Course Notes Template

Niven Achenjang

April 24, 2022

These are my course notes for "Class name" at School name. Each lecture will get its own "chapter." These notes are live-texed or whatever, so there will likely to be some (but hopefully not too much) content missing from me typing more slowly than one lectures. They also, of course, reflect my understanding (or lack thereof) of the material, so they are far from perfect.[1] Finally, they contain many typos, but ideally not enough to distract from the mathematics. With all that taken care of, enjoy and happy mathing.

The instructor for this class is Prof name, and the course website can be found by clicking this link. Extra extra read all about it

Contents

[1] In particular, if things seem confused/false at any point, this is me being confused, not the speaker

List of Figures

List of Tables

1 GSS Week 1: Motivic Homotopy Theory

Notes and problems sets for GSS lectures can be found at this link.

1.1 Philippe Gille Lecture 1 (7/12): Torsors over Affine Curves

1.1.1 Administrative stuff

Some links

- `http://math.univ-lyon1.fr/homes-www/gille/prenotes/gille_pcmi_part1.pdf` (notes)
- `http://math.univ-lyon1.fr/homes-www/gille/prenotes/beamer_gille_pcmi_part1.pdf`
- `http://math.univ-lyon1.fr/homes-www/gille/prenotes/gille_pcmi_exercices.pdf`
- `http://math.univ-lyon1.fr/homes-www/gille/prenotes/gille_pcmi.pdf`

1.1.2 Start of Material

In algebraic geometry, we like to adapt notions from differential geometry. Vector bundles, for example, were studied in differential geometry before algebraic geometry. Another differential notion one would like to adapt is that of 'principal G-bundles' or 'principle homogeneous spaces.' Sounds like the algebraic theory of these started with Serre and Grothendieck.

Some references

- Knus (?): Quadratic and homogeneous (?) forms over rings
- Donaldson (?) - someone else: groupe algebraique

Today we will work over rings (i.e. affine schemes) instead of arbitrary base schemes. The general theory is not much different since most definitions are of a local nature.

1.1.3 Swan-Serre Correspondence

There is a correspondence between projective finite modules of finite rank and vector bundles arising in the case of a paracompact topological space. We'll make this explicit in the case of affine schemes.

Definition 1.1.1. Let R be a (commutative, unital) ring. Let M be an R-module. We let $V(M)$ denote the R-scheme $V(M) = \operatorname{spec}(\operatorname{Sym}^* M)$, so it represents the R-functor

$$S \mapsto \operatorname{Hom}_{S\text{-mod}}(M \otimes_R S, S) = \operatorname{Hom}_{R\text{-mod}}(M, R).$$

This is the **vector group scheme attached to** M. This construction commutes w/ arbitrary base change of rings $R \to R'$.

Proposition 1.1.2. *The functor $M \to V(M)$ induces an antiequivalence of categories between the category of R-modules and that of vector group schemes over R. An inverse functor is $\mathfrak{G} \mapsto \mathfrak{G}(R)$.*

Remark 1.1.3. Say M is locally free of finite rank w/ dual $M^\vee$. In this case, $\operatorname{Sym}^*(M)$ is of finite presentation. Also, the R-functor $S \mapsto M \otimes_R S$ is representable by the affine R-scheme $V(M^\vee) =: W(M)$.

Romagny has shown that the finite locally freeness condition on M is a necessary condition for the representatibility of $W(M)$ by a group scheme.

Definition 1.1.4. Fix some $r \geq 0$. A **vector bundle of rank r over** $\operatorname{spec} R$ is an affine R-scheme X s.t. there exists a partition $1 = f_1 + \cdots + f_n$ and isomorphisms $\varphi_i : V((R_{f_i})^r) \xrightarrow{\sim} X \times_R R_{f_i}$ such that

$$\varphi_i^{-1}\varphi_j : V((R_{f_i f_j})^r) \xrightarrow{\sim} V(R^r_{f_i f_j})$$

is a linear automorphism of $V((R_{f_i f_j})^r)$ for all i, j.

Theorem 1.1.5 (Swan-Serre correspondence). *The above functor $M \mapsto V(M)$ induces an equivalence of categories between the groupoid of locally free R-modules of rank r and the groupoid of vector bundles over* $\operatorname{spec} R$ *of rank r.*

Example. Let $\operatorname{spec} S = X \to Y = \operatorname{spec} R$ be a smooth map of affine schemes of relative dimension $r \geq 1$. The tangent bundle $T_{X/Y} = V(\Omega^1_{S/R})$ is a vector bundle over $X = \operatorname{spec} S$ of dimension r.

Example. The tangent bundle of the real sphere

$$Z = \operatorname{spec}\left(\mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)\right)$$

is an example of a vector bundle of dimension 2 which is not trivial. It can be proven by differential topology (hairy ball theorem[2]), but there are also algebraic proofs. A consequence is that Z cannot be equipped with the structure of a real algebraic group.

Question 1.1.6 (Audience). *For which fields k does the sphere have a non-trivial tangent bundle?*

Answer. Not sure off the top of my head, but answer tomorrow.

1.1.4 Linear groups

Let M be a locally free R-module of finite rank, and consider the R-algebra $\operatorname{End}_R(M) = M^\vee \otimes_R M$. It is locally free of finite rank as well, so can consider the vector R-group scheme $V(\operatorname{End}_R(M))$ which is an R-functor in associate and unital algebras.

Can also consider the R-functor $S \mapsto \operatorname{Aut}_S(M \otimes_R S)$. It is representable by an open R-subscheme of $W(\operatorname{End}_R(M))$, denoted by $\operatorname{GL}_1(M)$.

Warning 1.1.7. Keep in mind that the action of the group scheme $\operatorname{GL}(M)$ on $W(M)$ (resp. $V(M)$) is a left (resp. right) action.

Fact (Nitsure)**.** If R noetherian, then M locally free of finite rank $\iff$ $\operatorname{GL}(M)$ is representable.

Notation 1.1.8. $\operatorname{GL}_r(R) := \operatorname{GL}(R^r)$.

If $\mathscr{B}$ is a locally free $\mathscr{O}_S$-algebra of finite rank, we recall that the functor of invertible elements of $\mathscr{B}$ is representable by an affine S-group scheme which is a principal open subset of $W(\mathcal{B})$. We denote is $\operatorname{GL}_1(\mathcal{B})$.

[2] There's no nonvanishing section

1.1.5 Cocycles

Let M be a locally free R-module of rank r. Consider a partition $1 = f_1 + \cdots + f_n$ w/ isomorphisms $\varphi_i : (R_{f_i})^r \xrightarrow{\sim} M \times_R R_{f_i}$. The $R_{f_i f_j}$-isos

$$\varphi_i^{-1}\varphi_j : (R_{f_i f_j})^r \xrightarrow{\sim} (R_{f_i f_j})^r$$

is linear, so defines an element $g_{i,j} \in \mathrm{GL}_r(R_{f_i f_j})$. More precisely, $(\varphi_i^{-1}\varphi_j)(v) = g_{i,j}v$ for each $v \in (R_{f_i f_j})^r$ (column vector).

Lemma 1.1.9. *These $g_{i,j}$'s form a 1-**cocycle**, i.e.*

$$g_{i,j}g_{j,k} = g_{i,k} \in \mathrm{GL}_r(R_{f_i f_j f_k})$$

for all $i, j, k = 1, \ldots, n$.

Basically just write $\varphi_i^{-1}\varphi_k = (\varphi_i^{-1}\varphi_j) \circ (\varphi_j^{-1}\varphi_k)$.

Remark 1.1.10. If we replace that φ_i's by $\varphi_i' = \varphi_i \circ g_i$ for $g_i \in \mathrm{GL}_r(R_{f_i})$, we get $g_{i,j}' = g_i^{-1}g_{i,j}g_j$, and say that the $(g_{i,j}')$ is **cohomologous** to $(g_{i,j})$.

Let $\mathscr{U} = (\operatorname{spec} R_{f_i})_{i=1,\ldots,n}$ the affine cover of $\operatorname{spec} R$. We let $Z^1(\mathscr{U}/R, \mathrm{GL}_r)$ denote the set of 1-cocycles and $\mathrm{H}^1(\mathscr{U}/R, \mathrm{GL}_r) = Z^1(\mathscr{U}/R, \mathrm{GL}_r)/\sim$ the set of 1-cocycles modulo the cohomology relation. Attached to any vector bundle $V(M)$ of rank r is a class $\gamma(M) \in \mathrm{H}^1(\mathscr{U}/R, \mathrm{GL}_r)$.

Conversely, by Ariski gluing, we can start w/ a cocycle $(g_{i,j})$ a vector bundle V_g over R of rank r equipped w/ trivializations s.t. $\varphi_i^{-1}\varphi_j = g_{i,j}$.

The upshot is that $\mathrm{H}^1(\mathcal{U}/R, \mathrm{GL}_r)$ classifies rank r vector bundles trivialized by the cover $\mathcal{U}$. Can pass to the direct limit, i.e. set

$$\check{\mathrm{H}}^1_{\mathrm{Zar}}(R, \mathrm{GL}_r) = \varinjlim_{\mathcal{U}} \mathrm{H}^1(\mathcal{U}/R, \mathrm{GL}_r)$$

the Čech non-abelian cohomology of GL_r wr.t. the Zariski topology of $\operatorname{spec} R$. This pointed set classifies iso classes of vector bundles of rank r over $\operatorname{spec} R$.

The principle is that nice constructions for vector bundles arise from homomorphisms of group schemes. Given a map $f : \mathrm{GL}_r \to \mathrm{GL}_s$, we can attach to a vector bundle V_g of rank r, the vector bundle $V_{f(g)}$ of rank s. This extends to a functor $X \mapsto f_*(X)$ for r-bundles to s-bundles.

Example. If $r = r_1 + r_2$, can consider $f : \mathrm{GL}_{r_1} \times \mathrm{GL}_{r_2} \to \mathrm{GL}_r, (A_1, A_2) \mapsto A_1 \oplus A_2$. This gives direct sum of vector bundles.

In the case $r = 1 + \cdots + 1$, the diagonal map $\mathbb{G}_m^r \to \mathrm{GL}_r$ leads to decomposable vector bundles, i.e. direct sums of rank one vector bundles.

Example. If $r = r_1 r_2$, the map $f : \mathrm{GL}_{r_1} \times \mathrm{GL}_{r_2} \to \mathrm{GL}_r, (A_1, A_2) \mapsto A_1 \otimes A_2$ gives tensor product of vector bundles.

Example. $\det : \mathrm{GL}_r \to \mathrm{GL}_1$ gives the **determinant bundle** $\det(V) = \det_*(V)$.

1.1.6 Dedekind ring

Let R be a Dedekind ring. That is, a noetherian domain such that the localization at each maximal ideal is a discrete valuation ring.

Fact. A locally free R-module of rank $r \geq 1$ will be isomorphic to $R^{r-1} \oplus I$ for I an invertible R-module, which is unique up to isomorphism.

(note I is the determinant so uniqueness is clear)

Corollary 1.1.11. *A locally free R-module of rank $r \geq 1$ is trivial iff its determinant is trivial.*

Proof. Let's prove this w/o the fact. Start w/ a vector bundle $V(M)$ trivialized over an open affine $\operatorname{spec}(R_f)$. Set $\Sigma = \operatorname{spec} R \setminus \operatorname{spec} R_f = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_c\}$ w/ the $\mathfrak{p}_j$'s maximal ideals of R. Let $\widehat{R}_{\mathfrak{p}_j}$ be the completion w/ fraction field $\widehat{K}_{\mathfrak{p}_j} = K \otimes_R \widehat{R}_{f_i}$. By Nakayama, the module $M \otimes_R \widehat{R}_{\mathfrak{p}_i}$ is free so pick a trivialization $\varphi_i : (\widehat{R}_{\mathfrak{p}_i})^r \xrightarrow{\sim} M \times_R \widehat{R}_{\mathfrak{p}_i}$.

Let $\varphi_f : (R_f)^r \xrightarrow{\sim} M \times_R R_f$ be a trivialization. The linear map

$$\varphi_f^{-1} \widehat{\varphi}_i : (\widehat{K}_{\mathfrak{p}_i})^r \to (\widehat{K}_{\mathfrak{p}_i})^r$$

gives rise to some element $g_i \in \mathrm{GL}_r(\widehat{K}_{\mathfrak{p}_i})$. Taking choices into account, we get a well-defined element of the double coset

$$c_\Sigma(R, \mathrm{GL}_r) := \mathrm{GL}_r(R_f) \Big\backslash \prod_{j=1}^{c} \mathrm{GL}_r(\widehat{K}_{\mathfrak{p}_i}) \Big/ \prod_{j=1}^{c} \mathrm{GL}_r(\widehat{R}_{\mathfrak{p}_i})$$

The map

$$\ker \big(\mathrm{H}^1(R, \mathrm{GL}_r) \to \mathrm{H}^1(R_f, \mathrm{GL}_r) \big) \to c_\Sigma(R, \mathrm{GL}_r)$$

is injective.

Now suppose $V(M)$ is trivial, so (g_i) belongs to the kernel of the map

$$\underset{*}{\det} : c_\Sigma(R, \mathrm{GL}_r) \to c_\Sigma(R, \mathbb{G}_m) = R_f^\times \setminus \prod_{j=1,\ldots,c} \left(\widehat{K^\times}_{\mathfrak{p}_i} / \widehat{R^\times}_{\mathfrak{p}_i} \right).$$

Up to change of trivializations, we can assume that $g_i \in \mathrm{SL}_n(\widehat{K}_{\mathfrak{p}_i})$ for $i = 1, \ldots, c$. Since $\mathrm{SL}_n(\widehat{K}_{\mathfrak{p}_i})$ is generated by elementary matrices and since R_f is dese in $\prod_i \widehat{K}_{\mathfrak{p}_i}$ (strong approx?), it follows that $\mathrm{SL}_r(R_f)$ is dense in $\prod_{i=1,\ldots,c} \mathrm{SL}_r(\widehat{K}_{\mathfrak{p}_i})$.

On the other hand, each group $\mathrm{SL}_n(\widehat{R}_{\mathfrak{p}_i})$ is open (actually clopen) in $\mathrm{SL}_r(\widehat{K}_{\mathfrak{p}_i})$ s.t. $c_\Sigma(R, \mathrm{SL}_r) = 1$. The injectivity facts then lets us conclude that $V(M)$ is a trivial vector bundle. ■

We will see a similar argument again later.

1.1.7 Zariski topology is not fine enough

We start w/ the example of quadratic bundles.

Definition 1.1.12. A **quadratic form** over an R-module M is a map $q : M \to R$ satisfying

(i) $q(\lambda x) = \lambda^2 q(x)$ for all $\lambda \in R$, $x \in M$

(ii) The form $M \times M \to R$

$$(x, y) \mapsto b_q(x, y) := q(x + y) - q(x) - q(y)$$

is symmetric and bilinear.

This is stable under arbitrary base change. We say q is **regular** if b_q induces an iso $M \xrightarrow{\sim} M^\vee$.

Let (M, q) be a regular quadratic form w/ M locally free of rank r. It is tempting to make analogies w/ vector bundles and use the orthogonal group scheme $O(q; M) \leq \mathrm{GL}(M)$. For an open cover $\mathscr{U}$ of R as before, we can similarly define $Z^1(\mathscr{U}/R, O(q, M))$ and $\mathrm{H}^1(\mathscr{U}/R, O(q, M))$.

Lemma 1.1.13. *The set $\mathrm{H}^1(\mathscr{U}/R, O(q, M))$ classifies the iso classes of regular quadratic forms (q', M') which are locally iso over $\mathscr{U}$ to (q, M).*

This is nice, but not quite what we want. Regular quadratic forms of R of dimension r have no reason to be locally isomorphic to (M, q) (e.g. even if $R = \mathbb{R}$), so $\mathrm{H}^1(R, O(q, M))$ is only a piece of what' we'd like to understand.

If we have a map $f : G \to H$ of group schemes, we would like some control on the map $f_* : \mathrm{H}^1(R, G) \to \mathrm{H}^1(R, H)$.

Example. The Kummer map $f_d : \mathbb{G}_m \to \mathbb{G}_m, t \mapsto t^d$ induces multiplication by d on the Picard group $\mathrm{Pic}(R)$. In terms of invertible modules, it is $M \mapsto M^{\otimes d}$.

What can we say about its kernel and image? For the kernel, given $[M] \in \ker\left(\mathrm{Pic}(R) \xrightarrow{\times d} \mathrm{Pic}(R)\right)$, there exists a trivialization $\theta : R \xrightarrow{\sim} M^{\otimes d}$. Consider commutative group $A_d(R)$ of iso class of pairs (M, θ) w/ M an invertible R-module and $\theta : R \xrightarrow{\sim} M^{\otimes d}$. We have a forgetful map $A_d(R) \to \mathrm{Pic}(R)$ sitting in an exact sequence

$$R^\times/(R^\times)^d \xrightarrow{\varphi} A_d(R) \to \mathrm{Pic}(R) \xrightarrow{\times d} \mathrm{Pic}(R)$$

w/ $\varphi(r) = [(R, \theta_d)]$ where $\theta_d : R \xrightarrow{\sim} R^{\otimes d} = R, x \mapsto dx$. This $A_d(R)$ can be given a cohomological meaning using étale cohomology.

The idea of Grothendieck-Serre is to extend to notion of covers in alg. geo. THey did it originally w/ étale covers, but it turns out flat covers provide a simpler setting in a first approach.

Definition 1.1.14. A **flat cover** (fppf cover) of R is a finite collection $(S_i)_{i \in I}$ of R-rings s.t.

(i) S_i is a flat R-algebra of finite presentation for $i = 1, \ldots, c$

(ii) $\operatorname{spec} R = \bigcup_{i \in I} \mathrm{Im}\left(\mathbf{Spec}(S_i) \to \mathbf{Spec}(R)\right)$.

If we put $S = \prod_{i \in I} S_i$, the conditions just say that S is a faithfully flat R-algebra of finite presentation. We can always deal w/ covers by a single ring.

Remark 1.1.15. Zariski covers are flat covers too.

What does Čech cohomology look like for flat covers?

Let S be a faithfully flat R-algebra of finite presentation. Let $p_i^* : S \to S \otimes_R S$ denote the coprojections $(i = 1, 2)$ and similarly $q_i^* : S \to S \otimes_R S \otimes_R S$ as well as $q_{ij}^* : S \otimes_R S \to S \otimes_R S \otimes_R S$.

Definition 1.1.16. Let G be an R-group scheme. A **1-cocycle** for G and S/R is an element $g \in G(S \otimes_R S)$ satisfying

$$q_{1,2}^*(g) q_{2,3}^*(g) = q_{1,3}^*(g) \in G(S \otimes_R S \otimes_R S).$$

We let $Z^1(S/R, G)$ denote the set of 1-cocycles, and similarly define $\check{\mathrm{H}}^1(S/R, G)$.

We can pass to the limit of all flat covers of $\operatorname{spec} R$, and so define $\check{\mathrm{H}}^1_{fppf}(R, G) = \varinjlim \check{\mathrm{H}}^1(S/R, G)$. This construction is functorial in R and in the gorup scheme G.

1.1.8 Torsors

Definition 1.1.17. A (right) **G-torsor** X (w.r.t. flat topology) is an R-scheme equipped w/ a right G-action satisfying

- **(i)** The action map $X \times_R G \to X \times_R X, (x, g) \mapsto (x, x.g)$ is an isomorphism
- **(ii)** There's a flat cover R'/R s.t. $X(R') \neq \emptyset$

The first condition reflects the simple transitivity of the action, i.e. $G(T)$ acts simply transitively on $X(T)$ for all R-rings T. The second condition is a local triviality condition.

Example. Take $X = G$ with G acting by right translation.

Remark 1.1.18. If $X(R) \neq \emptyset$, a point $x \in X(R)$ defines a morphism $G \to X$, $\varphi_x : g \mapsto x.g$ which is an isomorphism by the simple transitive property; in this case, we say X is trivial w/ φ_x a trivialization. Hence, condition **(ii)** says that an R-torsor X under G is locally trivial for the flat topology.

Definition 1.1.19. A **morphism of G-torsors** $X \to Y$ is a G-equivariant map. By the simple transitivity condition, any such morphism is an isomorphism. The category of G-torsors is a groupoid.

Remark 1.1.20. The R-functor of automorphisms of the trivial G-torsor G is representable by G (acting by left translations) since you only need to know where 1 goes.

We let $\mathrm{H}^1_{fppf}(R, G)$ denote the set of iso classes of G-torsors for the flat topology. If S is a flat cover of R, we let $\mathrm{H}^1_{fppf}(S/R, G)$ by the iso classes of G-torsors split by S.

Fact. There's a class map $\gamma : \mathrm{H}^1_{fppf}(S/R, G) \to \check{\mathrm{H}}^1_{fppf}(S/R, G)$.

We finish w/ faithfully flat descent.

Let T be a faithfully flat extension of the ring R (not necessarily of finite presentation). Consider the **Amitsur complex**

$$0 \to M \to M \otimes_R T \xrightarrow{d_2} M \otimes_R T \otimes_R T \xrightarrow{d_3} M \otimes_R T^{\otimes 3} \to \cdots$$

This complex is exact for each R-module M. This implies that for any affine R-scheme X, we have an identification

$$X(R) = \{x \in X(T) : p_1^*(x) = p_2^*(x) \in X(T \otimes_R T)\}$$

which holds actually for any R-scheme.

Given a T-module N, we consider the $T \otimes_R T$-modules $p_1^*(N) = T \otimes_R N$ and $p_2^*(N) = N \otimes_R T$. **Descent data** on N is an isomorphism $\varphi : p_1^*(N) \xrightarrow{\sim} p_2^*(N)$ such that the diagram below commutes

$$\begin{tikzcd}
T \otimes_R T \otimes_R N \arrow[r, "\varphi_2"'] \arrow[rr, bend left, "\varphi_3"] & T \otimes_R N \otimes_R T \arrow[r, "\varphi_1"'] & N \otimes_R T \otimes_R T
\end{tikzcd}$$

Theorem 1.1.21 (faithfully flat descent theorem). *The functor $M \mapsto (M \otimes_R T, can_M)$ is an equivalence of categories between the category of R-modules and that of T-modules w/ descent data. An inverse functor is*

$$(N, \varphi) \mapsto \{n \in N : n \otimes 1 = \varphi(1 \otimes n)\}.$$

The above functor in fact induces an equivalence of categories between the category of R-algebras and that of T-algebras w/ descent data.

Note above theorem is in the affine setting.

By the above theorem (+ the fact that being locally free of rank r is local for the flat topology), we see

Theorem 1.1.22. *Let $r \geq 0$ be an integer.*

(1) *Let M be a locally free R-module of rank r. Then the R-functor*

$$S \mapsto \mathrm{Isom}_{S\text{-}mod}(S^r, M \otimes_R S)$$

is representable by a GL_r-torsor X^M over $\operatorname{spec} R$

(2) *The functor $M \mapsto X^M$ induces an equivalence of categories between the groupoid of locally free R-modules of rank r and the category of GL_r-torsors over $\operatorname{spec} R$*

This extends Swan-Serre. This implies that the GL_r-torsors are the same w/ flat topology or w/ Zariski topology.

Corollary 1.1.23 (Hilbert-Grothendieck 90). *We have $\mathrm{H}^1_{Zar}(R, \mathrm{GL}_r) = \mathrm{H}^1_{fppf}(R, \mathrm{GL}_r)$.*

In particular, if R is a local (or semilocal) ring, we have $\mathrm{H}^1_{fppf}(R, \mathrm{GL}_r) = 1$.

Back to torsors and cocycles Let's return to the class map.

Lemma 1.1.24. *The class map $\gamma : \mathrm{H}^1_{fppf}(S/R, G) \to \check{\mathrm{H}}^1_{fppf}(S/R, G)$ is injective.*

Theorem 1.1.25. *If G is affine, the class map*

$$\mathrm{H}^1_{fppf}(S/R, G) \to \check{\mathrm{H}}^1_{fppf}(S/R, G)$$

is an isomorphism.

The fact that we can descend torsors under an affine scheme is a consequence of the faithfully flat descent theorem.

Proof Sketch. We are given a cocycle $g \in G(S \otimes_R S)$.

Remark 1.1.26. Seems $S[G]$ is a coordinate ring

We consider the map $L_g^* : (S \otimes_R S)[G] \xrightarrow{\sim} (S \otimes_R S)[G]$ and we define φ_g via the diagram

$$\begin{tikzcd}
S \otimes_R S[G] \arrow[r, "\varphi_g"] \arrow[d, "\alpha"'] & S[G] \otimes_R S \arrow[d, "\beta"] \\
(S \otimes_R S)[G] \arrow[r, "L_g^*"] & (S \otimes_R S)[G].
\end{tikzcd}$$

Above, $\alpha(s_1 \otimes f) = (s_1 \otimes 1)p_2^*(f)$ and $\beta(f \otimes s_2) = p_1^*(f)(1 \otimes s_2)$. The cocycle condition implies that φ_g is descent data for the S-algebra $S[G]$. The descent theorem dfeines an R-algebra $R[X]$ and X is actually a G-torsor denoted by E_g. ■

This construction is a special case of *twisting*. More generally, if Y is an affine R-scheme equipped w/ a left G-action, the the action map

$$g : Y \times_R (S \otimes_R S) \xrightarrow{\sim} Y \times_R (S \otimes_R S)$$

defines a descent data. This gives rise to the twist Y_g of Y by the one cocycle g. it is affine over R.

A special case is the action of G on itself by inner automorphisms, G_g is called the twisted R-group scheme. It acts on Y_g for Y as above.

Above construction does not depend on choices of cocycles or of trivializations. We can define for a G-torsor E, the twists ${}^E Y$ and ${}^E G$. In practice, affiness is too strong of an assumption. More generally, we can twist G-schemes equipped w/ an ample invertible G-linearized bundle.

1.2 Gille Lecture 2 (7/13)

Note 1. *Roughly 5 minutes late*

1.2.1 Question from yesterday about tangent bundle of sphere

Theorem 1.2.1. *On $S^2_{\mathbb{C}}$, the tangent bundle is trivial.*

Proof. Hard to find elementary proof in literature. It is, for example, a consequence of Maudly (?)-Swan theorem. I missed the theorem statement. ■

1.2.2 Recap

What did we do last time?

We introduced the flat topology. For G/R an affine group scheme, we constructed a map $\mathrm{H}^1(R, G) \to \check{\mathrm{H}}^1_{fppf}(R, G)$ which is an isomorphism when G is affine (note, R a ring).

Notation 1.2.2. If we have cohomology w/o a subscript, assume it's fppf cohomology.

1.2.3 Examples

Let's talk about vector group schemes. Let M be a finite locally free R-module of finite rank. We claim $\check{\mathrm{H}}^1(R, W(M)) = 0$, so each $W(M)$-torsor is trivial.

Proof. given flat cover S/R, the complex

$$M \otimes_R S \xrightarrow{p_1^* - p_2^*} M \otimes_R S \otimes_R S \to M \otimes_R S \otimes_R S \otimes_R S$$

is exact, so each cocycle $g \in W(M)(S \otimes_R S)$ is a coboundary. ■

Note 2. Missed some stuff because of touchpad issues

In the case of $G = \Gamma_R$-torsos $\operatorname{spec} S \to \operatorname{spec} R$ is the same thing as a Galois Γ-algebra S and is often called a Galois cover.

As for GL_r, a special nice case is the case of forms, that is when G is the automorphism group of some algebraic structure.

