Asymptotics of Number Fields: Theory and Computation

Henri Cohen

Institut de Mathématiques de Bordeaux

January 31, 2011, MSRI Berkeley

Number Fields

Recall that a number field K is a finite extension of $\mathbb{Q}$. Its elements are algebraic numbers. Examples :

$$K = \mathbb{Q}(\sqrt{2})\ \ K = \mathbb{Q}(\sqrt{5})\ \ K = \mathbb{Q}(i),\ \ K = \mathbb{Q}(e^{2i\pi/5})\ .$$

These are abelian extensions (see below). Or

$$K = \mathbb{Q}(\alpha) \quad \text{with} \quad \alpha^3 - \alpha - 1 = 0\ .$$

This is nonabelian.

The set of all algebraic integers (roots of monic polynomials in $\mathbb{Z}[X]$) in K forms a ring (of course an integral domain), denoted $\mathbb{Z}_K$ and also called the maximal order of K. Its essential property is that it is a Dedekind domain : existence and essentially unique factorization of an ideal as a power product of prime ideals. NOT TRUE for suborders, e.g., $\mathbb{Z}[\sqrt{5}]$ is not Dedekind.

Number Fields

Recall that a number field K is a finite extension of $\mathbb{Q}$. Its elements are algebraic numbers. Examples :

$$K = \mathbb{Q}(\sqrt{2})\ \ K = \mathbb{Q}(\sqrt{5})\ \ K = \mathbb{Q}(i),\ \ K = \mathbb{Q}(e^{2i\pi/5})\ .$$

These are abelian extensions (see below). Or

$$K = \mathbb{Q}(\alpha) \quad \text{with} \quad \alpha^3 - \alpha - 1 = 0\ .$$

This is nonabelian.

The set of all algebraic integers (roots of monic polynomials in $\mathbb{Z}[X]$) in K forms a ring (of course an integral domain), denoted $\mathbb{Z}_K$ and also called the maximal order of K. Its essential property is that it is a Dedekind domain : existence and essentially unique factorization of an ideal as a power product of prime ideals. NOT TRUE for suborders, e.g., $\mathbb{Z}[\sqrt{5}]$ is not Dedekind.

Field-Theoretic Invariants of a Number Field I

A nf first has invariants which are mainly linked to the field structure, and not so much on the ring structure of $\mathbb{Z}_K$. Its most important are :

- Its degree $n = [K : \mathbb{Q}]$, the dimension of K as a $\mathbb{Q}$-vector space.
- Its signature (r_1, r_2) with $r_1 + 2r_2 = n$, number of real and half the number of complex embeddings of K.
- The Galois group G of its Galois closure (abuse : call the Galois group even if $K/\mathbb{Q}$ not Galois), considered as a permutation group on the roots of a defining polynomial for G, hence with an embedding into the symmetric group S_n, a permutation representation. It will be a transitive subgroup.

Field-Theoretic Invariants of a Number Field I

A nf first has invariants which are mainly linked to the field structure, and not so much on the ring structure of $\mathbb{Z}_K$. Its most important are :

- Its degree $n = [K : \mathbb{Q}]$, the dimension of K as a $\mathbb{Q}$-vector space.
- Its signature (r_1, r_2) with $r_1 + 2r_2 = n$, number of real and half the number of complex embeddings of K.
- The Galois group G of its Galois closure (abuse : call the Galois group even if $K/\mathbb{Q}$ not Galois), considered as a permutation group on the roots of a defining polynomial for G, hence with an embedding into the symmetric group S_n, a permutation representation. It will be a transitive subgroup.

Field-Theoretic Invariants of a Number Field I

A nf first has invariants which are mainly linked to the field structure, and not so much on the ring structure of $\mathbb{Z}_K$. Its most important are :

- Its degree $n = [K : \mathbb{Q}]$, the dimension of K as a $\mathbb{Q}$-vector space.
- Its signature (r_1, r_2) with $r_1 + 2r_2 = n$, number of real and half the number of complex embeddings of K.
- The Galois group G of its Galois closure (abuse : call the Galois group even if $K/\mathbb{Q}$ not Galois), considered as a permutation group on the roots of a defining polynomial for G, hence with an embedding into the symmetric group S_n, a permutation representation. It will be a transitive subgroup.

Field-Theoretic Invariants of a Number Field I

A nf first has invariants which are mainly linked to the field structure, and not so much on the ring structure of $\mathbb{Z}_K$. Its most important are :

• Its degree $n = [K : \mathbb{Q}]$, the dimension of K as a $\mathbb{Q}$-vector space.

• Its signature (r_1, r_2) with $r_1 + 2r_2 = n$, number of real and half the number of complex embeddings of K.

• The Galois group G of its Galois closure (abuse : call the Galois group even if $K/\mathbb{Q}$ not Galois), considered as a permutation group on the roots of a defining polynomial for G, hence with an embedding into the symmetric group S_n, a permutation representation. It will be a transitive subgroup.

Field-Theoretic Invariants of a Number Field II

Conjecture (Inverse Galois Problem). For any transitive subgroup G of S_n there exists a number field K of degree n over $\mathbb{Q}$ with Galois group (of Galois closure) isomorphic to G.
In fact conjecture infinitely many.

Note that if we allow the base field to vary (not $\mathbb{Q}$) the result is trivially true.
Sample results :

• Equivalent to same with added condition totally real $r_2 = 0$ (J.-P. Serre).

• True for all transitive subgroups of S_n for $n \leq 15$ (Klüners–Malle).

• True for 25 of the 26 sporadic simple groups, with the exception of the Mathieu group M_{23} (realizable over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-23})$).

• However, absolutely not known for all the infinite families of simple groups, except for instance for A_n.

Field-Theoretic Invariants of a Number Field II

Conjecture (Inverse Galois Problem). For any transitive subgroup G of S_n there exists a number field K of degree n over $\mathbb{Q}$ with Galois group (of Galois closure) isomorphic to G.
In fact conjecture infinitely many.

Note that if we allow the base field to vary (not $\mathbb{Q}$) the result is trivially true.
Sample results :

- Equivalent to same with added condition totally real $r_2 = 0$ (J.-P. Serre).
- True for all transitive subgroups of S_n for $n \leq 15$ (Klüners–Malle).
- True for 25 of the 26 sporadic simple groups, with the exception of the Mathieu group M_{23} (realizable over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-23})$).
- However, absolutely not known for all the infinite families of simple groups, except for instance for A_n.

Field-Theoretic Invariants of a Number Field II

Conjecture (Inverse Galois Problem). For any transitive subgroup G of S_n there exists a number field K of degree n over $\mathbb{Q}$ with Galois group (of Galois closure) isomorphic to G.
In fact conjecture infinitely many.

Note that if we allow the base field to vary (not $\mathbb{Q}$) the result is trivially true.
Sample results :

- Equivalent to same with added condition totally real $r_2 = 0$ (J.-P. Serre).
- True for all transitive subgroups of S_n for $n \leq 15$ (Klüners–Malle).
- True for 25 of the 26 sporadic simple groups, with the exception of the Mathieu group M_{23} (realizable over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-23})$).
- However, absolutely not known for all the infinite families of simple groups, except for instance for A_n.

Field-Theoretic Invariants of a Number Field II

Conjecture (Inverse Galois Problem). For any transitive subgroup G of S_n there exists a number field K of degree n over $\mathbb{Q}$ with Galois group (of Galois closure) isomorphic to G.
In fact conjecture infinitely many.

Note that if we allow the base field to vary (not $\mathbb{Q}$) the result is trivially true.
Sample results :

- Equivalent to same with added condition totally real $r_2 = 0$ (J.-P. Serre).
- True for all transitive subgroups of S_n for $n \leq 15$ (Klüners–Malle).
- True for 25 of the 26 sporadic simple groups, with the exception of the Mathieu group M_{23} (realizable over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-23})$).
- However, absolutely not known for all the infinite families of simple groups, except for instance for A_n.

Field-Theoretic Invariants of a Number Field II

Conjecture (Inverse Galois Problem). For any transitive subgroup G of S_n there exists a number field K of degree n over $\mathbb{Q}$ with Galois group (of Galois closure) isomorphic to G.
In fact conjecture infinitely many.

Note that if we allow the base field to vary (not $\mathbb{Q}$) the result is trivially true.
Sample results :

- Equivalent to same with added condition totally real $r_2 = 0$ (J.-P. Serre).
- True for all transitive subgroups of S_n for $n \leq 15$ (Klüners–Malle).
- True for 25 of the 26 sporadic simple groups, with the exception of the Mathieu group M_{23} (realizable over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-23})$).
- However, absolutely not known for all the infinite families of simple groups, except for instance for A_n.

Field-Theoretic Invariants of a Number Field II

Conjecture (Inverse Galois Problem). For any transitive subgroup G of S_n there exists a number field K of degree n over $\mathbb{Q}$ with Galois group (of Galois closure) isomorphic to G.
In fact conjecture infinitely many.

