Norm equations and More in Oscar

Claus Fieker

July 17, 2024

SYMBOLIC TOOLS

SYMBOLIC TOOLS

Topics:

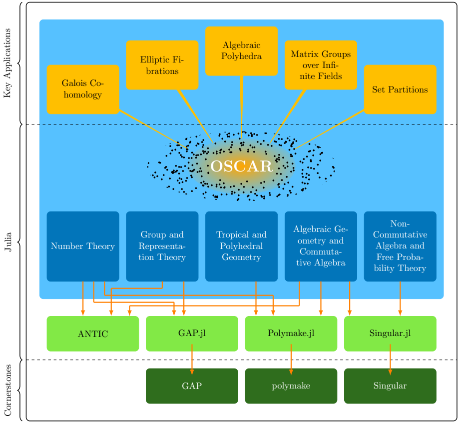
- Oscar
- Norm Equations
- ... and more

Develop a visionary, next generation, open source computer algebra system, integrating all systems, libraries and packages developed within the TRR.
(Be able to compete with Magma in our area of expertise.)

What is Oscar?

http://oscar-system.org/ https://oscar-system.github.io/oscar-website/

- (software) project of the CRC 195
- funded by DFG
- in Julia
- funding (planned) 2017 – 2028
- in three phases



Oscar

```
julia> Pkg.add("Oscar")
... [wait some time] ...
julia> using Oscar
  ___   ____   ____    _    ____
 / _ \ / ___| / ___|  / \  |  _ \   |  Combining ANTIC, GAP, Polymake, Singul
| | | |\___ \| |     / _ \ | |_) |  |  Type "?Oscar" for more information
| |_| | ___) | |___ / ___ \|  _ <   |  Manual: https://docs.oscar-system.org
 \___/ |____/ \____/_/   \_\_| \_\  |  1.2.0-DEV #master f489220 2024-06-24
```

What is Oscar?

- **O** pen
- **S** ource
- **C** omputer
- **A** lgebra
- **R** esearch

Why Julia?

- Interactive
- As fast as C
- Solves 2-language problem
- Not maintained by us
- Modern
- Interoperates well with C
- (Originates at the MIT, group of Alan Edelman)

Intro

Given some finite extension

$$A/B$$

with a norm map $N : A \to B$ and some $b \in B$, find one/all $a \in A$ s.th.

$$N(a) = b$$

.

First Examples

- $K/\mathbb{Q}$ a number field (absolute norm equation)
- K/k number fields (relative norm equation)
- $\mathcal{O}_K/\mathbb{Z}$ (Diophantine case)
- $\mathbb{Z}[\alpha]/\mathbb{Z}$ (for Thue equations)
- K/k finite fields
- K/k local fields
- $\mathbb{I}_K/\mathbb{I}_k$ idele-ic case

... and the decision problems as well. ... and function fields.

Motivation/Applications

- In representation theory of finite groups: norm equations determine/ are used to find minimal fields for the representation.
- Points on conics (= isotropic vectors for quad. forms) are used in elliptic curves.
- Solving Thue equations starts by solving norm equations.
- (Some) Embedding problems reduce to norm equations
- Base case of Galois cohomology

Broadly

Different cases require different techniques and show different runtime characteristica:

- K/k number fields, K/k normal: S-units and linear algebra
- K/k number fields, not normal: very interesting!
- $\mathcal{O}_K/\mathbb{Z}$: S-units and lattice points in polytopes.
- K/k finite fields: irreducibility and roots.
- K/k local fields: finite fields and linear algebra.
- $\mathbb{I}_K/\mathbb{I}_k$: local fields and their mult. group.

Decision Problems

- finite fields: no problem, norm is surjective
- K/k number fields, cyclic case: Hasse norm theorem: solvable iff locally solvable everywhere
- K/k normal: “known” obstacle to Hasse norm theorem, the *Knot*
- K/k not normal: Knot is known in some cases.
- K/k local, unramified: valuation only, trivial

Finite Fields

K/k finite fields, $b \in k$, $b \neq 0$.

- pick random irreducible monic polynomial f of degree $[K : k]$ with constant term $(-1)^{[K:k]}b$
- return a root a of f
- Steel (approx. 2002) from Shoup (s.t. before), folklore

In almost all other cases we have to work.