Example. The orthogonal group scheme O_{2n} is the automorphism group of the hyperbolic quadratic form attached to R^n. As regular quadratic forms of rank $2n$ are locally isomorphic (for flat topology) to the hyperbolic form, descent theory provides an equiv of cats between the groupoid of regular quadratic forms of rank $2r$ and $\mathrm{H}^1_{fppf}(R, O_{2r})$.

Another important example is that of the symmetric group S_n. For any R-algebra S, the group $S_n(S)$ is the automorphism group of the S-algebra $S^n = S \times \ldots \times S$. Since finite étale algebras of degree n are locally isomorphic to R^d in the étale topology, the same yoga shows there's an equiv of cats between S_n-torsors and finite étale R-algebras of rank n. The inverse functor is defined by descent but can be described explicitly. This is the Galois closure construction due to Serre.

1.2.4 Functoriality issues

Let $G \to H$ be a *monomorphism* of R-group schemes.

Definition 1.2.3. We say that an R-scheme X equipped w/ a map $f : H \to X$ is a **flat quotient of** H **by** G if for each R-algebra S, the map $H(S) \to X(S)$ induces an injective map $H(S)/G(S) \hookrightarrow X(S)$ and if for each $x \in X(S)$, there exists a flat cover S' of S s.t. $x_{S'}$ belongs to the image of $H(S') \to X(S')$ (in French, one says f is 'couvrant').

Above, we want an epimorphism of sheaves in the flat topology.

If a flat quotient exists, it is unique up to unique iso. Furthermore, if G is normal in H (i.e. $G(S) \triangleleft H(S)$ always), then X carries a natural structure of R-group schemes, and we say $1 \to G \to H \to X \to 1$ is an exact sequence of R-group schemes (for the flat topology).

Assume that X is the flat quotient of H by G.

Lemma 1.2.4.

(1) The map $H \to X$ is a G-torsor

(2) There is an exact sequence of pointed set

$$1 \to G(R) \to H(R) \to X(R) \xrightarrow{\varphi} \mathrm{H}^1_{fppf}(R, G) \to \mathrm{H}^1_{fppf}(R, H)$$

where $\varphi(x) = [f^{-1}(x)]$ is the ***characteristic map***.[3]

Remark 1.2.5. If X is affine (or equppied w/ an ample G-linearized invertible sheaf), descent is effective, i.e. the cat of G-torsors over $\operatorname{spec} R$ is equivalent to the cat of couples (F, x) where F is an H-torsor and $x \in \left({}^F X\right)(R)$.

Remark 1.2.6. If G is normal in H, then X has natural structure of an R-group scheme. In this case, the above says that the category of G-torsors over $\operatorname{spec} R$ is equivalent to the category of couples... (I'm too slow)

[3] Here, $f : H \to X$ is a G-torsor. We pull it back along a map $x : \operatorname{spec} R \to X$ to get a G-torsor on R. Think

$$\begin{tikzcd}
f^{-1}(x) \arrow[r] \arrow[d] \arrow[dr, phantom, "\ulcorner", very near start] & \operatorname{spec} R \arrow[d, "x"] \\
H \arrow[r, "f"] & X
\end{tikzcd}$$

Using the extended Swan-Serre correspondence, an example is that the category of SL_r-torsors is equivalent to the category of pairs (M, θ) where M is a locally free R-module of rank r, and $\theta : R \xrightarrow{\sim} \bigwedge^r M$ is a trivialization of the determinant of M.

For an integer d, have **Kummer exact sequence** $1 \to \mu_d \to \mathbb{G}_m \xrightarrow{\times d} \mathbb{G}_m \to 1$. Similarly, the category of μ_d-torsors is equivalent to the category of pairs (M, θ) for M an invertible R-bundle, and ...

1.2.5 Étale covers

Definition 1.2.7. An étale morphism of rings $R \to S$ is a smooth morphism of relative dimension zero.

Several equiv definitions

- S is a flat R-module s.t. for each R-field F, $S \otimes_R F$ is an étale F-algebra (i.e. finite geometrically reduced F-algebra)

  Example. Localization $R \to R_f$ is étale

  If $d \in R^\times$, the Kummer map $\mathbb{G}_m \to \mathbb{G}_m, t \mapsto t^d$ is étale

  If $d \in R^\times$ and $r \in R^\times$, then $S = R[x]/(x^d - r)$ is a finite étale R-algebra.

Proposition 1.2.8. *If G is (affine) smooth, then* $\mathrm{H}^1_{\acute{e}t}(R, G) = \mathrm{H}^1_{fppf}(R, G)$.

1.2.6 Isotrivial torsors and Galois cohomology

We are given a Galois R-algebra S of group Γ. The action isomorphism

$$\operatorname{spec} S \times_R \Gamma_S \xrightarrow{\sim} \operatorname{spec} S \times_R \operatorname{spec} S$$

reads as the isomorphism $S \otimes_R S \xrightarrow{\sim} S \otimes_R R^{(\Gamma)} = S^{(\Gamma)}$. A 1-cocycle is then an element $z = (z_\gamma)_{\gamma \in \Gamma} \in G(S \otimes_R S) = G(S)^{(\Gamma)}$ satisfying

$$z_{\sigma\tau} = z_\sigma \sigma(z_\tau)$$

for all $\sigma, \tau \in \Gamma$ (Note Γ acts on the left on $G(S)$ since it acts on the left on S).

Notation 1.2.9. $R^{(\Gamma)} = \mathrm{Hom}_{\mathrm{Set}}(\Gamma, R)$ is the group algebra.

We find that $Z^1(S/R, G)$ is the set of Galois cocycles $Z^1(\Gamma, G(S))$ and that $\check{\mathrm{H}}^1(S/R, G)$ is the set of non-abelian Galois cohomology $\mathrm{H}^1(\Gamma, G(S)) = Z^1(\Gamma, G(S))/\sim$ w/ $z \sim z'$ iff $z_\gamma = g^{-1} z'_\gamma \gamma(g)$ for some $g \in G(S)$.

Example. Say G is the constant group scheme associated to an abstract group Θ. Then,

$$Z^1(S/R, G) = \mathrm{Hom}_{R\text{-gp}}(\Gamma_S, \Theta_S) \text{ and } \check{\mathrm{H}}^1(S/R, G) = \mathrm{Hom}_{S\text{-gp}}(\Gamma_S, \Theta_S)/\Theta_R(S).$$

In particular, if S is connected, then $Z^1(S/R, G) = \mathrm{Hom}_{gp}(\Gamma, \Theta)$ and $\check{\mathrm{H}}^1(S/R, G) = \mathrm{Hom}_{gp}(\Gamma, \Theta)/\Theta$.

Galois descent is then a special case of faithfully flat descent. Can check, for example, that the cat of R-modules is equiv to the cat of couples (N, ρ) with N an S-modules equipped w/ semilinear Γ-action, i.e. $\rho(\sigma)(\lambda.n) = \sigma(\lambda)\rho(n)$ (I think).

Definition 1.2.10. We say a torsor E under an R-group scheme G is **isotrivial** if it is split by a Galois (i.e. connected) finite étale cover.

Such torsors can be understood w/ Galois cohomology.

Fact. For the ring of Laurent polynomials in characteristic zero, all torsors over a reductive group scheme are isotrivial.

1.2.7 The Dedekind case

Let R be a Dedeking ring of fraction field K. Let $f \in R$ and put $\Sigma = \operatorname{spec} R \setminus \operatorname{spec} R_f = \{\mathfrak{p}_1, \dots, \mathfrak{p}_c\}$. Take the notation of yesterday for the completions.

Let G be an affine R-group scheme. As in the proof of the GL_n-case, we have a class map

$$\ker\left(\mathrm{H}^1_{fppf}(R,G) \to \mathrm{H}^1_{fppf}(R_f,G) \times \prod_{i=1}^{c} \mathrm{H}^1_{fppf}(\widehat{R}_{\mathfrak{p}_i},G)\right) \to c_\Sigma(R,G) := G(R_f)\backslash \prod_{j=1}^{c} G(\widehat{K}_{\mathfrak{p}_i})/G(\widehat{R}_{\mathfrak{p}_i}).$$

This map is injective.

Corollary 1.2.11. *If $c_\sigma(R,G) = 1$ (e.g. if $G(R_f)$ is dense in $\prod_{j=1}^{c} G(\widehat{K}_{\mathfrak{p}_i})/G(\widehat{R}_{\mathfrak{p}_i})$), then this kernel vanishes as well.*

Corollary 1.2.12. *Assume that G is a semisimple simply connected split R-group scheme. Then,*

$$\ker\left(\mathrm{H}^1(R,G) \to \mathrm{H}^1(R_f,G)\right) = 1.$$

Above, simply connected here is in the sense of semisimple algebraic groups or semisimple group schemes. Over $\mathbb{C}$, this coincides w/ the topological notion. The simplification in the above corollary comes from injectivity of

$$\mathrm{H}^1(\widehat{R}_{\mathfrak{p}_i},G) \hookrightarrow \mathrm{H}^1(\widehat{K}_{\mathfrak{p}_i},G)$$

(proved by Bruhat-Tits).

Example. This gives $\mathrm{H}^1_{Zar}(R,\mathrm{SL}_n) = 1$ and also $\mathrm{H}^1_{Zar}(R,E_8) = 1$.

1.2.8 Affine curves over an algebraically closed field

Theorem 1.2.13. *Let G be a semisimple algebraic k-group ($k = \overline{k}$). Let C be a smooth connected affine curve. Then, $\mathrm{H}^1_{fppf}(C,G) = 1$.*

The main ingredient is Steinberg's theorem stating that $\mathrm{H}^1(k(C),G) = 1$. A special case is that of PGL_n which rephrases by saying that the central simple algebras over $k(C)$ are matrix algebras, which is a consequence of Tsen's theorem.

A second ingredient is that fact that the group $\mathrm{Pic}(C)$ is divisible which follows from the structure of $\mathrm{Pic}(C^c)$, where C^c is a smooth compactification of C. In particular, we have an exact sequence

$$0 \to J_{C^c}(k) \to \mathrm{Pic}(C^c) \to \mathbb{Z} \to 0$$

w/ J_{C^c} the Jacobian, an abelian variety. If $C = C^c \setminus \{x_1, \dots, x_s\}$ the surjective map $\mathrm{Pic}(C^c) \to \mathrm{Pic}(C)$ induces an epimorphism $J_{C^c}(k) \twoheadrightarrow \mathrm{Pic}(C)$, so $\mathrm{Pic}(C)$ is divisible.

Proof Sketch of Theorem. First assume G is simply connected. We are given a class $\gamma \in \mathrm{H}^1(C,G)$. By Steinberg, there's some $f \in k[C]$ such that $\gamma_{C_f} = 1$ (trivial at generic point so trivial in some neighborhood). The corollaries from last (subsub)section then shows that $\mathrm{H}^1(C,G) = 1$.

In the general case, let $f : G^{sc} \to G$ be the universal cover. Let T^{sc} be a maximal torus of G^{sc}, so $T := T^{sc}/\ker f$ is a maximal torus of G. Let B be a Borel subgroup of G containing T. We claim that the map

$$\mathrm{H}^1(C,B) \to \mathrm{H}^1(C,G)$$

is onto. Let E be a C-torsor under G. The idea is to introduce the twisted C-scheme $Y = E(G/B)$ (the scheme of Borel subgroups of the twisted C-group scheme $E(G)$, so it is projective over C). By Steinberg, $Y(k(C)) \neq \emptyset$ (torsor trivial). Since Y projective (so proper), $Y(C) = Y(k(C))$ by valuative criterion, so Y has a C-point (i.e. $E(G)$ carries a Borel subgroup scheme). By functoriality, it follows that $[E]$ belongs to the image of $\mathrm{H}^1(C,B) \to \mathrm{H}^1(C,G)$.

We have $B = U \rtimes T$ where U admits a T-equivariant filtration $U_0 = 1 \subset \cdots \subset U_r = U$ s.t. U_{i+1}/U_i is isomorphic to $\mathbb{G}_a^{\ell_i}$. Since $\mathrm{H}^1(C,\mathbb{G}_a) = 1$, a dévissage argument shows that the map $\mathrm{H}^1(C,T) \to \mathrm{H}^1(C,B)$ is bijective. Thus, we have a diagram

$$\begin{tikzcd}
\mathrm{H}^1(C,T^{sc}) \arrow[r] \arrow[d] & \mathrm{H}^1(C,T) \arrow[r, "\sim"] \arrow[d] & \mathrm{H}^1(C,B) \arrow[dl, two heads] \\
1 = \mathrm{H}^1(C,G^{sc}) \arrow[r] & \mathrm{H}^1(C,G) &
\end{tikzcd}$$

Since the map $T^{sc} \to T$ is an isogeny and $\mathrm{Pic}(C)$ is divisible, it follows that $\mathrm{H}^1(C,T^{sc}) \to \mathrm{H}^1(C,T)$ is onto. Thus, we win. ■

The reductive case is of the same vein. Let $S = G/DG$ be the coradical torus of G. One can show that $\mathrm{H}^1(C,G) \to \mathrm{H}^1(C,S)$ is bijective, generalizing the bijection $\mathrm{H}^1(C,\mathrm{GL}_r) \xrightarrow{\sim} \mathrm{H}^1(C,\mathbb{G}_m) = \mathrm{Pic}(C)$ of yesterday.

1.2.9 The case of the affine line

Theorem 1.2.14. *Let G be a reductive k-group over a field k. Then we have a bijection*

$$\mathrm{H}^1(k,G) \xrightarrow{\sim} \ker\left(\mathrm{H}^1(k[t],G) \to \mathrm{H}^1(k_s[t],G)\right).$$

If k is perfect of characteristic of k is "good" for G, we have $\mathrm{H}^1(k_s[t],G) = 1$ so that $\mathrm{H}^1(k,G) = \mathrm{H}^1(k[t],G)$. When it happens, we say that G-torsors over $k[t]$ are constant.

There are a few exotic cases when this does not fold, e.g. $G = \mathrm{PGL}_p$ over k with k imperfect of characteristic $p > 0$.

We want to end by sketching a proof of this theorem.

Assumption. Say $\operatorname{char} k = 0$ to keep things simple. We want a bijection $\mathrm{H}^1(k,G) \xrightarrow{\sim} \mathrm{H}^1(k[t],G)$.

The common ingredient of all proofs of this statement is to use Grothendieck-Harder's theorem on bundles over the projective line.

Theorem 1.2.15 (Grothendieck-Harder). *Let G be a reductive k-group over a field k. Let S be a maximal k-split torus*[4] *of G, and let $W_G(S) = N_G(S)/C_G(S)$ be the finite (constant) associated Weyl group. Then we have a bijection*

$$\mathrm{H}^1_{Zar}(\mathbb{P}^1_k, S)/W_G(S) \xrightarrow{\sim} \ker\left(\mathrm{H}^1(\mathbb{P}^1_k, G) \xrightarrow{\mathrm{ev}_0} \mathrm{H}^1(k, G)\right).$$

In particular, if a G-torsor over $k[t]$ is trivial at $t = 0$ *and* extends to a G-torsor over $\mathbb{P}^1_k$, then it is trivial.

When can we extend? Say we're given a G-torsor X over $k[t]$ and WLOG we may assume X is trivial on $t = 0$. The original method to extend X to the projective line was to use Bruhat-Tits' theory. We shall instead provide a short trick proof in characteristic zero.

First find an integer $d \geq 1$ such that the restriction $\gamma_{k[t^{1/d}]}$ extends to the projective line. Note $\gamma = [X]$ is the class of X. This is "local at ∞" in the sense that it suffices to show there's some d s.t. $\gamma_{k((t^{-d}))}$ comes from $\mathrm{H}^1(k, G)$.

A folklore result (Gille gave a reference in the slides) tells us that there's a finite k-subgroup S of G s.t. $\mathrm{H}^1(F, S) \to \mathrm{H}^1(F, G)$ is onto for any k-field F. In particular, $\mathrm{H}^1(k((t^{-1})), S) \to \mathrm{H}^1(k((t^{-1})), G)$ is onto. The absolute Galois group of $k((t^{-1}))$ is

$$\varprojlim \mu_n(k_s) \rtimes \mathcal{G}(k_s/K) = I \rtimes \mathcal{G}(k_s/k).$$

We are given a cocycle $z : I \rtimes \mathcal{G}(k_s/k) \to S(k_s)$. Its restriction to the inertia group I is a group homomorphism, so factors through $\mu_d(k_s)$ for some d. It follows that $[z]_{k((t^{-1/d}))}$ belongs to the image of $\mathrm{H}^1(k, S) \to \mathrm{H}^1(k((t^{-1/d})), S)$ so that $\gamma_{k((t^{-1/d}))}$ belongs to the image of $\mathrm{H}^1(k) \to \mathrm{H}^1(k((t^{-1/d})))$.

We can actually take d to be the order of $S(k_s)$. Our reasoning shows that $\gamma_{k[t^{1/d}]} = 1$... I'm lost so gonna stop taking notes (see the slides).

1.2.10 Punctured affine line

The $\mathbb{G}_m$ case is more complicated than the $\mathbb{A}^1$ case.

Theorem 1.2.16 (Chernousov-G.-Pianzola). *Let G be a reductive k-group over a field k of characteristic zero. The map*

$$\mathrm{H}^1(k[t^{\pm 1}], G) \xrightarrow{\sim} \mathrm{H}^1(k((t)), G)$$

is bijective.

Surjectivity is "easy" and comes by reduction to a finite subgroup. The hard part is injectivity where one crucial step is to show an existence of a maximal torus the relevant twisted group scheme. This involves Bruhat-Tits theory and twin buildings.

[4] maximal among the k-split tori. We *do not* suppose $S_{\overline{k}}$ is a maximal torus of $G_{\overline{k}}$.

1.3 Danny Krashen Lecture 1 (7/12)

1.3.1 Summary

There are a lot of problems in field arithmetic and complexity of algebraic structures. Motivic cohomology has been helpful in the past. Maybe it will continue to help us.

That's the basic idea. Now's just the details. Today we'll focus more on field arithmetic, and tomorrow we'll focus more on algebraic structures.

Given a field k, ask: which systems of polynomial equations have solutions and why? We would like to answer this based on measurements of our field. E.g. if one special (type of) system has solutions, which others do as well? This leads to "boundeness questions."

The basic tools are Galois cohomology, Milnor K-theory, Witt ring, and Motivic cohomology. Also, algebraic structures. Today's lecture will have three parts

(1) Galois cohomology and relatives

(2) Basic field measurements

(3) problems

1.3.2 Galois Cohomology

Let k be a field w/ absolute Galois group G_k. Let Ab_{G_k} denote the category of abelian groups with continuous G_k-action. We'll usually want our groups to be discrete. Given $M \in \mathrm{Ab}_{G_k}$, let M^{G_k} denote its G_k-invariants. This is a left exact functor, so we get right derived functors $\mathrm{H}^q(G_k, -)$.

Remark 1.3.1. Ab_{G_k} has a $\otimes$-structure which gives rise to cup products

$$\mathrm{H}^k(G_k, M) \otimes_{\mathbb{Z}} \mathrm{H}^n(G_k, N) \to \mathrm{H}^{n+k}(G_k, M \otimes_{\mathbb{Z}} N).$$

A particular case of interest is $M = \mu_\ell^{\otimes n}$ is some tensor power of the group of ℓth roots of unity. The groups $\mathrm{H}^n(G_k, \mu_\ell^{\otimes n})$ form a ring under cup product. These groups start

$$\mathrm{H}^0(G_k, \mu_\ell^0) = \mathbb{Z}/\ell\mathbb{Z} \text{ and } \mathrm{H}^1(G_k, \mu_\ell) = k^\times/(k^\times)^\ell.$$

Notation 1.3.2. Given $a \in k^\times$, we denote its corresponding class in H^1 via $(a) = (a)_\ell \in k^\times/(k^\times)^\ell$. We also denote

$$(a_1, \dots, a_n) = (a_1, \dots, a_n)_\ell = (a_1) \cup \cdots \cup (a_n) \in \mathrm{H}^n(k, \mu_\ell^{\otimes n}).$$

These are called 'symbols'. The Bloch-Kato Conjecture (now Norm-Residue Isomorphism Theorem) tells us that $\mathrm{H}^n(k, \mu_\ell^{\otimes n})$ is generated by these symbols.

Remark 1.3.3. Galois cohomology is a special case of étale cohomology. In particular,

$$\mathrm{H}^n(G_k, M) = \mathrm{H}^n_{\text{ét}}(\operatorname{spec} k, M) = \mathrm{H}^n_{\text{ét}}(k, M).$$

This is useful since étale cohomology makes sense for arbitrary schemes (not just $\operatorname{spec} k$).

1.3.3 Milnor K-Theory

Given a field k, we define the **Milnor K-theory ring** $K_*^M(k) = \bigoplus_{i=0}^{\infty} K_i^M(k)$ via

- $K_0^M(k) = \mathbb{Z}$
- $K_1^M(k) = k^\times$ written additively. Say $a \in k^\times$ is usually written as $\{a\} \in K_1^M(k)$ so $\{a\}+\{b\} = \{ab\}$.
- It is generated by $K_1^M(k)$ with products written using concatenation

  $$\{a_1, \dots, a_n\} := \{a_1\}\{a_2\}\dots\{a_n\}$$

  (again called 'symbols') subject only to the relations

  $$\{a, b\} = 0 \text{ when } a + b = 1$$

  (i.e. $\{a, 1-a\} = 0$ when $a \neq 1$).

Remark 1.3.4. In Galois cohomology, one also has $(a, b)_\ell = 0 \in \mathrm{H}^2(k, \mu_\ell^{\otimes 2})$ if $a + b = 1$. Thus, we have a ring map

$$K_*^M(k) \to \mathrm{H}^*(k, \mu_\ell^{\otimes *})$$

defined by $\{a\} \mapsto (a)$.

Theorem 1.3.5 (**Bloch-Kato Conjecture**). *The above map induces an isomorphism*

$$K_*^M(k)/\ell \xrightarrow{\sim} \mathrm{H}^*(k, \mu_\ell^{\otimes *}).$$

(when $\ell \neq \operatorname{char} k$).

Note the independence of ℓ on the LHS above. Can think of $K_*^M(k)$ as being 'integral' or as 'tying together all the different ℓ's'.

1.3.4 Witt Ring

This ring encodes information about quadratic forms over a field.

Assumption. Let's assume $\operatorname{char} k \neq 2$ so that quadratic forms and symmetric bilinear forms are one in the same. This corresponds is given by $q(x) = b(x, x)$ and $b(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y))$.

Definition 1.3.6. We say a quadratic form q is **non-degenerate** is the associated symmetric bilinear form is non-degenerate.

Definition 1.3.7. The **Witt ring** $W(k)$ of k is generated as an abelian group by iso. classes of non-deg quadratic forms $q = (V, q) = (V, b)$ modulo the ideal generated by

- $(q_1 + q_2) - (q_1 \perp q_2)$
- $xy = 0 \in W(k)$ "hyperbolic plane"

The ring structure is given by the tensor product.

How is this related to Galois cohomology?

Remark 1.3.8. Gram-Schmidt tells us that any non-deg quadratic form can be put in the form $q \simeq a_1x_1^2 + \cdots + a_nx_n^2$. We denote this form as $\langle a_1, \ldots, a_n\rangle$. We also set

$$\langle\langle a\rangle\rangle = \langle 1, -a\rangle \, .$$

Similarly we define the **n-fold Pfister forms**

$$\langle\langle a_1, \ldots, a_n\rangle\rangle = \langle\langle a_1\rangle\rangle \otimes \cdots \otimes \langle\langle a_n\rangle\rangle.$$

These generate $I^n(k)$ defined below.

Let $I(k) \subset W(k)$ be the ideal of even dimensional forms. This is called the **fundamental ideal**. Consider its powers $I^n(k) := I(k)^n$. It turns out that there is a map $K_n^M(k) \to I^n(k)/I^{n+1}(k)$ defined by sending

$$\{a_1, \ldots, a_n\} \mapsto \langle\langle a_1, \ldots, a_n\rangle\rangle.$$

This induces an isomorphism

$$K_n^M(k)/s \xrightarrow{\sim} I^n(k)/I^{n+1}(k)$$

(**Milnor conjecture**, though now a theorem).

Combined with Bloch-Kato, we have

$$\mathrm{H}^n(k, \mu_2) \simeq K_n^M(k)/2 \simeq I^n(k)/I^{n+1}(k)$$

(note $\mu_2 = \mathbb{Z}/2\mathbb{Z}$ has trivial Galois action).

1.3.5 Motivic Cohomology

One reason to care about Motivic cohomology is that it provides integral versions of naturally arising étale cohomology groups $\mathrm{H}^i(k, \mu_\ell^{\otimes j})$. We saw above that Milnor K-theory gives an integral version when $i = j$.

These come from constructing "motivic complexes" $\mathbb{Z}(m)$. These are complexes of presheaves on smooth schemes over k usually considered in Zariski, étale, or Nisnevich topologies. We won't write these complexes down here, but probably someone will at some point this week. The Zariski hypercohomology of these are the Motivic cohomology groups

$$\mathbb{H}^n(X, \mathbb{Z}(m)) = \mathrm{H}^{n,m}(X, \mathbb{Z}) = \mathrm{H}^n(X, \mathbb{Z}(m))$$

(three notations for the same thing).

How are these related to Galois cohomology?

- These is a quasi-isomorphism of complexes of sheaves $\mu_\ell^{\otimes n} \simeq \mathbb{Z}/\ell\mathbb{Z}(n)$ (in the étale topology).

- There is also an isomorphism

$$\mathrm{H}^n_{\mathrm{Zar}}(k, \mathbb{Z}(n)) = K_n^M(k).$$

- Bloch-Kato identifies
$$\mathrm{H}^n_{\mathrm{Zar}}(X, \mathbb{Z}/\ell\mathbb{Z}(n)) \simeq \mathrm{H}^n_{\text{ét}}(X, \mathbb{Z}/\ell\mathbb{Z}(n)).$$
(this latter group is $\mathrm{H}^n_{\text{ét}}(X, \mu_\ell^{\otimes n})$ by the first bullet)

1.3.6 Basic invariants of field arithmetic

The first is "dimension of a field." There are several competing definitions of dimension. We give a few.

Definition 1.3.9. If k is finitely generated over a prime field or an algebraically closed field k_0, we say

$$\dim(k) = \begin{cases} \operatorname{trdeg}_{k_0} k & \text{if } k_0 = \overline{k}_0 \\ \operatorname{trdeg}_{k_0} k + 1 & \text{if } \#k_0 < \infty \\ \operatorname{trdeg}_{k_0} k + 2 & \text{if } k_0 = \mathbb{Q} \end{cases}$$

Definition 1.3.10. The **cohomological dimension** of a field k is at most n if $\mathrm{H}^m(G_k, M) = 0$ for all $m > n$ and M torsion. The cohomological dimension $\operatorname{cdim}(k)$ is then the minimal n s.t. the cohomological dimension of k is at most n. That is, $\operatorname{cdim}(k) = n \iff \mathrm{H}^n(G_k, M) \neq 0$ for some M torsion and $\mathrm{H}^m(G_k, M) = 0$ for all $m > n$ and M torsion.

Fact. $\operatorname{cdim}(k) = \dim(k)$ if k f.g. over a finite or algebraically closed field. If k is f.g. over $\mathbb{Q}$, then they are equal if it also has no real orderings; if k in this case has orderings, then $\operatorname{cdim}(k) = \infty$ (exercise[5]).

Definition 1.3.11. We say k is C_n if for $d > 0$ and $m > d^n$, every homogeneous polynomial f od degree d in m variables has a nontrivial zero.