Note that if we allow the base field to vary (not $\mathbb{Q}$) the result is trivially true.
Sample results :

- Equivalent to same with added condition totally real $r_2 = 0$ (J.-P. Serre).
- True for all transitive subgroups of S_n for $n \leq 15$ (Klüners–Malle).
- True for 25 of the 26 sporadic simple groups, with the exception of the Mathieu group M_{23} (realizable over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-23})$).
- However, absolutely not known for all the infinite families of simple groups, except for instance for A_n.

Ring-Theoretic Invariants of a Number Field I

There are many specifically ring-theoretic invariants of a nf. Its most important are :

- Its discriminant $d(K)$ (know that $\mathrm{sign}(\mathrm{d}(\mathrm{K}))=(-1)^{\mathrm{r}_2}$ and $d(K)\equiv 0,1 \pmod 4$ by a theorem of Stickelberger). This is a reasonable measure of the size of number field, but other measures can be used. Note that $p \mid d(K)$ iff p ramifies in $K/\mathbb{Q}$, so weak measure of ramification.
- The prime ideals, and the decomposition of prime numbers as power products of prime ideals.
- All this is encoded in the Dedekind zeta function $\zeta_K(s)$ of K, defined by

$$\zeta_K(s)=\sum_{\mathfrak{a}}\frac{1}{\mathcal{N}(\mathfrak{a})^s}=\prod_{\mathfrak{p}}\frac{1}{1-\mathcal{N}(\mathfrak{p})^{-s}}\;,$$

the sum on (nonzero) integral ideals of K, the product on (nonzero) prime ideals. Essential property : functional equation $s\mapsto 1-s$ (Hecke, Tate).

Ring-Theoretic Invariants of a Number Field I

There are many specifically ring-theoretic invariants of a nf. Its most important are :

• Its discriminant $d(K)$ (know that $\mathrm{sign}(\mathrm{d}(\mathrm{K})) = (-1)^{\mathrm{r}_2}$ and $d(K) \equiv 0, 1 \pmod 4$) by a theorem of Stickelberger). This is a reasonable measure of the size of number field, but other measures can be used. Note that $p \mid d(K)$ iff p ramifies in $K/\mathbb{Q}$, so weak measure of ramification.

• The prime ideals, and the decomposition of prime numbers as power products of prime ideals.

• All this is encoded in the Dedekind zeta function $\zeta_K(s)$ of K, defined by

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathcal{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \mathcal{N}(\mathfrak{p})^{-s}},$$

the sum on (nonzero) integral ideals of K, the product on (nonzero) prime ideals. Essential property : functional equation $s \mapsto 1 - s$ (Hecke, Tate).

Ring-Theoretic Invariants of a Number Field I

There are many specifically ring-theoretic invariants of a nf. Its most important are :

- Its discriminant $d(K)$ (know that $\mathrm{sign}(d(K)) = (-1)^{r_2}$ and $d(K) \equiv 0, 1 \pmod 4$) by a theorem of Stickelberger). This is a reasonable measure of the size of number field, but other measures can be used. Note that $p \mid d(K)$ iff p ramifies in $K/\mathbb{Q}$, so weak measure of ramification.

- The prime ideals, and the decomposition of prime numbers as power products of prime ideals.

- All this is encoded in the Dedekind zeta function $\zeta_K(s)$ of K, defined by

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathcal{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \mathcal{N}(\mathfrak{p})^{-s}} ,$$

the sum on (nonzero) integral ideals of K, the product on (nonzero) prime ideals. Essential property : functional equation $s \mapsto 1 - s$ (Hecke, Tate).

Ring-Theoretic Invariants of a Number Field I

There are many specifically ring-theoretic invariants of a nf. Its most important are :

• Its discriminant $d(K)$ (know that $\mathrm{sign}(d(K)) = (-1)^{r_2}$ and $d(K) \equiv 0, 1 \pmod 4$ by a theorem of Stickelberger). This is a reasonable measure of the size of number field, but other measures can be used. Note that $p \mid d(K)$ iff p ramifies in $K/\mathbb{Q}$, so weak measure of ramification.

• The prime ideals, and the decomposition of prime numbers as power products of prime ideals.

• All this is encoded in the Dedekind zeta function $\zeta_K(s)$ of K, defined by

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathcal{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \mathcal{N}(\mathfrak{p})^{-s}} ,$$

the sum on (nonzero) integral ideals of K, the product on (nonzero) prime ideals. Essential property : functional equation $s \mapsto 1 - s$ (Hecke, Tate).

Ring-Theoretic Invariants of a Number Field II

Slightly more subtle invariants are :

- The class group $Cl(K)$ and its cardinality the class number $h(K) = |Cl(K)|$, which measures the nonuniqueness of decomposition into prime elements.
- The group of units $U(K)$ (invertible elements of Z_K), and its "logarithmic volume" $R(K)$, called the regulator of K.

The Dedekind zeta function contains information about this : its residue at $s = 1$ is an easy multiple of $h(K)R(K)$. Better expressed at $s = 0$:

$$\zeta_K(s) \sim -\frac{h(K)R(K)}{w(K)} s^{r_1+r_2-1} ,$$

where $w(K) = |U(K)_{\text{tors}}|$ is the number of roots of unity in K, $r_1 + r_2 - 1$ rank of unit group.

However the product $h(K)R(K)$ makes it very difficult to separate properties of the class group and the unit group.

Ring-Theoretic Invariants of a Number Field II

Slightly more subtle invariants are :

- The class group $Cl(K)$ and its cardinality the class number $h(K) = |Cl(K)|$, which measures the nonuniqueness of decomposition into prime elements.
- The group of units $U(K)$ (invertible elements of Z_K), and its "logarithmic volume" $R(K)$, called the regulator of K.

The Dedekind zeta function contains information about this : its residue at $s = 1$ is an easy multiple of $h(K)R(K)$. Better expressed at $s = 0$:

$$\zeta_K(s) \sim -\frac{h(K)R(K)}{w(K)} s^{r_1+r_2-1} ,$$

where $w(K) = |U(K)_{\text{tors}}|$ is the number of roots of unity in K, $r_1 + r_2 - 1$ rank of unit group.

However the product $h(K)R(K)$ makes it very difficult to separate properties of the class group and the unit group.

Results and Conjectures I

Hermite : the set of isomorphism classes of nf of given discriminant D is finite, equivalently the number $N(X)$ of iso. cl. of nf with $|d(K)| \leq X$ is finite.

Conjecture : the cardinality of the set of iso. cl. of nf with given $d(K) = D$ is $O(|D|^{\varepsilon})$ for all $\varepsilon > 0$.

Trivial for quadratic fields, but not even known for cubic fields : $O(|D|^{1/2})$ easy, but Pierce, then Helfgott–Venkatesh who obtain $O(|D|^{0.442})$.

Minkowski : if $K \neq \mathbb{Q}$ then $|d(K)| > 1$, and in fact $|d(K)| > C^n$ with $n = [K : \mathbb{Q}]$ for some $C > 1$, more precisely $|d(K)| > C_1^{r_1} C_2^{r_2}$ with $C_1 > 1$, $C_2 > 1$.

Minkowski used geometry of numbers. Best constants known by analytic methods initiated by H. Stark, followed by A. Odlyzko and several others. Assuming GRH, constants very close to optimal.

Results and Conjectures I

Hermite : the set of isomorphism classes of nf of given discriminant D is finite, equivalently the number $N(X)$ of iso. cl. of nf with $|d(K)| \leq X$ is finite.

Conjecture : the cardinality of the set of iso. cl. of nf with given $d(K) = D$ is $O(|D|^{\varepsilon})$ for all $\varepsilon > 0$.

Trivial for quadratic fields, but not even known for cubic fields : $O(|D|^{1/2})$ easy, but Pierce, then Helfgott–Venkatesh who obtain $O(|D|^{0.442})$.

Minkowski : if $K \neq \mathbb{Q}$ then $|d(K)| > 1$, and in fact $|d(K)| > C^n$ with $n = [K : \mathbb{Q}]$ for some $C > 1$, more precisely $|d(K)| > C_1^{r_1} C_2^{r_2}$ with $C_1 > 1$, $C_2 > 1$.

Minkowski used geometry of numbers. Best constants known by analytic methods initiated by H. Stark, followed by A. Odlyzko and several others. Assuming GRH, constants very close to optimal.

Results and Conjectures I

Hermite : the set of isomorphism classes of nf of given discriminant D is finite, equivalently the number $N(X)$ of iso. cl. of nf with $|d(K)| \le X$ is finite.

Conjecture : the cardinality of the set of iso. cl. of nf with given $d(K) = D$ is $O(|D|^{\varepsilon})$ for all $\varepsilon > 0$.

Trivial for quadratic fields, but not even known for cubic fields : $O(|D|^{1/2})$ easy, but Pierce, then Helfgott–Venkatesh who obtain $O(|D|^{0.442})$.