Number Fields and Rings

Now fix a finite extension K/k of number fields.
Fundamental idea: $a \in K$ s.th. $N(a) = b$ is a S-unit. Find a suitable set S, compute the S-unit group and find a.
Problem:

- S will depend on b, but may depend on K as well
- for number rings, we also want integrality
- for non Dedekind domains using ideals (and S-units) is tricky

Roughly

T a set of ideals in K and S in k s.th.

$$N : T\text{-units in } K \to S\text{-units in } k$$

is well defined. Assume that the S- and T-unit groups are given algorithmically, ie.

- as an abstract abelian group
- with disc. log and disc. exponential

Then N can be constructed explicitly as a map between abelian groups, and the rest is easy.

Example: Number Field

Want

$$N(b) = 31$$

for $b \in \mathbb{Q}(\sqrt{10})$:

```
julia> k, a = quadratic_field(10)
(Real quadratic field defined by x^2 - 10, sqrt(10))

julia> zk = maximal_order(k)
Maximal order of Real quadratic field defined by x^2 - 10
with basis AbsSimpleNumFieldElem[1, sqrt(10)]

julia> a = 31
```

Example: Number Field

We choose $S = \{31\}$ and T the primes above.

```
julia> S, mS = sunit_group([31])
(Z/2 x Z, SUnits map of Rational field for ZZRingElem[31]
)

julia> T, mT = sunit_group(prime_ideals_over(zk, 31))
(Z/2 x Z^(3), SUnits  map of k for AbsSimpleNumFieldOrderIdeal[<31, sqrt(1
Norm: 31
Minimum: 31
two normal wrt: 31, <31, sqrt(10) + 14>
Norm: 31
Minimum: 31
two normal wrt: 31]
)
```

Example: Number Field

Now we set up the norm map: Using `mT` to map abstract generators for the T-unit group into elements on K, then applying the norm and finally using the disc. log in the S-units (of $\mathbb{Q}$), via the preimage of `mS`. All of this is collected in an (abstract) homomorphism.

```
julia> N = hom(T, S, [preimage(mS, norm(mT(x)))
                                    for x = gens(T)])

Map
  from Z/2 x Z^(3)
  to Z/2 x Z
```

Example: Number Field

Now testing for solvability just requires to write a as an element of S and using the abstract norm map... In order to get a solution, the abstract preimage has to be converted into an element of K again.

```
julia> preimage(mS, a)
Abelian group element [0, 1]

julia> has_preimage(N, ans)
(true, Abelian group element [0, -1, 0, 1])

julia> mT(ans[2])
3*sqrt(10) + 11

julia> norm(ans)
31
```

Problem(s)

Trying for $K = \mathbb{Q}(\sqrt{34})$, we see that

$$\mathcal{O}_K^* = \langle -1, 35 - 6\sqrt{34} \rangle$$

Since $N(35 - 6\sqrt{34}) = 1$, there is no integral element with norm -1.
However

$$N(\frac{1}{3}\sqrt{34} - \frac{5}{3}) = -1$$

so in general finding S and T is non-trivial, T cannot just depend on the RHS.
Furthermore, since units can be **extremely** large, solutions can not be expected to be small.

Factored elements

One (well known) improvement is to use factored elements: since units are (frequently) huge, we use a multiplicative representation

$$\prod \alpha_i^{n_i}$$

for (smallish) α_i and (largeish) exponents $n_i \in \mathbb{Z}$.

- Magma: `ProductRepresentation` or `Raw`
- Pari/gp: $\mathbb{Z}[K]$ presentation
- Oscar: factorised elements, `FacElem`

We need to replace `sunit_group` by `sunit_group_fac_elem`...or even `sunit_mod_units_group_fac_elem`. And add evaluate at the end.
Note: we can also obtain a `compact_presentation`.

Norm Equations - Factored Elements

```
julia> T, mT = sunit_group_fac_elem(prime_ideals_over(maximal_order(k), 31
(Z/2 x Z^(3), SUnits (in factored form) map of Factored elements over Real
)
...
julia> N = hom(T, S, [preimage(mS, norm(mT(t))) for t = gens(T)])
...
julia> preimage(N, ans)
Abelian group element [0, -1, 0, 1]
julia> mT(ans)
(2*sqrt(10))^2*(sqrt(10) + 17)^-1*7^-1*71^-1*67^1*4^-2*13^3*(sqrt(10) + 9)

julia> evaluate(ans)
3*sqrt(10) + 11
```

Ideals

So:

$$N(a) = b$$

for a a T-unit. How do we find T?
Observation:

- wlog b is integral
- if $N(a) = b$, then $N(a\mathcal{O}_K) = b\mathcal{O}_k$ as well
- on ideals we have unique factorisation

So, assume we have a solution $a \in K$ and any integral ideal $\mathfrak{A}$ of the correct norm.
Then $N(a\mathfrak{A}^{-1}) = \mathcal{O}_k$.