Definition 1.3.12. The **diophantine dimension** of k is

$$\operatorname{ddim}(k) = \min\{n : k \text{ is } C_n\}.$$

Example. If k is f.g. over a finite or algebraically closed field, then $\operatorname{ddim}(k) = \dim(k) = \operatorname{cdim}(k)$.

Definition 1.3.13. k is T_n if for $d_r, \dots, d_r > 0$ and $m > \sum d_i^n$, every system of homogeneous polynomial equations

$$f_1 = \cdots = f_r = 0 \text{ with } \deg f_i = d_i$$

in m variables has a nontrivial solution. We set

$$\operatorname{trk}(k) := \min\{n : k \text{ is } T_n\}$$

Note that $T_n \implies C_n$, so $\operatorname{trk}(k) \geq \operatorname{ddim}(k)$.

Open Question 1.3.14 (Probably open)**.** $\operatorname{trk}(k) \overset{?}{=} \operatorname{ddim}(k)$

Example. There's a famous example of Ax of a field k with $\operatorname{cdim}(k) = 1$, but $\operatorname{ddim}(k) = \infty$.

Open Question 1.3.15 (Serre)**.** $\operatorname{ddim}(k) \geq \operatorname{cdim}(k)$*?*

[5] Use Bloch-Kato stuff. Something about $\{-1\}$ being non-nilpotent

Serre observed that Milnor conjecture tells us that $\mathrm{ddim}(k) \geq \mathrm{cdim}_2(k)$, where cdim_2 is defined only by considering the 2-primary part of cohomology (highest degree in which you can find 2-torsion). Serre's question can be thought of as asking if $\mathrm{ddim}(k) \geq \mathrm{cdim}_p(k)$ for all p?

Theorem 1.3.16 (K.-Matzri (?))**.** *Showed that* $\mathrm{cdim}_p(k)$ *groups at most linearly in* $\mathrm{ddim}(k)$ *w/ slope* $\sim \log_2 p$.

Why should ddim and cdim be related at all? One's about cohomology and the other is about solving polynomial equations. To obtain something like $\mathrm{ddim}(k) \geq \mathrm{cdim}(k)$ you would like a statement of the form: given $\alpha \in \mathrm{H}^*(k)$, there exists a poly f_α s.t. f_α has a zero $\iff$ $\alpha = 0$.

Example. When α is a symbol, this is related to "norm varities"

1.3.7 Structural problems in Galois Cohomology

Period-Index problem Note that ℓ not necessarily prime below.

Definition 1.3.17. If $\alpha \in \mathrm{H}^i(k)$ (really, $\mathrm{H}^i(k, \mu_\ell^{\otimes j})$ where we're not worried about what ℓ, j are just yet), we say L/k **splits** α if $\alpha_L = 0 \in \mathrm{H}^i(L)$. The **index** of α is

$$\mathrm{index}\alpha = \gcd \{[L : k] : L/k \text{ finite and splits } \alpha\}.$$

The **period** of α is the order of α, so $\mathrm{pr}\,\alpha \mid \ell$.

One can show that $\mathrm{pr}\,\alpha \mid \mathrm{index}\alpha$ and that they have the same prime factors, i.e. $\mathrm{ind}\alpha \mid (\mathrm{pr}\,\alpha)^m$ for some m.

Question 1.3.18. *For a given k (and i, j, ℓ), what is the minimal m such that* $\mathrm{ind}\alpha \mid (\mathrm{pr}\,\alpha)^m$*?*

Conjecture 1.3.19 (C-T)**.** *If k has* $\mathrm{ddim}(k) = n$ *or* $\dim(k) = n$*, and* $\alpha \in \mathrm{H}^2(k, \mu_\ell)$*, then* $\mathrm{ind}(\alpha) \mid (\mathrm{pr}\,\alpha)^{n-1}$.

Even in this case, no known bound for $k = \mathbb{Q}(t)$.

Can think of this equation as asking, "How complicated are cohomology classes of a given period and degree?" Rough idea: for $\mathrm{H}^i(k)$ w/ i close to $\dim k$ should have small index ("classes should be more simple as i approaches the biggest it can be").

Symbol length problem From the Bloch-Kato conjecture, we know that $\mathrm{H}^n(k, \mu_\ell^{\otimes n})$ is generated by symbols $(a_1, \ldots, a_n)$.

Question 1.3.20. *Given k, n, what's the minimum # m s.t. every* $\alpha \in \mathrm{H}^n(k)$ *is a sum of no more than m symbols?*

Think of this as, "How easy is it to write a class α?"

We would like a bound in terms of $\mathrm{ddim}(k)$ or $\dim(k)$ or something like that. Sounds like there are known fields with $\mathrm{ddim}(k) = \infty$ for which you need arbitrarily many summands.

What's known?

- For number fields (Global fields more generally) – so $\dim k = 2$ – w/ a primitive ℓth root of unity, we know that every class in H^2 is a symbol.

- Matzri $\implies$ for H^2 assuming roots of unity, if $\ell = p^t$ is a prime power, then we need at most $t\left(p^{\mathrm{ddim}(k)-1} - 1\right)$ symbols. This gives bound when ddim finite. It's suspected that the bound should not depend on p.
- For higher degree cohomology, almost nothing is known.

1.4 Krashen Lecture 2 (7/13)

Note 3. Roughly 3 minutes late

1.4.1 Arithmetic Problems

Fix a field k. Look at complexity of cohomology or algebraic structures over k. For example, study $\mathrm{ddim}, \mathrm{cdim}$, period-index problem, period-symbol length, etc.

On the other hand, there are also algebraic structure problems (maybe over a fixed ground field). The game here is to describe structural features of algebraic structures of a given type over all field extensions k/k_0.

We want today to connect these two things using the notion of essential dimension. We'll also discuss how to compute this. Something about canonical dimension for upper bounds and using cohomological invariants to get lower bounds.

1.4.2 An particular problem

Consider the group $\mathrm{H}^2(k, \mu_\ell) \subset \mathrm{H}^2(k, \mathbb{G}_m)[\ell]$. Recall $\mathrm{H}^2(k, \mathbb{G}_m) = \mathrm{Br}(k)$ is the Brauer group of k.

(Are we assuming $\ell \neq \mathrm{char}\, k$?)

Given $\alpha \in \mathrm{H}^2(k, \mu_\ell)$ with index $\mathrm{ind}(\alpha) = n$.

Recall 1.4.1.

$$\mathrm{ind}(\alpha) = \gcd\left\{[L : k] \mid \alpha_L = 0\right\}.$$

In the case of the Brauer group, this happens to also be $\min\left\{[L : k] \mid \alpha_L = 0\right\}$. Open if one has this equality in general.

Recall 1.4.2. If k contains a primitive ℓth root of unity (so $\mu_\ell = \mathbb{Z}/\ell\mathbb{Z} = \mu_\ell^{\otimes 2}$), then

$$\mathrm{H}^2(k, \mu_\ell) = \mathrm{H}^2(k, \mu_\ell^{\otimes 2}) = K_2^M(k)/\ell.$$

Hence we can write $\alpha = \alpha_1 + \cdots + \alpha_r$ as a sum of symbols $\alpha_i = (b_i, c_i)_\ell$ with $b_i, c_i \in k^\times$.

Question 1.4.3. *How big does r have to be?*

It follows from "the literature" (need to string a few results together) that there exists an absolute bound (depending only on ℓ, n, and not on k), but this bound is not (yet) explicit. Some cases are known

- If $\ell = n \in \{2, 3\}$, then $r \leq 1$
- If $\ell = n = 4$, then $r \leq 2$ (probably. The bound is known. May have misrecalled it)
- If $(\ell, n) = (2, 4)$, then $r \leq 2$

- If $(\ell, n) = (2, 8)$, then $r \leq 4$

In the case that k contains k_0 with $\operatorname{ddim}(k_0) < \infty$, then you can produce an explicit bound. In particular, one exists always in characteristic p.

How does this work? Given some $\alpha \in \mathrm{H}^2(k, \mu_\ell)$ as above, can find some intermediate field L ($k_0 \subset L \subset k$) s.t. L is f.g./k_0 w/ $\operatorname{trdeg}(L/k_0)$ depending only on ℓ, n[6] such that α is in the image of $\mathrm{H}^2(L, \mu_\ell) \to \mathrm{H}^2(k, \mu_\ell)$.

Slogan. Central simple algebras / cohomology classes of a given period and index have finite essential dimension

If $\operatorname{ddim}(k_0)$ bounded, then $\operatorname{ddim} L \leq \operatorname{ddim}(k_0) + \operatorname{trdeg}_{k_0} L$.

Recall 1.4.4. Matzri says that we can bound symbol length in $\mathrm{H}^2(k, \mu_\ell)$ in terms of $\operatorname{ddim} L$. Explicitly, if $\ell = p^t$ and $n = p^s$, then the length is at most

$$t\left(p^{\left(p^{2s-2}+1+\operatorname{ddim}(k)\right)} - 1\right).$$

Note 4. Got distracted and missed stuff, but sounds like maybe one can show a lower bound of the form $\left\lceil \frac{s}{t} \right\rceil + 1$.

Example. If $(\ell, n) = (2, 8)$ so $(p, t, s) = (2, 1, 3)$, then this bound gives

$$2^{17+\operatorname{ddim}(k_0)} - 1.$$

On the other hand, we know we can get a bound of 4, so this more general result is not sharp.

How about $k_0 = \mathbb{Q}$? Note that $\operatorname{ddim}\mathbb{Q} = \infty$. In this case, we know a bound exists, but we don't know how to write one down.

1.4.3 Pfister numbers

Recall 1.4.5. The Witt ring $W(k)$ has elements isometry classes of non-deg quadratic forms. The addition is perpendicular sum. The product is the (Kronecker) tensor product. We also declare the hyperbolic plane to be trivial.

Recall 1.4.6. The hyperbolic plane is the form xy or $x^2 - y^2 = \langle 1, -1 \rangle$ (equivalent when $\operatorname{char} k \neq 2$).

Recall 1.4.7. We let $I(k) \lhd W(k)$ denote the even dimensional forms, so it contains elements like $\langle\langle a \rangle\rangle := \langle 1, -a \rangle \in I(k)$. Products of these give n-fold Pfister forms

$$\langle\langle a_1, \dots, a_n \rangle\rangle = \langle\langle a_1 \rangle\rangle \dots \langle\langle a_n \rangle\rangle \in I^n(k).$$

These generate the nth power $I^n(k)$ of $I(k)$.

Question 1.4.8. *Given q a quadratic form of dimension d in I^n, we know we can write $q \sim q_1 \perp \cdots \perp q_r$ with q_i an n-fold Pfister form. How many do we need, how big can r have to be? Is there even a bound on r?*

[6] (Think) ℓ = period and n = index

Fact (Vishik)**.** If $d < 2^n + 2^{n-1}$, then r is bounded (by a small number, possibly 3). For $d \geq 2^n + 2^{n-1}$, it's unclear if r is bounded.

(Sounds like it is bounded for $n \leq 3$)

Why is $n \leq 3$ ok, but $n \geq 4$ hard? This brings us to essential dimension.

1.4.4 Essential Dimension

Fix a type of algebraic object (e.g. classes in $\mathrm{H}^2(k, \mu_\ell)$, in $\mathrm{Br}(k)$, in $W(k)$, in $I^n(k)$, etc. or quadratic forms of dimension d in I^n or something else). We think of these as functors from a category of field extensions of k_0 to sets.

Definition 1.4.9. Given a functor F as above and some $\alpha \in F(k)$ for some k/k_0, then we define the **essential dimension** of α to be

$$\mathrm{ed}(\alpha) = \min\left\{\mathrm{trdeg}(L/k_0) : \alpha \in \mathrm{im}\left(F(L) \to F(k)\right)\right\}.$$

Think of this as "how many parameters really needed to define α." Furthermore, the essential dimension of the functor is

$$\mathrm{ed}(F) = \max\left\{\mathrm{ed}(\alpha) : \alpha \in F(k) \text{ for all } k/k_0\right\}.$$

Example. Sounds like if F is the functor of points of a(n) (integral?) scheme over k_0, then the essential dimension of the functor will just be the dimension of that scheme.[7]

Definition 1.4.10. Given a functor F from k_0-algebras to sets, we say that some $\alpha \in F(R)$ is **versal** if for any $\beta \in F(k)$ for any k/k_0, there exists a homomorphism $R \to k$ so that $F(R) \to F(k)$ sends $\alpha \mapsto \beta$.

Remark 1.4.11. If there exists a versal $\alpha \in F(R)$ (say with R f.g. over k_0), then $\dim(R) \geq \mathrm{ed}(F)$ where $\dim R$ is Krull dimension.

Example. Say $F(k) = \{\text{quadratic forms over } k \text{ of dimension } n\}$. Then, $\mathrm{ed}(F) = n$. The point is that we can always diagonalize $q \simeq \langle a_1, \dots, a_n\rangle$ which is defined over $L = k_0(a_1, \dots, a_n)$. Alternatively,

$$q = \langle x_1, \dots, x_n\rangle \text{ over } k_0\left[x_1^{\pm 1}, \dots, x_n^{\pm 1}\right]$$

is versal. All quadratic forms come from this one by just specifying values for the x_i's.

How about fundamental ideals and their powers? Recall the Milnor conjectures identify

$$I^n/I^{n+1} \simeq \mathrm{H}^n(k, \mu_2),$$

i.e. we have a short exact sequence

$$1 \longrightarrow I^{n+1} \longrightarrow I^n \xrightarrow{e_n} \mathrm{H}^n(k, \mu_2) \longrightarrow 1.$$

This tells us that a quadratic form of dimension d in I^{n+1} is the same thing as a quadratic form of dimension d in I^n such that $e_n(q) = 0$.

[7] Something something generic point something something

1.4.5 Canonical dimension

Suppose F is a functor from field extensions k/k_0 to pointed sets. For $\alpha \in F(k)$, we define a new functor $\check{F}_\alpha$ (on extensions of k) via

$$\check{F}_\alpha(L) = \begin{cases} \emptyset & \text{if } \alpha_L \neq * \\ * & \text{if } \alpha_L = * \end{cases}$$

(above $*$ is the point of our pointed sets, so $\#\check{F}_\alpha(L) \leq 1$ always). The **canonical dimension** of α is $\operatorname{cd}(\alpha) = \operatorname{ed}(\check{F}_\alpha)$.

Remark 1.4.12. $\operatorname{cd}(\alpha) \leq r$ means that if $\alpha_L = *$, then there exists some intermediate field $k \subset E \subset L$ w/ $\operatorname{trdeg}_k E \leq r$ so that $\alpha_E = *$.

Think, "How many parameters needed to split α?"

The typical approach to bounding $\operatorname{cd}(\alpha)$ is the concept of 'generic splitting schemes'.

Definition 1.4.13. Given F as above and $\alpha \in F(k)$, we say a scheme X/k is a generic splitting scheme for α if $\alpha_L = * \iff X(L) \neq 0$.

Exercise. X is a generic splitting scheme of α of f.type over $k \implies \operatorname{cd}(\alpha) \leq \dim X$.

Open Question 1.4.14. *Do there exist finite type generic splitting schemes for cohomology classes in* $\mathrm{H}^i(k, \mu_\ell^{\otimes j})$*?*

We do know this in special cases

- For $i = 1$, this is known (torsors)
- For $i = 2$, this is known (and due to Krashen?). When $i = 2$ and $j = 1$, this is classical (Severi-Brauer varieties)
- For symbols in $(i, j, \ell) = (3, 2, \text{prime})$, Markyrev-Suslusars (?)
- For symbols in $(i, j, \ell) = (4, 3, 3)$, Albert algebra construction
- For symbols in ℓ prime, one can show this up to prime to ℓ extensions, Rosts's "Norm varieties"
- For symbols in $\ell = 2$, Pfister quadrics

Remark 1.4.15. If there exists generic splitting schemes for classes in $\mathrm{H}^i(k, \mu_\ell)$ for $i \geq 3$, then we could bound Pfister #'s (for quadratic forms of fixed dimension in I^n). Let

$$\mathscr{I}_d^n(k) = \{\text{quad forms of dim } d \text{ in } I^n\}.$$

If there is a versal element in $\mathscr{I}_d^n$, then it only needs some particular finite # of Pfister forms to write it. Everything else is a specialization of it, so this particular length gives a universal upper bound for all other lengths.[8]

[8] This is secretly not a correct argument as stated, but it can be made to work.

1.5 Déglise Lecture 1 (7/14): Voevodsky's Motivic Complexes

1.5.1 L-functions

Recall 1.5.1 (Euler product)**.**

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}.$$

Sounds like we'll talk about L-functions for a bit. In one direction, one has function fields and the Weil conjectures (ca. '49). This leads one to étale ℓ-adic sheaves (SGA4 '64) as well as the notion of weights (letters from Grothendieck to Serre). Grothendieck introduced (but never published?) the notion of pure motives (ca. '69).

In the other direction, one has number fields. An early result in this direction is Dirichlet's class number formula (1838). In general, people had studied special values of L-functions (e.g. Lichtenbaum '73). This is related to K-theory.

Also a part of this story is the notion of perverse sheaves (and of t-structures). Also, before pure motvies was Deligne's notion of mixed Hodge structures.

Everything here feeds into Bellinson's conjecture ('84) as well as Voevodsky's motivic homotopy theory and motivic complexes.

There are also p-adic L-functions and maybe (conjecturally?) some notion of p-adic motives?

1.5.2 Plan

(i) (homotopy) sheaves w/ transfers

(ii) perfect field case and main theorem

(iii) Motivic complexes

Fix a base S, a regular noetherian finite dimensional scheme (e.g. take a regular integral model of a curve over a number field)

There are a few difference w/ étale sheaves

(1) transfer (algebraic cycles)

(2) Use (big) smooth Nisnevich site

(3) $\mathbb{A}^1$-homotopy relation (algebro-topological techniques)

1.5.3 Finite correspondences

Definition 1.5.2. Say $X, Y \in \mathrm{Sm}_S$ (smooth, separated, of finite type over S). A **finite corresondence** α from $X \to Y$ is an algebraic cycles

$$\alpha = \sum_{i=1}^{n} n_i [Z_i]$$

where $Z_i \subset X \times_S Y$ is closed, integral and the projections $Z_i \to X$ is finite, surjective over some connected component, i.e. $\mathrm{supp}(\alpha)/X$ finite equidimensional. We let $C_S(X, Y)$ denote the set of correspondences.

One can compose correspondences. Given $\alpha \in C_S(X, Y)$ and $\beta \in C_S(Y, Z)$, first consider the product $X \times Y \times Z$ with projections p, r, q to $X \times Y, X \times Z, Y \times Z$. Then, $p^*(\alpha)$ and $q^*(\beta)$ are well-defined algebraic cycles on $X \times Y \times Z$ (e.g. $p^*(\alpha) = \sum m_i [Z_i \times_S Z]_{X \times Y \times Z}$). These intersect properly (something about Serre's tor formula), so we can intersect to get another algebraic cycle $\gamma := p^*(\alpha).q^*(\beta)$ in $X \times Y \times Z$. Think of this intersection as the fiber product $\alpha \times_Y \beta$. One deduces that $T = \operatorname{supp}(\gamma)$ is finite and equidimensional, so $h := r|_T : T \to R(T)$ is a finite morphism. Now, $\beta \circ \alpha := h_*(\gamma)$. This is composition.

One check that this composition law is associative and has a neutral element.

Example. Say $f : X \to Y$ is a morphism in Sm_S. Let Γ_f be its graph. This is the pullback

$$\begin{tikzcd}
\Gamma_f \arrow[r] \arrow[d] \arrow[dr, phantom, very near start, "\ulcorner"] & X \times_S Y \arrow[d, "f \times \mathrm{Id}"] \\
Y \arrow[r, "\Delta"] & Y \times_S Y
\end{tikzcd}$$

(note $\Delta : Y \hookrightarrow Y \times_S Y$ is a closed immersion). One gets a correspondence $''f'' = (\Gamma_f) \in c_S(X, Y)$. The neutral element is simply "Id_X"

Example. Say $f : X \to Y$ is finite equidimensional. Let $\varepsilon : X \times_S Y \xrightarrow{\sim} Y \times_S X$. Then, $\varepsilon_* \Gamma_f$ is a cycle in $Y \times_S X$ which lives in $C_S(Y, X)$. We call this the **transpose** of f, denoted ${}^t f$.

Definition 1.5.3. Sm_S^{Cor} is the category of smooth S-schemes whose morphisms are finite S-correspondences.

We have a **graph functor** $\gamma : \mathrm{Sm}_S \to \mathrm{Sm}_S^{Cor}$ sending $X \mapsto X$ and $f \mapsto \gamma(f) = (\Gamma_f)$.

Let $f : T \to S$ be a morphism of regular schemes. Get a base change functor $f^* : \mathrm{Sm}_S^{Cor} \to \mathrm{Sm}_T^{Cor}$ sending $X/S \mapsto X \times_S T$ and $\alpha \in C_S(X, Y)$ to $f^*(\alpha) \in C_T(X_T, Y_T)$.

Say $p : T \to S$ a smooth morphism. Then we get another functor $p_\# : \mathrm{Sm}_T^{Cor} \to SM_S^{Cor}$ sending $Y/T \mapsto (Y \to T \xrightarrow{f} S)$ and $\beta \in C_T(Y, Y')$ to $\nu_*(\beta) \in C_S(Y, Y')$ where $\nu : X \times_T Y' \hookrightarrow Y \times_S Y'$. This is 'forget the base'.

Remember: For us, 'smooth' = 'smooth, separated, and finite type'

There is a monoidal structure on Sm_S^{Cor}. Given objects $X/S, Y/S$, we can take their usual product $X \times_S Y$. Given correspondences $\alpha \in C_S(X, X')$ and $\beta \in C_S(Y, Y')$, we get $\alpha \times_S \beta \in C_S(XY, S'Y')$.

1.5.4 Transfers (I think)

Definition 1.5.4. A **presheaf with transfers** is a contravariant functor $\mathrm{Sm}_S^{Cor} \to \mathrm{Ab}$ which is furthermore additive.

The category of such presheaves, denoted $\mathrm{Psh}^{tr}(S)$, is abelian and (co)complete. We also still have a Yoneda embedding $\mathrm{Sm}_S^{Cor} \to \mathrm{Psh}^{tr}(S)$ sending $X/S \mapsto C_S(-, X) := \mathbb{Z}_S^{tr}(X)$.

Example. Consider $\mathbb{G}_m : X/S \mapsto \mathscr{O}_X(X)^\times$. This is a presheaf w/ transfers.

Example. Say A is an abelian variety over k. Then, $\underline{A} : X/k \mapsto \mathrm{Hom}(X, A)$ is a presheaf w/ transfers. This holds also if A is semi-abelian (extension of torus by abelian variety).

Example. Say H^* is a "good" cohomology theory (e.g. étale of de Rham cohomology). Say S/k smooth (regular enough if using ℓ-adic étale cohomology w/ $\ell \in \mathscr{O}_S(S)^\times$). Then, $X/S \mapsto \mathrm{H}^m(X)$ is a presheaf w/ transfers.

By "good" we at least want to have cycle class maps.

1.5.5 Nisnevich topology

Definition 1.5.5. A **Nisnevich cover** $W \xrightarrow{p} X \in \mathrm{Sm}_S$ is an étale morphism s.t. for all $x \in X$, there exists some $y \in W$ w/ $p(y) = x$ and $\kappa(x) \xrightarrow{\sim} \kappa(y)$.

Note that all Zariski covers are Nisnevich and all Nisnevich covers are étale.

Definition 1.5.6. A **Nisnevich distinguished square** in Sm_S is a square of the form

$$\begin{tikzcd} W \arrow[r] \arrow[d] \arrow[dr, phantom, "\ulcorner", very near start] & V \arrow[d, "p"] \\ U \arrow[r, "j"] & X \end{tikzcd}$$

such that j is an open immersion, p is étale, and for $Z := (X \setminus U)_{\mathrm{red}} \subset X$, we have an induced iso $T := p^*(Z) \xrightarrow{\sim} Z$.

Note (X, Z) is a closed pair. We say $p : (V, T) \to (X, Z)$ above is an **excisive morphism of closed pairs**.

Lemma 1.5.7 (Exercise)**.** *Say $F : \mathrm{Sm}_S \to \mathrm{Ab}$ contravariant. Then, F is a Nisnevich sheaf iff for any Nis. distinguished square Δ, its image $F(\Delta)$ is cocartesian (a pushout).*

Definition 1.5.8. $F \in \mathrm{Psh}^{tr}(S)$ is a (Nis) **sheaf w/ transfers** if

$$\gamma_*(F) := F \circ \gamma : \mathrm{Sm}_S \to \mathrm{Sm}_S^{Cor} \to \mathrm{Ab}$$

is a Nisnevich sheaf.

Example. Say $f : Y \to X$ a finite equidimensional surjective morphism. If $F \in \mathrm{Sh}^{tr}(S)$, we get a 'transfer' or 'wrong way' map

$$f_* := F({}^t f) : F(Y) \to F(X).$$

Remark 1.5.9 ("big" site). Say $X \in \mathrm{Sm}_S$. There's the small Nisnevich site X_{Nis} whose objects are étale schemes V/X. Given $F \in \mathrm{Sh}^{tr}(S)$, can get a sheaf $F_X := F|_{X_{Nis}}$ on the small site. Given $f : Y \to X \in \mathrm{Sm}_S$, obtain $f^* F_X \to F_Y$, a morphism of sheaves on Y_{Nis}.

A sheaf on Sm_S corresponds to the data of sheaves $(F_X)_{X \in \mathrm{Sm}_S}$ on the small sites + the data of transition maps $\tau_f : f^* F_X \to F_Y$ (usually not isos). Note in particular that we have an inclusion $\mathrm{Sh}(S_{Nis}) \hookrightarrow \mathrm{Sh}(\mathrm{Sm}_{S,Nis})$ (whose transition maps are isomorphisms).

Recall that on Sm_S^{Cor}, we had 3 operations: $f^*, p_\#, \otimes$. All of these can be extended to sheaves.

Remark 1.5.10. Say we have $f : T \to S$ and $F \in \mathrm{Sh}^{tr}(S)$. Then we can form

$$F \circ f^* : \mathrm{Sm}_S^{Cor} \to \mathrm{Sm}_T^{Cor} \to \mathrm{Ab}\,.$$

This is the direct image $f_*(F)$ (note it sends $X \mapsto F(X \times_S T)$). This gives a functor $\mathrm{Sh}^{tr}(S) \leftarrow \mathrm{Sh}^{tr}(T) : f_*$. It has a left adjoint $f^* : \mathrm{Sh}^{tr}(S) \to \mathrm{Sh}^{tr}(T)$. This adjoint is characterized by the fact that

$$f^* \mathbb{Z}_S^{tr}(X) = \mathbb{Z}_S^{tr}(X \times_S T).$$

Example. Say X/S is smooth, so we have $\mathbb{Z}_S^{tr}(X) = C_S(-, X)$. One can check that this is a Nisnevich sheaf.

The examples of $\mathbb{G}_m$ and $\underline{A}$ from before also give sheaves w/ transfer (over S or over a field).