Minkowski : if $K \neq \mathbb{Q}$ then $|d(K)| > 1$, and in fact $|d(K)| > C^n$ with $n = [K : \mathbb{Q}]$ for some $C > 1$, more precisely $|d(K)| > C_1^{r_1} C_2^{r_2}$ with $C_1 > 1$, $C_2 > 1$.

Minkowski used geometry of numbers. Best constants known by analytic methods initiated by H. Stark, followed by A. Odlyzko and several others. Assuming GRH, constants very close to optimal.

Results and Conjectures I

Hermite : the set of isomorphism classes of nf of given discriminant D is finite, equivalently the number $N(X)$ of iso. cl. of nf with $|d(K)| \leq X$ is finite.

Conjecture : the cardinality of the set of iso. cl. of nf with given $d(K) = D$ is $O(|D|^{\varepsilon})$ for all $\varepsilon > 0$.

Trivial for quadratic fields, but not even known for cubic fields : $O(|D|^{1/2})$ easy, but Pierce, then Helfgott–Venkatesh who obtain $O(|D|^{0.442})$.

Minkowski : if $K \neq \mathbb{Q}$ then $|d(K)| > 1$, and in fact $|d(K)| > C^n$ with $n = [K : \mathbb{Q}]$ for some $C > 1$, more precisely $|d(K)| > C_1^{r_1} C_2^{r_2}$ with $C_1 > 1$, $C_2 > 1$.

Minkowski used geometry of numbers. Best constants known by analytic methods initiated by H. Stark, followed by A. Odlyzko and several others. Assuming GRH, constants very close to optimal.

Results and Conjectures II

Brauer–Siegel theorem : if n is fixed, then $\log(h(K)R(K)) \sim \log(|d(K)|^{1/2})$ as $|d(K)| \to \infty$. Thus, in a weak sense $h(K)R(K)$ is of the order of $|d(K)|^{1/2}$ ("joke proof ! ! ! ! !" : the value of $\zeta_K(s)/\zeta(s)$ at $s = 1$ is essentially $h(K)R(K)/|d(K)|^{1/2}$, and the Euler product giving the quotient shows that this is not large or small).

Imaginary quadratic fields : $R(K) = 1$, so only case where describes behavior of $h(K)$ alone. Although it says $|d(K)|^{1/2-\varepsilon} < h(K) < |d(K)|^{1/2+\varepsilon}$, finding explicit lower bounds for $|d(K)|$ is difficult if GRH not assumed. For instance, class number 1 problem (show $h(K) \geq 2$ when $|d(K)| > 163$) difficult, only solved in the 1960's by Stark and Baker (important ideas of Heegner).

Without GRH, Lower bound tending to infinity with $|d(K)|$ (and quite weak : order of $\log(|d(K)|)$ instead of the expected $|d(K)|^{1/2-\varepsilon}$) had to wait for Goldfeld, Gross–Zagier using the L-function of an elliptic curve of conductor 5077 and rank 3.

Results and Conjectures II

Brauer–Siegel theorem : if n is fixed, then $\log(h(K)R(K)) \sim \log(|d(K)|^{1/2})$ as $|d(K)| \to \infty$. Thus, in a weak sense $h(K)R(K)$ is of the order of $|d(K)|^{1/2}$ ("joke proof ! ! ! ! !" : the value of $\zeta_K(s)/\zeta(s)$ at $s = 1$ is essentially $h(K)R(K)/|d(K)|^{1/2}$, and the Euler product giving the quotient shows that this is not large or small).

Imaginary quadratic fields : $R(K) = 1$, so only case where describes behavior of $h(K)$ alone. Although it says $|d(K)|^{1/2-\varepsilon} < h(K) < |d(K)|^{1/2+\varepsilon}$, finding explicit lower bounds for $|d(K)|$ is difficult if GRH not assumed. For instance, class number 1 problem (show $h(K) \geq 2$ when $|d(K)| > 163$) difficult, only solved in the 1960's by Stark and Baker (important ideas of Heegner).

Without GRH, Lower bound tending to infinity with $|d(K)|$ (and quite weak : order of $\log(|d(K)|)$ instead of the expected $|d(K)|^{1/2-\varepsilon}$) had to wait for Goldfeld, Gross–Zagier using the L-function of an elliptic curve of conductor 5077 and rank 3.

Results and Conjectures II

Brauer–Siegel theorem : if n is fixed, then $\log(h(K)R(K)) \sim \log(|d(K)|^{1/2})$ as $|d(K)| \to \infty$. Thus, in a weak sense $h(K)R(K)$ is of the order of $|d(K)|^{1/2}$ (“joke proof ! ! ! ! !” : the value of $\zeta_K(s)/\zeta(s)$ at $s = 1$ is essentially $h(K)R(K)/|d(K)|^{1/2}$, and the Euler product giving the quotient shows that this is not large or small).

Imaginary quadratic fields : $R(K) = 1$, so only case where describes behavior of $h(K)$ alone. Although it says $|d(K)|^{1/2-\varepsilon} < h(K) < |d(K)|^{1/2+\varepsilon}$, finding explicit lower bounds for $|d(K)|$ is difficult if GRH not assumed. For instance, class number 1 problem (show $h(K) \geq 2$ when $|d(K)| > 163$) difficult, only solved in the 1960's by Stark and Baker (important ideas of Heegner).

Without GRH, Lower bound tending to infinity with $|d(K)|$ (and quite weak : order of $\log(|d(K)|)$ instead of the expected $|d(K)|^{1/2-\varepsilon}$) had to wait for Goldfeld, Gross–Zagier using the L-function of an elliptic curve of conductor 5077 and rank 3.

Results and Conjectures III

Recall $h(K)R(K)$ of the order of $|d(K)|^{1/2}$. Excluding imaginary quadratic fields, general belief is that $h(K)$ is very small (order $|d(K)|^{\varepsilon}$) and $R(K)$ therefore very large (order $|d(K)|^{1/2-\varepsilon}$). However not even known infinitely many class number 1 :

Conjectures

1. Exists infinitely many iso. cla. nf of class number 1 (unique factorization into prime elements).
2. Exists infinitely many which are Euclidean for the norm.
3. Exists infinitely many real quadratic fields $K = \mathbb{Q}(\sqrt{p})$ (necessarily of prime discriminant) with class number 1.
4. (C.–Lenstra) In fact, positive proportion of such fields, approx. $0.75446\cdots$ (hence many !).
5. If $r_1 + r_2 - 1 \geq 3$, most nf should be norm-Euclidean (and a fortiori of class number 1), the proportion tending to 1 as $r_1 + r_2 - 1$ tends to infinity.

Results and Conjectures III

Recall $h(K)R(K)$ of the order of $|d(K)|^{1/2}$. Excluding imaginary quadratic fields, general belief is that $h(K)$ is very small (order $|d(K)|^{\varepsilon}$) and $R(K)$ therefore very large (order $|d(K)|^{1/2-\varepsilon}$). However not even known infinitely many class number 1 :

Conjectures

1. Exists infinitely many iso. cla. nf of class number 1 (unique factorization into prime elements).
2. Exists infinitely many which are Euclidean for the norm.
3. Exists infinitely many real quadratic fields $K = \mathbb{Q}(\sqrt{p})$ (necessarily of prime discriminant) with class number 1.
4. (C.–Lenstra) In fact, positive proportion of such fields, approx. $0.75446\cdots$ (hence many !).
5. If $r_1 + r_2 - 1 \geq 3$, most nf should be norm-Euclidean (and a fortiori of class number 1), the proportion tending to 1 as $r_1 + r_2 - 1$ tends to infinity.

Results and Conjectures IV

Main problem : finding a lower bound for the regulator. Example for real quadratics : one can construct an infinite family of $\mathbb{Q}(\sqrt{D})$ with $R(D) > C\log(D)^3$, $C > 0$. Unknown if true with $C\log(D)^4$ (recall expect $R(D) > |D|^{1/2-\varepsilon}$ with probability 1).

In a different setting : can define p-adic regulator $R_p(K)$, a p-adic number. Worse situation : not even known if nonzero, except if K abelian (Leopoldt's conjecture).

Results and Conjectures IV

Main problem : finding a lower bound for the regulator. Example for real quadratics : one can construct an infinite family of $\mathbb{Q}(\sqrt{D})$ with $R(D) > C\log(D)^3$, $C > 0$. Unknown if true with $C\log(D)^4$ (recall expect $R(D) > |D|^{1/2-\varepsilon}$ with probability 1).

In a different setting : can define p-adic regulator $R_p(K)$, a p-adic number. Worse situation : not even known if nonzero, except if K abelian (Leopoldt's conjecture).

Counting Number Fields I

Ordering of nf : usually by $|d(K)|$. But can also be by conductor (when it exists) or by ramified primes. If G is a transitive subgroup of S_n, notation

$$N_{k,n}(G;X)\ ,\quad N_n(G;X);\ ,\quad N_{r_1,r_2}(G;X)$$

number of iso. cl. of nf (or number field extensions K/k) of degree n (or signature (r_1, r_2)) with Galois group (of Galois closure) permutation-isomorphic to G.