Ideals - Hilbert 90 and Normal Fields

Simplifying to $k = \mathbb{Q}$ and $K/\mathbb{Q}$ normal, we have Hilbert 90 for ideals:

Theorem

$N(\mathfrak{A}) = 1$ *iff* $\mathfrak{A} = \prod P_i^{1-\sigma_i}$.

Or even more fancy (I_K the group of invertable ideals of K):

Theorem

Both $H^1(\mathit{Gal}(K/k), I_K)$ *and* $H_1(\mathit{Gal}(K/k), I_K)$ *are trivial.*

Ideals - Hilbert 90 and Normal Fields

So $N(a) = b$, $N(\mathfrak{A}) = b\mathcal{O}_k$ so $N(a\mathfrak{A}^{-1}) = \mathcal{O}_k$ and

$$a\mathfrak{A}^{-1} = \prod P_i^{1-\sigma_i}$$

If $\mathrm{Cl}_K = \langle \mathfrak{B}_j | 1 \le j \le k \rangle$, then for any P_i there is some α_i s.th. $P_i = \alpha_i \prod \mathfrak{B}_j^{n_{i,j}}$, thus

$$a\mathfrak{A}^{-1} = \prod \alpha_i^{1-\sigma_i} \prod \mathfrak{B}_i^{n_{i,j}(1-\sigma_i)}$$

Sorting:

$$a \prod \alpha_i^{\sigma_i - 1} \mathcal{O}_K = \mathfrak{A} \prod \mathfrak{B}_i^{n_{i,j}(1-\sigma_i)}$$

The LHS is now a solution as well and the RHS has a known support.
Hence: we have a set T of prime ideals s.th. if there is a solution, there is one with support in T!
T depends on the RHS b and the class group.

Non-normal Fields

- Siegel (1973), Bartel (1980): choose T as the set of primes of norm bounded by the Minkowski constant of the normal closure.
- Simon (1998) choose T to generate the class groups of all relative cyclic subfields of the normal closure.

Pros and Cons:

- Bartel: no need to compute in a large field, many primes
- Simon: many class groups, small set T, can use GRH

Would like small set T, use GRH and do computations in K only.

Norm 1 Ideals

Fix K/k finite. $N = N_{K/k}$ denotes the norm (on elements and ideals).
For ideals $\mathfrak{A}$ and $\mathfrak{B}$ of norm $1 = \mathcal{O}_k$ s.th. $[\mathfrak{A}] = [\mathfrak{B}]$ in the class group we get

$$\mathfrak{A} = \beta\mathfrak{B}$$

and $N(\beta)\mathcal{O}_k = \mathcal{O}_k$, so $N(\beta) \in U_k$, a unit:

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & & \downarrow & & & & \\ 1 & \longrightarrow & \frac{U_K}{\{u|N(u)=1\}} & \longrightarrow & \frac{\{a|N(a)\in U_k\}}{\{a|N(a)=1\}} & \longrightarrow & \frac{\{\mathfrak{A}|N(\mathfrak{A})=\mathcal{O}_k\}}{\{a|N(a)=1\}} & \longrightarrow & \mathrm{Cl} \\ & & & & \downarrow N & & & & \\ & & & & U_k & & & & \end{array}$$

Norm 1 Ideals

Collapsing from the left:

$$\begin{array}{ccccccccc} & & 1 & & & & 1 & & \\ & & \downarrow & & & & \downarrow & & \\ 1 & \longrightarrow & \frac{\{a|N(a)\in U_k\}}{U_K\{a|N(a)=1\}} & \longrightarrow & \frac{\{\mathfrak{A}|N(\mathfrak{A})=\mathcal{O}_k\}}{\{a|N(a)=1\}} & \longrightarrow & X & \longrightarrow & 1 \\ & & \downarrow N & & & & \downarrow & & \\ & & \frac{U_k}{N(U_K)} & & & & \mathrm{Cl}_K & & \end{array}$$

And since $U_k^n < N(U_K)$, we get

- $\frac{U_k}{N(U_K)}$ is finite
- $\frac{\{a|N(a)\in U_k\}}{U_K\{a|N(a)=1\}}$ is finite
- X, the subgroup of Cl_K gen. by ideals of norm 1 is finite,

so:

