Outline for Sage lecture:

where to go : www.sagemath.org

(download Sage for home computer or use online through remote servers)
easiest for Mac users. requires email.
online account to store "worksheets"

what is Sage? open source software, also acts as front end to
other open source mathematics
software e.g. Pari/GP
(GAP)

Programming language is Python

Try standard tutorial in Sage documentation.

upshot is that many programming commands feel like natural language.

e.g. [factor(n) for n in range(1001, 1021)]

output is list L, to take components, type L[3]
to take 4th element in list.

(In python, first element of list is labeled "0")
common to C, C++

Many examples in tutorials which will get you up to speed quickly.

In Sage, objects and routines on objects belong to classes

Great because this is how mathematicians think too.

"class" is sage's version of mathematical category.

Finally, Sage is good for number theory.

(developed by W. Stein, now at Washington, works in number theory - Galois reps and elliptic curves - and his friends.

Also subsumes all of GAP, which is very polished software)

Still, because Sage is relatively new (~10 yrs old), and a constant work-in-progress, there can be occasional bugs.

That is less likely with basic routines.

Another source for material: Stein's book on algebraic number theory.

modular.math.washington.edu/books/ant/ant.pdf

which incorporates routines from Sage.

Also: Henri Cohen, A Course in Computational Algebraic Number Theory Springer GTM 138. "148 algorithms" in pseudocode.

Main computational problems for algebraic number theory (à la Cohen)

p.214: Given $K = \mathbb{Q}(\theta)$ θ: primitive elt.

(1) Compute integral basis of $\mathcal{O}_K$, find decomposition of rational primes in $\mathcal{O}_K$, divisibility of other ideals in $\mathcal{O}_K$ by $\mathfrak{p}$: prime (fractional)

(2) Compute Galois gp. of Galois closure of K.

(3) Compute fundamental units / regulator / class gp / class #

(4) Determine if ideal in $\mathcal{O}_K$, presented as list of generators, is principal

In exercises from Neukirch, saw that by changing our convex set in lattice argument, get better bound:

Every ideal $\mathfrak{a} \neq 0$ in $\mathcal{O}_K$ contains $a \neq 0$ with

$$|N_{K/\mathbb{Q}}(a)| \leq M_K \cdot \underbrace{(\mathcal{O}_K : \mathfrak{a})}_{N(\mathfrak{a})} \quad \text{with } M_K = \text{Minkowski bound} = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}$$

$\Rightarrow$ every ideal class contains integral rep with norm $\leq M_K$

Use this quantitatively: $K = \mathbb{Q}(\sqrt{10})$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$

$|d(\mathcal{O}_K)| = 40$

s = pairs of cx embeddings $= 0$

$n = 2$.

$$M_K = \frac{1}{2}\sqrt{40} = \sqrt{10} \text{ with } \lfloor \sqrt{10} \rfloor = 3.$$

(computed in Sage by `K.minkowski_bound()`, `.n()` gives numerical approx.)

Note: Can refine our earlier statement: class gp. is generated by prime ideals lying over $p \in \mathbb{Z}$ with $p \leq M_K$

If $N(\mathfrak{a}) \leq M_K$ and $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ then $N(\mathfrak{p}_i) \leq N(\mathfrak{a}) \leq M_K$

$\mathcal{O}_K/\mathfrak{p}$ is finite field of char p, so $p \mid N(\mathfrak{p}_i)$ i.e. $p \leq M_K$.

So in our example, analyze primes above 2, 3 in $\mathbb{Q}(\sqrt{10})$.

Analyze $2 \cdot \mathcal{O}_K$ via $x^2 - 10 \equiv x^2 \pmod 2$

so 2 ramifies : $\mathfrak{p}^2 \mid (2)$ with $\mathfrak{p} = \langle 2, \underbrace{\text{monic linear factor @ } \theta \text{ reducing to } x \bmod 2}_{\sqrt{10}} \rangle$

Question: Is this principal? Is there some a, b

s.t. $\langle a + b\sqrt{10} \rangle = \langle 2, \sqrt{10} \rangle$?

If so, then have soln to $a^2 - 10b^2 = N(a+b\sqrt{10}) = \pm 2$

check no solns, e.g. ± 2 are non-res. mod 5.

So no. And already know that $\langle 2, \sqrt{10} \rangle^2 = 2\mathcal{O}_K$ is principal,

so we have elt. of order 2 in $J_K \neq K^\times$.

To finish, analyze primes above 3, they split since $x^2 - 10 \equiv x^2 - 1 \ (3)$
$= (x^2+1)(x-1)$

so have ideals $\mathfrak{p}_3, \mathfrak{p}_2$ over (3) of form

$\langle 3, 1 + \sqrt{10} \rangle$, $\langle 3, 2 + \sqrt{10} \rangle$. Show they differ by principal ideal

$\Rightarrow$ at most 3 ideal classes, and have elt. of order 2

$\Rightarrow$ $J_K / K^\times \simeq \mathbb{Z}/2\mathbb{Z}$.

verify in Sage using generator

How does Sage calculate class #? It appears in special value of certain generating function — $L(s, \chi_d)\Big|_{s=1}$ Dirichlet L-function $\sum_{n=1}^{\infty} \left(\frac{\blacksquare}{n}\right)\left(\frac{n}{d}\right)\frac{1}{n^s}$

But for general # fields, we do use above techniques, combined with facts about Dedekind zeta function.

For computing Galois gps, $K = \mathbb{Q}(\theta)$, $G : \mathrm{Gal}(\mathrm{Spl}(\phi_\theta(x))$

two facts are useful: (1) if $\deg(\phi_\theta) = n$,

then G is transitive subgp. of S_n

(since G acts on roots of ϕ_θ, one for orbit each irreducible factor)

(2) $G \subseteq A_n$: alternating subgp $\iff$ disc. (ϕ_θ) is square.

$$\| $$

$$\prod_{i<j} (\theta_j - \theta_i)^2 =: f^2$$

then $\sigma \cdot f = \mathrm{sgn}(\sigma) f$

E.g. for cubic extensions, this determines Galois gp since only transitive sgps are $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ and S_3.