2. Die Vermutungen zeigen, daß $pr(h_K=m)=0$ wenn K von C.M. Typus über einem gegebenen total-reellen Körper ist ($h_K = Cl_K$ mod. 2 - Komponente). Das ist eine Folgerung des Satzes von Brauer und Siegel, wenn man sich auf Körper mit einer ungeraden Relativklassenzahl beschränkt.

3.3. Ein Satz von Davenport und Heilbronn gibt die Dichte der kubischen Diskriminanten, und ermöglicht die Errechnung des Mittelwerts einer mit den 3- Komponenten der Klassengruppen quadratischen Körper verbundener Funktion (siehe [3], § 9, C_5 und C_{10}).

3.4. Der Spiegelungssatz von Scholz ([8]) zeigt eine Beziehung der 3-Ränge der Klassengruppen der Körper $\mathbb{Q}(\sqrt{m})$ und $\mathbb{Q}(\sqrt{-3m})$ zueinander. Es war von Georges Gras bemerkt, daß man die Vermutungen für den 3-Rang im reellen Falle auf Grund der Vermutungen im imaginären Falle beweisen kann.

3.5. Für die nicht-primitiven Körper vom Grade 4 gibt es mehrere Verfahren um die heuristischen Ergebnisse zu berechnen. Diese verschiedenen Verfahren sind miteinander verträglich.

3.6. Ein Satz von Gerth ([6]) errechnet die Mittelwerte der 4-Ränge der Klassengruppen der quadratischen Zahlkörper. Die Mittelwerte sind gleich den Ergebnissen, die wir in 2.8. gefunden hätten, wenn p den Wert 2 haben könnte. So soll der Rang von ${}_4Cl_K/{}_2Cl_K$ ein zufälliges Ereignis sein.

3.7. **Bemerkung.** Wenn man die Ergebenisse des Beispiels 2.8. für quadratische Körper benutzt, kann man auf Primdiskriminanten, die zu einer gegebenen Kongruenzklasse gehören, sich beschränken. Wahrscheinlich gilt auch diese Möglichkeit für die Führer der kubischen Körper, wenn $p \neq 2$ ist. Die Primzahl 2 aber ist speziell : wegen der 2- Komponente scheint nach der Tabellen die Dichte der Körper $k = \mathbb{Q}(\sqrt[3]{p})$ ($p \equiv -1$ mod.3) mit $h_K=1$ größer für $p \equiv 8$ als für $p \equiv 2$ oder 5 mod.9 : Nur der Mittelwert der drei Kongruenzklassen für wachsenden Diskriminanten erreicht die vorgesehene Dichte (siehe [4], III). Wahrscheinlich sind die gute p, die die Ordnung von Γ teilen, nicht ganz gut !

IV - Wir geben in diesem letzten Abschnitt einige Ergebnisse, die p- Komponenten betreffen, und prüfen die Annahmen 1 und 2 mit diesen (vermutlichen) Ergebnissen nach. Diese Ergebnisse sind nicht in [4] geschrieben.

4.1. Nach [3], Example 5-9, (i), gilt für eine Abelsche p-Gruppe H und einen ganzen Rang u

$$pr(Cl_{K,p} \simeq H) = \frac{1}{|\mathrm{Aut}H|\cdot|H|^u} \prod_{k\geq u+1}\left(1 - \frac{1}{p^k}\right)$$

(man nehme u=0 (bzw. u=1) für K imaginär- (bzw. reell-) quadratisch). Die genauen Werte von $|\mathrm{Aut}\ |G|)$ wurden von Cohen in [2] berechnet.

Für $H \simeq \bigoplus_i (Z/p^iZ)^{m_i}$ gilt ([3], prop. 2.5)

$$|\mathrm{Aut}\ H| = p^{\Sigma M_i^2} \prod_i \prod_{1\leq k\leq M_i} (1-p^{-k}), \text{ wo}$$

$$M_i = m_i + m_{i+1} + \cdots,$$

und ferner die einfache Formel ([3], Cor. 3.2)

$$\sum_{|H|=p^\alpha} \frac{1}{|\mathrm{Aut}\, H|} = p^{-\alpha}(1-p^{-1})\dots(1-p^{-\alpha}).$$ So ist

$$\mathrm{pr}\,(|Cl_{K,p}| = p^\alpha) = \frac{1}{p^{\alpha(u+1)}} \; \frac{\alpha(p)}{\prod_{1\leq k\leq \alpha}(1-p^{-k}) \prod_{1\leq k\leq u}(1-p^{-k})}\,,$$ wo

$$\alpha(p) = \prod_{k\geq 1}(1-p^{-k})$$

(siehe [3], Example 5-9, (ii)).

4.2. Die Annahme A_1 ist klar für die p-Komponenten nach der oben angeführten Formeln.

4.3. Für eine p-Gruppe H ist die Anzahl der Elementen $x \in H$ mit $|H/\langle x\rangle| = p$ gleich

- 0 für $|H| = 1$, für Rang $(H)\geq 3$ und für $H \simeq (p^r, p^s)$ mit $r,s\geq 2$;
- 1 für $|H| = p$;
- $p^{r-1}-p^{r-2}$ für $H \simeq (p,p)$;
- p^2-1 für $H \simeq (p^r,p)$, $r\geq 2$.

Mit Hilfe der Ergebnisse für den imaginären Fall muß man für die reellen quadratischen Körper

$$\mathrm{pr}(|Cl_K|=p) = \alpha(p)\left[\frac{1}{p}\cdot\frac{1}{p-1} + \frac{p-1}{p^2}\sum_{r=2}^{\infty}\frac{1}{p^r-p^{r-1}} + \frac{1}{(p^2-1)(p^2-p)}\right.$$

$$\left. + \frac{p-1}{p}\sum_{r\geq 2}\frac{1}{p^{r+1}(p-1)^2}\right]$$ finden.

Es ist leicht nachzuweisen, daß die Summe gleich $\dfrac{\alpha(p)}{(p-1)^2}$ ist, d.h. die Wahrschbeinlichkeit, daß $|Cl_{K,p}| = p$ für reelle quadratische Körper.

Literaturverzeichnis

[1] D.A. BUELL.- *The expectation of success using a Monte-Carlo factoring method - Some statistics on quadratic class numbers*, Math. Comp. 43 (1984), 313-327.

[2] H. COHEN.- *On the p^k-rank of finite obelian groups and Andrews' generalizations of the Rogers - Ramanujan identities*, Proc. Kon. Ned. Akad. Wetens. A88 (1985), 377-383.

[3] H. COHEN und H.W.LENSTRA.- *Heuristics on class groups of number fields*, Springer Lecture Notes 1068, Heildelberg, 1984, 33-62.

[4] H. COHEN und J. MARTINET.- *Class groups of number fields : Numerical heuristics*, Math. Comp. (1987), erscheint demnächst.

[5] H. COHEN und J. MARTINET.- *Etude heuristique des groupes de classes*, in Vorbereitung.

[6] F. GERTH.- *The 4-class ranks of quadratic fields*, Invent. Math. 77 (1984), 489-515.

[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 angew. Math. 277 (1975), 89-116.

[8] A. SCHOLZ.- *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J.reine angew. Math. 166 (1932), 201-203.

[9] H.C. WILLIAMS.- In Vorbereitung.

H. Cohen
Mathématiques et Informatique
Université de Bordeaux I
351, cours de la Libération
F-33405 TALENCE

J. Martinet
Mathématiques et Informatique
Université de Bordeaux I
351, cours de la Libération
F-33405 TALENCE