Norm 1 Ideals

$$\begin{array}{ccccccccc} & & 1 & & & & 1 & & \\ & & \downarrow & & & & \downarrow & & \\ 1 & \longrightarrow & \frac{\{a|N(a)\in U_k\}}{U_K\{a|N(a)=1\}} & \longrightarrow & \frac{\{\mathfrak{A}|N(\mathfrak{A})=\mathcal{O}_k\}}{\{a|N(a)=1\}} & \longrightarrow & X & \longrightarrow & 1 \\ & & \downarrow N & & & & \downarrow & & \\ & & \frac{U_k}{N(U_K)} & & & & \mathsf{Cl}_K & & \end{array}$$

Yields:

$$\mathsf{Cl}_K^1 := \frac{\{\mathfrak{A} \mid N(\mathfrak{A}) = \mathcal{O}_k\}}{\{a \mid N(a) = 1\}}$$

is finite!

Partly constructive, $X = \{x \in \mathsf{Cl}_K \mid \exists \mathfrak{A} \in x, N(\mathfrak{A}) = 1\}$

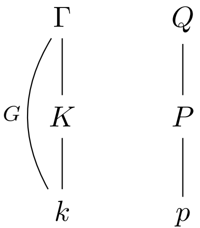
- we can generate ideals of norm 1
- given two such ideals we can check equality in X (and Cl_K^1)

So we can just do this to get a subgroup, but completeness?
Similarly, we can test if $\mathfrak{A}$ and $\mathfrak{B}$ coincide in Cl_K^1: $\mathfrak{A} = \beta\mathfrak{B}$ and $N(\beta) \in N(U_K)$.
So we can obtain a subgroup of Cl_K^1, but completeness?

Assume $\mathrm{Cl}_K^1 = \langle \mathfrak{A}_i | i \rangle$, then we solve norm equations as before: (wlog $b \in \mathcal{O}_k$), assume $N(a) = b$

1. find $\mathfrak{A} \le \mathcal{O}_K$ s.th. $N(\mathfrak{A}) = b\mathcal{O}_k$
2. then $N(a\mathfrak{A}^{-1}) = \mathcal{O}_k$
3. thus $a\mathfrak{A}^{-1} \in \mathrm{Cl}_K^1$
4. there is β, $N(\beta) = 1$ and $a\mathfrak{A}^{-1} = \beta\mathfrak{A}_i$
5. then $a\beta^{-1}\mathcal{O}_K = \mathfrak{A}\mathfrak{A}_i$ yields a solution with a known support.

The set S



- Γ be the normal closure of K/k
- $Q/P/p$ (unramified) primes
- $G = \text{Aut}(\Gamma/k)$

Then $P\mathcal{O}_\Gamma = \prod Q_i$. G operates transitively on the primes, so for $Q = Q_1$ we have $Q_i = Q_1^{s_i}$ for $s_i \in G$, hence, $\sigma := \sum s_i \in \mathbb{Z}[G]$:

$$P\mathcal{O}_\Gamma = Q^\sigma$$

Let $\mathfrak{A}$ be an ideal in K, $N(\mathfrak{A}) = \mathcal{O}_k$ and supported only at primes above p.

$$\mathfrak{A}\mathcal{O}_\Gamma = \prod P_i^{n_i}\mathcal{O}_\Gamma = \prod Q^{n_i\sigma_i} = Q^{\sum n_i\sigma_i} =: Q^\tau$$

Since $N(\mathfrak{A}) = \mathcal{O}_k$, also $N_{\Gamma/k}(\mathfrak{A}\mathcal{O}_\Gamma) = \mathcal{O}_k$ as well. So

$$\tau \in I_G = \langle 1 - s | s \in G\rangle \leq \mathbb{Z}[G],$$

the augmentation ideal.
$\mathfrak{A} \subset K$, so τ is stable under $\mathrm{Aut}(\Gamma/K)$, $\tau s = \tau$ for all $s \in \mathrm{Aut}(\Gamma/K)$!
Thus: $\alpha^\tau \in K$ and $N(\alpha^\tau) = 1$ for all $\alpha \in \Gamma$.