Remark 1.5.11. Say $p : T \to S$ is smooth and $F \in \mathrm{Sh}^{tr}(T)$. Then, (one can check that) $p^*(F) = F \circ p_\#$ where $p_\#$ is this 'forget the base' guy from before. One can show that this admits a left adjoint

$$p_\# : \mathrm{Sh}^{tr}(T) \leftrightarrows \mathrm{Sh}^{tr}(S) : p^*$$

characterized by

$$p_\# \mathbb{Z}_T(Y) = \mathbb{Z}_S(Y \to T \to S).$$

Remark 1.5.12. One can give a tensor product $\otimes^{tr}$ on $\mathrm{Sh}^{tr}(S)$ characterized by $\mathbb{Z}_S^{tr}(X) \otimes^{tr} \mathbb{Z}_S^{tr}(Y) = \mathbb{Z}(X \times_S Y)$. This has an adjoint which is internal Hom.

This gives 6 functors organized into adjoint pairs.

1.5.6 $\mathbb{A}^1$-invariance

Definition 1.5.13. A sheaf $F \in \mathrm{Sh}^{tr}(S)$ is **$\mathbb{A}^1$-invariant** if for any smooth scheme X/S, the induced map $F(X) \to F(\mathbb{A}_X^1)$ is an isomorphism.

Given, $\alpha, \beta \in C_S(X, Y)$ they are $\mathbb{A}^1$-homotopic, $\alpha \sim_{\mathbb{A}^1} \beta$, if there exists $H \in C_S(\mathbb{A}^1 \times X, Y)$ so that $H \circ s_0 = \alpha$ and $H \circ s_1 = \beta$. This induces an equiv relation on Sm_S^{Cor} which gives rise to a corresponding homotopy category $\Pi \, \mathrm{Sm}_S^{Cor}$.

Remark 1.5.14. $\mathbb{A}^1$-invariance $\iff$ F factors through $\Pi \, \mathrm{Sm}_S^{Cor}$.

Example (exercise)**.** $\mathbb{G}_m$ is $\mathbb{A}^1$-invariant. $\underline{A}$ is also $\mathbb{A}^1$-invariant (over a field).

Relative Picard groups: say (X, Z) a closed pair. Then,

$$\mathrm{Pic}(X, Z) = \{(\mathscr{L}, \varphi) : \mathscr{L} \text{ invertible sheaf on } X \text{ and } \varphi : \mathscr{L}|_Z \ldots\}$$

(I was too slow)

Theorem 1.5.15 (Sudsin (?)-Voevodsky)**.** *Say S is an affine regular scheme and C/S a smooth affine curve. Furthermore, say there exists a normal, proper $\overline{C}/S$ s.t. $C \overset{open}{\subset} \overline{C}$ with $C_\infty = \overline{C} - C \neq \emptyset$ admits an affine open neighborhood in $\overline{C}$. This is called a* ***good compactification****.*

Then, for all X/S smooth affine, $\Pi_S(X, C) \simeq \mathrm{Pic}(X \times_S \overline{C}, X \times_S C_\infty)$ (correspondences up to homotopy).

1.5.7 Next part

Say $S = \mathrm{spec}\, k$ with k a field (later: k a perfect field).

Lemma 1.5.16. *Say $j : U \to X$ is an open immersion in Sm_k. Then, there is a Zariski cover $p : W \to X$*

and a finite correspondence $\alpha \in C_k(W, U)$ such that

$$\begin{tikzcd} W \arrow[rr, "\alpha"] \arrow[dr, "p"'] & & U \arrow[dl, "j"] \\ & X & \end{tikzcd}$$

commutes up to homotopy.

That is, open immersions admit splittings up to homotopy.

Corollary 1.5.17. *For $F \in \mathrm{Sh}^{tr}(k)$ an $\mathbb{A}^1$-invariant sheaf, ... (missed it)*

For $X \in \mathrm{Sm}_k$, the map $F(X) \to \prod_{x \in X^{(0)}} F(\kappa(x))$ is a monomorphism ($X^{(0)}$ is the generic points); here, $F(\kappa(x)) = \varinjlim_{x \in U \overset{\text{open}}{\subset} X} F(U)$.
(missed something)

Definition 1.5.18. Let $HI^{tr}(k)$ be the category of $\mathbb{A}^1$-invariant sheaves w/ transfers.

This is an abelian category. The forgetful functor $HI^{tr}(k) \to \mathrm{Sh}^{tr}(k)$ has a left adjoint.

Example. There is a fully faithful embedding (abelian varities over k) $\to HI^{tr}(k)$

1.5.8 (-1) construction

Definition 1.5.19. Say $F \in HI^{tr}(k)$. Define

$$F_{-1}(X) := \ker\left(F(\mathbb{G}_m \times X) \xrightarrow{s_1^*} F(X)\right)$$

(map induced by unit section). Then, $F_{-1} \in HI^{tr}(k)$.

Example (exercise)**.** $F_{-1} = \underline{\mathrm{Hom}}(\mathbb{G}_m, F) =$ "$\Omega_{\mathbb{G}_m}(F)$" is the "$\mathbb{G}_m$-loop space of F"

Example. $(\mathbb{G}_m)_{-1} = \underline{\mathbb{Z}}$ is a constant sheaf

Example. If A is an abelian variety, then $(\underline{A})_{-1} = 0$.

Theorem 1.5.20 (devissage lemma of Voevodsky)**.** *Now say k is a perfect field.*[9] *Let $i : Z \hookrightarrow X$ be a closed immersion of a divisor ($X/k \in \mathrm{Sm}_k$). Let $U = X \setminus Z$ with inclusion $j : U \hookrightarrow X$. We have an exact sequence*

$$0 \longrightarrow F_X \longrightarrow j_* F_U \longrightarrow i_*(F_{-1,Z}) \longrightarrow 0$$

of sheaves on the small site X_{Nis}.

In terms of cohomology with supports, this becomes $\mathrm{H}^1_Z(X, F) \simeq \mathrm{H}^0(Z, F_{-1}) = F_{-1}(Z)$ so it's really a kind of purity theorem.

[9] Unclear if this is necessary yet

1.5.9 Main theorem

For this we do need k a perfect field.

Theorem 1.5.21 (Voevodsky). *Say $F \in HI^{tr}(k)$. For all m and all $X/k \in \mathrm{Sm}_k$, the map*

$$\mathrm{H}^m_{Nis}(X, F) \xrightarrow{p^*} \mathrm{H}^m_{Nis}(\mathbb{A}^1_X, F)$$

is an isomorphism.

This uses the devissage lemma from above. The key point is to prove that for any open immersion $j : U \to X$, one has $R^m j_*(F) = 0$ for all $m > 0$.

Corollary 1.5.22 (purity). *Say $Z \hookrightarrow X$ closed of codimension c. Then,*

$$\mathrm{H}^n_Z(X, F) = \mathrm{H}^{n-c}(Z, F_{-c}).$$

We can reformulate this. For $x \in X^{(n)}$ (so $\mathrm{codim}_X(x) = n$), one has that $\mathrm{H}^i_{\{x\}}(X_{(x)}, F) = 0$ for $i \neq n$ and is $F_{-n}(\kappa(x))$ for $i = n$.

Corollary 1.5.23. *For all X smooth over k, F_X is Cohen-Macaulay (in sense of Residue and dualities)*

As a consequence there is some cousin complex $C^*(X, F)$... (I didn't really get what was going on). Another key word here is Gersten (?) complex. Apparently these complexes compute the Nisnevish (or Zariski) cohomology of F.

Exercise. Consider the case of $\mathbb{G}_m$

There was more stuff after, but I was too distracted to record it

1.6 Frédéric Déglise Lecture 2 (7/15)

Déglise began by recalling the web of related ideas, but I didn't copy this down.

1.6.1 Some definitions

To state these definitions, we'll use the language of ∞-categories. This will allow us to give precise definitions that are not bogged down in technical details.

Notation 1.6.1. Let $\mathcal{S}_*$ denote the ∞-category of pointed spaces (pointed simplicial sets). Let $\mathcal{D}(\mathrm{Ab})$ denote the derived category of abelian groups.

Fix a (noetherian?) scheme S.

(1) pointed $\mathbb{A}^1$-homotopy category $\mathcal{H}^{\mathbb{A}^1}_*(S)$

∞-functors $\chi : \mathrm{Sm}_S \to \mathcal{S}_*$ (contravariant) satisfying

- Excision: for all $f : (Y, T) \to (X, Z)$ excisive, $\chi(X, Z) \to \chi(Y, T)$ is a weak equivalence (iso in ∞-categorical sense)

- $\mathbb{A}^1$-invariance: for all $X \in \mathrm{Sm}_S$
$$\chi(X) \to \chi(\mathbb{A}^1 \times X)$$
is a weak eq

Example. Let K be a pointed simplicial set. Can take the constant functor $X \mapsto K$.

Example (Almost Yoneda)**.** Say $X \in \mathrm{Sm}/S$. Then, $X(-)$ may not be excisive or may not be $\mathbb{A}^1$-invariant.

To remedy this, use ∞-categorical localization theory. Describe category as localization of $\mathrm{Psh}(\mathrm{Sm}_S, \mathcal{S}_*)$ by Nisnevich topology and $\mathbb{A}^1$-equivalences.

Example. Now any $X \in \mathrm{Sm}/S$ will give rise to a presheaf $X(-)$ which can then be localized.

(2) motivic complexes $\mathcal{D}\Pi(S)$

Additive contravariant ∞-functors $K : \mathrm{Sm}_S^{Cor} \to \mathcal{D}(\mathrm{Ab})$. Also required to excisive and $\mathbb{A}^1$-invariant.

Here localize $\mathrm{Psh}^{tr}(\mathrm{Sm}^{Cor}, \mathcal{D}(\mathrm{Ab})) = \mathcal{D}(\mathrm{Psh}^{tr}(S))$ by Nisnevich and $\mathbb{A}^1$-equivs.

Note that $\chi(X, Z)$ is the homotopy fiber of $\chi(X) \to \chi(Z)$ (or something like this).

Remark 1.6.2*.* Can replace 'excision' by saying...

Definition 1.6.3. $\mathcal{H}_*^{\mathbb{A}^1}(S)$ is localization of $\mathrm{Sh}_{Nis}(\mathrm{Sm}_S, \mathcal{S}_*)$. As models, can take 'spaces' $\chi : \mathrm{Sm}_S^{\mathrm{op}} \to \Delta^{\mathrm{op}}\mathrm{Set}_*$ localized w.r.t. $\mathbb{A}^1$.

Definition 1.6.4. On the other side, take $\mathrm{Sh}^{tr}(S)$ localized w.r.t $\mathbb{Z}_S^{tr}(\mathbb{A}_X^1) \to \mathbb{Z}_S^{tr}(X)$. This gives $\mathcal{D}\Pi(S)$.

This is not the name he gave it, but I can't tell what's written down (this has happened several times before in these notes w/o me pointing it out)

Now say k is a perfect field. Consider a complex of sheaves w/ transfer $K \in \mathrm{Comp}(\mathrm{Sh}^{tr}(S))$. Can define its cohomology sheaves as usual $\underline{\mathrm{H}}^i(K) = \ker \mathrm{d}^{i+1}/\mathrm{Im}(\mathrm{d}^i) \in \mathrm{Sh}^{tr}(S)$.

Theorem 1.6.5. *K as above is $\mathbb{A}^1$-local iff for all $n \in \mathbb{Z}$, $\underline{\mathrm{H}}^n K$ is $\mathbb{A}^1$-invariant, i.e. live in $HI^{tr}(k)$.*

Can define $D\Pi(k)$ as the full subcategory of $\mathcal{D}(\mathrm{Sh}^{tr}(k))$ made by $\mathbb{A}^1$-local complexes.

Let $\Delta_k^n = \mathrm{spec}\,(k[t_0, \dots, t_n]/(t_0 + \dots + t_n - 1))$. For $K \in \mathrm{Comp}(\mathrm{Sh}^{tr}(k))$, can define $\underline{C}_*^S(k)$ via $X \mapsto \mathrm{Tot}^{\oplus} K(\Delta^n \times_k X)$.

Ok, I'm already lost. There's no real point in me pretending like I'm getting anything out of this. I'm gonna stop here.

1.7 Kirsten Wickelgren Lecture 1 (7/14): An introduction to $\mathbb{A}^1$-homotopy theory using enumerative examples

Enumerative geometry is (classically) about counting algebro-geometric objects over $\mathbb{C}$.

Question 1.7.1. *How many lines meet 4 lines in $\mathbb{P}^3$.*

Answer. 2

Goal. Introduce $\mathbb{A}^1$-homotopy theory and have fun.

Goal (More mathematical). Record arithmetic information about geometric objects over a field k (whose # is fixed over $\overline{k}$), e.g. are any of those lines defined over $\mathbb{R}$?

The tool for achieving this goal will be to use $\mathbb{A}^1$-homotopy theory developed by Morel-Voevodsky.

1.7.1 Classical homotopy theory

Let's start w/ usual homotopy. Consider the sphere

$$S^n = \left\{(x_0, \ldots, x_n) \in \mathbb{R}^{n+1} : \sum x_i^2 = 1\right\} \cong \mathbb{P}^n(\mathbb{R})/\mathbb{P}^{n-1}(\mathbb{R}).$$

There's a degree map $\deg : [S^n, S^n] \to \mathbb{Z}$ which, roughly, counts the number of preimages of a point. Given $f : S^n \to S^n$ and $p \in S^n$ s.t. $f^{-1}(p) = \{q_1, \ldots, q_N\}$, one has

$$\deg f = \sum_{i=1}^{N} \deg_{q_i} f$$

where these local degrees $\deg_{q_i} f$ can be computed as follows: let V be a small ball around p, and let $f^{-1}(V) \supset U$ with U a small ball s.t. $U \cap p^{-1}(f) = q_i$. Then, f induces a map

$$S^n \simeq U/\partial U \simeq U/(U - q_i) \xrightarrow{\overline{f}} V/(V - p) \simeq V/\partial V \simeq S^n$$

and $\deg_{q_i} f = \deg(\overline{f})$.

There is a formula from differential topology allowing one to compute this via calculus. Choose (oriented) loca coordinates $(x_1, \ldots, x_n)$ near q_i and $(y_1, \ldots, y_n)$ in p, so $f = (f_1, \ldots, f_n) : \mathbb{R}^n \to \mathbb{R}^n$. Consider

$$J = \det\left(\frac{\partial f_i}{\partial x_j}\right).$$

Then,

$$\deg_{q_i} f = \begin{cases} +1 & \text{if } J(q_i) > 0 \\ -1 & \text{if } J(q_i) < 0. \end{cases}$$

Example. If f is complex analytic (f a polynomial map over $\mathbb{C}$), and $J(q_i) \neq 0$, then $\deg_{q_i} f = 1$ always. Thus, $\deg f = \left|f^{-1}(pt)\right|$ is the number of solutions to $\{f_1 = f_2 = \cdots = f_n = 0\}$.

Example. Say $f(x) \in \mathbb{C}[x]$ of degree n. Then, f induces $f : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ so $n = \deg f = \#\{f = 0\}$. This is the fundamental theorem of algebra.

Remark 1.7.2. We can also count solutions to $f = 0$ where f is a section of a rank n vector bundle $V \xrightarrow{p} X$. In this case, the Euler class of V can be computed as a sum of local degrees,

$$e(V) = e(V, f) = \sum_{q \in \{f=0\}} \deg_q f.$$

Example. Say $\mathrm{Gr}(1, 3)$ be the Grassmannian parameterizing $\mathbb{P}^1$'s in $\mathbb{P}^3$ (i.e. dim 2 subspaces $W \subset \mathbb{C}^4$). There is a tautological rank 2 bundle $S \to \mathrm{Gr}(1, 3)$ w/ fibers $S_{[\mathbb{P}W]} = W$. Let L_1, L_2, L_3, L_4 be four lines in $\mathbb{P}^3$. Note that a line L means L_1, say, if their W's have nonempty intersection. As a consequence,

$$\{\text{lines meeting } L_1, L_2, L_3, L_4\} = \{f = 0\}$$

for f a section (depending on the L_i) of

$$\bigoplus_{i=1}^{4} \bigwedge^2 S^* \longrightarrow \mathrm{Gr}(1,3).$$

Thus, the #lines meeting L_1, L_2, L_3, L_4 is the Euler number $e\left(\bigoplus_{i=1}^4 \bigwedge^2 S^*\right)$. In particular, this number is independent of the choice of lines (generally chosen[10]). One can compute that this Euler number is 2 using splitting principal, cohomology of Grassmannians, and other such tools.

1.7.2 $\mathbb{A}^1$-homotopy theory

We'd like a version of the (sort of stuff going on in the) previous example over any field k. The first thing we need is a notion of degree.

Lannes/Morel gave a notion of degree for $f : \mathbb{P}^1 \to \mathbb{P}^1$ over any field k. This degree will not be an integer, but will instead by valued in the **Grothendieck-Witt group** $\mathrm{GW}(k)$ of k. This is the group completion of the semiring of (iso. classes of) nondegenerate, symmetric bilinear forms.

Recall 1.7.3 (from other lectures)**.** The Witt group of k is the quotient $\mathrm{GW}(k)/\mathbb{Z}\left(\langle 1\rangle + \langle -1\rangle\right)$ by the ideal generated by the hyperbolic plane.

Note that we have a rank homomorphism $\mathrm{GW}(k) \to \mathbb{Z}$ determined by $\mathrm{rank}(V \times V \xrightarrow{B} k) = \dim_k V$. The Grothendieck-Witt group can be recovered from the Witt group via the pullback square

$$\begin{tikzcd}
\mathrm{GW}(k) \arrow[r] \arrow[d, "\mathrm{rank}"'] & W(k) \arrow[d, "\mathrm{rank}"] \\
\mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z}.
\end{tikzcd}$$

Remark 1.7.4. All quadratic forms can be diagonalized, so $\mathrm{GW}(k)$ is generated by $\langle a\rangle$ for $a \in k^\times/(k^\times)^2$. This is the element associated to the rank 1 bilinear form $(x,y) \mapsto axy$.

Over a field, we have the relations

(1) $\langle a\rangle \langle b\rangle = \langle ab\rangle$

(2) $\langle u\rangle + \langle v\rangle = \langle uv(u+v)\rangle + \langle u+v\rangle$

(3) $\langle u\rangle + \langle -u\rangle = \langle 1\rangle + \langle -1\rangle =: h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Example. $\mathrm{GW}(\mathbb{C}) \cong \mathbb{Z}$ via rank. True for any field k with $k^\times = (k^\times)^2$.

Example. $(\mathrm{rank}, \mathrm{signature}) : \mathrm{GW}(\mathbb{R}) \to \mathbb{Z} \times \mathbb{Z}$ is an isomorphism onto its image which is the subgroup consisting of (a,b) with $a \equiv b \pmod 2$.

Example. $(\mathrm{rank}, \mathrm{disc}) : \mathrm{GW}(\mathbb{F}_q) \xrightarrow{\sim} \mathbb{Z} \times (\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2)$

Example (Springer's Theorem). Let K be a complete discrete valued field with residue field k (e.g. $K = \mathbb{Q}_p$ or $K = \mathbb{F}_p((t))$). Assume $\mathrm{char}\, k \neq 2$. Then, $W(K) = W(k) \oplus W(k)$.

[10] Want section to have isolated zeros

We also have transfer: say $K \subset E$ is a finite, separable extension of fields. Then we get a trace map $\mathrm{Tr}_{E/k} : \mathrm{GW}(E) \to \mathrm{GW}(K)$ determined by

$$\mathrm{Tr}_{E/K}\left(V \times V \xrightarrow{B} E\right) = \left(V \times V \xrightarrow{B} E \xrightarrow{\mathrm{Tr}_{E/K}} K\right).$$

This is well-defined (i.e. image non-degenerate) by Gaois theory.

Let's get back to Lannes/Morel. Say we have $f : \mathbb{P}^1_k \to \mathbb{P}^1_k$ and $p \in \mathbb{P}^1(k)$ with $f^{-1}(p) = \{q_1, \dots, q_N\}$. Suppose $J(q_i) = f'(q_i) \neq 0$ for all i. Then define

$$\deg f := \sum_{i=1}^{n} \mathrm{Tr}_{\kappa(q_i)/k} \langle J(q_i) \rangle .$$

Fact. This does not depend on the choice of p.

More generally, Morel gave a map

$$\deg^{\mathbb{A}^1} : \left[\mathbb{P}^n/\mathbb{P}^{n-1}, \mathbb{P}^n/\mathbb{P}^{n-1}\right]_{\mathbb{A}^1} \longrightarrow \mathrm{GW}(k)$$

with LHS above the 'unstable $\mathbb{A}^1$-homotopy classes of maps'.

Example. Say $k = \mathbb{R}$. Then we get a commutative diagram

$$\begin{tikzcd}
{[S^n, S^n]} \arrow[d, "\deg"] & {\left[\mathbb{P}^n/\mathbb{P}^{n-1}, \mathbb{P}^n/\mathbb{P}^{n-1}\right]} \arrow[l, "\mathbb{R}\text{-pts}"'] \arrow[r, "\mathbb{C}\text{-pts}"] \arrow[d, "\deg^{\mathbb{A}^1}"] & {\left[S^{2n}, S^{2n}\right]} \arrow[d, "\deg"] \\
\mathbb{Z} & \mathrm{GW}(\mathbb{R}) \arrow[l, "\mathrm{sig}"'] \arrow[r, "\mathrm{rank}"] & \mathbb{Z}
\end{tikzcd}$$

Remark 1.7.5. Cazanave and Brazelton-McKean-Pauli give formulas for $\deg^{\mathbb{A}^1}(\text{poly})$ in terms of Bézoutians

Assume all spaces are pointed.

Notation 1.7.6. Smash product is $X \wedge Y = \frac{X \times Y}{(X \times *) \cup (* \times Y)}$.

Example. In topology, $S^n \wedge S^m = S^{n+m}$. Also suspension is $\Sigma_{S^1} X := S^1 \wedge X$.

Example. We have a pushout

$$\begin{tikzcd}
\mathbb{G}_m \arrow[r] \arrow[d] & \mathbb{A}^1 \arrow[d] \\
\mathbb{A}^1 \arrow[r] & \mathbb{P}^1
\end{tikzcd}$$

Since we're doing $\mathbb{A}^1$-homotopy theory, we have $\mathbb{A}^1 \simeq *$, so this says that $\Sigma_{S^1}\mathbb{G}_m \simeq \mathbb{P}^1$.

Definition 1.7.7. We have **'spheres'** S^1 and $\mathbb{G}_m = \operatorname{spec} k[z^{\pm 1}] = \mathbb{A}^1 \setminus 0$. In general, we set

$$S^{p+q\alpha} := (S^1)^{\wedge p} \wedge (\mathbb{G}_m)^{\wedge q} \simeq S^{p+q,q}.$$

Example. $\mathbb{A}^n \setminus 0 \simeq (S^1)^{\wedge(n-1)} \wedge (\mathbb{G}_m)^{\wedge n}$. This comes from the pushout square

$$\begin{tikzcd}
(\mathbb{A}^1 \setminus 0) \times (\mathbb{A}^{n-1} \times 0) \arrow[r] \arrow[d] & \mathbb{A}^1 \times (\mathbb{A}^{n-1} \times 0) \arrow[d] \\
(\mathbb{A}^1 \setminus 0) \times \mathbb{A}^{n-1} \arrow[r] \arrow[ur, phantom, very near end, "\lrcorner"] & \mathbb{A}^n \setminus 0
\end{tikzcd}$$

+ induction. Note that in general, we have a pushout square

$$\begin{tikzcd}
X \times Y \arrow[r] \arrow[d] & Y \arrow[d] \\
X \arrow[r] \arrow[ur, phantom, very near end, "\lrcorner"] & \Sigma X \wedge Y
\end{tikzcd}$$

Example.

$$\mathbb{P}^n/\mathbb{P}^{n-1} \simeq \mathbb{P}^n/(\mathbb{P}^n \setminus 0) \simeq \mathbb{A}^n/(\mathbb{A}^n \setminus 0) \simeq */(\mathbb{A}^n \setminus 0) \simeq \Sigma_{S^1}(\mathbb{A}^n \setminus 0) \simeq (S^1)^{\wedge n} \wedge (\mathbb{G}_m)^{\wedge n} \simeq (\mathbb{P}^1)^{\wedge n}$$

Stable homotopy theory allows desuspension Σ^{-1}. In stable $\mathbb{A}^1$-homotopy theory, can also desuspend $\mathbb{P}^1$, i.e. have $\Sigma_{\mathbb{P}^1}^{-1}$ (where $\Sigma_{\mathbb{P}^1} = \mathbb{P}^1 \wedge (-)$). This category will be denote $SH(k)$.

Theorem 1.7.8 (Morel, Hopkins-Morel)**.** *Fix a field k. Stably,*

$$[S^0, S^0] \cong [\mathbb{P}^n/\mathbb{P}^{n-1}, \mathbb{P}^n/\mathbb{P}^{n-1}] \cong \mathrm{GW}(k).$$

Moreover, we have a ring isomorphism

$$\bigoplus_{n \in \mathbb{Z}} [S^0, \mathbb{G}_m^{\wedge n}] \cong K_*^{MW}(k)$$

to Milnor-Witt K-theory.

This Milnor-Witt K-theory is some combination of Milnor K-theory $K_*^M(k)$ and the Witt ring $W(k)$. It is the graded associative algebra generated by $[u] \in K_1^{MW}(k)$ for $u \in k^\times$ and $\eta \in K_{-1}^{MW}(k)$ (the 'Hopf map') subject to the relations

(1) (Steinberg relation) $[u][1-u] = 0$

(2) $[ab] = [a] + [b] + \eta[a][b]$

(3) $[a]\eta = \eta[a]$

(4) $\eta h = 0$ with $h = \eta[-1] + 2$ the hyperbolic element.

Remark 1.7.9. $\mathrm{GW}(k) \cong K_0^{MW}(k)$ via $\langle a \rangle \leftrightarrow 1 + \eta[a]$. In particular $h = \langle 1 \rangle + \langle -1 \rangle \leftrightarrow 1 + (1 + \eta[-1])$ (note $[1] = 0$).

How does one prove this theorem?

In terms of maps from S^0, $[a] : S^0 \to \mathbb{G}_m$ is the (based) map sending the non base point to a (note $S^0 = \operatorname{spec} k \sqcup \operatorname{spec} k$). Also, $\eta : \mathbb{A}^2 \setminus 0 \to \mathbb{P}^1$ sends $(x, y) \mapsto [x : y]$. On $\mathbb{C}$-pts this is the Hopf map $S^3 \simeq \mathbb{C}^2 \setminus 0 \to \mathbb{CP}^1 \simeq S^2$. On $\mathbb{R}$-pts, it's multiplication by 2, $S^1 \xrightarrow{2} S^1$. Note that η is not nilpotent.

Recall we have a (cofiber?) sequence $X \vee Y \to X \times Y \to X \wedge Y$. We can suspend to get $\Sigma(X \vee Y) \to \Sigma(X \times Y) \to \Sigma(X \wedge Y)$. We can add the maps $\Sigma(X \times Y) \rightrightarrows \Sigma X, \Sigma Y$ to get a splitting map showing that $\Sigma(X \times Y) = \Sigma X \vee \Sigma Y \vee \Sigma(X \wedge Y)$.

Lemma 1.7.10. *In $SH(k)$ one has*

$$\begin{tikzcd}
\mathbb{G}_m \times \mathbb{G}_m \arrow[r, "mult"] \arrow[d, "\wr"] & \mathbb{G}_m \arrow[d, "\wr"] \\
\mathbb{G}_m \vee \mathbb{G}_m \vee (\mathbb{G}_m \wedge \mathbb{G}_m) \arrow[r, "{(1,1,\eta)}"] & \mathbb{G}_m
\end{tikzcd}$$

Lemma 1.7.11.

$$\begin{pmatrix} \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 \\ z & \longmapsto & az \end{pmatrix} = 1 + \eta[a]$$

in $SH(k)$.