Main problem : give estimates, or compute exactly. In small degree, closely linked through elementary class field theory : estimates for the class group $Cl(K)$, more precisely the 2-rank or 3-rank for instance.

Counting Number Fields I

Ordering of nf : usually by $|d(K)|$. But can also be by conductor (when it exists) or by ramified primes. If G is a transitive subgroup of S_n, notation

$$N_{k,n}(G;X)\ ,\quad N_n(G;X);\ ,\quad N_{r_1,r_2}(G;X)$$

number of iso. cl. of nf (or number field extensions K/k) of degree n (or signature (r_1,r_2)) with Galois group (of Galois closure) permutation-isomorphic to G.

Main problem : give estimates, or compute exactly. In small degree, closely linked through elementary class field theory : estimates for the class group $Cl(K)$, more precisely the 2-rank or 3-rank for instance.

Counting Number Fields II

Experimental checks : need two things :

1. Make complete tables of number fields, ordered by $|d(K)|$, for given n, (r_1, r_2), and/or G.
2. Given K, compute its invariants $d(K)$, $Cl(K)$, $R(K)$ for instance.

The first problem is the most difficult : one does not even know the number field of degree 10 with smallest $|d(K)|$!!! (not sure if one knows it for degree 9).

Trivial for $n = 2$, very efficient for $n = 3$ (K. Belabas), for $n = 4$ work of M. Bhargava should also lead to an efficient method, which apparently has not been implemented (and would also apply to S_5-fields), for $5 \leq n \leq 8$ difficult, use Hunter's theorem, very inefficient (for imprimitive fields, i.e., with a nontrivial subfield, everything much more efficient using relative methods).

Counting Number Fields II

Experimental checks : need two things :

1. Make complete tables of number fields, ordered by $|d(K)|$, for given n, (r_1, r_2), and/or G.
2. Given K, compute its invariants $d(K)$, $Cl(K)$, $R(K)$ for instance.

The first problem is the most difficult : one does not even know the number field of degree 10 with smallest $|d(K)|$!!! (not sure if one knows it for degree 9).

Trivial for $n = 2$, very efficient for $n = 3$ (K. Belabas), for $n = 4$ work of M. Bhargava should also lead to an efficient method, which apparently has not been implemented (and would also apply to S_5-fields), for $5 \leq n \leq 8$ difficult, use Hunter's theorem, very inefficient (for imprimitive fields, i.e., with a nontrivial subfield, everything much more efficient using relative methods).

Counting Number Fields II

Experimental checks : need two things :

1. Make complete tables of number fields, ordered by $|d(K)|$, for given n, (r_1, r_2), and/or G.
2. Given K, compute its invariants $d(K)$, $Cl(K)$, $R(K)$ for instance.

The first problem is the most difficult : one does not even know the number field of degree 10 with smallest $|d(K)|$! ! ! (not sure if one knows it for degree 9).
Trivial for $n = 2$, very efficient for $n = 3$ (K. Belabas), for $n = 4$ work of M. Bhargava should also lead to an efficient method, which apparently has not been implemented (and would also apply to S_5-fields), for $5 \leq n \leq 8$ difficult, use Hunter's theorem, very inefficient (for imprimitive fields, i.e., with a nontrivial subfield, everything much more efficient using relative methods).

Counting Number Fields III

The second goal, computing invariants, has now become straightforward : $d(K)$ (or equivalently a $\mathbb{Z}$-basis of the ring of integers) computed using Zassenhaus' round 4 algorithm, very efficient, negligible time if $d(K)$ factored (no problem here).
For the more subtle invariants $Cl(K)$ and $R(K)$, work of Hafner–McCurley, Buchmann, C.–Diaz y Diaz–Olivier has made this also very efficient (degrees up to 40 or 50 for fields of reasonable $d(K)$), and excellent implementations (requiring years of work) in the usual packages `Pari/GP, Sage` (which is the Pari impl.), and `magma`.

Malle's Conjecture

General conjecture due to G. Malle :

Conjecture

$$N_{k,n}(G;X) \sim c_k(G)\, X^{a(G)} \log(X)^{b_k(G)-1} ,$$

where $a(G) = 1/i(G)$, $i(G) \geq 1$ integer independent of k, $b_k(G) \geq 1$ integer, and $c_k(G) > 0$ real.

Definition of $i(G)$ easy :

$$i(G) = \min_{\sigma \in G \setminus \{1\}} (n - |\text{orbits of } \sigma|) .$$

Examples : $i(S_n) = 1$, and if G abelian and ℓ is smallest prime divisor of $|G|$ then $i(G) = |G|(1 - 1/\ell)$.

Malle also gives definition of $b_k(G)$, but had to be corrected in certain cases (counterexample of J. Klüners), done by S. Türkelli.

Malle's Conjecture

General conjecture due to G. Malle :

Conjecture

$$N_{k,n}(G;X) \sim c_k(G)\,X^{a(G)}\log(X)^{b_k(G)-1}\ ,$$

where $a(G) = 1/i(G)$, $i(G) \geq 1$ integer independent of k, $b_k(G) \geq 1$ integer, and $c_k(G) > 0$ real.

Definition of $i(G)$ easy :

$$i(G) = \min_{\sigma \in G \setminus \{1\}} (n - |\text{orbits of } \sigma|)\ .$$

Examples : $i(S_n) = 1$, and if G abelian and ℓ is smallest prime divisor of $|G|$ then $i(G) = |G|(1 - 1/\ell)$.

Malle also gives definition of $b_k(G)$, but had to be corrected in certain cases (counterexample of J. Klüners), done by S. Türkelli.

Malle's Conjecture

General conjecture due to G. Malle :

Conjecture

$$N_{k,n}(G;X) \sim c_k(G)\,X^{a(G)}\log(X)^{b_k(G)-1}\ ,$$

where $a(G) = 1/i(G)$, $i(G) \geq 1$ integer independent of k, $b_k(G) \geq 1$ integer, and $c_k(G) > 0$ real.

Definition of $i(G)$ easy :

$$i(G) = \min_{\sigma \in G \setminus \{1\}} (n - |\text{orbits of } \sigma|)\ .$$

Examples : $i(S_n) = 1$, and if G abelian and ℓ is smallest prime divisor of $|G|$ then $i(G) = |G|(1 - 1/\ell)$.

Malle also gives definition of $b_k(G)$, but had to be corrected in certain cases (counterexample of J. Klüners), done by S. Türkelli.

General conjectures/results I

"folk" conjecture : $N_k(X) = O(X)$, where all Galois groups and all degrees are put together, and even $N_k(X) \sim c_k X$ for some $c_k > 0$. More precisely, for all n we have $N_{k,n}(X) \sim c_{k,n} X$ for some $c_{k,n} > 0$. Implied by Malle's conjecture.

By work that we will mention below, known to be true for $n \leq 4$ (also $n = 5$?). Elementary counting argument gives $N_k(X) = O(X^{(n+2)/4})$, much too weak. Ellenberg–Venkatesh prove the following :

1. $N_{k,n}(X) = O_{k,n}(X^{\exp(C(\log(n))^{1/2})}) = O_{k,n,\varepsilon}(X^{n^{\varepsilon}})$.
2. $N_{k,n}(S_n; X) > c_{k,n} X^{1/2+1/n^2}$ (expect X^1 of course).
3. $N_{k,n}(Galois; X) = O(X^{3/8+\varepsilon})$, in particular Galois extensions are negligible, as can be expected.

General conjectures/results I

"folk" conjecture : $N_k(X) = O(X)$, where all Galois groups and all degrees are put together, and even $N_k(X) \sim c_k X$ for some $c_k > 0$. More precisely, for all n we have $N_{k,n}(X) \sim c_{k,n} X$ for some $c_{k,n} > 0$. Implied by Malle's conjecture.

By work that we will mention below, known to be true for $n \leq 4$ (also $n = 5$?). Elementary counting argument gives $N_k(X) = O(X^{(n+2)/4})$, much too weak. Ellenberg–Venkatesh prove the following :

1. $N_{k,n}(X) = O_{k,n}(X^{\exp(C(\log(n))^{1/2})}) = O_{k,n,\varepsilon}(X^{n^\varepsilon})$.
2. $N_{k,n}(S_n; X) > c_{k,n} X^{1/2+1/n^2}$ (expect X^1 of course).
3. $N_{k,n}(Galois; X) = O(X^{3/8+\varepsilon})$, in particular Galois extensions are negligible, as can be expected.

Abelian Extensions I

Well understood and is one of the justifications of Malle's conjecture. Initially, many special cases : quadratic/$\mathbb{Q}$ easy, cyclic cubic/$\mathbb{Q}$ H. Cohn, abelian quartic/$\mathbb{Q}$ Baily (several mistakes). General abelian/$\mathbb{Q}$ treated by S. Mäki, cyclic/k of prime order treated by C. and collaborators, cyclic/k by M. Taylor, general abelian/k by D. Wright, using adelic techniques, but their "explicit" formula for $c_k(G)$ is difficult (but not impossible) to compute in practice.