Let $\mathrm{Cl}_\Gamma = \langle [S_i] | i \rangle$ for unramified ideals S_i and $\mathfrak{A} \leq \mathcal{O}_K$ of norm 1 as above, so $\exists S = \prod S_i^{n_i}$ and $\alpha \in \Gamma$:

$$\mathfrak{A}\mathcal{O}_\Gamma = R^\tau = (\alpha S)^\tau = \alpha^\tau S^\tau$$

Thus in Cl_K^1 all (unramified) ideals of norm 1 come from generators of the class group of Γ. — GRH or unconditional.
(The (few) (fintely many) ramified ideals of norm 1 are easily added.)

Let $\mathfrak{m}$ be an integral ideal in k s.th. for all units $u \in \mathcal{O}_k^*$, $u \equiv 1 \bmod \mathfrak{m}$ we have that $u = v^n$ for $n = [K : k]$
Let $X \leq \mathrm{Cl}_{\mathfrak{m}\mathcal{O}_K}$ be subgroup of rays containing ideals of norm 1. Then

$$1 \to X \to \mathrm{Cl}_{\mathfrak{m}\mathcal{O}_K}$$

is exact:
$\mathfrak{A} = \mathfrak{B}$ in $\mathrm{Cl}_{\mathfrak{m}\mathcal{O}_K}$ implies $\mathfrak{A} = \beta\mathfrak{B}$ and $\beta = 1 \bmod \mathfrak{m}\mathcal{O}_K$. $N(\mathfrak{A}) = N(\mathfrak{B}) = \mathcal{O}_k$ implies $N(\beta) \in U_k$. Since $N(\beta) = 1 \bmod \mathfrak{m}$. So $N(\beta) = \epsilon^n$ and $N(\beta/\epsilon) = 1$ and $\mathfrak{A} = \mathfrak{B} \in \mathrm{Cl}_K^1$ as well.
This is easier to work with than Cl_K^1 directly - but misses the primes in $\mathfrak{m}$.

The algorithm(s)

Solve $N(a) = b$.

1. Find a suitable $\mathfrak{m}$
2. $S = \{\}$, $X = \langle \mathcal{O}_K \rangle \leq \mathrm{Cl}_\mathfrak{m}$
3. for p (unramified) primes in k (coprime to $\mathfrak{m}$) do
   1. $p\mathcal{O}_K = \prod P^i$ with $N(P_i) = p^{f_i}$
   2. Let $n_{i,j}$ a $\mathbb{Z}$-basis for $\sum n_{i,j} f_i = 0$
   3. if $\prod P_i^{n_{i,j}} \notin X$, then add p to S and enlarge X

We can

- use the Minkowski/ Bach/ Belabas et. al./ ... bound for S,
- stop the search when X did not change for ? primes p.

We have to supplement with the primes in $\mathfrak{m}$ and the ramified ones.
T is the set of primes above S.

Knots - the Decision Problem

Let $\mathbb{I}_K$, resp. $\mathbb{I}_k$ the idele groups, then Scholz (1936) defined the (number) knot

$$\delta_{K/k} := N(\mathbb{I}_K)/N(K^*)$$

to measure the error in the Hasse norm theorem:

Theorem

For cyclic extensions K/k, the knot is trivial, hence solvability can be tested locally.

Well, actually, not, he studied:

> *Wir nennen K_0 die Restklassengruppe der Normreste nach den Zahlnormen den (Gesamt-, Zahl-) Knoten $\mathcal{K} = \mathcal{K}_\alpha$ von K.*

(We call the quotient group of norm residues modulo norms the (total-, number-) knot.) Free of ideles.

Knots - the Decision Problem

$$\delta_{K/k} := N(\mathbb{I}_K)/N(K^*)$$

- The knot is trivial for cyclic extensions.
- There are infinitely many bi-quadratic fields where the knot is non trivial, but also infinitely many where the norm theorem holds. Newton et. al. studied this quantitatively.
- Testing local solvability is also not always easy.
- Jehne defined many more knots in 1979.

For K/k normal, the knot can be computed classically (Tate)

$$1 \to \delta_{K/k} \to H^2(G, \mathbb{Q}/\mathbb{Z}) \to \oplus H^2(G_p, \mathbb{Q}/\mathbb{Z})$$

(The sum runs over all places of K and G_p are the decomposition groups, the local Galois groups.)
For abelian G, this is easy, for general G one needs more group theory (Schur multipliers, group cohomology).