Note this has has degree $\langle a \rangle$ by the Jacobian stuff from before. Also note that this map is the suspension of $\mathbb{G}_m \to \mathbb{G}_m, z \mapsto az$. That is,

$$\begin{pmatrix} \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 \\ z & \longmapsto & az \end{pmatrix} = \Sigma\left(\mathbb{G}_m \times k \xrightarrow{1 \times a} \mathbb{G}_m \times \mathbb{G}_m \xrightarrow{\text{mult}} \mathbb{G}_m\right).$$

Combining this with the previous lemma gives the more recent lemma.

Furthermore,

Lemma 1.7.12. $[ab] = [a] + [b] + \eta[a][b]$

Can show this using above lemmas.

This induces a map $K_*^{MW}(k) \to \bigoplus_{n \in \mathbb{Z}} [S^0, \mathbb{G}_m^{\wedge n}]$. Morel and Hopkins show this is an isomorphism. In particular, this nets a degree map $\deg : [\mathbb{P}^n/\mathbb{P}^{n-1}, \mathbb{P}^n/\mathbb{P}^{n-1}] \to \mathrm{GW}(k)$.

Notation 1.7.13.

$$\bigoplus_{n \in \mathbb{Z}} [S^0, \mathbb{G}_m^{\wedge n}] \cong \bigoplus_{n \in \mathbb{Z}} \Pi_{n,n} \mathbb{S}$$

is the '0-line' of stable homotopy groups of spheres. This is also the r-line $\bigoplus_{n \in \mathbb{Z}} \pi_{n+r,n} \mathbb{S}$.

What do we know about this $\mathbb{A}^1$-homotopy groups of spheres?

- Röndigs-Spitzweck-Ostvaer compute 1-line in terms of Hermtiian K-theory and other stuff (2019, char $k \neq 2$)
- have some information about 2-line

There are still plenty big open questions

- Over more general rings, how do things work? e.g. what is $[\mathbb{P}^n/\mathbb{P}^{n-1}, \mathbb{P}^n/\mathbb{P}^{n-1}]$?

  Bachmann-Ostvaer compute this over $\mathbb{Z}[1/2]$. THey show $\pi_{(0,0)} \otimes \mathbb{Z}_{(2)} \cong \mathrm{GW}(\mathbb{Z}[1/2]) \otimes \mathbb{Z}_{(2)}$.
- $\underline{\pi}_{*,*}\mathbb{S}$
- Freudenthal suspension theorem? Which stable $\pi_{*,*}$ correspond to unstable groups?

1.7.3 $\mathbb{A}^1$-Euler class

Let's get back to counting things. Barge-Morel defined one. Sounds like also Fasel, Morel, Asok-Fasel, Leving, Kass-W., Déglise-Jin-Khan, Bachmann-W., Levine-Raksit have defined/used/worked with them as well.

Say X is a smooth k-scheme of dimension d. Let $V \to X$ be a rank r vector bundle.

Definition 1.7.14. We say V is **oriented** by (L, φ) where $L \to X$ is a line bundle and

$$\varphi : \det V \xrightarrow{\sim} L^{\otimes 2}.$$

Remember: Intuition is that being postiive over $\mathbb{R}$ is the same as being a square

We say X is oriented if its tangent bundle is.

Definition 1.7.15. $V \to X$ is **relatively oriented** when $\operatorname{Hom}(\det TX, \det V)$ is oriented.

Example. Say $X = \mathbb{P}^n$ or $\operatorname{Gr}(m, n)$ ($\mathbb{P}^m$'s in $\mathbb{P}^n$). Then, $\omega_X = \det T^*X = \mathscr{O}(-n-1)$. So X oriented iff n odd.

Example. $\mathscr{O}(n)$ on $\mathbb{P}^1$ is relatively orientable $\iff$ n even.

Euler "number" in $\operatorname{GW}(k)$ Suppose X/k is a smooth, proper scheme of dimension d, and $V \to X$ is a rank d vector bundle relatively oriented by (L, φ), equipped w/ a section $f : X \to V$ s.t.

- $\{f = 0\}$ consists of multiplicity 1 zeros; or equivalently,
- for all x s.t. $f(x) = 0$, the induced[11] $Tf : T_xX \to T_{f(x)}V \cong T_xX \oplus V_x \to V_x$ has nonvanishing determinant.

Then,

Definition 1.7.16. The **Euler number** of (V, φ) w.r.t. f is

$$n(V, \varphi, f) = \sum_{x : f(x) = 0} \deg_x f$$

where $\deg_x f$ can be computed by

- choosing Nisnevich-local coordinates on X and a local trivialization of V which are compatible w/ φ – so $f : \mathbb{A}^d \to \mathbb{A}^d$ w/ $Jf = \det\left(\frac{\partial f_i}{\partial x_j}\right)$ and $Jf(x) \neq 0 \in \kappa(x)$ – and then setting $\deg_x(f) = \operatorname{Tr}_{\kappa(x)/k} \langle Jf(x) \rangle$.
- Equivalently, $T_x f \in \operatorname{Hom}(T_xX, V_x)$ and $Jf(x) = \det T_x f \in \operatorname{Hom}(\det T_xX, \det V_x)$. The orientation gives an isomorphism
$$Jf(x) \in \operatorname{Hom}(\det T_xX, \det V_x) \cong L_x^{\otimes 2}$$
and so induces a well-defined element $Jf(x)$ of $\kappa^\times(x)/(\kappa^\times(x))^2$ by choosing a trivialization of L_x.

[11] $f(x) = (x, 0)$ in local coordinates

1.7.4 Questions for next time

Question 1.7.17. *What happens if the zeros of f are not multiplicity 1?*

Answer. Next time

Question 1.7.18. *Why is the Euler number $n(V,f)$ independent of the section f?*

Answer. sections w/ isolated zeros can often be connected by families of such sections parameterized by $\mathbb{A}^1$, leading to an element of $\mathrm{GW}(k[x]) \cong \mathrm{GW}(k)$. This is kind of a pain to carry out.

Answer. Alternatively, Euler number is pushforward of an Euler class (in a nice cohomology theory) $n(V,f) = \pi_* e(V,f)$.

1.8 Wickelgren Lecture 2 (7/16)

Last time we were discussing an enrichment of degree.

Recall 1.8.1 (Topological degree)**.** We have $\deg : [S^n, S^n] \to \mathbb{Z}$ which can be computed as a sum of local degrees. In particular, for $f : S^n \to S^n$ and $p \in S^n$ s.t. $f^{-1}(p) = \{q_1, \dots, q_N\}$, we have $\deg f = \sum_{i=1}^N \deg_{q_i} f$. To compute these local degrees, one can choose local coordinates $(x_1, \dots, x_n)$ near q_i and $(y_1, \dots, y_n)$ near p (compatible w/ orientation), so $f = (f_1, \dots, f_n) : \mathbb{R}^n \to \mathbb{R}^n$ becomes a tuple of functions. We consider the Jacobian $J = \det\left(\frac{\partial f_i}{\partial x_j}\right)$, and then have $\deg_{q_i} f = \operatorname{sign} J(q_i)$.

Question 1.8.2. *What if the zeros of f are not multiplicity 1, so $J(q_i) = 0$?*

Theorem 1.8.3 (Eisenbud-Harold Levin/Khimshiaskuili (?) Signature formula)**.** *$\deg_x f$ is the signature of the $\mathbb{R}$-bilinear form ω^{EKL}. This ω^{EKL} is the (isomorphism class of the) following bilinear form ($k = \mathbb{R}$): first let*

$$Q = \frac{k[x_1, \dots, x_n]_x}{\langle f_1, \dots, f_n \rangle}$$

(finite dimensional local complete intersection since x an isolated zero). This Q is Gorenstein[12]*, so* $\mathrm{Hom}_k(Q,k) \cong Q$*. Even better: there is a distinguished isomorphism coming from distinguished socle element (see e.g. Scheja-Storch) and this iso gives a particular bilinear form.*

Explicitly, $Jf = \det\left(\frac{\partial f_i}{\partial x_j}\right) \in Q$. Choose k-linear $\eta : Q \to k$ s.t. $\eta(Jf) = \dim_k Q$. Then,

$$\begin{array}{rccc} \omega_{EKL} : & Q \times Q & \longrightarrow & k \\ & (g,h) & \longmapsto & \eta(gh) \end{array}$$

(iso class independent of choice of η).

Example. Say $f : \mathbb{A}^1 \to \mathbb{A}^1$, $z \mapsto z^2$ and take $q = 0$. Then, $Q = k[x]_0/x^2 = k[x]/x^2$ with jacobian $J = 2x$. In this case,

$$\omega^{EKL} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

(the top left element, $\omega^{EKL}(1,1)$ could be something else if we wanted). Hence, $\omega^{EKL} = \langle 1 \rangle + \langle -1 \rangle = h$ is the hyperbolic plane.

[12] dualizing sheaf locally free

Eisenbud: ω^{EKL} is defined over arbitrary field k of char $\neq 2$ and acts as a "degree." Does ω^{EKL} have a topological interpretation?

Theorem 1.8.4 (Kass-W.)**.** *$\omega^{EKL} = \deg_q^{\mathbb{A}^1} f \in \mathrm{GW}(k)$ when $\kappa(q) = k$ (i.e. q a rational point).*

Theorem 1.8.5 (Brazelton-Burkland-Mckean-Montaro-Opie)**.** *Above when $\kappa(q)/k$ separable.*

1.8.1 Detour on $\mathbb{A}^1$-Milnor numbers

Say char $k \neq 2$. The simplest sort of singularity is a **node**, defined over $\overline{k}$ to be a point $p \in X$ such that

$$\widehat{\mathscr{O}}_{X,p} \cong \frac{\overline{k}\,[\![x_1,\dots,x_n]\!]}{(x_1^2 + \cdots + x_n^2 + (\text{higher order terms}))}.$$

Say we have a hypersurface singularity $p \in \{f = 0\} =: X$. If you vary X in a family:

$$X_t = \{f(x_1,\dots,x_n) + a_1x_1 + \cdots + a_nx_n = t\},$$

then p bifurcates into nodes.

When $k = \mathbb{C}$, the "Milnor number" μ_p is the #nodes in family X_t for any sufficiently small $(a_1,\dots,a_n)$. Milnor shows this is the same as the topological degree at p of the gradient of f.

Over k? Notes come in different types depending on field of definition of p (and of the tangent directions).

Example ($\mathbb{R}$-nodes over $\mathbb{R}$)**.** Can have $x_1^2 + x_2^2 = 0$ which is a non-split node (non-rational tangent directions). Can also have $x_1^2 - x_2^2 = 0$ which is a split node (rational tangent directions).

Definition 1.8.6. The **type** of a node p with

$$\widehat{\mathscr{O}}_{X,p} \cong \frac{L\,[\![x_1,\dots,x_n]\!]}{\sum a_i x_i^2}$$

is defined to be the local degree of the gradient:

$$\mathrm{type}(p) := \mathrm{Tr}_{L/k}\left\langle 2^n \prod_{i=1}^{n} a_i \right\rangle \in \mathrm{GW}(k).$$

Definition 1.8.7. **$\mathbb{A}^1$-Milnor number**

$$\mu_p := \deg_p^{\mathbb{A}^1} \nabla f = \sum_{\substack{\text{nodes } p \text{ in family} \\ \text{for generic } (a_1,\dots,a_n)}} \mathrm{type}(p)$$

This has been looked at by e.g. Kass-W. and Sabrina-W.

Example. $f(x,y) = x^3 - y^2$ over char $k \neq 2,3$. Say $p = (0,0) \in \{f = 0\}$. Then, $\nabla f = (3x^2, -2y)$. This is secretly a smash product of maps, so

$$\deg^{\mathbb{A}^1} \nabla f = \deg^{\mathbb{A}^1}(x \mapsto 3x^2)\deg(y \mapsto -2y) = (\langle 1\rangle + \langle -1\rangle)\cdot\langle -2\rangle = \langle 1\rangle + \langle -1\rangle$$

is our $\mathbb{A}^1$-Milnor number.

Consider the family $y^2 = x^3 + ax + t$. When $a = 0$, have cusp at $t = 0$ and smooth otherwise. When $a \neq 0$, singular fibers when $-4a^3 - 27t^2 = 0$ (nodes at these values) and smooth otherwise. Hence, we've bifurcated the cusp into 2 nodes. Thus, we see in this example that the classical Milnor number is the rank of the $\mathbb{A}^1$-Milnor number.

We have more information though. Over $\mathbb{F}_5$, $\langle 1\rangle = \langle -1\rangle$, so can't bifurcate into 1 split and 1 non-split rational node. Over $\mathbb{F}_7$, $\langle 1\rangle \neq \langle -1\rangle$, so can't bifurcate into 2 split and 2 non-split rational nodes.

The classical Milnor number appears in conductor formulas and is related to χ (Euler characteristic) of Milnor fiber. Mark Levine0Lehallew-Srinivas and R. Azouri have subtle results on GW(k)0enrichments.

1.8.2 $\mathbb{A}^1$-Euler characteristic $\chi^{\mathbb{A}^1}$

Let X be a smooth projective k-variety.

Recall 1.8.8. A vector bundle $V \to X$ is relatively oriented by (L, φ) where $L \to X$ is a line bundle, and

$$L^{\otimes 2} \cong \operatorname{Hom}(\det TX, \det V).$$

Example. TX has a canonical relative orientation since

$$\operatorname{Hom}(\det TX, \det TX) \simeq \mathscr{O} \simeq \mathscr{O}^{\otimes 2}$$

It follows that we may define

$$\chi^{\mathbb{A}^1}(X) := n(TX) \in \mathrm{GW}(k)$$

(with $n(-)$ denoting Euler number from last time).

Theorem 1.8.9 (M. Levine)**.** *$\chi^{\mathbb{A}^1}(X)$ above is also the categorical Euler characteristic.*

Example (M. Levine-Raksit)**.** Say smooth $X \subset \mathbb{P}^{n+1}$ with n even defined by $X = \{f = 0\}$ for $f \in k[x_0, \dots, x_n]_e$ (homogeneous of degree e). Define B_{Jac} to be the restriction of

$$Q \times Q \xrightarrow{\omega^{EKL}} k \text{ where } Q = \frac{k[x_0, \dots, x_n]}{\left\langle \frac{\partial f}{\partial x_0}, \dots, \frac{\partial f}{\partial x_n} \right\rangle}$$

to $\bigoplus_{q=0}^n Q_{(q+1)e-n-2}$. Then,

$$\chi^{\mathbb{A}^1}(X) = \langle e\rangle + \langle -e\rangle\, B_{\mathrm{Jac}} + \frac{n}{2}h.$$

Example. Say

$$C = \left\{[x_0, x_1, x_2, x_3] : \sum x_i^2 = (\sum x_i)^3\right\} \subset \mathbb{P}^3$$

is the Clebsch cubic surface. This has $\chi(C) = 9$. One can compute (via computer) that

$$\chi^{\mathbb{A}^1}(C) = 2h + \langle -10\rangle + \langle -6\rangle + \langle -21\rangle + \langle -14\rangle + \langle -2\rangle$$

1.8.3 Cohomology

Recall that $SH(k)$ is our stable $\mathbb{A}^1$-homotopy category. This produces cohomology theories H on smooth k-schemes X.

Example. $H\mathbb{Z}$ motivic cohomology
$\widehat{H\mathbb{Z}}$ extended motivic cohomology
K K-theory
KO Hermitian K-theory

Given a cohomology theory (spectrum) H, we get cohomology groups

$$\mathrm{H}^n(X) = \pi_{-n}\operatorname{Hom}(X, H) = [X, \Sigma^n H].$$

Let $V \to X$ be a vector bundle. We also define

$$\mathrm{H}^V(X) := [X, \mathrm{Th}(V) \wedge H] \;\text{ where }\; \mathrm{Th}(V) = V^*/(V^* - 0) = \mathbb{P}(V^* \oplus \mathscr{O})/\mathbb{P}(V^*).$$

When $V = \mathscr{O}_X^{\oplus n}$ is the trivial rank n vector bundle on X, then $\mathrm{H}^V = \mathrm{H}^n$.

Example. $H\mathbb{Z}^n(X) \cong \mathrm{H}^{2n}_{mot}(X, \mathbb{Z}(n)) \cong \mathrm{H}^{2n,n}_{mot}(X) \cong CH^n(X)$ is the Chow group of codim n cycles, modulo rational equivalence.

Example. $\widehat{H\mathbb{Z}}^n(X) \cong \widetilde{CH}^n(X)$ are the "Chow-Witt groups" also called the "oriented Chow groups." This are formal sums of codim n subvarieties Z w/ coefficients in $\mathrm{GW}(\kappa(Z))$ subject to conditions modulo equivalence.

Example. $K^0(X)$ is the group completion of vector bundles on X. $KO^0(X)$ is the group completion of vector bundles on X equipped w/ a symmetric non-degenerate form.

These are representable (expressed as hom into something). For such theories, we also get cohomology w/ supports. For a $Z \overset{\text{closed}}{\subset} X$, we define

$$\mathrm{H}^V_Z(X) := \left[\frac{X}{X - Z}, \mathrm{Th}(V) \wedge H\right].$$

1.8.4 Euler class

Let H be a cohomology theory, and say it's a ring $\mathbb{S} \to S$. Let $V \to X$ be a vector bundle with a section $f : X \to V$ (e.g. $f = 0$). We can then define an Euler class

$$e^H(V, f) \in \mathrm{H}^{V^*}_{\{f=0\}}(X)$$

is the class of the map

$$X/(X - \{f = 0\}) \xrightarrow{f} V/(V - 0) \wedge H$$

To define the Euler number, we want to take a pushforward.

Definition 1.8.10. Say $f : X \to S$ is **lci** if it locally factors as

$$U \overset{\text{closed}}{\hookrightarrow} P \xrightarrow{p \text{ smooth}} S$$

w/ closed immersion determined by a Koszul regular sequence.[13]

[13] regular sequence + higher cohomology of Koszul complex is 0

Properties:

- well-behaved cotangent complex L_f
- $L_i \simeq N^*_{U/P}[1]$ is the conormal bundle placed in degree 1
- $L_p \simeq \Omega_{P/S} \simeq T^*_p$
- L_{pi} determined by $i^* L_p \to L_{pi} \to L_i$

Also have a pushforward: let $p : X \to S$ be proper, lci. Get Becker-Göttlieb transfer $\Sigma^\infty_+ S \to \mathrm{Th}(L_p)$. This gives $p_* : \mathrm{H}^{L_p}(X) \to \mathrm{H}^0(S)$.

Oriented cohomology theories We say H is GL-**oriented** if $\mathrm{H}^n_Z(X) \cong \mathrm{H}^V_Z(X)$ when $n = \operatorname{rank} V$.

Example. $H\mathbb{Z}, K$ are oriented.

Non-example. $\widetilde{H\mathbb{Z}}, KO$ are not oriented.

Weaker, H is SL-**oriented** if $\mathrm{H}^V_Z(X) \cong \mathrm{H}^{V'}_Z(X)$ if $\operatorname{rank} V = \operatorname{rank} V'$ and $\det V \simeq \det V'$. It turns out these give an 'SL$_c$-orientation' which only requires $\det V \cong \det V' \otimes L^{\otimes 2}$ for some line bundle $L \to X$.

Example. $\widehat{H\mathbb{Z}}, KO$ are SL-oriented.

Thus, for a relatively oriented vector bundle $V \to X$ on smooth proper $p : X \to R$, and H and ($\mathrm{SL} = \mathrm{SL}_c$)-oriented cohomology theory, we indeed have $\mathrm{H}^{V^*}(X) \cong \mathrm{H}^{T^*X}(X)$.

Let f be any section of V (e.g. $f = 0$). Then we get

$$\begin{tikzcd}
\mathrm{H}^{V^*}_{\{f=0\}}(X) \arrow[r, "\iota", "\text{forget support}"'] & \mathrm{H}^{V^*}(X) \arrow[r, "\sim"] & \mathrm{Hom}^{L_p}(X) \arrow[r, "p_*"] & \mathrm{H}^0(S) \\
\rotatebox{90}{$\in$} & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\
e^H(V,f) \arrow[r, mapsto] & e^H(V) \arrow[rr, mapsto] & & n^H(V)
\end{tikzcd}$$

Any two sections f_1, f_2 of V are connected by families of $\mathbb{A}^1$'s in $\mathrm{H}^0(V)$, so $\iota(e^H(V, f_1)) = \iota(e^H(V, f_2))$.

Definition 1.8.11. The **Euler number** $n^H(V)$ of V in $\mathrm{H}^0(S)$ is $n^H(V) = p_* e^H(V)$.

This agrees with the earlier definition $n(V, f) = \sum_{x: f(x)=0} \deg_x f$ (with $\deg_x f \in \mathrm{GW}(k)$) for $H = \widetilde{H\mathbb{Z}}, KO$ over $S = \operatorname{spec} k$. As a consequence, we see Independence from section.

1.8.5 An Arithmetic count of the lines on a smooth cubic surface

(joint w/ Jesse Kass)

Say $X \subset \mathbb{P}^3$ is a cubic surface $X = \{f = 0\}$ (i.e. $f \in k[w, x, y, z]_3$).

Theorem 1.8.12 (Salmon-Cayley 1849). *Any smooth cubic surface over $\mathbb{C}$ has exactly 27 lines.*

Example (Fermat Cubic surface). Take $f(x, y, z, w) = x^3 + y^3 + z^3 + w^3$. For $\omega^3 = \lambda^3 = 1$, we get the lines

$$\left\{[S, -S, T, -T] : [S, T] \in \mathbb{P}^1(\mathbb{C})\right\}.$$

We can permute the variables $\binom{4}{2}/2 = 3$ ways. Hence, we find $3 \times 3 \times 3 = 27$ lines.

Proof. Let $\mathrm{Gr}(1,3)$ be the Grassmiann of $\mathbb{P}^1$'s in $\mathbb{P}^3$. Let $S \to \mathrm{Gr}(1,3)$ be the Tautological bundle, so $S_{[\mathbb{P}W]} = W$ ($W \subset \mathbb{C}^4$ 2-dimensional). Note that

$$\left(\mathrm{Sym}^3 S^*\right)_{[\mathbb{P}W]} = \mathrm{Sym}^3 W^* = \{\text{cubic polys on } W\}.$$

We see that f determines a section σ_f on $V := \mathrm{Sym}^3 S^*$ given by $\sigma_f([\mathbb{P}W]) = f|_W$. Note that

$$\sigma_f([\mathbb{P}W]) = 0 \iff \mathbb{P}W \subset X.$$

Thus, we only need to count the number of zeros of a section. This is just the Euler number

$$n(V) = \sum_{\text{lines } L \text{ in } X} \deg_L \sigma_f.$$

Fact. For a smooth cubic surface, all zeros of σ_f have multiplicity 1.

Since we're over $\mathbb{C}$, it follows that $\deg_L \sigma_f = 1$. Hence $n(V) = \#$ lines. We can compute $n(V) = 27$ either by understanding cohomology of Grassmannians or by looking at the specific example of the Fermat cubic. ■

What about cubic surfaces over $\mathbb{R}$?

- (Schlafli 1863) There can be 3, 7, 15, or 27 lines
- (Segre 1942) distinguished b/w hyperbolic and elliptic lines. Say $L \subset X$ is a real line.

  L gives an involution $I : L \to L$. Note that T_pX contains L, so $T_pX \cap X = L \cup C$ w/ C of degree 2 (total degree 3). Hence, we may define $I(p)$ via $L \cap C = \{p, q\}$. That is, $q = I(p)$ is other point with $T_pX = T_qX$. The involution swaps them. Since I is an involution, it has two fixed points. If they're a $\mathbb{C}$-conjugate pair, we call the line elliptic. If they are two $\mathbb{R}$-points, the line is hyperbolic.

Theorem 1.8.13 (Segre + (Okonek-Teleman '14), (Finashin-Kharlamov '12), (Benedetti-Silhol '94), (Horev-Soloman '12))**.** *#hyperbolic lines - #elliptic lines = 3*

Question 1.8.14. *What about over other fields?*

Answer. The above proof goes through in $\mathbb{A}^1$-homotopy theory.

Say lines $L \subset X \subset \mathbb{P}^3$ (X a smooth cubic surface). The *type* of L is defined to by $\langle D \rangle \in \mathrm{GW}(\kappa(L))$ where $D \in \kappa(L)^\times/(\kappa(L)^\times)^2$ is s.t. the fixed points of I are a conjugate pair of points defined over $\kappa(L)[\sqrt{D}]$.

Theorem 1.8.15 (Kass-W.)**.** *Let k be a field of characteristic not* 2. *Let X be a smooth cubic surface in $\mathbb{P}^3_k$. Then,*

$$\sum_{\textit{lines } L \subset X} \mathrm{Tr}_{\kappa(L)/k}\, \mathrm{type}(D) = 15\langle 1 \rangle + 12 \langle -1 \rangle \in \mathrm{GW}(k).$$

1.9 Matthew Morrow Lecture 1 (7/15): Aspects of Motivic Cohomology

By this point in the week, we have already seen some of the following relevant to this talk

- Motivic complexes

- Milnor K-theory
- Relation to étale cohomology (e.g. Bloch-Kato)
- $\mathbb{A}^1$-homotopy theory, categorical aspects
- Mostly for (smooth) varieties over fields

Our goals:

- Motivic cohomology, as a tool to analyse algebraic K-theory
- Progress in mixed characteristic

1.9.1 K_0 and K_1

Here are some phenomena to keep in mind

- K-theory encodes other invariants
- It also breaks into (simpler?) pieces. These will be motivic in nature.

Definition 1.9.1 (Grothendieck 50's)**.** Let R be a ring. Then, $K_0(R)$ is the following abelian group: it is generated by symbols $[P]$ for $P \in \{\text{finite projective } R\text{-modules}\}/\simeq$. The only relation we impose is that $[P] = [P'] + [P'']$ if there exists a short exact sequence $0 \to P' \to P \to P'' \to 0$.

One can give the same definition of K_0 for any scheme by replacing "finite projective module" with "vector bundle."

Example. Say F is a field. Then, finite projective modules are vector spaces, so we have $\dim_F : K_0(F) \xrightarrow{\sim} \mathbb{Z}$.

Example. Say $\mathscr{O}$ is a Dedekind domain. Then, any ideal $I \subset \mathscr{O}$ is a finite projective module, so we get a class $[I] \in K_0(\mathscr{O})$. It turns out there is a (split) short exact sequence

$$0 \longrightarrow \mathrm{Cl}(\mathscr{O}) \xrightarrow{I \mapsto [I]-[\mathscr{O}]} K_0(\mathscr{O}) \xrightarrow{\text{rank}} \mathbb{Z} \longrightarrow 0$$

(recall this fact from an earlier talk that all project modules are of the form $\mathscr{O}^n \oplus I$). Hence, $K_0(\mathscr{O})$ breaks up into a copy of the class group and a copy of $\mathbb{Z}$.