In 2008, M. Wood showed that by ordering abelian extensions by conductor instead of discriminant (same for C_ℓ-extensions but not in general) one obtains a completely explicit formula, including for $c_k(G)$. Thus, the problem of abelian extensions can be considered as completely solved.

Abelian Extensions I

Well understood and is one of the justifications of Malle's conjecture. Initially, many special cases : quadratic/$\mathbb{Q}$ easy, cyclic cubic/$\mathbb{Q}$ H. Cohn, abelian quartic/$\mathbb{Q}$ Baily (several mistakes). General abelian/$\mathbb{Q}$ treated by S. Mäki, cyclic/k of prime order treated by C. and collaborators, cyclic/k by M. Taylor, general abelian/k by D. Wright, using adelic techniques, but their "explicit" formula for $c_k(G)$ is difficult (but not impossible) to compute in practice.

In 2008, M. Wood showed that by ordering abelian extensions by conductor instead of discriminant (same for C_ℓ-extensions but not in general) one obtains a completely explicit formula, including for $c_k(G)$. Thus, the problem of abelian extensions can be considered as completely solved.

Abelian Extensions II

Simplest examples over $\mathbb{Q}$, for explicit constants (Euler products and sums), computable to hundreds of decimal digits if desired :

$$N_2(C_2;X) \sim c(C_2)\,X\ , \quad N_3(C_3;X) \sim c(C_3)\,X^{1/2}\ ,$$

$$N_4(C_4;X) = c(C_4)\,X^{1/2} + c'(C_4)\,X^{1/3} + O(X^{1/4+\varepsilon})\ ,$$

$$N_4(V_4;X) = (c(V_4)\log^2(X) + c'(V_4)\log(X) + c''(V_4))\,X^{1/2} + O(X^{1/3+\varepsilon})$$

$$N_5(C_5;X) \sim c(C_5)\,X^{1/4}\ , \quad N_6(C_6;X) \sim c(C_6)\,X^{1/3}\ ,$$

$$N_7(C_7;X) \sim c(C_7)\,X^{1/6}\ .$$

In addition, I mention the following simple result due to Datskowsky–Wright and independently the author and collaborators :

$$N_{k,2}(C_2;X) \sim \frac{1}{2^{r_2(k)}}\frac{\zeta_k(1)}{\zeta_k(2)}\,X$$

(by abuse, $\zeta_k(1)$ denotes the residue of $\zeta_k(s)$ at $s=1$).

Abelian Extensions II

Simplest examples over $\mathbb{Q}$, for explicit constants (Euler products and sums), computable to hundreds of decimal digits if desired :

$$N_2(C_2;X)\sim c(C_2)\,X\ ,\quad N_3(C_3;X)\sim c(C_3)\,X^{1/2}\ ,$$
$$N_4(C_4;X)=c(C_4)\,X^{1/2}+c'(C_4)\,X^{1/3}+O(X^{1/4+\varepsilon})\ ,$$
$$N_4(V_4;X)=(c(V_4)\log^2(X)+c'(V_4)\log(X)+c''(V_4))\,X^{1/2}+O(X^{1/3+\varepsilon})$$
$$N_5(C_5;X)\sim c(C_5)\,X^{1/4}\ ,\quad N_6(C_6;X)\sim c(C_6)\,X^{1/3}\ ,$$
$$N_7(C_7;X)\sim c(C_7)\,X^{1/6}\ .$$

In addition, I mention the following simple result due to Datskowsky–Wright and independently the author and collaborators :

$$N_{k,2}(C_2;X)\sim\frac{1}{2^{r_2(k)}}\frac{\zeta_k(1)}{\zeta_k(2)}\,X$$

(by abuse, $\zeta_k(1)$ denotes the residue of $\zeta_k(s)$ at $s=1$).

Cases of medium difficulty I

• Quartic D_4-extensions. This was completely solved over an arbitrary k and with or without signature conditions by C.–Diaz y Diaz–Olivier. Result is

$$N_{k,4}(D_4;X) = c_k(D_4)\,X + O(X^{1-\alpha})$$

with an explicit $\alpha > 0$ ($\alpha = 1/4 - \varepsilon$ if $k = \mathbb{Q}$) and explicit $c_k(D_4)$.

However, contrary to the abelian case (and Bhargava's S_n cases below), formula for $c_k(D_4)$ slow convergence : for $k = \mathbb{Q}$ only 8 decimals.

Since $N_{k,4}(S_4;X) > c.X$ (see below), this shows that the proportion of quartic extensions which are S_4 is strictly less than 1 (contrary to the cubic or quintic case for instance), in accordance with Malle's conjecture. In fact Malle proves that the proportion of degree n S_n-extensions is stricly less than 1 if n is divisible by 4 or 6, and conjectures that it is strictly less than 1 if and only if n is composite.

Cases of medium difficulty I

• Quartic D_4-extensions. This was completely solved over an arbitrary k and with or without signature conditions by C.–Diaz y Diaz–Olivier. Result is

$$N_{k,4}(D_4;X) = c_k(D_4)\,X + O(X^{1-\alpha})$$

with an explicit $\alpha > 0$ ($\alpha = 1/4 - \varepsilon$ if $k = \mathbb{Q}$) and explicit $c_k(D_4)$. However, contrary to the abelian case (and Bhargava's S_n cases below), formula for $c_k(D_4)$ slow convergence : for $k = \mathbb{Q}$ only 8 decimals.

Since $N_{k,4}(S_4;X) > c.X$ (see below), this shows that the proportion of quartic extensions which are S_4 is strictly less than 1 (contrary to the cubic or quintic case for instance), in accordance with Malle's conjecture. In fact Malle proves that the proportion of degree n S_n-extensions is stricly less than 1 if n is divisible by 4 or 6, and conjectures that it is strictly less than 1 if and only if n is composite.

Cases of medium difficulty I

• Quartic D_4-extensions. This was completely solved over an arbitrary k and with or without signature conditions by C.–Diaz y Diaz–Olivier. Result is

$$N_{k,4}(D_4;X) = c_k(D_4)\,X + O(X^{1-\alpha})$$

with an explicit $\alpha > 0$ ($\alpha = 1/4 - \varepsilon$ if $k = \mathbb{Q}$) and explicit $c_k(D_4)$.
However, contrary to the abelian case (and Bhargava's S_n cases below), formula for $c_k(D_4)$ slow convergence : for $k = \mathbb{Q}$ only 8 decimals.

Since $N_{k,4}(S_4;X) > c.X$ (see below), this shows that the proportion of quartic extensions which are S_4 is strictly less than 1 (contrary to the cubic or quintic case for instance), in accordance with Malle's conjecture. In fact Malle proves that the proportion of degree n S_n-extensions is stricly less than 1 if n is divisible by 4 or 6, and conjectures that it is strictly less than 1 if and only if n is composite.

Cases of medium difficulty II

A number of results for other groups are due to J. Klüners and G. Malle. To my knowledge, the only results they have deals with the weak Malle conjecture, i.e.

$$X^{a(G)-\varepsilon} < N_{k,n}(G,X) < X^{a(G)+\varepsilon}\ .$$

Thanks to these authors, such results are known for nilpotent groups in their regular representation, for the wreath product of such a group with C_2, for the dihedral group D_ℓ (ℓ prime) both for degree ℓ extensions and for the Galois degree 2ℓ extensions (assuming C.–Lenstra heuristics, otherwise weaker, use work of Ellenberg–Venkatesh), for quaternion groups $Q_{4\ell}$, for certain types of ℓ-groups, etc... In every case one uses the fact that these groups have subgroups and one can use induction on simpler groups.

Cases of medium difficulty II

A number of results for other groups are due to J. Klüners and G. Malle. To my knowledge, the only results they have deals with the weak Malle conjecture, i.e.

$$X^{a(G)-\varepsilon} < N_{k,n}(G,X) < X^{a(G)+\varepsilon} \ .$$

Thanks to these authors, such results are known for nilpotent groups in their regular representation, for the wreath product of such a group with C_2, for the dihedral group D_ℓ (ℓ prime) both for degree ℓ extensions and for the Galois degree 2ℓ extensions (assuming C.–Lenstra heuristics, otherwise weaker, use work of Ellenberg–Venkatesh), for quaternion groups $Q_{4\ell}$, for certain types of ℓ-groups, etc... In every case one uses the fact that these groups have subgroups and one can use induction on simpler groups.