Strategy

If not locally solvable: return fail.
Start with choosing S to contain

- all primes dividing the RHS
- all ramified primes
- enough primes to likely generate Cl_K^1

And try to find a solution using U_S units.
If this fails then

- if knot is trivial: increase S until it works
- use GRH (or not) to enlarge S and try again

Integral Norm Equations

Let K/k be finite and $b \in \mathcal{O}_k$. Find

$$N(a) = b$$

for $a \in \mathcal{O}_K$. Modulo units in K, this equation has only fin. many solutions.
Classical: turn into lattice problem. Let the units operate, to obtain a finite search domain.
Solve by enumeration:

- bound into a box (classical)
- cover by ellipsoids (Fincke/Pohst (1988), Jurk (1993), F.(1997)).

Very nice, beautiful pictures, slow.

Using Class Group

$$N(a) = b$$

For $a \in \mathcal{O}_K$. Any solution a generates a principal ideal $a\mathcal{O}_K$ of norm $b\mathcal{O}_k$. So

1. find all integral ideals of norm $b\mathcal{O}_k$
2. for each ideal test if principal
3. for each principal ideal test if the generator can be made to work

Let P_i be the primes in $\mathcal{O}_K$ dividing a prime in $\mathcal{O}_k$ of the support of b.
We have $N(P_i) = p_{j_i}^{f_i}$ and, $P_i \rightsquigarrow c_i \in \mathrm{Cl}_K$.
To list all integral principal ideals of the correct norm is a classical combinatorial problem:
Find $n = (n_i)_i$ s.th.

- $n_i \geq 0$ for all i (integrality)
- Let $A = (v_{p_j}(P_i))_{i,j}$ and $An = (v_{p_j}(b))_j$ (norm)
- $\sum n_i c_i = 0$ (principality)

Then $\prod P_i^{n_i}$ is an integral principal ideal of the correct norm (up to units).

Using S-Units

The same, without the class group, using S-units directly:

- find $S := \{P \le \mathcal{O}_K | v_P(b) > 0\}$
- compute $U_S/U_K = \langle \epsilon_i \mid i \rangle$
- $A := (v_{P_j}(\epsilon_i))_{i,j}$, $B := (v_p(N(\epsilon_j)))_{i,j}$
- solve $An \ge 0$ s.th. $Bn = (v_p(b))_p$ and (try to) adjust by units

In all cases, this is a combinatorial problem: points in a lattice (in ellipsoids) or points in a polytope.

Non-maximal Order

Final case:

$$N(a) = b$$

for $a \in \mathcal{O}$ a non-maximal order. This is used e.g. in Thue equations where $\mathcal{O} = \mathbb{Z}[\alpha]$ is an equation order.
If $N(a) = b$ for $a \in \mathcal{O} \subseteq \mathcal{O}_K$, then any solution is also one from the last case.
Step 1: solve in the maximal order, find all solutions.
Since $U_K/\mathcal{O}^*$ is finite, any solution in $\mathcal{O}$ is obtained from one in $\mathcal{O}_K$ and a unit $\epsilon \in U_K/\mathcal{O}^*$ of norm 1.

For the final step, assuming b is coprime to the conductor $\mathfrak{f}$ of $\mathcal{O}$ in $\mathcal{O}_K$, then a is also coprime, so

$$\begin{array}{ccccccc} & & & & & & a \in (\mathcal{O}_K/\mathfrak{f})^* \\ & & & & & & \downarrow \\ 0 & \longrightarrow & \mathcal{O}^* & \longrightarrow & U_K & \longrightarrow & (\mathcal{O}_K/\mathfrak{f})^*/(\mathcal{O}/\mathfrak{f})^* =: X \end{array}$$

This is always used to compute $\mathcal{O}^*$ or $\mathcal{O}_K^*/\mathcal{O}^*$, but can also be used in the last step: solutions in $\mathcal{O}$ correspond to preimages in U_K of $a \in X$

- https://oscar-system.org
- The Oscar book: The Computer Algebra System OSCAR
- development on https://github.com/oscar-system/Oscar.jl
- most number theory https://github.com/thofma/Hecke.jl
- foundations on https://github.com/Nemocas/AbstractAlgebra.jl
- optimizations https://github.com/Nemocas/Nemo.jl
- active slack community https://oscar-system.org/slack

Features (Number Theory)

- number fields, (non)-simple extensions
- orders, maximal order
- class groups, (S-)units
- Galois groups, automorphisms
- constructive class field theory
- localizations and completions
- Galois cohomology
- algebras and orders
- lattices, automorphisms, isomorphisms
- function fields and orders
- verified real computations using arb
- ...