Apparently this characterizes regular rings in dimension ≤ 1

Example. Say X a smooth algebraic k-variety (probably need X quasi-projective or something). For $Z \hookrightarrow X$ an irreducible closed subvariety, pick a resolution

$$0 \leftarrow \mathscr{O}_Z \leftarrow P_0 \leftarrow \ldots \leftarrow P_d \leftarrow 0$$

by vector bundles P_i.[14] We then define

$$[Z] := \sum_{i=0}^{d} (-1)^i [P_i] \in K_0(X),$$

[14] If X quasi-projective, can (probably) take this to be $P_i = \mathscr{O}_X(n_i)$

and can can check that this class is well-defined. Inspired by this, we associate a filtration on $K_0(X)$:

$$\mathrm{Fil}_j K_0(X) := \langle [Z] : Z \hookrightarrow X \text{ irred. closed of dimension } \leq j \rangle .$$

Hence, $K_0(X) \supset \mathrm{Fil}_d K_0(X) \supset \cdots \supset \mathrm{Fil}_0 K_0(X) \supset 0$.

Theorem 1.9.2 (Part of Riemann-Roch)**.** *Let $CH_j(X)$ be the Chow group of j-dimensional cycles modulo rational equivalence. Then, there is a well-defined map*

$$CH_j(X) := \frac{j\text{-dim cycles}}{\text{rational equiv}} \longrightarrow \frac{\mathrm{Fil}_j K_0(X)}{\mathrm{Fil}_{j-1} K_0(X)}$$

sending $Z \mapsto [Z]$. This is surjective (by definition) with kernel killed by $(d-j-1)!$.

Slogan. Up to small torsion, $K_0(X)$ breaks into Chow groups.

That was K_0, what about K_1? The idea here is to classify isomorphisms between finite projective modules, up to trivial isomorphisms.

Definition 1.9.3 (Bass 50s)**.** First let $\mathrm{GL}(R) := \bigcup_{n \geq 1} \mathrm{GL}_n(R)$ with $\mathrm{GL}_n \hookrightarrow \mathrm{GL}_{n+1}$ via $g \mapsto g \oplus 1$. Similarly, $E(R) := \bigcup_{n \geq 1} E_n(R)$ where $E_n(R) \subset \mathrm{GL}_n(R)$ is the subgroup of "elementary matrices," those obtained by applying elementary row and column operations to I_n (this gives a normal subgroup in the limit). We set

$$K_1(R) := \mathrm{GL}(R)/E(R).$$

Example. There is a determinant map $\det : K_1(R) \to R^\times$ sending $g \mapsto \det(g)$. This has a right inverse sending $r \in R^\times$ to $\mathrm{diag}(r, 1, 1, 1, \dots)$.

Example. Say F is a field. Then, $E_n(F) = \mathrm{SL}_n(F)$ by Gaussian elimination. Hence, the determinant map $\det : K_1(F) \xrightarrow{\sim} F^\times$ is an iso.

In particular, for m prime to $\mathrm{char}\, F$, we can identify

$$K_1(F)/m \cong F^\times/m \cong \mathrm{H}^1(F, \mu_m)$$

w/ second iso coming from Kummer theory. This is a baby case of Bloch-Kato.

Example. Let $\mathscr{O}$ be the ring of integers in a number field. Then again $\det : K_1(\mathscr{O}) \xrightarrow{\sim} \mathscr{O}^\times$ is again an iso, but now this is a deep theorem (originally due to Bass-Milnor-Serre w/ second proof due to Kazhdan).

Example. When $\mathcal{D} = \mathbb{R}[x,y]/(x^2+y^2-1)$, a Dedekind domain, one can produce a nonzero class in $\ker \det$. Specifically, $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ is such a nonzero class, so previous example fails for arbitrary Dedekind domains. In this case $K_1(\mathcal{D}) \cong \mathcal{D}^\times \oplus$ ("info about loops"). This element we wrote down corresponds to going once around the circle.

1.9.2 Higher algebraic K-theory

By the 60s, it had become clear that K_0, K_1 should just be the beginning of some cohomology theory $K_n(R)$ for $n \geq 0$. The question remained: how do we define these?

Definition 1.9.4 (Quillen '73)**.** Quillen gave multiple definitions of a K-theory spectrum $K(R)$, for example by "deriving $K_1(-)$": $K(R) = (B\mathrm{GL}(R))^+ \times K_0(R)$ (note $\mathrm{GL}(R)$ and $K_0(R)$ discrete); this +-construction forces π_* to be abelian w/o modifying the homology. One can then set $K_n(R) := \pi_n K(R)$.

Other, more modern, points of view are closer in spirit in K_0:

- $K(R) := \infty$-group completion of the $\mathbb{E}_\infty$-space $\mathrm{Proj}(R)^{\simeq}$
- $K(-)$ is the universal invariant of stable ∞-categories taking exact sequences to cofiber sequences of spectra. From this perspective, $K(R) := K(\text{perfect complexes of } R\text{-modules})$.

In any case, output is these mysterious K-groups $K_n(R)$ for $n \geq 0$.

Example (Quillen '73)**.**

$$K_n(\mathbb{F}_q) \cong \begin{cases} \mathbb{Z} & \text{if } n = 0 \\ 0 & \text{if } n > 0 \text{ even} \\ \dfrac{\mathbb{Z}}{\left(q^{\frac{n+1}{2}} - 1\right)\mathbb{Z}} & \text{if } n > 0 \text{ odd} \end{cases}$$

Example. $K_{4n}(\mathbb{Z}) = 0$ for all $n > 0 \iff$ Vandiver conjecture holds.

Example. Say R a regular, finite type $\mathbb{Z}$-algebra. Then, $K_n(R)$ should be finitely generated abelian group for all n. This is wide open (but known if $\dim R \leq 1$).

Example. Say F is a field of characteristic prime to $m \geq 1$. Then,

$$K_2(F)/m \cong \mathrm{H}^2(F, \mu_m^{\otimes 2})$$

(Merkurjev (?)-Suslein (?) theorem, now a special case of Bloch-Kato)

Example (Lichtenbaum, Quillen 70s)**.** Partly motivated by zeta functions, for a number field F and any $m \geq 1$, they conjectured formulae for $K_n(F; \mathbb{Z}/m\mathbb{Z})$ in terms of étale cohomology.

Note that this K-theory w/ coefficients fits into short exact sequences

$$0 \to K_n(F)/m \to K_n(F; \mathbb{Z}/m\mathbb{Z}) \to K_{n-1}(F)[m] \to 0.$$

1.9.3 Arrival of Motivic Cohomology

Question 1.9.5. *In what generality do the above phenomena hold?*

Example. Always true in topology. Given a topological space X, can define $K_0^{top}(X)$ in terms of complex vector bundles. Suspension/Bott periodicity gives $K_n^{top}(X)$ for all $n \in \mathbb{Z}$.

Theorem 1.9.6 (Atiyah-Hirzebruch)**.** *There is a spectral sequence*

$$E_2^{ij} = \mathrm{H}^{i-j}(X; \mathbb{Z}) \implies K_{-i-j}^{top}(X).$$

It degenerated rationally, i.e. 'topological K-theory breaks into singular cohomology'.

Motivated by all these phenomena in the 80s, Beillinson (?) and Lichtenbauc proposed

Conjecture 1.9.7 (Existence of motivic cohomology)**.** *For any smooth variety X over a field, there should exist complexes $\mathbb{Z}_{mot}(j)(X)$ for $j \geq 0$, called* ***weight j motivic cohomology of X*** *such that*

(1) *Analogue of Atiyah-Hirzebruch spectral sequence:*

$$E_2^{ij} = \mathrm{H}^{i-j}_{mot}(X, \mathbb{Z}(-j)) \implies K_{-i-j}(X)$$

degenerating rationally.

(2) *Low weights: $\mathbb{Z}_{mot}(0)(X) = \mathbb{Z}^{\pi_0(X)}[0]$ just counts number of connected components. In weight 1,*

$$\mathbb{Z}_{mot}(1)(X) = R\Gamma_{Zar}(X, \mathscr{O}_X^\times)[-1].$$

Note that the weight 0 complex is supported in degree 0 and the weight 1 complex is supported in degrees $1, 2$.

(3) *Range of support: $\mathbb{Z}_{mot}(j)(X)$ is supported in degrees $0, 1, \ldots, 2j$ (even in degrees $\leq j$ if $X =$ spec(local ring)).*

(4) *Relation to algebraic cycles: $\mathrm{H}^{2j}_{mot}(X, \mathbb{Z}(j)) = CH^j(X)$*

(5) *Relation to étale cohomology (**Beilinson-Lichtenbaum conjecture**):*

$$\mathrm{H}^i_{mot}(X, \mathbb{Z}/m\mathbb{Z}(j)) \cong \mathrm{H}^i_{\acute{e}t}(X, \mu_m^{\otimes j})$$

is m is prime to char of base field, and $i \leq j$.

Example. Let's compute K-groups of number fields F, as predicted by Lichtenbaum-Quillen, at least modulo m for m odd.

The mod m AHSS is very simple:

$$\begin{array}{ccccc}
0 & 0 & 0 & \mathrm{H}^0(F, \mathbb{Z}/m\mathbb{Z}) & \\
0 & 0 & \mathrm{H}^0(F, \mu_m) & \mathrm{H}^1(F, \mu_m) & \mathrm{H}^2(F, \mu_m) \\
 & \mathrm{H}^0(F, \mu_m^{\otimes 2}) & \mathrm{H}^1(F, \mu_m^2) & \mathrm{H}^2(F, \mu_m^2) & 0 \\
 & & \mathrm{H}^2(F, \mu_m^3) & 0 &
\end{array}$$

Assuming I copied things done correctly, this should give $K_{2j-1}(F, \mathbb{Z}/m\mathbb{Z}) \cong \mathrm{H}^1(F, \mu_m^{\otimes j})$ and give an exact sequence

$$0 \to \mathrm{H}^2(F, \mu_m^{\otimes(j+1)}) \to K_{2j}(F; \mathbb{Z}/m\mathbb{Z}) \to \mathrm{H}^0(F, \mu_m^{\otimes j}) \to 0.$$

Theorem 1.9.8 (Bloch,Levine,Friedlander,Rost,Suslin,Voevodsky,...)**.** *The above conjectures are true (except for "Beilinson-Soulé vanishing," that $\mathbb{Z}_{mot}(j)(X)$ is supported in nonnegative degree).*

Let's write down the original definition of $\mathbb{Z}_{mot}(j)(X)$, due to Bloch.

Definition 1.9.9. For a variety X over a field F, let

$Z^j(X, n) :=$ free abelian group on codim j irred closed subschemes of $X \times_F \Delta^n$ intersecting all faces properly

Question: Does $\mathrm{H}^j(X, \mathscr{O}_X^\times) = 0$ for $j \geq 2$?

Answer: (Stolen from chat since someone else asked this) well, on a regular scheme, you have a flasque resolution of $\mathbb{G}_m$ by the constant sheaf on the units in the function field and then the divisor map to the sum of the integers supported at codim 1 points. I'm not sure about a simple proof in the normal case

m odd so cohomological

Above, Δ^n is the **algebraic n-simplex**

$$\Delta^n := \text{spec}\left(\frac{k[T_0, \ldots, T_n]}{(\sum_{i=0}^{n} T_i - 1)}\right) \cong \mathbb{A}^n_F.$$

Inside of here are various "faces" Δ^m for $m < n$; the 'faces' mentioned above are $X \times_F \Delta^m$ for $m < n$. Furthermore, 'intersecting properly' means doing so in the expected codimension.

Bloch's complex of higher cycles is

$$Z^j(X, \bullet) = \left[\cdots \to Z^j(X, 2) \to Z^j(X, 1) \to Z^j(X, 0)\right]$$

with boundary maps given by alternating sums of intersections:

$$Z^j(X, n) \ni Z \mapsto \sum_{i=0}^{n} (-1)^i \left[Z \cap (i\text{th face of } X \times \Delta^{n-1})\right].$$

Bloch's higher Chow groups are the cohomology of this complex

$$CH^j(X, n) := \mathrm{H}_n(Z^j(X, \bullet)).$$

Part of the previous theorem on the existence of Motivic cohomology includes the fact that

$$\mathbb{Z}_{mot}(j)(X) = Z^j(X, \bullet)[-2j].$$

To prove the desired properties, one does not directly use this definition. They use machinery closer to what was in Déglise's talk, and then independently show that machinery recovers these higher Chow groups.

1.9.4 Milnor K-theory and Bloch-Kato

How is motivic cohomology related to the Bloch-Kato conjecture?

Recall 1.9.10 (Krashen's (first) talk)**.** Let F be a field. We have these Milnor K-groups

$$K_j^M(F) = \frac{F^\times \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} F^\times}{\text{Steinberg relation}}.$$

For $m \geq 1$ prime to $\operatorname{char} F$, have the Tate (Galois) cohomological symbol

$$K_j^M(F)/m \to \mathrm{H}^j(F, \mu_m^{\otimes j}).$$

The Bloch-Kato conjecture (theorem of Rost and Voevodsky) says this is an isomorphism.

This is related to motivic cohomology thanks to

Theorem 1.9.11 (Nosterenko-Suslin, Totaro)**.** *For any field F, there is a natural isomorphism*

$$K_j^M(F) \cong \mathrm{H}^j_{mot}(F, \mathbb{Z}(j))$$

for each $j \geq 1$.

Definition of this map might appear in the exercises.

Looking mod m, we see that

$$K_j^M(F)/m \cong \mathrm{H}^j_{mot}(F, \mathbb{Z}/m\mathbb{Z}(j)) \cong \mathrm{H}^j_{\text{ét}}(F, \mu_m^{\otimes j})$$

(w/ latter iso the Beilinson-Lichtenbaum conjecture).

Thus, Beilinson-Lichtenbaum $\implies$ Bloch-Kato, but the converse is basically also true.

1.10 Morrow Lecture 2 (7/16)

1.10.1 Yesterday

(i) K-theory of a smooth variety X can be refined by motivic cohomology, i.e. have Atiyah-Hirzebruch spectral sequence (even better: $K(X)$ has "motivic" filtration w/ graded pices $\mathbb{Z}_{mot}(j)$)

(ii) $\mathbb{Z}_{mot}(j)(X)$ is related to algebraic cycles and to étale cohomology mod m (for m prime to characteristic)

What about today?

- Classical mod p theory when $p =$ char of base field
- Variations on theme: replace K-theory by other similar invariants, weaken hypotheses on X
- Recent progress: the case of étale K-theory, especially p-adically

1.10.2 Mod p Motivic cohomology in char p

Recall 1.10.1. Say F a field and $m \in \mathbb{Z}$ prime to char F, then the mod m AHSS looks like

$$E_2^{ij} = \mathrm{H}^{i-j}_{mot}(F, \mathbb{Z}/m\mathbb{Z}(-j)) = \begin{cases} \mathrm{H}^{i-j}_{Gal}(F, \mu_m^{\otimes(-j)}) & \text{if } i \leq 0 \\ 0 & \text{otherwise.} \end{cases} \implies K_{-i-j}(F; \mathbb{Z}/m\mathbb{Z})$$

(so the sequence takes place in like half of the third quadrant (between 225 and 270 degrees))

Note that the j-axis is $\mathrm{H}^j(F, \mu_m^{\otimes j}) \cong K_j^M(F)/m$.

What if $m = p = \operatorname{char} F > 0$?

Theorem 1.10.2 (Izhboldin '90, Bloch-Kato-Gabber '86, Geisser-Levine 2000)**.** *Let F be a field of characteristic p. Then,*

(i) *$K_j^M(F)$ and $K_j(F)$ are p-torsion free*

(ii) *We have*

$$K_j(F)/p \xleftarrow{\sim} K_j^M(F)/p \xhookrightarrow{\mathrm{d}\log} \Omega^j_F$$

Question: $\Omega_F = \Omega_{F/\mathbb{Z}}$?

The image of

$$\begin{array}{rccc} \mathrm{d}\log: & K_j^M(F)/p & \longrightarrow & \Omega_F^j \\ & a_1 \otimes \cdots \otimes a_j & \longmapsto & \dfrac{\mathrm{d}a_1}{a_1} \wedge \cdots \wedge \dfrac{\mathrm{d}a_j}{a_j} \end{array}$$

is denoted by $\Omega^j_{F,\log}$*. This is isomorphic to* $K_j^M(F)/p$*.*

Geisser-Levine really prove that

$$\mathbb{Z}_{mot}(j)(F)/p \simeq \Omega^j_{F,\log}[-j]$$

(in particular, it is concentrated in a single degree). So the mod p AHSS is just

$$E_2^{ij} = \begin{cases} \Omega^{-j}_{F,\log} & \text{if } i = 0 \\ 0 & \text{otherwise.} \end{cases} \implies K_{-i-j}(F;\mathbb{Z}/p\mathbb{Z})$$

whence $K_j(F)/p \cong \Omega^j_{F,\log}$ *as above.*

Remark 1.10.3. $K_j(F)/p \cong \Omega^j_{F,\log}$ remains true if we replace F by any regular Noetherian local $\mathbb{F}_p$-algebra.

Question 1.10.4. *The hard part of Geisser-Levine is to show that* $K_j^M(F) \to K_j(F)$ *is surjective mod* p*. Proof goes through* $Z^j(F,\cdot)+$ *AHSS. Is there a more direct proof? Or even, is there a direct proof that* $K_j(F)/p = 0$ *if* $j > \operatorname{trdeg}(F)$*?*

This is apparently a consequence of this stuff above

Conjecture 1.10.5. *A conjecture of Beilinson predicts that*

$$K_j^M(F) \to K_j(F)$$

is an isomorphism after $- \otimes_{\mathbb{Z}} \mathbb{Q}$*. Equivalently,* $\mathrm{H}^i_{Mot}(F,\mathbb{Z}(j))$ *is torsion unless* $i = j$*.*

This is wide open, but would follow from another conjecture

It's know if F is finite by Quillen's computation

Conjecture 1.10.6 (Parshin)**.** *Say* X *is smooth, projective over a finite field. Then,*

$$\mathrm{H}^i_{mot}(X,\mathbb{Z}(j))$$

is torsion unless $i = 2j$*.*

This is also wide open.

1.10.3 Variants on a theme

Question 1.10.7. *What can we "motivically refine" instead of K-theory?*

G-theory Bloch's complex $Z^j(X,\bullet)$ from last time (Definition 1.9.9 makes sense for any scheme. For X finite type over a field or a Dedekind domain, it is also something interesting to look at; specifically, its homology groups fit into an AHSS:

$$E_2^{ij} = CH^{-j}(X,-i-j) \implies G_{-i-j}(X).$$

Here, **G-theory** is K-theory, not of finite projective modules, but of coherent sheaves on X.

(See Levine)

The punchline: $Z^j(X,\bullet)$ defines **motivic Borel-Moore homology**, refining G-theory.

KH-theory This KH-theory is Weibel's '**homotopy invariant K-theory**'. This is obtained by taking K-theory and forcing it, in a universal fashion, to be homotopy invariant. That is, it is the universal modification KH of K such that

$$\mathrm{KH}(R[T]) \cong \mathrm{KH}(R) \text{ for all } R.$$

This is true for K-theory of *regular* rings, but not for K-theory of arbitrary rings.

Definition 1.10.8.

$$\mathrm{KH}(R) := \left| q \mapsto K\left(\frac{R[T_0,\ldots,T_q]}{1-\sum_{i=0}^{q} T_i}\right)\right|$$

(geometric realization of simplicial spectrum)

For reasonable schemes X, should exist a theory of $\mathbb{A}^1$-invariant motivic cohomology such that

- There's an AHSS converging to $\mathrm{KH}_{-i-j}(X)$
- Some B-L type properties
- Some relation to cycles

At least for X noetherian of finite Krull dimension, can get such an AHSS using representability of KH in the stable homotopy category + slice filtration.

Motivic Cohomology w/ modulus Say X is a smooth variety, and $D \hookrightarrow X$ is an effective Cartier divisor (not nec. reduced). The theory of motivic cohomology w/ modulus aims to construct certain cycle complexes $Z^j(X|D,\bullet)$ – complex of cycles in "good position" w.r.t. the boundary D.

Various people have worked on/are still working on this theory: Bloch-Esnault, Binda, Krishna, Saito, ... (Levine claimed to have made a "negative contributation")

Conjecture 1.10.9. *There exists an AHSS*

$$E_2^{ij} = CH^j(X|D,-i-j) \implies K_{-i-j}(X,D)$$

(relative K-groups on RHS)

(At least one expert in the audience does *not* believe this conjecture, at least in this generality)

The moral is that it aims to describe some motivic/cycle-theoretic description of relative K-theory.

Étale K-theory K-theory is quite simple étale locally, at least away from the residue characteristic:

Theorem 1.10.10 (Gabber, Suslin). *Let A be a strictly henselian local ring, and fix $m \geq 1$ prime to the characteristic of the residue field k. Then,*

$$K_n(A;\mathbb{Z}/m\mathbb{Z}) \cong K_n(k,\mathbb{Z}/m\mathbb{Z}) \cong \begin{cases} \mu_m(k)^{\otimes \ell} & \text{if } n = 2\ell \\ 0 & \text{if } n \text{ odd} \end{cases}$$

(Note k above separably closed. Gabber proved first iso and Suslin computed mod m K-theory of sep. closed fields).

Warning 1.10.11. K-theory does not satisfying étale descent.

If $A \subset B$ is a finite Galois extension w/ Galois group G, then

$$K(B)^{hG} \neq K(A)$$

(homotopy fixed points of K-theory spectrum upstairs does not reproduce spectrum downstairs)

Let's fix this in some universal fashion.

Definition 1.10.12. Let **étale K-theory** $K^{\text{ét}}$ be the universal modification of K-theory having étale descent in the above sense.

Basically, view K-theory as a presheaf of spectra, and then take sheafification w.r.t. étale topology.

This was considered classically by Thomason, Soulé, Friedlinder (?), ...

Remark 1.10.13. Even better than $K^{\text{ét}}$ is Clausen's Selmer K-theory.

Up to subtle convergence issues (Thomason, Clausen-Mathew), get an AHSS

$$E_2^{ij} = \mathrm{H}^{i-j}_{\text{ét}}(X, \mu_m^{\otimes(-j)}) \implies K^{\text{ét}}_{-i-j}(X, \mathbb{Z}/m\mathbb{Z})$$

for m prime to characteristic of X (prime to char. of all residue fields).

Let's write out this sequence for F a field w/ m prime to $\operatorname{char} F$

$$\begin{array}{ccccc}
 & & \mathrm{H}^0(F, \mathbb{Z}/m\mathbb{Z}) & \mathrm{H}^1(F; \mathbb{Z}/m\mathbb{Z}) & \dots \\
 & \mathrm{H}^0(F, \mu_m) & \mathrm{H}^1(F, \mu_m) & \mathrm{H}^2(F, \mu_m) & \dots \\
\mathrm{H}^0(F, \mu_m^{\otimes 2}) & \mathrm{H}^1(F, \mu_m^{\otimes 2}) & \mathrm{H}^2(F, \mu_m^{\otimes 2}) & \mathrm{H}^3(F, \mu_m^{\otimes 2}) & \dots \\
 & & \vdots & &
\end{array}$$

(maps on this page of bidegree $(2, -1)$)

This whole thing converges to $K^{\text{ét}}_{-i-j}(F; \mathbb{Z}/m\mathbb{Z})$. Beilinson-Lichentbaum says that if you discard the fourth quadrant, then you get a sequence converging to $K_{-i-j}(F; \mathbb{Z}/m\mathbb{Z})$ instead.

1.10.4 Recent progress

We now focus on

- (étale) K-theory
- mod p coefficients (even p-adic)
- p-adic complete rings

  Not a major restriction. Can be removed using arithmetic gluing square

$$\begin{tikzcd}
R \arrow[r] \arrow[d, "p\text{-adic compl.}"'] & R[1/p] \arrow[d] \\
\widehat{R} \arrow[r] & \widehat{R}[1/p]
\end{tikzcd}$$

Everything but R is either p-adically complete or has p prime to its residue characteristics.

Theorem 1.10.14 (Chatt-M-Scholze, Antieau-Mathew-M-Nikolaus, Lüders-M, Kelly-M.)**.** *To any p-adic complete ring R, we may associate a theory of p-**adic étale motivic cohomology**, i.e have motivic p-complete complexes $\mathbb{Z}_p(j)(R)$ for $j \geq 0$ satisfying analogues of BL-type conjectures:*

(i) *There is an AHSS*

$$E_2^{ij} = \mathrm{H}^{i-j}(\mathbb{Z}_p(j)(R)) \implies K^{\acute{e}t}_{-i-j}(R;\mathbb{Z}_p)$$

(ii) *In low weights,*

$$\mathbb{Z}_p(0)(R) \simeq R\Gamma_{\acute{e}t}(R,\mathbb{Z}_p)$$
$$\mathbb{Z}_p(1)(R) \simeq R\Gamma_{\widehat{\acute{e}t}(R,\mathbb{G}_m})[-1]$$

(The $\widehat{\cdot}$ is p-adic completion)

(iii) *Range of support: $\mathbb{Z}_p(j)(R)$ is supported in degrees $\leq j+1$ (even in degrees $\leq n+1$ if the R-module $\Omega^1_{R/pR}$ is generated as an R-module by $< n$ elements). Also support in ≥ 0 if R is quasisyntonic (mild smoothness condition, e.g. R regular).*

(iv) *Nestenenko-Suslin: for R local (still p-complete),*

$$\widehat{K^M_j(R)} \cong \mathrm{H}^j(\mathbb{Z}_p(j)(R)).$$

(v) *Comparison to Gesser-Levine: if R is smooth over a perfect field of char p, then*

$$\mathbb{Z}_p(j)(R)/p \simeq R\Gamma_{\acute{e}t}\left(\operatorname{spec} R, \Omega^j_{\log}\right)[-j].$$

Let's include a picture of the spectral sequence. To keep notation simple, set $\mathrm{H}^i(j) := \mathrm{H}^i(\mathbb{Z}_p(j)(R))$.

$$\begin{array}{ccccc} & & \mathrm{H}^0(0) & \mathrm{H}^1(0) & 0 \\ & \mathrm{H}^0(1) & \mathrm{H}^1(1) & \mathrm{H}^2(1) & 0 \\ \mathrm{H}^0(2) & \mathrm{H}^1(2) & \mathrm{H}^2(2) & \mathrm{H}^3(2) & 0 \\ & & \vdots & & \end{array}$$

(converging to $K^{\text{ét}}_{-i-j}(R;\mathbb{Z}_p)$) The central (second from the right) column is $\widehat{K^M_{-j}(R)}$. The rightmost column is

$$\mathrm{H}^{j+1}(j) \cong \varprojlim_r \widetilde{\nu}_r(j)(R) \text{ where } \widetilde{\nu}_r(j)(R) := \text{"mod } p^r\text{, weight } j \text{ Artin-Schrier obstruction"}$$

Example.

$$\widetilde{\nu}_1(j)(R) := \operatorname{coker}\left(1 - C^{-1} : \Omega^j_{R/pR} \longrightarrow \frac{\Omega^j_{R/pR}}{\mathrm{d}\Omega^{j-1}_{R/pR}}\right).$$

Question: What is C, this "Cartier map"?

If $j = 0$, this is

$$\frac{R}{pR + \{a^p - a : a \in R\}}.$$

These terms are related to class field theory, Tate conjecture, Kato conjecture.

Remark 1.10.15 (Theorem continued). If R is local (+ p-adically complete), then the 3rd quadrant of the spectrum sequence gives an AHSS converging to honest K-theory, $K_{-i-j}(R;\mathbb{Z}_p)$.

For *any* local, p-adic complete R, we have not broken $K_*(R;\mathbb{Z}_p)$ into 'motivic' pieces.