Difficult Cases : $n = 3$, $G = S_3$ I

Excluding the trivial cases $n \le 2$, the first difficult result was obtained for $n = 3$, $G = S_3$, and $k = \mathbb{Q}$ by Davenport–Heilbronn in 1969, using the Delone–Fadeev correspondence between cubic fields and binary cubic forms :

$$N_3(S_3; X) \sim c(S_3)\, X \ , \quad N_{(3,0)}(S_3; X) \sim \frac{c(S_3)}{4}\, X \ ,$$

$$N_{(1,1)}(S_3; X) \sim \frac{3c(S_3)}{4}\, X \ , \quad \text{with}$$

$$c(S_3) = \frac{1}{3\zeta(3)} \ .$$

Sketch of proof : (1) description of the D–F correspondence between binary cubic forms and cubic rings. (2) description of nec. and suf. local conditions for the image to be a maximal order. (3) compute the local densities, count the forms, compute the product, prove the theorem.

Difficult Cases : $n = 3$, $G = S_3$ I

Excluding the trivial cases $n \le 2$, the first difficult result was obtained for $n = 3$, $G = S_3$, and $k = \mathbb{Q}$ by Davenport–Heilbronn in 1969, using the Delone–Fadeev correspondence between cubic fields and binary cubic forms :

$$N_3(S_3; X) \sim c(S_3)\, X \;, \quad N_{(3,0)}(S_3; X) \sim \frac{c(S_3)}{4} X \;,$$

$$N_{(1,1)}(S_3; X) \sim \frac{3c(S_3)}{4} X \;, \quad \text{with}$$

$$c(S_3) = \frac{1}{3\zeta(3)} \;.$$

Sketch of proof : (1) description of the D–F correspondence between binary cubic forms and cubic rings. (2) description of nec. and suf. local conditions for the image to be a maximal order. (3) compute the local densities, count the forms, compute the product, prove the theorem.

Difficult Cases : $n = 3$, $G = S_3$ II

Error terms : first error term by K. Belabas in 1999, first power-saving error term by Belabas–Bhargava–Pomerance in 2005, precise conjecture of D. Roberts that there exists a second main term in $X^{5/6}$, finally proved in 2010 by Bhargava–Shankar–Tsimmerman using techniques of Bhargava. Independently, T. Taniguchi and F. Thorne using Shintani zeta functions found the best result to date :

$$N_3(S_3;X) = c(S_3)\,X + (1+\sqrt{3})c'(S_3)\,X^{5/6} + O(X^{7/9+\varepsilon})\ ,$$

$$N_{3,0}(S_3;X) = \frac{c(S_3)}{4}\,X + c'(S_3)\,X^{5/6} + O(X^{7/9+\varepsilon})\ ,$$

$$N_{1,1}(S_3;X) = \frac{3c(S_3)}{4}\,X + \sqrt{3}c'(S_3)\,X^{5/6} + O(X^{7/9+\varepsilon})\ ,$$

where $c(S_3) = 1/(3\zeta(3))$ as above, and

$$c'(S_3) = \frac{4}{5}\frac{\zeta(1/3)}{\Gamma(2/3)^3\zeta(5/3)}\ ,$$

as conjectured by Roberts.

Difficult Cases : $n = 3$, $G = S_3$ III

The case $n = 3$, $G = S_3$, and general k is much harder : 20 years later, fundamental work of Datskowsky–Wright in 1988 using adelic techniques :

$$N_{k,3}(S_3; X) \sim \left(\frac{2}{3}\right)^{r_1(k)-1} \left(\frac{1}{6}\right)^{r_2(k)} \frac{\zeta_k(1)}{3\zeta_k(3)} X \ .$$

Simpler methods : can also give precise asymptotics for the number of S_3-extensions with given quadratic resolvent field (C.–Morra). This is also possible for the number of S_4 or A_4-extensions with given cubic resolvent field, but unfortunately does not help for the total number because of error terms (see below, however).

Difficult Cases : $n = 3$, $G = S_3$ III

The case $n = 3$, $G = S_3$, and general k is much harder : 20 years later, fundamental work of Datskowsky–Wright in 1988 using adelic techniques :

$$N_{k,3}(S_3; X) \sim \left(\frac{2}{3}\right)^{r_1(k)-1} \left(\frac{1}{6}\right)^{r_2(k)} \frac{\zeta_k(1)}{3\zeta_k(3)} X \ .$$

Simpler methods : can also give precise asymptotics for the number of S_3-extensions with given quadratic resolvent field (C.–Morra). This is also possible for the number of S_4 or A_4-extensions with given cubic resolvent field, but unfortunately does not help for the total number because of error terms (see below, however).

Difficult Cases : $n = 3$, $G = S_4$ I

Breakthrough by M. Bhargava in 2000, new methods for many problems in the field. In this precise case : Delone–Fadeev correspondence replaced by a correspondence between suitable pairs of ternary quadratic forms (i.e., pencils of projective conics) and maximal quartic rings.

This corresponds to a prehomogeneous vector space : rough count : Ternary qf : 6 homogeneous parameters, pencil $12 = 2 \times 6$ projective parameters. Group acting : $\mathrm{GL}_3(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$: the GL_3 on ternary quadratic forms, the GL_2 on the pencil, condition determinant product equals 1 for a total of $3^2 + 2^2 - 1 = 12$ parameters, same number. Expect orbits to be finite.

Proof then goes along same lines : study in detail the correspondence, local conditions for maximal orders, compute local densities, count the forms, prove theorem. Here there are additional problems coming from the shape of the fundamental domain which must be solved.

Difficult Cases : $n = 3$, $G = S_4$ I

Breakthrough by M. Bhargava in 2000, new methods for many problems in the field. In this precise case : Delone–Fadeev correspondence replaced by a correspondence between suitable pairs of ternary quadratic forms (i.e., pencils of projective conics) and maximal quartic rings.

This corresponds to a prehomogeneous vector space : rough count : Ternary qf : 6 homogeneous parameters, pencil $12 = 2 \times 6$ projective parameters. Group acting : $\mathrm{GL}_3(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$: the GL_3 on ternary quadratic forms, the GL_2 on the pencil, condition determinant product equals 1 for a total of $3^2 + 2^2 - 1 = 12$ parameters, same number. Expect orbits to be finite.

Proof then goes along same lines : study in detail the correspondence, local conditions for maximal orders, compute local densities, count the forms, prove theorem. Here there are additional problems coming from the shape of the fundamental domain which must be solved.

Difficult Cases : $n = 3$, $G = S_4$ I

Breakthrough by M. Bhargava in 2000, new methods for many problems in the field. In this precise case : Delone–Fadeev correspondence replaced by a correspondence between suitable pairs of ternary quadratic forms (i.e., pencils of projective conics) and maximal quartic rings.

This corresponds to a prehomogeneous vector space : rough count : Ternary qf : 6 homogeneous parameters, pencil $12 = 2 \times 6$ projective parameters. Group acting : $\mathrm{GL}_3(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$: the GL_3 on ternary quadratic forms, the GL_2 on the pencil, condition determinant product equals 1 for a total of $3^2 + 2^2 - 1 = 12$ parameters, same number. Expect orbits to be finite.

Proof then goes along same lines : study in detail the correspondence, local conditions for maximal orders, compute local densities, count the forms, prove theorem. Here there are additional problems coming from the shape of the fundamental domain which must be solved.

Difficult Cases : $n = 4$, $G = S_4$ II

Bhargava's theorem :

$$N_4(S_4, X) \sim r_4(S_4) z(S_4)\, X \quad N_{r_1,r_2}(S_4, X) \sim r_{r_1,r_2}(S_4) z(S_4)\, X\ ,$$

where

$$z(S_4) = \prod_{p \geq 2} \left(1 + \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^4}\right) \quad \text{and}$$

$$r_4(S_4) = \frac{5}{24},\ r_{4,0}(S_4) = \frac{1}{48},\ r_{2,1}(S_4) = \frac{1}{8},\ r_{0,2}(S_4) = \frac{1}{16}\ .$$

Probably additional main term, perhaps $X^{23/24}$. Available numerical data only up to 10^9 (Malle for totally real) far from sufficient.
Relative case treated by A. Yukie, but convergence problems remain.
Solved by Bhargava ?

Difficult Cases : $n = 4$, $G = S_4$ II

Bhargava's theorem :

$$N_4(S_4, X) \sim r_4(S_4) z(S_4)\, X \quad N_{r_1,r_2}(S_4, X) \sim r_{r_1,r_2}(S_4) z(S_4)\, X\ ,$$

where

$$z(S_4) = \prod_{p \geq 2} \left(1 + \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^4}\right) \quad \text{and}$$

$$r_4(S_4) = \frac{5}{24},\ r_{4,0}(S_4) = \frac{1}{48},\ r_{2,1}(S_4) = \frac{1}{8},\ r_{0,2}(S_4) = \frac{1}{16}\ .$$

Probably additional main term, perhaps $X^{23/24}$. Available numerical data only up to 10^9 (Malle for totally real) far from sufficient.
Relative case treated by A. Yukie, but convergence problems remain.
Solved by Bhargava ?

