
581b -- finiteness of the class group

* Make sure to mention that 581d will be on a number theory topic
  this week -- elliptic curve computation in Sage.

* Announce ECC is next week: http://2010.eccworkshop.org/

* Plan for course:

   * Prove the main theorem of the course (starts this week, may
     continue to next week): finiteness of class group; Dirichlet's
     unit theorem (both for ring of integers of number fields)

   * Key theorems and structure that make it possible to compute (next week):
     computing O_K, factoring p*O_K, computing class group
     (and examples of how to use Sage to compute these things...)

   * Local structure (and Galois representations):
     Theorems about decomposition and inertia groups,
     Definition of Frobenius elements, zeta functions, L-series

   * Adeles, ideles, and finiteness of the class group: a language
     that you must know to understand a lot of number theory
     literature.

   * Class field theory: statements using both ideal and idelic language

   * If time permits -- Automorphic forms and representations, the
     Langlands program, what did that new Fields Medalist do? (prove
     the "Fundamental Lemma") (Adeles are required to talk about
     this stuff...)

The class group of a Dedekind domain

Recall:

  R = Dedekind domain (noetherian, krull.dim(R)<=1,
                       R integrally closed in K=Frac(R))

  Div(R) = group of fractional ideals

Using "Div" since like divisors on a curve; notation only good because
of following theorem, we proved completely last week:

Theorem: Div(R) is a free abelian group (free on the nonzero prime ideals of R).

Defn: A *principal fractional ideal* is one of the form:
               I = alpha*R for 0 != alpha in K.

Defn: Prin(R) = group of principal fractional ideals

Defn: Cl(R) = Div(R) / Prin(R)   <------- so it's an abelian group

Prop: Prin(R) isom K^* / R^*.
Proof: K^* --> Prin(R), by definition.
     kernel = {u in K^* : u*R has no prime factors} = {u in K^* : u*R = R } = R^*
   Note: if u in K^* with u*R = R, then u in R, since 1 in R, so u=u*1 in R.

Thus exact sequence:

   1 --> R^* --> K^* --> Div(R) --> Cl(R) --> 1

Our main goal is to prove the following *deep theorem* (the deepest in this class?):

Theorem: If R = O_K is ring of integers of number field, then Cl(R) is *finite*.

Strategy of proof:

  * (easy) Use maps K \--> C and log to embed O_K into some Euclidean space R^n.

  * (hard) Use a geometric argument ("geometry of numbers") to show that each ideal class in Cl(R) contains an ideal I with
          Norm(I) <= (4/pi)^s*(n!/n^n)*sqrt(|d_K|)
    Here, Norm(I) = #(R/I) and d_K = "discriminant" of K.

  * (trivial) Observe that there are finitely many ideals of bounded norm.

Remark: Above theorem not true in general! Even "Norm(I)" doesn't make sense in general, since R/I need not be finite, e.g., if R=Q[x] and I=(x), then R/I = Q is infinite. Also, whatever d_K is, it wouldn't make sense in general either.

Example in which Cl(R) is not finite.

  R = C[x,y]/(y^2 - (x^3 + 1)),   C = complex numbers

The nonzero prime ideals of R are the ideals

        P_{a,b} = (x-a, y-b)

where (a,b) is a complex point on the affine curve y^2 = x^3+1.

A principal fractional ideal is got by a taking any rational function alpha(x,y) = f(x,y)/g(x,y), with f,g polys, and considering the fractional ideal it generates. We think about this fractional ideal in terms of its prime factorization (divisor!), so

    alpha*R = prod P_{a_i,b_i} / prod Q_{c_j, d_j}

where the (a_i,b_i) are the zeros of f(x,y) and (c_j,d_j) the poles,
with appropriate multiplicities.

Claim:
    P_{a,b} is not in Prin(R)

Proof: If alpha=f/g and alpha*R = P_{a,b}, then alpha is a rational
function on y^2=x^3+1 which has no poles and one zero. It thus
extends to a rational function of degree 1 on the projective closure C
of y^2=x^3+1, which would extend to an isomorphism to P^1 (see ch 1 of
Hartshorne), a contradiction since C has genus 1 and P^1 has genus 0.

NOTE: Totally false if we instead use a genus 0 curve, e.g., C[X].

To see that Cl(R) is infinite, take any nonzero point z = (a,b)
and note that P_{a,b} defines a nonzero element of Cl(R).

  * The group law is compatible with the the group operation on Cl(R).
    (explain this)

  * For n=1,2,3,..., get P_{n*z} distinct primes that are all nonzero
    elements of Cl(R), so Cl(R) is infinity.

In fact, Cl(R) is *uncountable*.

So there is something very special with R = O_K that we haven't seen
so far, which makes the classgroup small.

DISCRIMINANTS:

A key step in our argument is to introduce a notion of discriminant D of
O_K, and note that there are only finitely many ideals with norm at
most |D|.

Definition: Let a1, ..., an be a Q-basis for K. Then
   Disc(a1,...,an) = det(Tr(ai*aj))

Let R = ring of integers O_K of K.

Definition:

    Disc(R) = Disc(a1,...,an)

where a1,...,an any basis for R as a ZZ-module. Often one writes Disc(K) := Disc(R).

Remark: Disc(R) is nonzero and well defined. (Exercise)

More generally, if S is any finite index subring of R, let Disc(S) be the discriminant of any ZZ-basis for S.

Proposition: Disc(S) = Disc(R) * [R:S]^2

NORMS OF IDEALS:

Definition (Lattice Index):

L, M -- "lattices" in vector space V over Q
so L, M are Z-module of rank dim(V) st Q*L=Q*M = V.

[L:M] =defn= |det(A)| where A any linear automorphism st A(L)=M.

If M contained in L, then [L:M]=#(L/M) is usual index
In general, for any M,L,N:

[L:N] = [L:M]*[M:N]

by basic properties of linear transformations and determinants.

Defn:

I - fractional ideal of R
Norm(I) = [R : I]

which is a nonzero rational number.

Prop:
B = positive integer
Then set of integral ideals I in R with norm(I) <= B is finite.

Proof:

An integral ideal I is a subgroup of R of index equal to the norm of I. If G is any finitely generated abelian group, then there are only finitely many subgroups of G of index at most B, since the subgroups of index dividing an integer n are all subgroups of G that contain nG, and the group G/nG is finite.