Example. Say $A = k[T]/T^r$ where k perfect field of characteristic p, and $r \geq 1$. General bounds give $\mathrm{H}^i(j) = 0$ unless $0 \leq i \leq 2$. More work shows H^0 and H^2 are 0 (unless $i = j = 0$). Hence, we only have H^1's (and $\mathrm{H}^0(0)$), so the spectral sequence is simple and collapses to

$$K_n\left(\frac{k[T]}{T^r}, \langle T\rangle\right) \cong \begin{cases} \mathrm{H}^1\left(\mathbb{Z}_p\left(\frac{n+1}{2}\right)(R)\right) & \text{if } n \text{ odd} \\ 0 & \text{if } n \text{ even} \end{cases}$$

(aparently these relative K-groups are the same as the p-adic ones in this case). When $r = 2$, can even compute these motivic groups (e.g. see Matthew's survey paper).

2 USS Weeks 2 and 3: Quadratic Forms, Milnor K-Theory and Arithmetic

First half (∼7.5 lectures) by Akhil Mathew and second half by Dustin Clausen. Missed the first week because of GSS.

2.1 Akhil Mathew, Lecture 6 (7/19)

2.1.1 Last time/week

- Introduced the field $\mathbb{Q}_p$ of p-adic numbers.

  Discussed e.g. Hensel's lemma.

- For $p > 2$, discussed the classification of quadratic forms over $\mathbb{Q}_p$. The main result was $W(\mathbb{Q}_p) \simeq W(\mathbb{F}_p) \oplus W(\mathbb{F}_p)$, i.e. an anisotropic form over $\mathbb{Q}_p$ is equivalent to a pair of anisotropic forms over $\mathbb{F}_p$.

  Where did this come from? Can always write a quadratic form over $\mathbb{Q}_p$ in the form

  $$\langle u_1, \ldots, u_r, pv_1, \ldots, pv_s\rangle \text{ with } u_i, v_j \in \mathbb{Z}_p^\times.$$

  This correponds to the pair $(\langle \overline{u}_1, \ldots, \overline{u}_r\rangle, \langle \overline{v}_1, \ldots, \overline{v}_s\rangle) \in W(\mathbb{F}_p) \oplus W(\mathbb{F}_p)$.

  Question 2.1.1. *Why does this need $p > 2$?*

  Answer. Note that it's not obvious that this construction is well-defined in the first place. In order to construct $W(\mathbb{F}_p) \oplus W(\mathbb{F}_p) \to W(\mathbb{Q}_p)$, need to use Hensel's lemma/the structure of squares in $\mathbb{Q}_p$. In particular, you need to know that any $x \equiv 1 \mod p$ is a square in $\mathbb{Z}_p$. This is only true for $p > 2$.

Corollary 2.1.2. *Any anisotropic form over $\mathbb{Q}_p$ ($p > 2$) has dimension ≤ 4. In fact, $u(\mathbb{Q}_p) = 4$.*

Note that there are exactly 16 anisotropic classes of quadratic forms over $\mathbb{Q}_p$ (for $p > 2$) since $\#W(\mathbb{F}_p) = 4$.

What will we do today?

Goal. Describe $W(\mathbb{Q}_p)$ in a more uniform way.

2.1.2 Local fields

We will really describe $W(\mathcal{E})$ for any local field $\mathcal{E}$, not just $\mathbb{Q}_p$.

Definition 2.1.3. A **local field** is a field $\mathcal{E}$ w/ a nontrivial absolute value (up to equiv.) s.t. $\mathcal{E}$ is locally compact ($\implies$ complete).

Example. $\mathbb{Q}_p$ is a local field ($\mathbb{Z}_p$ is compact).

Example. $\mathbb{R}, \mathbb{C}$ are local fields.

Theorem 2.1.4 (**Classification of local fields**). *Let $\mathcal{E}$ be a local field.*

(1) If $\mathcal{E}$ is archimedean, then $\mathcal{E} \simeq \mathbb{R}$ or $\mathbb{C}$.

(2) If $\operatorname{char} \mathcal{E} > 0$, then $\mathcal{E} \simeq \mathbb{F}_q((t))$ for some $q = p^i$ for some i.

Here, we use the "t-adic absolute value" and the unit disk is $\mathbb{F}_q[\![t]\!]$. As a topological space, this is $\cong \prod_{\mathbb{N}} \mathbb{F}_q$ which is compact.

(3) If $\operatorname{char} \mathcal{E} = 0$, but $\mathcal{E}$ is non-archimedea, then $\mathcal{E}$ is a finite extension of some $\mathbb{Q}_p$.

Example. $\mathcal{E} = \mathbb{Q}_p(\sqrt{p})$

(Informally, $\mathbb{Q}_p$ is like $\mathbb{F}_p((t))$ except the "variable" is p and the rules for adding/multiplying are more complicated).

In general, there is a pretty explicit description of quadratic forms over local fields. Explaining this will require us to introduce the Hilbert symbol.

Theorem 2.1.5. *Let $\mathcal{E}$ be a nonarchimedean local field of characteristic $\neq 2$ (e.g. $\mathbb{Q}_2$ is ok but $\mathbb{F}_2((t))$ is not). Then, any quadratic form in ≥ 5 variables is isotropic, and there exists a unique anisotropic form of dimension 4.*

In general, if F any field, can consider $W(F)$. The ring $W(F)$ has an ideal $I \subset W(F)$ of even-dimensional forms. Here, I is additively generated by the forms

$$\langle 1, -a \rangle \quad \text{for } a \in F^\times.$$

Example. $\langle a, b \rangle = (\langle 1 \rangle + \langle a \rangle) - (\langle 1 \rangle - \langle b \rangle) = \langle 1, a \rangle - \langle 1, -b \rangle$.

Fact. There is an isomorphism

$$I/I^2 \xrightarrow{\sim} F^\times/(F^\times)^2$$

sending $\langle 1, -a \rangle \mapsto a$ (the **signed determinant**). Explicitly, this sends the class of an even-dimensional form (V, q) to $(-1)^{\dim V/2} \operatorname{disc}(V, q)$. The is also called the **discriminant** $\operatorname{disc} : I \to F^\times/(F^\times)^2$.

We have the sign factor above since the map needs to be trivial on hyperbolic spaces.

To prove the fact, note that I^2 is generated by elements of the form

$$\langle 1, -a\rangle \cdot \langle 1, -b\rangle = \langle 1, -a, -b, ab\rangle$$

which have discriminant one, so we get a factorization

$$\mathrm{disc} : I/I^2 \xrightarrow{\sim} F^\times/(F^\times)^2$$

with inverse $F^\times/(F^\times)^2 \ni a \mapsto \langle 1, -a\rangle \in I/I^2$.

Let's get back to general facts. For any field F, can consider $I \subset W(F)$ as above, and the filter $W(F)$ by powers of I, i.e. consider

$$W(F) \supset I \supset I^2 \supset I^3 \supset \dots.$$

We always have

$$I/I^2 \cong F^\times/(F^\times)^2 \text{ and } W(F)/I \cong \mathbb{Z}/2\mathbb{Z}.$$

In the case that $F = \mathcal{E}$ is a local field, we always have $I^3 = 0$ (coming from $u(\mathcal{E}) = 4$), so the filtration is finite.[15] In fact, $I^2 \simeq I^2/I^3 \simeq \mathbb{Z}/2\mathbb{Z}$ (recall unique 4-dimensional anisotropic form) in the case of a local field. Thus, we have a filtration (arrows labeled by quotients)

$$\begin{tikzcd}
W(\mathcal{E}) & I \arrow[l, hook', "\mathbb{Z}/2\mathbb{Z}"] & I^2 \arrow[l, hook', "\mathcal{E}^\times/(\mathcal{E}^\times)^2"] \arrow[d, equal] & 0 \arrow[l, hook', "\mathbb{Z}/2\mathbb{Z}"] \arrow[d, equal] \\
 & & \mathbb{Z}/2\mathbb{Z} & I^3
\end{tikzcd}$$

Remark 2.1.6. As a consequence of this 3-step filtration, we see that $W(\mathbb{Q}_2) \not\simeq W(\mathbb{F}_2) \oplus W(\mathbb{F}_2)$ e.g. since $\#W(\mathbb{Q}_2) = 32$ is not a square.

Remark 2.1.7. So far, we have only shown $u(\mathcal{E}) = 4$ when $\mathcal{E} = \mathbb{Q}_p$ for $p > 2$. It is not too hard to extend this to $\mathbb{Q}_2$; show directly that every 5-dim form is isotropic, and that for any anisotropic 4-dim form is isom to $\langle 1, -5, 2, -10\rangle$. For this, consider congruences mod 8 (since $x \in \mathbb{Z}_2^\times$ is a square iff $x \equiv 1 \pmod 8$)

Remark 2.1.8. There's a multiplication map

$$I/I^2 \times I/I^2 \longrightarrow I^2/I^3.$$

In the case of a local field, there is a pairing

$$\mathcal{E}^\times/(\mathcal{E}^\times)^2 \times \mathcal{E}^\times/(\mathcal{E}^\times)^2 \to \mathbb{Z}/2\mathbb{Z}.$$

This is of fundamental importance, and gives the Hilbert symbol.

[15] For a general field, it does not have to be

2.1.3 Hilbert symbol

Definition 2.1.9. Let $\mathcal{E}$ be a local field (with $\operatorname{char}\mathcal{E} \neq 2$). Given $a, b \in \mathcal{E}^\times$, define the **Hilbert symbol**

$$(a,b)_{\mathcal{E}} := \begin{cases} 1 & \text{if } z^2 = ax^2 + by^2 \text{ has a nontrivial solution} \\ -1 & \text{otherwise.} \end{cases}$$

Note that $(a,b) = 1 \iff \langle 1, -a, -b \rangle$ is isotropic.

Let's give some of its properties

- The Hilbert symbol $(a,b)_{\mathcal{E}}$ is the image of (a,b) under the composition

  $$\mathcal{E}^\times/(\mathcal{E}^\times)^2 \otimes \mathcal{E}^\times/(\mathcal{E}^\times)^2 \xrightarrow{\sim} I/I^2 \otimes I/I^2 \xrightarrow{\text{mult}} I^2/I^3 \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}.$$

  That is, it is encoded in the Witt ring.

- $$(a,b)_{\mathcal{E}} = \begin{cases} 1 & \text{if } \langle 1, -a, -b, ab \rangle \text{ is hyperbolic} \\ -1 & \text{if } \langle 1, -a, -b, ab \rangle \text{ is anisotropic.} \end{cases}$$

- $(a,1)_{\mathcal{E}} = 1$ (can solve $z^2 = ax^2 + y^2$ e.g. with $(x,y,z) = (0,1,1)$)

- $(a, 1-a)_{\mathcal{E}} = 1$

- $(a, -a)_{\mathcal{E}} = 1$.

- (Using that $\mathcal{E}$ is local), the Hilbert symbol is bilinear as a pairing

  $$\mathcal{E}^\times/(\mathcal{E}^\times)^2 \times \mathcal{E}^\times/(\mathcal{E}^\times)^2 \to \mathbb{Z}/2\mathbb{Z}.$$

  It is in fact nondegenerate.

For any field F, con considers this I-adic filtration

$$W(F) \supset I \supset I^2 \supset \dots.$$

The Milnor conjecture (now a theorem) says that the associated grading is

$$\bigoplus I^n/I^{n+1} \xrightarrow{\sim} \mathrm{H}^*(F, \mathbb{Z}/2\mathbb{Z}),$$

so one recovers some Galois cohomology.

2.2 Lecture 7 (7/20)

2.2.1 Picking up where we left off

Let $\mathcal{E}$ be a local field (of char $\neq 2$).

Recall 2.2.1. The *Hilbert symbol*

$$(\cdot,\cdot)_{\mathcal{E}} : \mathcal{E}^{\times}/(\mathcal{E}^{\times})^2 \times \mathcal{E}^{\times}/(\mathcal{E}^{\times})^2 \longrightarrow \{\pm 1\}$$

is defined by

$$(a,b)_{\mathcal{E}} = \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 \text{ has a nontriv soln} \\ -1 & \text{otherwise.} \end{cases}$$

Here are some properties of the Hilbert symbol

(1) $(a,b)_{\mathcal{E}} = (b,a)_{\mathcal{E}}$

(2) $(a,-a)_{\mathcal{E}} = 1$

(3) $(a,1-a)_{\mathcal{E}} = 1$ (for $a \in \mathcal{E}^{\times} \setminus \{1\}$)

$(z,x,y) = (1,1,1)$ solves $z^2 - ax^2 - (1-a)y^2$.

(4) $(a,b)_{\mathcal{E}} = (a,-ab)_{\mathcal{E}}$

$z^2 - ax^2 - by^2$ has zero $\iff$ $az^2 - a^2x^2 - aby^2$ has zero $\iff$ $a^2x^2 - az^2 + aby^2$ has zero $\iff$ $x^2 - az^2 + aby^2$ has zero.

All of these properties hold for the analogously defined symbol over any field, but we will only be interested in this when $\mathcal{E}$ is a local field (of char $\neq 2$). This is because, in this case, we have the additional property

(5) $(\cdot,\cdot)_{\mathcal{E}}$ is $\mathbb{F}_2$-bilinear and nondegenerate.

Given $a \in \mathcal{E}^{\times}$, then $(a,b)_{\mathcal{E}} = 1 \iff z^2 - ax^2 - by^2$ has a solution. Rewriting this, this really says

$$(a,b)_{\mathcal{E}} = 1 \iff b \in \operatorname{im}\left(\operatorname{Nm} : \mathcal{E}(\sqrt{a})^{\times} \to \mathcal{E}^{\times}\right).$$

(think $b = \operatorname{Nm}\left(\frac{z - x\sqrt{a}}{y}\right)$).

Local class field theory tells you that this norm map has index 2 image in $\mathcal{E}^{\times}$. This is really a rephrasing of bilinearity. In general, proving bilinearity directly is not so easy, but can do it directly by hand for $\mathcal{E} = \mathbb{Q}_p$.

Example. Say $p > 2$ and pick $x, y \in \mathbb{Q}_p^{\times}$. Write $(x,y) = \left(p^a u, p^b v\right)$ with $a, b \in \mathbb{Z}$ and $u, v \in \mathbb{Z}_p^{\times}$. We claim that

$$(x,y)_{\mathbb{Q}_p} = (-1)^{ab\varepsilon(p)} \left(\frac{u}{p}\right)^b \left(\frac{v}{p}\right)^a \quad \text{where } \varepsilon(p) = \frac{p-1}{2}.$$

The general cases really reduces to the following subexamples

- $(u,v)_{\mathbb{Q}_p} = 1$ (u, v just p-adic units). This is because $z^2 - ux^2 - vy^2$ has a solution iff it does mod p by Hensel's lemma and any quad form in 3 variables is isotropic mod p.
- $(pu, v)_{\mathbb{Q}_p} = \left(\frac{v}{p}\right)$. Consider $z^2 - pux^2 - vy^2$. This will be isotropic $\iff$ $z^2 - vy^2$ is isotropic or ux^2 is isotropic $\iff$ $z^2 - vy^2$ is isotropic $\iff$ $v \in \mathbb{Z}_p^{\times}$ is a square $\iff$ $\left(\frac{v}{p}\right) = 1$.

By computing directly, it follows that it is a nonsingular bilinear map.

Example. Say $\mathcal{E} = \mathbb{R}$. Then,

$$(a,b)_{\mathbb{R}} = \begin{cases} -1 & \text{if } a,b < 0 \\ 1 & \text{otherwise.} \end{cases}$$

Example. For $p = 2$, need to use classification of squares in $\mathbb{Q}_2$. Recall that $x \in \mathbb{Z}_2^\times$ is a 2-adic square $\iff x \equiv 1 \pmod 8$. Suppose $x = 2^a u$ and $y = 2^b v$. Then,

$$(x,y)_{\mathbb{Q}_2} = (-1)^{\varepsilon(u)\varepsilon(v) + a\omega(v) + b\omega(u)} \text{ where } \varepsilon(u) = \frac{u-1}{2} \mod 2 \text{ and } \omega(u) = \frac{u^2-1}{8} \mod 2.$$

For example,

$$(u,v)_{\mathbb{Q}_2} = (-1)^{\left(\frac{u-1}{2}\right)\left(\frac{v-1}{2}\right)} (2,u)_{\mathbb{Q}_2} = (-1)^{\left(\frac{u^2-1}{8}\right)}.$$

The Hilbert symbol is closely related to the structure of $W(\mathcal{E})$ via the observation

$$(a,b)_{\mathcal{E}} = 1 \iff \langle 1, -a, -b \rangle \text{ isotropic} \iff \langle 1, -a, -b, ab \rangle = \langle 1, -a \rangle \otimes \langle 1, -b \rangle \text{ hyperbolic.}$$

Fact. $W(\mathcal{E}) \supset I$ (even-dim forms) from yesterday. Recall the filtration

$$W(\mathcal{E}) \supset I \supset I^2 \supset I^3 = 0$$

with graded terms

$$\mathrm{gr}^0 = W(\mathcal{E})/I = \mathbb{Z}/2\mathbb{Z}, \;\; \mathrm{gr}^1 = I/I^2 = \mathcal{E}^\times/(\mathcal{E}^\times)^2, \;\text{ and }\; \mathrm{gr}^2 = \mathbb{Z}/2\mathbb{Z}.$$

The multiplication pairing

$$\begin{tikzcd}
\mathrm{gr}^1 \arrow[d, equal] & \times & \mathrm{gr}^1 \arrow[r] \arrow[d, equal] & \mathrm{gr}^2 \arrow[d, equal] \\
\mathcal{E}^\times/(\mathcal{E}^\times)^2 & \times & \mathcal{E}^\times/(\mathcal{E}^\times)^2 \arrow[r] & \mathbb{Z}/2\mathbb{Z}
\end{tikzcd}$$

is exactly the Hilbert symbol. This gives another way to think about bilinearity; it reduces to computing $\mathrm{gr}^2 = \mathbb{Z}/2\mathbb{Z}$.

2.2.2 Symbols and invariants of quadratic forms

Definition 2.2.2. Let F be a field, and let A be an abelian group. A **symbol** on F w/ values in A is a $\mathbb{Z}$-bilinear map

$$\varphi : F^\times \times F^\times \to A$$

such that $\varphi(a, 1-a) = 0$ if $a \neq \{0,1\}$.

(Axiomatizes some of the properties of the Hilbert symbol).

One can quickly deduce further properties

- $\varphi(a,-a)=0$ using $-a=\frac{1-a}{1-a^{-1}}$. Spelled out,

$$\varphi(a,-a)=\varphi\left(a,\frac{1-a}{1-a^{-1}}\right)=\varphi(a,1-a)-\varphi(a,1-a^{-1})=\varphi(a^{-1},1-a^{-1})=0.$$

- $\varphi(a,b)=-\varphi(b,a)$

$$\begin{aligned}0&=\varphi(ab,-ab)\\&=\varphi(a,-a)+\varphi(a,b)+\varphi(b,-a)+\varphi(b,b)\\&=\varphi(a,b)+(\varphi(b,a)+\varphi(b,-1))+\varphi(b,b)\\&=\varphi(a,b)+\varphi(b,a)+\varphi(b,-b)\\&=\varphi(a,b)+\varphi(b,a)\end{aligned}$$

For the purposes of quadratic forms, main interest is in symbols valued in $\mathbb{F}_2$-vector spaces.

Given such a symbol, there is a natural way to extract invariants of quadratic forms.

Definition 2.2.3. Let $\varphi:F^\times\times F^\times\to A$ be a symbol, and supposes that A is an $\mathbb{F}_2$-vector space.

Then, we can use the symbol φ to define an invariant of quadratic forms over F, which we'll call ε_φ. We define

$$\varepsilon_\varphi\left(\langle a_1,\dots,a_n\rangle\right)=\sum_{i<j}\varphi(a_i,a_j)$$

(usually, we'll take $A=\{\pm1\}$ and write this sum as a product). We need to show this is well-defined (i.e. independent of the diagonalization).

Recall 2.2.4 (last week)**.** One can always move from one diagonalization to another via repeated application of the moves

- $\langle a,b\rangle\simeq\langle b,a\rangle$
- $\langle a,b\rangle\simeq a,bu^2$
- $\langle a,b\rangle\simeq\left\langle a+b,\frac{ab}{a+b}\right\rangle$ (when $a+b\neq0$).

(always applied to only two of the terms in your diagonalization)

Thus, to show that ε_φ is well defined, we only need to show[16] that if $\langle a,b\rangle\cong\langle c,d\rangle$, then $\varphi(a,b)=\varphi(c,d)$. Note that, in this case, we can write $c=ax^2+by^2$; we can re-scale by squares to assume $c=a+b$. Hence, $a/c+b/c=1$, so

$$1=\varphi\left(\frac{a}{c},\frac{b}{c}\right)=\varphi(a,b)\varphi(a,c)\varphi(b,c)\varphi(c,c)=\varphi(a,b)\varphi(abc,c).$$

Since $abc=d$ up to squares (since disc $\langle a,b\rangle=$ disc $\langle c,d\rangle$), this shows that $\varphi(a,b)=\varphi(c,d)$.

[16] Use that

$$\varepsilon_\varphi\left(\langle a_1,\dots,a_n\rangle\oplus\langle b_1,\dots,b_m\rangle\right)=\varepsilon_\varphi(\langle a_1,\dots,a_n\rangle)\varepsilon_\varphi(\langle b_1,\dots,b_m\rangle)\varphi(a_1\dots a_n,b_1\dots b_m)$$

Example. If $\mathcal{E}$ is a local field of char $\neq 2$, we can define for each quadratic space V an invariant in $\{\pm 1\}$ by the above construction applied to the Hilbert symbol. We call this $\varepsilon(V) \in \{\pm 1\}$. This is called the **Hasse invariant**.

Warning 2.2.5. The Hasse invariant is not additive. Instead,

$$\varepsilon(V \oplus V') = \varepsilon(V)\varepsilon(V') \cdot (\det V, \det V')_{\mathcal{E}}\,.$$

That is, it is *not* a map on $\mathrm{GW}(\mathcal{E})$.

Theorem 2.2.6. *If $\mathcal{E}$ is any local field of* char $\neq 2$*, then quadratic forms over E are isomorphic iff they have the same dimension, determinant $\in \mathcal{E}^\times/(\mathcal{E}^\times)^2$, and Hasse invariant $\in \{\pm 1\}$.*

The main point in proving the above theorem is that quadratic forms of dimension 5 are isotropic and that there is a unique anisotropic form of dimension 4. If (V, q) and (V', q') have the same invariants, you want to show that $(V \oplus V', q \oplus (-q'))$ is hyperbolic. So really just need a criterion for a quadratic form to be hyperbolic. Can check that this has the same invariants as a hyperbolic form of the right dimension, so now one checks (via induction on dimension) that have the invariants of a hyperbolic form make you hyperbolic. Splitting off hyperbolic forms reduces you to the case of dimension ≤ 4 which you can do by hand.

Question 2.2.7 (Audience)**.** *What's so special about this $\varphi(a, 1-a) = 0$ relation? Why does it give rise to nice results?*

Answer. This is really a question about why Milnor k-theory is nice. For any field E (char $k \neq 2$), can define the free commutative $\mathbb{F}_2$-algebra on classes $\langle x \rangle \in E^\times$ w/ relation $\langle x \rangle \cdot \langle 1-x \rangle = 0$. This a a graded ring called $K_*^m(E)/2$, the *mod* 2 *Milnor K-theory*, where $\langle x \rangle$ has degree 1. Milnor conjectured (and it has now been proved) that

$$\mathrm{H}^*(\mathrm{Gal}_E; \mathbb{Z}/2\mathbb{Z}) \simeq K_*^M(E) \simeq \bigoplus_{n \geq 0} I^n/I^{n+1}$$

where $I \subset W(E)$ is the ideal of even-dim forms.

So somehow this relation is encoding interesting information (related to Witt rings and Galois cohomology). The motivation for conjecturing this originated in results about local fields, but these results show that this relation really is interesting.

There were other questions, but I was too lazy to write more down...

2.3 Dustin Clausen, Lecture 8 (7/21): Hilbert Reciprocity

2.3.1 Recap

What have we seen so far in this course?

- Quadratic forms over general fields (Witt's theorems[17], ...)
- Classification over $F = \mathbb{F}_p$

[17] diagonalizing forms and the moves between then

- Classification over $\mathbb{Q}_p, \mathbb{R}$ (local fields)

What about from now on? From now on we'll be doing number theory. That is, we'll be mainly concerned with $F = \mathbb{Q}$ (and later think about quadratic forms over $\mathbb{Z}$).

The work from the first half will not be in vain.

Intuition. To study $\mathbb{Q}$, first study it's nontrivial completions $\mathbb{Q}_p, \mathbb{R}$, and then see how they fit together.

2.3.2 Hilbert symbols

Recall 2.3.1. Given $a, b \in \mathbb{Q}_p^\times$, we defined the Hilbert symbol $(a,b)_{\mathbb{Q}_p} \in \{\pm 1\}$ via

$$(a,b)_{\mathbb{Q}_p} = +1 \iff z^2 = ax^2 + by^2 \text{ has a nontrivial solution.}$$

We also saw other descriptions of this same symbol

- If p is odd, then
$$(a,b)_{\mathbb{Q}_p} = (-1)^{v(a)v(b)} \left(\frac{a^{v(b)}/b^{v(a)}}{p} \right)$$
Note that $v(a^{v(b)}) = v(a)v(b) = v(b^{v(a)})$, so we are taking the legendre symbol of a p-adic unit above.

  Example. If $a, b \in \mathbb{Z}_p^\times$, then $(a,b)_{\mathbb{Q}_p} = 1$.
  If $a \in \mathbb{Z}_p^\times$, then $(a,p)_{\mathbb{Q}_p} = \left(\frac{a}{p}\right)$.

- Above not true for $p = 2$. One has, for $a, b \in \mathbb{Z}_2^\times$,
$$(a,b)_{\mathbb{Q}_2} = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} \text{ and } (a,2)_{\mathbb{Q}_2} = (-1)^{\frac{a^2-1}{8}}$$

- $(a,b)_{\mathbb{R}} = -1 \iff b, a < 0$

Note that we can extract the following corollary from the above remarks

Corollary 2.3.2. *If $a, b \in \mathbb{Q}^\times$, then $(a,b)_{\mathbb{Q}_p} = +1$ for all but finitely many p.*

This is because a given rational number is a p-adic unit for all but finitely many primes (i.e. for all primes not appearing in the denominator or numerator).

This fact is important in being able to state the Hilbert product formula.

Theorem 2.3.3 (Hilbert reciprocity). *Let $a, b \in \mathbb{Q}^\times$. Then,*

$$(a,b)_{\mathbb{R}} \cdot \prod_p (a,b)_{\mathbb{Q}_p} = +1.$$

(This product is secretly finite by the previous corollary)

Concretely, this says that the set of completions of $\mathbb{Q}$ in which the equation $ax^2 + by^2 = z^2$ does not have a nontrivial solution is finite and even.

Notation 2.3.4. We'll write ν to denote a 'place' of the rational numbers which we think of as a prime number p or ∞. So $\mathbb{Q}_\nu = \mathbb{Q}_p$ (for some p) or $\mathbb{Q}_\nu = \mathbb{R}$.