Difficult Cases : $n = 5$, $G = S_5$

Also by Bhargava. Similar but more complicated, here a 40-dimensional space instead of a 12-dimensional one in the S_4 case : quadruples of alternating 5-forms on the one hand, group $\mathrm{GL}_5(\mathbb{C}) \times \mathrm{GL}_4(\mathbb{C})$ plus the determinant condition on the other hand , for a total of $5^2 + 4^2 - 1 = 40$ parameters, the same number once again.

Bhargava's theorem :

$$N_5(S_5, X) \sim r_5(S_5) z(S_5) X \quad N_{r_1,r_2}(S_5, X) \sim r_{r_1,r_2}(S_5) z(S_5) X ,$$

where

$$z(S_5) = \prod_{p \geq 2} \left(1 + \frac{1}{p^2} - \frac{1}{p^4} - \frac{1}{p^5}\right) \quad \text{and}$$

$$r_5(S_5) = \frac{13}{120}, \; r_{5,0}(S_5) = \frac{1}{240}, \; r_{3,1}(S_5) = \frac{1}{24}, \; r_{1,2}(S_5) = \frac{1}{16} .$$

Difficult Cases : $n = 5$, $G = S_5$

Also by Bhargava. Similar but more complicated, here a 40-dimensional space instead of a 12-dimensional one in the S_4 case : quadruples of alternating 5-forms on the one hand, group $GL_5(\mathbb{C}) \times GL_4(\mathbb{C})$ plus the determinant condition on the other hand , for a total of $5^2 + 4^2 - 1 = 40$ parameters, the same number once again.

Bhargava's theorem :

$$N_5(S_5, X) \sim r_5(S_5) z(S_5) X \quad N_{r_1,r_2}(S_5, X) \sim r_{r_1,r_2}(S_5) z(S_5) X \ ,$$

where

$$z(S_5) = \prod_{p \geq 2} \left(1 + \frac{1}{p^2} - \frac{1}{p^4} - \frac{1}{p^5}\right) \quad \text{and}$$

$$r_5(S_5) = \frac{13}{120}, \ r_{5,0}(S_5) = \frac{1}{240}, \ r_{3,1}(S_5) = \frac{1}{24}, \ r_{1,2}(S_5) = \frac{1}{16} \ .$$

Difficult Cases : $n = 6$, $G = S_3$

The case of Galois sextic extensions with Galois group S_3 has been solved in 2008 independently by Belabas–Fouvry and Bhargava–Wood.
In accordance with Malle's conjecture, they prove the following :

$$N_6(S_3; X) \sim c(S_3(6))\, X^{1/3} \quad \text{with}$$

$$c(S_3(6)) = \frac{1}{3} \prod_p c_p \left(1 - \frac{1}{p}\right)$$

$$c_{p \neq 3} = 1 + \frac{1}{p} + \frac{1}{p^{4/3}} \quad \text{and} \quad c_3 = 1 + \frac{1}{3} + \frac{1}{3^{5/3}} + \frac{1}{3^{7/3}}\ .$$

Difficult Cases : $G = S_n$, $n \geq 6$

Unfortunately, there are no prehomogeneous v.s. to help us now. On the other hand, one can still use the idea of local densities, and using a mass formula of Serre counting étale extensions, M. Bhargava has given a very convincing conjecture concerning $N_n(S_n; X)$ and $N_{r_1,r_2}(S_n; X)$, which of course agrees with the known results for $n \leq 5$.

For a number field k and a place v of k define sequences $a_v(n)$:

$$\sum_{n\geq 1} a_v(n)T^n = \begin{cases} \exp(T) & \text{if } v \text{ is complex,} \\ \exp(T + T^2/2) & \text{if } v \text{ is real,} \\ \prod_{k\geq 1}(1 - T^k/q_v^{k-1})^{-1} & \text{if } v = \mathfrak{p}, \text{ with } q_v = \mathcal{N}\mathfrak{p} \,. \end{cases}$$

Conjecture (Bhargava) :

$$N_{k,n}(S_n; X) \sim c_k(S_n)\, X \,, \quad \text{with}$$

$$c_k(S_n) = \frac{\zeta_k(1)}{2} \prod_v a_v(n) \left(1 - \frac{1}{q_v}\right) \,,$$

(if v is infinite set $q_v = \infty$, in other words omit the factor $1 - 1/q_v$).
Easy to modify to take into account signatures.

Difficult Cases : $G = S_n$, $n \geq 6$

Unfortunately, there are no prehomogeneous v.s. to help us now. On the other hand, one can still use the idea of local densities, and using a mass formula of Serre counting étale extensions, M. Bhargava has given a very convincing conjecture concerning $N_n(S_n;X)$ and $N_{r_1,r_2}(S_n;X)$, which of course agrees with the known results for $n \leq 5$.

For a number field k and a place v of k define sequences $a_v(n)$:

$$\sum_{n\geq 1} a_v(n)T^n = \begin{cases} \exp(T) & \text{if } v \text{ is complex,} \\ \exp(T + T^2/2) & \text{if } v \text{ is real,} \\ \prod_{k\geq 1}(1 - T^k/q_v^{k-1})^{-1} & \text{if } v = \mathfrak{p}, \text{ with } q_v = \mathcal{N}\mathfrak{p} \ . \end{cases}$$

Conjecture (Bhargava) :

$$N_{k,n}(S_n;X) \sim c_k(S_n)\,X \ , \quad \text{with}$$

$$c_k(S_n) = \frac{\zeta_k(1)}{2} \prod_v a_v(n)\left(1 - \frac{1}{q_v}\right) \ ,$$

(if v is infinite set $q_v = \infty$, in other words omit the factor $1 - 1/q_v$). Easy to modify to take into account signatures.

Difficult Cases : $G = S_n$, $n \geq 6$

Unfortunately, there are no prehomogeneous v.s. to help us now. On the other hand, one can still use the idea of local densities, and using a mass formula of Serre counting étale extensions, M. Bhargava has given a very convincing conjecture concerning $N_n(S_n; X)$ and $N_{r_1,r_2}(S_n; X)$, which of course agrees with the known results for $n \leq 5$.

For a number field k and a place v of k define sequences $a_v(n)$:

$$\sum_{n\geq 1} a_v(n)T^n = \begin{cases} \exp(T) & \text{if } v \text{ is complex,} \\ \exp(T + T^2/2) & \text{if } v \text{ is real,} \\ \prod_{k\geq 1}(1 - T^k/q_v^{k-1})^{-1} & \text{if } v = \mathfrak{p}, \text{ with } q_v = \mathcal{N}\mathfrak{p} \,. \end{cases}$$

Conjecture (Bhargava) :

$$N_{k,n}(S_n; X) \sim c_k(S_n)\, X \,, \quad \text{with}$$

$$c_k(S_n) = \frac{\zeta_k(1)}{2} \prod_v a_v(n) \left(1 - \frac{1}{q_v}\right) \,,$$

(if v is infinite set $q_v = \infty$, in other words omit the factor $1 - 1/q_v$). Easy to modify to take into account signatures.

Difficult Cases : other Galois groups

Note that as part of their beautiful 2010 ICM paper, Ellenberg–Venkatesh give a number of heuristic arguments for a precise conjecture for more general groups than S_n.

Difficult Cases : $n = 4$, $G = A_4$

Only remaining Galois group for quartic extensions. Conjecture due to the author and coll., a special case of Malle's, is :

Conjecture : exists $c > 0$ such that

$$N_{k,4}(A_4; X) \sim c\, X^{1/2} \log(X)^{b_k - 1} ,$$

with $b_k = 2$ if $\zeta_3 \notin k$, $b_k = 3$ if $\zeta_3 \in k$ (ζ_3 primitive cube root of 1).

Best result due to S. Wong : $N_{k,4}(A_4; X) = O(X^{5/6+\varepsilon})$ (exponent reduced to $2/3$ if assumes ABC, BSD, GRH).

Difficult Cases : $n = 4$, $G = A_4$

Only remaining Galois group for quartic extensions. Conjecture due to the author and coll., a special case of Malle's, is :

Conjecture : exists $c > 0$ such that

$$N_{k,4}(A_4; X) \sim c\, X^{1/2} \log(X)^{b_k - 1} ,$$

with $b_k = 2$ if $\zeta_3 \notin k$, $b_k = 3$ if $\zeta_3 \in k$ (ζ_3 primitive cube root of 1).

Best result due to S. Wong : $N_{k,4}(A_4; X) = O(X^{5/6+\varepsilon})$ (exponent reduced to $2/3$ if assumes ABC, BSD, GRH).

Exact Numerical Computation of $N_{k,n}(G; X)$ I

One may also want to count exactly the quantities $N_{k,n}(G; X)$, either to test the validity or the plausibility of the asymptotics (it is incredibly easy to make a mistake in the formulas), as a challenge and/or attempt at record-breaking. Four ways that I know of :

- For abelian extensions, the use of Kummer theory, or equivalently of class field theory. This allows the computations to go very far (see below).
- For A_4 and D_4-extensions, the use of the work of the author and collaborators also leads to a very efficient algorithm, almost as efficient as in the abelian case, since one can still use Kummer theory on relative extensions.

Exact Numerical Computation of $N_{k,n}(G; X)$ I

One may also want to count exactly the quantities $N_{k,n}(G; X)$, either to test the validity or the plausibility of the asymptotics (it is incredibly easy to make a mistake in the formulas), as a challenge and/or attempt at record-breaking. Four ways that I know of :

- For abelian extensions, the use of Kummer theory, or equivalently of class field theory. This allows the computations to go very far (see below).
- For A_4 and D_4-extensions, the use of the work of the author and collaborators also leads to a very efficient algorithm, almost as efficient as in the abelian case, since one can still use Kummer theory on relative extensions.

Exact Numerical Computation of $N_{k,n}(G; X)$ II

- For S_n-extensions for $n = 3$, 4, and 5, the use of the explicit correspondences leading to the theorems of Davenport–Heilbronn and Bhargava. This leads to quasi-linear algorithms, and has been beautifully done by K. Belabas for $n = 3$. Although everybody speaks about doing it, it should be done for $n = 4$ (and $n = 5$), since clearly it will work.
- For other extensions, the very inefficient use of Hunter's theorem, together with a relative generalization due to J. Martinet.

Exact Numerical Computation of $N_{k,n}(G; X)$ III

The computations are done separating different signatures, although of course the splitting behavior of other primes could be taken into account. Here are some of the limits attained a few years ago for fields of degree up to 4 (easy to go higher if desired) :

group :	C_2	C_3	S_3	C_4	V_4	D_4	A_4	S_4
limit :	10^{25}	10^{37}	10^{13}	10^{32}	10^{36}	10^{17}	10^{16}	10^{9*}

(*) (totally real only).

Relative case :

1. As usual, abelian extensions easy.
2. Cubic S_3-extensions of quadratic fields tabulated by A. Morra.
3. Quartic extensions of quadratic fields tabulated by M. Olivier.
4. A few other cases.

Exact Numerical Computation of $N_{k,n}(G; X)$ III

The computations are done separating different signatures, although of course the splitting behavior of other primes could be taken into account. Here are some of the limits attained a few years ago for fields of degree up to 4 (easy to go higher if desired) :

group :	C_2	C_3	S_3	C_4	V_4	D_4	A_4	S_4
limit :	10^{25}	10^{37}	10^{13}	10^{32}	10^{36}	10^{17}	10^{16}	10^{9*}

(*) (totally real only).

Relative case :

1. As usual, abelian extensions easy.
2. Cubic S_3-extensions of quadratic fields tabulated by A. Morra.
3. Quartic extensions of quadratic fields tabulated by M. Olivier.
4. A few other cases.

The C.–Lenstra Heuristics I

Closely linked to the problem of counting nf in small degree are the problems of asymptotics of class groups and regulators. H. Lenstra and the author, and later J. Martinet, have formulated a number of general conjectures on this.

Basic idea : weigh finite abelian group proportionally to $1/|\mathrm{Aut}(G)|$. Then the odd part of class groups of imaginary quadratic fields should behave like such a “random” abelian group. The odd part of class groups of real quadratic fields should behave like $G/\langle g\rangle$, G being weighed as before and $\langle g\rangle$ cyclic subgroup generated by a random $g \in G$.

Exist generalizations to higher degree fields (C.–Lenstra, C.–Martinet), but need to be careful about certain prime numbers.

The C.–Lenstra Heuristics I

Closely linked to the problem of counting nf in small degree are the problems of asymptotics of class groups and regulators. H. Lenstra and the author, and later J. Martinet, have formulated a number of general conjectures on this.

Basic idea : weigh finite abelian group proportionally to $1/|\mathrm{Aut}(G)|$. Then the odd part of class groups of imaginary quadratic fields should behave like such a "random" abelian group. The odd part of class groups of real quadratic fields should behave like $G/\langle g\rangle$, G being weighed as before and $\langle g\rangle$ cyclic subgroup generated by a random $g \in G$.

Exist generalizations to higher degree fields (C.–Lenstra, C.–Martinet), but need to be careful about certain prime numbers.

The C.–Lenstra Heuristics I

Closely linked to the problem of counting nf in small degree are the problems of asymptotics of class groups and regulators. H. Lenstra and the author, and later J. Martinet, have formulated a number of general conjectures on this.

Basic idea : weigh finite abelian group proportionally to $1/|\mathrm{Aut}(G)|$. Then the odd part of class groups of imaginary quadratic fields should behave like such a “random” abelian group. The odd part of class groups of real quadratic fields should behave like $G/\langle g\rangle$, G being weighed as before and $\langle g\rangle$ cyclic subgroup generated by a random $g \in G$.

Exist generalizations to higher degree fields (C.–Lenstra, C.–Martinet), but need to be careful about certain prime numbers.

The C–Lenstra Heuristics II

Some consequences of the heuristic assumptions.

- For imaginary quadratic fields :

1. For $p \geq 3$ prime, $p \mid h(K)$ with probability close to $1/p + 1/p^2$ ($0.44\cdots$ for $p = 3$, much larger than expected $1/3$).
2. For $p \geq 3$ prime, the average of $p^{r_p(Cl(K))}$ should be always equal to 2 ($r_p(Cl(K))$ is the p-rank of $Cl(K)$). The Davenport–Heilbronn theorem above shows that this is a theorem for $p = 3$. To prove it for $p = 5$ would require asymptotics for D_5 quintic number fields.

The C–Lenstra Heuristics III

- For real quadratic fields :

1. The proportion of $K = \mathbb{Q}(\sqrt{p})$ with $p \equiv 1 \pmod 4$ prime with class number 1 should be $0.75446\cdots$ (recall that one does not even know if infinitely many !).
2. We have
$$\sum_{p \le x,\ p \equiv 1 \pmod 4} h(p) \sim \frac{x}{8}\ ,$$
also conjectured by C. Hooley using completely different ideas.
3. For $p \ge 3$ prime, the average of $p^{r_p(Cl(K))}$ should be $1 + 1/p$. Again a theorem for $p = 3$ by Davenport–Heilbronn.

The C–Lenstra Heuristics IV

• For noncyclic cubic fields :
If $p \neq 3$ is prime (including $p = 2$), the average of $p^{r_p(Cl(K))}$ should be $1 + 1/p$ for complex cubic fields, and $1 + 1/p^2$ for totally real cubic fields. This is now a theorem of Bhargava for $p = 2$.

• For cyclic cubic fields :
Recall in this case $r_p(Cl(K))$ always even. Initial conjectures of C.–Martinet : the average of $p^{r_p(Cl(K))}$ should be

$$\begin{cases} (1 + 1/p)^2 & \text{if } p \equiv 1 \pmod 3 \,, \\ 1 + 1/p^2 & \text{if } p \equiv 2 \pmod 3 \,. \end{cases}$$

The C–Lenstra Heuristics IV

• For noncyclic cubic fields :
If $p \neq 3$ is prime (including $p = 2$), the average of $p^{r_p(Cl(K))}$ should be $1 + 1/p$ for complex cubic fields, and $1 + 1/p^2$ for totally real cubic fields. This is now a theorem of Bhargava for $p = 2$.

• For cyclic cubic fields :
Recall in this case $r_p(Cl(K))$ always even. Initial conjectures of C.–Martinet : the average of $p^{r_p(Cl(K))}$ should be

$$\begin{cases} (1+1/p)^2 & \text{if } p \equiv 1 \pmod{3}\,, \\ 1+1/p^2 & \text{if } p \equiv 2 \pmod{3}\,. \end{cases}$$

The C–Lenstra Heuristics V

On the basis of additional heuristics and extensive convincing numerical evidence, following remarks of H. Lenstra, G. Malle has suggested that the existence of roots of unity in the base field will change the heuristic predictions (hence always for $p = 2$).

1. In the noncyclic cubic case, it changes the expected predictions for $p = 2$, but does not change the prediction for the first moment $p^{r_p(Cl(K))}$ (which is correct by Bhargava), but only for the higher moments $p^{nr_p(Cl(K))}$.
2. In the cyclic cubic case, his prediction is that the average of $2^{r_2(Cl(K))}$ should be $3/2$ instead of $5/4$ as predicted by C.–Martinet. This is extremely close to experimental evidence.

The C–Lenstra Heuristics V

On the basis of additional heuristics and extensive convincing numerical evidence, following remarks of H. Lenstra, G. Malle has suggested that the existence of roots of unity in the base field will change the heuristic predictions (hence always for $p = 2$).

1. In the noncyclic cubic case, it changes the expected predictions for $p = 2$, but does not change the prediction for the first moment $p^{r_p(Cl(K))}$ (which is correct by Bhargava), but only for the higher moments $p^{nr_p(Cl(K))}$.
2. In the cyclic cubic case, his prediction is that the average of $2^{r_2(Cl(K))}$ should be $3/2$ instead of $5/4$ as predicted by C.–Martinet. This is extremely close to experimental evidence.