Let's specialize to the case $(a,b) = (p,q)$ are distinct odd primes. Then, $(p,q) = \mathbb{Q}_\nu = 1$ if $\nu \notin \{p,q,2,\infty\}$. This just leaves four computations

$$(p,q)_\mathbb{R} = 1,\ \ (p,q)_{\mathbb{Q}_2} = (-1)^{\frac{p-1}{2}\left(\frac{q-1}{2}\right)},\ \ (p,q)_{\mathbb{Q}_p} = \left(\frac{q}{p}\right),\ \text{ and }\ (p,q)_{\mathbb{Q}_q} = \left(\frac{q}{p}\right).$$

Thus, the Hilbert product formula recovers **quadratic reciprocity**

This is really saying that the Hilbert product formula (for $\mathbb{Q}$) is equivalent to quadratic reciprocity

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

In fact, it also recovers the two supplementary laws to quadratic reciprocity'. That is, it also gives

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad\text{and}\quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

(by taking $(a,b) \in \{(-1,p),(2,p)\}$).

2.3.3 Tate's proof of Hilbert reciprocity

Two steps

(1) Classify all symbols over $\mathbb{Q}$.

Use this to deduce some relation of the form $\prod_\nu (a,b)_\nu^{\varepsilon_\nu} = 1$ for $\varepsilon_\nu \in \{0,1\}$.

(2) Prove that the only possible relation of this form is the one we want.

Recall 2.3.5. Let F be a field, and let A be an abelian group (written multiplicatively). A **symbol** on F w/ values in A is a $\mathbb{Z}$-bilinear function

$$\varphi : F^\times \times F^\times \to A$$

such that $\varphi(a,b) = 1$ if $a+b=1$ (and $a,b \in F^\times$).

Remark 2.3.6. bilinearity above means that $\varphi(ab,c) = \varphi(a,c)\varphi(b,c)$ and $\varphi(a,bc) = \varphi(a,b)\varphi(a,c)$.

Example. On $\mathbb{Q}_\nu$, the Hilbert symbol $(\cdot,\cdot)_{\mathbb{Q}_\nu}$ is a symbol in the above sense

Remark 2.3.7. If $f : F \to E$ is a field homomorphism and φ is a symbol on E, then $\varphi \circ f$ is a symbol on F. For example, $(\cdot,\cdot)_{\mathbb{Q}_\nu}$ gives a symbol on $\mathbb{Q}$.

Example. For p a prime, there's a so-called **tame symbol** on $\mathbb{Q}$

$$(a,b)_p := (-1)^{v_p(a)v_p(b)}\left(\frac{a^{v_p(b)}}{b^{v_p(a)}} \mod p\right) \in \mathbb{F}_p^\times.$$

So this composed with the legendre map $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \{\pm 1\}$ recovers the Hilbert symbol (when $p \neq 2$).

2.3.4 Universal symbol

Fix a field F. Let A be the free abelian group on the set $F^\times \times F^\times$ modulo the subgroup generated by

$$(ab,c)\,(a,c)^{-1}\,(b,c)^{-1}\,,\ \ (a,bc)\,(a,b)^{-1}\,(a,c)^{-1}\,,\ \text{ and }\ (a,1-a).$$

This A is denoted by $K_2(F)$. The image of $(a,b) \in F^\times \times F^\times$ in the group $A = K_2(F)$ is usually denoted $\{a,b\}$.

Proposition 2.3.8. *There is a symbol on F w/ values in $K_2(F)$ defined by $(a,b) \mapsto \{a,b\}$. Moreover, this symbol is universal in the sense that there is a bijection*

$$\left\{\begin{matrix}\textit{symbols on } F\\ \textit{w/ values in } A\end{matrix}\right\} \longleftrightarrow \operatorname{Hom}_{\mathrm{Ab}}(K_2(F),A).$$

Note 5. Got distracted and missed some stuff

Theorem 2.3.9 (Tate)**.** *$K_2(\mathbb{Q}) \cong A_2 \oplus A_3 \oplus A_5 \oplus \dots$ where*

$$A_p = \begin{cases} \{\pm1\} & \textit{if } p = 2\\ (\mathbb{Z}/p\mathbb{Z})^\times & \textit{if } p \textit{ odd.}\end{cases}$$

2.4 Lecture 9 (7/22): Proof of Hilbert Reciprocity

Let F be a field.

Recall 2.4.1. We constructed an abelian group $K_2(F)$ supporting the universal symbol. It's generators were pairs $\{a,b\}$ (not sets, order matters) with $a,b \in F^\times$ subject to the relations

$$(ab,c) = (a,c)(b,c),\ \ (a,bc) = (a,b)(a,c),\ \text{ and }\ (a,1-a) = 1$$

(last relation if $a \neq 1$). Thus was constructed so that homomorphisms $K_2(F) \to A$ were to same things as symbols $\varphi : F^\times \times F^\times \to A$.

Example. For any prime p, have the *tame symbol* on $\mathbb{Q}$

$$(a,b)_p := (-1)^{v_p(a)v_p(b)}\left(\frac{a^{v_p(b)}}{b^{v_p(a)}} \mod p\right)$$

valued in $\mathbb{F}_p^\times$. Note that $(a,p)_p = a \mod p$ if $v_p(a) = 0$ and $(a,b)_p = 1$ if $v_p(a) = 0 = v_p(b)$.

Example. We have also seen the 2-adic Hilbert symbol $\mathbb{Q}^\times \times \mathbb{Q}^\times \to \{\pm1\}$.

We ended last time by stating the following theorem due to Tate

Theorem 2.4.2 (Tate)**.** *$K_2(\mathbb{Q}) \xrightarrow{\sim} \bigoplus_p A_p$ where $A_2 = \{\pm1\}$ and $A_p = \mathbb{F}_p^\times$ for $p \neq 2$. This map is given on the pth factor by $(\cdot,\cdot)_{\mathbb{Q}_2}$ for $p = 2$, and by the tame symbol for $p \neq 2$.*

Remark 2.4.3. The map $K_2(\mathbb{Q}) \to \prod_p A_p$ described above actually lands in $\bigoplus A_p$ because the tame symbol of (x,y) is trivial in there are no p's in x or y. This verifies that the statement is well-posed.

2.4.1 The proof

We want to prove that $K_2(\mathbb{Q})$ is a direct sum. How will we do that? Well, to prove that a group is a direct sum, it's often useful to first prove something weaker. In particular, we will first give a filtration on $K_2(\mathbb{Q})$ whose associated graded pieces are the A_p's from before. We will then show this filtration splits, and so win.

For $n \geq 1$, define the subgroup $L_n \subset K_2(\mathbb{Q})$ generated by symbols $\{x, y\}$ where $x, y \in \mathbb{Z} \setminus \{0\}$ and $|x|, |y| \leq n$. This gives an exhaustive filtration

$$\{1\} \subset L_1 \subset L_2 \subset L_3 \subset \cdots \subset K_2(\mathbb{Q}).$$

Remark 2.4.4. $\bigcup_n L_n = K_2(\mathbb{Q})$ since any symbol will be represented by integers because of bilinearity.

Remark 2.4.5. L_1 is generated by $\{-1,-1\}, \{-1,1\}, \{1,-1\}, \{1,1\}$. By bilinearity we must have that $\{-1,1\} = \{1,-1\} = \{1,1\} = 1$ are all trivial. What about $\{-1,-1\}$, is this trivial?

It is not trivial because we have the $\mathbb{R}$-Hilbert symbol for which $(-1,-1)_{\mathbb{R}} = -1$ (we also could have used the $\mathbb{Q}_2$-Hilbert symbol). Hence, L_1 is generated by the single element $\{-1,-1\}$, so it is cyclic. In fact, cyclic of order 2 as $\{-1,-1\}^2 = \{-1,1\}$ by bi-multiplicativity. Thus,

$$L_1 = \langle \{-1,-1\} \rangle \simeq \mathbb{Z}/2\mathbb{Z}.$$

Remark 2.4.6. If n is not prime, then $L_{n-1} = L_n$, i.e. the jumps in the filtration only occur at prime numbers. Say we have $\{x, y\}$ with $|x|, |y| \leq n$. If n is not a prime, we can write x, y as products of primes each with absolute value $\leq n-1$. This observation + bi-multiplicativiy show $L_n \subset L_{n-1}$.

A natural next step is to identify L_p/L_{p-1}. Let

$$\varphi_p : K_2(\mathbb{Q}) \to \mathbb{F}_p^\times$$

be the homomorphism given by the tame symbol.

Remark 2.4.7. φ_p kills L_{p-1} since it kills $\{x, y\}$ when x an integer coprime to p (e.g. $|x| < p-1$). Thus, it induces a map

$$L_p/L_{p-1} \longrightarrow \mathbb{F}_p^\times.$$

Lemma 2.4.8 (Key Lemma). *This induced map $\varphi_p : L_p/L_{p-1} \to \mathbb{F}_p^\times$ is an isomorphism for all primes p.*

Let's assume this for now and use it to prove Tate's theorem. We'll come back and prove this lemma later.

We wish to inductively show that for all $n \geq 2$, the map

$$L_n \longrightarrow \bigoplus_{p \leq n} A_p$$

induced by the $\mathbb{Q}_2$-Hilbert symbol on the 2nd factor and the tame symbol of the pth factor is an isomorphism.

Proof. When $p = 2$, the Key lemma says $L_2/L_1 \simeq \mathbb{F}_2^\times = \{1\}$, so $L_2 = L_1$. We saw earlier that this was cyclic of order 2 generated by $\{-1, -1\}$, so the $\mathbb{Q}_2$-Hilbert symbol indeed induces an iso $L_2 \xrightarrow{\sim} \{\pm 1\}$.

Assume claim for $n - 1$. We're done if n is not prime, so we may assume that n is prime. Then, we have an iso of short exact sequences

$$\begin{tikzcd}
0 \arrow[r] & L_{n-1} \arrow[r] \arrow[d, "\wr"] & L_n \arrow[r] \arrow[d, "\wr"] & L_n/L_{n-1} \arrow[r] \arrow[d, "\wr"] & 0 \\
0 \arrow[r] & \bigoplus_{p \le n-1} A_p \arrow[r] & \bigoplus_{p \le n} A_p \arrow[r] & A_n \arrow[r] & 0
\end{tikzcd}$$

(the middle map is an isomorphism above since the other maps are both isos). This completes the argument. ■

This reduced us to the key lemma, restated below for convenience

Lemma 2.4.9 (Key Lemma)**.** *This map $\varphi_p : L_p/L_{p-1} \to \mathbb{F}_p^\times$ induced by the tame symbol is an isomorphism for all primes p.*

Proof. Start with surjectivity. Represent a class in $\mathbb{F}_p^\times$ by an integer x with $0 < x < p$. Then, $\varphi_p(x, p) = [x] \in \mathbb{F}_p^\times$, so this gives surjectivity.

It turns out to be tricky to directly tackle injectivity, so we'll do some a bit more roundabout. We will show that $\{x, p\}$ as above give all the classes in L_p/L_{p-1} (hence, this quotient has size $\le p - 1$ but also size $\ge p - 1$ by the surjectivity argument, so φ_p an iso since surjective between finite sets of the same size). We'll do this in two steps

- The $\{x, p\}$ form a subgroup of L_p/L_{p-1}.

  Consider $0 < x, y < p$. We want $\{xy, p\} = \{x, p\} \cdot \{y, p\} \equiv \{z, p\} \pmod{L_{p-1}}$ for some $0 < z < p$. Fix $z \in [1, p - 1]$ so that $z \equiv xy \pmod p$, and write $xy = z + pq$ with $q \in \mathbb{N}$. We're now at the point where we'll use the Steinberg relation $\{a, b\} = 1$ if $a + b = 1$. Observe that

  $$1 = \frac{z}{xy} + \frac{pq}{xy} \implies \left\{\frac{z}{xy}, \frac{pq}{xy}\right\} = 1.$$

  To finish, it'll suffice to show that

  $$\left\{\frac{z}{xy}, \frac{pq}{xy}\right\} \equiv \left\{\frac{z}{xy}, p\right\} \pmod{L_{p-1}}.$$

  This will follow if we know $|q| < p$ (expand out above symbol and observe that most terms lie in L_{p-1}), but this is obvious since

  $$q = \frac{xy - z}{p} < \frac{xy}{p} < \frac{p^2}{p} = p.$$

- The $\{x, p\}$ generated L_p/L_{p-1}.

  Exercise.

■

This finishes the proof that

$$K_2(\mathbb{Q}) \xrightarrow{\sim} \bigoplus_p A_p.$$

In other words, for every symbol $\varphi : \mathbb{Q}^\times \times \mathbb{Q}^\times \to A$, there exists unique homomorphisms $A_p \xrightarrow{f_p} A$ for all p such that

$$\varphi(x, y) = f_2((x, y)_{\mathbb{Q}_2}) \cdot \prod_{p>2} f_p((x, y)_p).$$

Let's apply this to $\varphi(x, y) = (x, y)_{\mathbb{R}}$, the real Hilbert symbol. Since this lands in the group $\{\pm 1\}$ of order 2, the maps $f_p : A_p \to \{\pm 1\}$ will factor through $A_p/2A_p \cong \{\pm 1\}$, i.e. will be maps of the Hilbert symbols instead of the tame symbols. Hence, we conclude that there exists $\varepsilon_p \in \{0, 1\}$ (for all p) so that

$$(x, y)_{\mathbb{R}} = \prod_p (x, y)_{\mathbb{Q}_p}^{\varepsilon_p}.$$

Thus, to prove Hilbert reciprocity, we only need show $\varepsilon_p = 1$ for all p.

To do this, we just plug in some numbers.

- $(-1, -1)$ gives

$$-1 = (-1, -1)_{\mathbb{Q}_2}^{\varepsilon_2} = (-1)^{\varepsilon_2} \implies \varepsilon_2 = 1.$$

- Say $p \equiv 3 \pmod 4$ and plug in $(-1, p)$. This gives

$$+1 = (-1, p)_{\mathbb{Q}_2}(-1, p)_{\mathbb{Q}_p}^{\varepsilon_p} = (-1)^{\frac{p-1}{2}}(-1)^{\varepsilon_p} = -(-1)^{\varepsilon_p} \implies \varepsilon_p = 1.$$

- The remaining cases are $p \equiv 1 \pmod 8$ and $p \equiv 5 \mod 8$. In these case (or just the latter?), you'll want to plug in $(2, p)$. These cases take more work. In particular, you'll want to lemma

  Lemma 2.4.10. *If $p \equiv 1 \pmod 8$, then there exists a prime $q < p$ such that $\left(\frac{p}{q}\right) = -1$.*

  If you have this, you can look at (p, q) and use some inductive argument.

Apparently you can prove Hilbert reciprocity use algebraic K-theory and working directly w/ K-theory spectra.

We can rephrase Tate's computation using algbraic K-theory via the short exact sequence

$$0 \longrightarrow K_2(\mathbb{Z}) \longrightarrow K_2(\mathbb{Q}) \longrightarrow \bigoplus_p \mathbb{F}_p^\times \longrightarrow 0$$

(map using Tame symbols on the right for every prime). Hence, Tate's calculation is saying $K_2(\mathbb{Z}) = \{\pm 1\}$. In general, one has

$$0 \longrightarrow K_2(\mathscr{O}_F) \longrightarrow K_2(F) \longrightarrow \bigoplus_{\nu \nmid \infty} \kappa_\nu^\times \longrightarrow 0.$$

Up to simple factors one knows (expects?) that $\#K_2(\mathscr{O}_F) = \zeta_F(-1)$.

2.5 Lecture 10 (7/23): Hasse-Minkowski Theorem

Back to quadratic forms. Let f be a quadratic form over $\mathbb{Q}$, i.e. a degree 2 homogeneous polynomial with rational coefficients. For every place v, get an induced quadratic form f_v over $\mathbb{Q}_v$.

The main theme of Hasse-Minkowski is the local-global principal.

Slogan (**Local-Global principle**)**.** Knowledge of f_v for all v gives knowledge of f.

Theorem 2.5.1 (**Hasse-Minkowski Theorem**)**.**

(1) If f_v is isotropic for all v, then f is isotropic.

(2) Given $a \in \mathbb{Q}$, if f_v represents a for all v, then f represents a.

(3) Say f, g are two quadratic forms over $\mathbb{Q}$. If $f_v \simeq g_v$ for all v, then $f \simeq g$.

Note that **(1)** above implies **(2)**,**(3)**.

Remark 2.5.2. For **(2)**, recall that f represents $a \iff f - aZ^2$ is isotropic. This + **(1)** gives **(2)**.

For **(3)**, need to do a little more. First note f represents a for some $a \neq 0$, so $f - aZ^2$ is isotropic. Hence, $f - aZ^2 \simeq H \oplus f'$ with f' one dimension lower than f. Since $f - aZ^2$ is isotropic, we conclude that $g_v - aX^2$ is isotropic for all v, so (by **(1)**), g representes a. Hence, $g - aZ^2 \simeq H \oplus g'$. For every v, Witt cancellation tells us that $f'_v \simeq g'_v$, so induction tells us that $f' \simeq g'$ and then Witt cancellation tells us that $f \simeq g$ since $f - aZ^2 \simeq g - aZ^2$.

Warning 2.5.3. This local-global principle is special to degree 2 (homogeneous) equations. For example (due to Selmer),

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

has nontrivial solutions in $\mathbb{Q}_\nu$ for all ν, but has no non-trivial solutions in $\mathbb{Q}$.

This Selmer equation gives a non-trivial torsor for an elliptic curve which becomes trivial over $\mathbb{Q}_v$ for all v, i.e. it represents a non-trivial element of the Tate-Shafervich group.

Remark 2.5.4. Proof of Hasse-Minkowski is difficult. It relies on two big theorems:

(1) Hilbert product formula

(2) Dirichlet's theorem on primes in arithmetic progressions, i.e. that for a, n coprime integers, there are infinitely many primes p such that $p \equiv a \pmod{n}$.

2.5.1 Collecting some lemmas

The proof will be by induction on the number of variables. Hence, much of the meat will be in the low variable cases.

Lemma 2.5.5. *Let v be a place of $\mathbb{Q}$, and fix $a, b, c \in \mathbb{Q}_v^\times$. Then,*

$$ax^2 + by^2 \text{ represents } c \iff (a,b)_v = (c, -ab)_v.$$

Proof. We have equivalences ax^2+by^2 represents $c \iff \frac{a}{c}x^2+\frac{b}{c}y^2$ represents $1 \iff \frac{a}{c}x^2+\frac{b}{c}y^2-z^2$ isotropic $\iff \left(\frac{a}{c},\frac{b}{c}\right)_v = 1$ by definition of Hilbert symbol $\iff (a,b)_v(c,c)_v = (a,c)_v(b,c)_v = (ab,c)_v \iff (a,b)_v = (-ab,c)_v$. Here, we've used $(c,c)_v = (c,-1)_v(c,-c)_v = (c,-1)_v$. ■

Lemma 2.5.6. *Let k be a field of* char $\neq 2$, *and fix $a,b \in k^\times$. Then,*

$$aX^2+bY^2-Z^2 \text{ is isotropic} \iff a \in \mathrm{Nm}_{k(\sqrt{b})}\left(k(\sqrt{b})^\times\right).$$

Proof Sketch. Vacuously true if b is a square, so say $b \neq \square$. Then write

$$ax^2+by^2=1 \implies a = 1/x^2 - b(y/x)^2 = \left(\frac{1}{x}-\sqrt{b}\frac{y}{x}\right)\frac{1}{x}+\sqrt{b}\frac{y}{x} = \mathrm{Nm}\left(\frac{1}{x}+\sqrt{b}\frac{y}{x}\right).$$

Not too hard to reverse implication. ■

Observe that the norm map is an homomorphism so it's image is a subgroup.

There will be some more lemmas, but we'll introduce them on a need-to-know basis.

2.5.2 Proof of Hasse-Minkowski

Fix f a quadratic form over $\mathbb{Q}$, and write $f \simeq \langle a_1, a_2, \dots, a_n\rangle$. Since we only care about f representing 0, we may safely assume $a_1 = 1$. Afterwards, can always modify each a_i by a square, so we may assume that each $a_i \in \mathbb{Z}\setminus\{0\}$ is a *squarefree* integer. That is, we have assume

$$f \simeq \langle 1, a_2, a_3, \dots, a_n\rangle \text{ where } a_i \text{ is a squarefree integer.}$$

To make the induction work, we'll need to handle $n = 1,2,3$ by hand.

- $n=1$

  This is $f = x_1^2$. This has no nontrivial zero over any field, so we win.

- $n=2$

  This is $f = x_1^2 + a_2x_2^2$ with a_2 a squarefree integer. If f is isotropic over $\mathbb{Q}_v$, then $-a_2 \in (\mathbb{Q}_v^\times)^2$. Hence, $-a_2 > 0$ ($v=\infty$) and $v_p(-a_2)$ is even for all p. This forces $-a_2 = 1$ ($v_p(a_2) \le 1$ for all p by the squarefree assumption). Thus, $f \simeq \langle 1,-1\rangle$ is the hyperbolic plane.

  The main thing here is that a rational number is a square iff it is a square locally at all places.

- $n=3$

  This is $f = aX^2+bY^2-Z^2$ with a,b squarefree integers. In this case, we will prove the desired statement by induction on $|a|+|b|$. The base case here is $|a|+|b|=2$; this forces $a,b \in \{\pm 1\}$ so only 4 cases which you can easily check by hand.[18] Hence we may assume $|a|+|b| \ge 3$.

  Lemma 2.5.7. *a is a square mod b.*

[18] Only case w/ no $\mathbb{Q}$-solution is $a=b=-1$, but in this case, no solution in $\mathbb{R}$

Proof. By CRT, suffices to show that a is a square mod p for all primes $p \mid b$. Recall by hypothesis that $aX^2 + bY^2 - Z^2 = 0$ has a solution in $\mathbb{Q}_p$. By clearing denominators, we have a solution in $\mathbb{Z}_p$ which we may moreover take to be primitive (i.e. $\min\{v_p(X), v_p(Y), v_p(Z)\} = 0$). Since $p \mid b$, we have $p \mid (aX^2 - Z^2)$ so $aX^2 \equiv Z^2 \pmod p$, so $a \equiv \left(\frac{Z}{X}\right)^2 \mod p$ is a square (note $X \equiv 0 \pmod p$ would imply $Y, Z \equiv 0 \pmod p$, contradicting primitivity). ■

Thus, there's some $b', t \in \mathbb{Z}$ such that $bb' = a - t^2 = (\sqrt{a} - t)(\sqrt{a} + t)$, so bb' is a norm from $\mathbb{Q}_v(\sqrt{a})$. Hence we conclude that $\langle a, b, -1 \rangle$ is isotropic $\iff$ $\langle a, b', -1 \rangle$ is isotropic! Choosing t appropriately, we can arrange $|b'| < |b|$ and so win by induction.

Dustin calls this the "bb' switcheroo"

- $n = 4$

  Do this next time

I guess we'll end by stating some of the ingredients we'll still need (and that are on the exercises?)

Theorem 2.5.8 (**Weak Approximation**)**.** *If S is a finite set of places of $\mathbb{Q}$, and you are given $x_v \in \mathbb{Q}_v$ and $\varepsilon_v \in \mathbb{R}_{>0}$ for all $v \in S$, then there is some $x \in \mathbb{Q}$ s.t. $|x - x_v|_v < \varepsilon_v$ for all $v \in S$. Equivalently, the diagonal map*

$$\mathbb{Q} \hookrightarrow \prod_{v \in S} \mathbb{Q}_v$$

has dense image.

Exercise. To see that the above is special, note that $\mathbb{Z}[1/p]$ is dense in $\mathbb{Q}_p$ and in $\mathbb{R}$ (is this true?), but show that it's not dense in $\mathbb{Q}_p \times \mathbb{R}$.

Exercise. $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}$ has dense image under both embeddings (i.e. $\sqrt{2} \mapsto \pm\sqrt{2}$), but $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R} \times \mathbb{R}$ using both maps has discrete, cocompact image.

There was more said, but I stopped paying attention.

2.6 Lecture 11 (7/26): Quadratic forms over $\mathbb{Z}$

2.6.1 ... But first

we need to finish the proof of Hasse-Minkowski.

Recall 2.6.1. Say f is a quadratic form over $\mathbb{Q}$ s.t. f_ν is isotropic for all places ν of $\mathbb{Q}$. Then, f is isotropic.

We say last time that this is true for $n \leq 3$. Today we'll do $n = 4$, and then be able to induct to do $n \geq 5$.

Recall 2.6.2 (Lemma from last time)**.** Say $a, b, c \in \mathbb{Q}_\nu^\times$. Then,

$$aX^2 + bY^2 \text{ represents } c \iff (a, b)_\nu = (c, -ab)_\nu,$$

so we can check representability in this case using the Hilbert symbol.

Proof of $n = 4$ case of Hasse-Minkowski. Say our form is $f = aX^2 + bY^2 - cZ^2 - dW^2$ w/ $a, b, c, d \in \mathbb{Q}^\times$. For all ν, we have f_ν represents 0, so there exists $t_\nu \in \mathbb{Q}_\nu$ s.t. both $aX^2 + bY^2$ and $cZ^2 + dW^2$ represent t_ν, for all ν (e.g. can locally solve $aX^2 + bY^2 = cZ^2 + dW^2$). Note that we may assume $t_\nu \in \mathbb{Q}_\nu^\times$.

Now, we would like to replace these t_ν all by a single $t \in \mathbb{Q}^\times$. For this, we use weak approximation in a clever way. This requires only a finite set of primes, so we need to be able to control things away from a finite set, so we let

$$S = \{\infty, 2\} \cup \{p : p \mid abcd\}$$

be the our set of "bad" primes. Now, weak approximation gives some $t \in \mathbb{Q}^\times$ as closed as we want to t_ν for all $\nu \in S$, i.e. $|t/t_\nu - 1|$ can be as small as we like. In particular, we can guarantee that $t/t_\nu \in (\mathbb{Q}_\nu^\times)^2$ is a square. In particular, we can arrange that $(t, ab)_\nu = (t_\nu, -ab)_\nu = (a, b)_\nu$, so t is represented by both $aX^2 + bY^2$ and $cZ^2 + dW^2$.

Recall 2.6.3 (from problem set)**.** We can also guarantee that $|t|_p = 1$ for all $p \notin S \cup \{p_0\}$.

Then, for $p \notin S \cup \{p_0\}$, we have $(t, -ab)_p = 1 = (a, b)_p$ (note that p odd) so t represented by $aX^2 + bY^2$ and $cZ^2 + dW^2$ in $\mathbb{Q}_p$. By Hilbert's product formula, we must also have $(t, -ab)_{p_0} = (a, b)_{p_0}$. Thus, t is represented by both $aX^2 + bY^2$ and $cZ^2 + dW^2$ in $\mathbb{Q}_\nu$ for all ν. Thus, $\langle a, b, -t\rangle$ and $\langle c, d, -t\rangle$ are isotropic for all ν, so they are both isotropic over $\mathbb{Q}$ by the 3 variable case. Thus, there exists x, y, z, w s.t. $ax^2 + by^2 = t = cz^2 + dz^2$, so these give a solution to our original form $f = aX^2 + bY^2 - cZ^2 - dW^2$. ■

This brings us to the end of the proof.

Proof of $n \geq 5$ case of Hasse-Minkowski. To keep notation simple, say $n = 5$[19]. Write

$$F = aX^2 + bY^2 - a_1Z^2 - b_1W^2 - c_1V^2,$$

and let S be the set of places where $\langle a, b, c\rangle$ is not isotropic; this is *finite* since for $p \nmid 2a_1b_1c_1$ have nontrivial zero in $\mathbb{F}_p$ by u-invariants (so in $\mathbb{Z}_p$ by Hensel). For $\nu \in S$, choose a shared value t_ν of $aX^2 + bY^2$ and $a_1Z^2 + b_1W^2 + c_1V^2$, say

$$ax_\nu^2 + by_\nu^2 = t_\nu = a_1z_\nu^2 + b_1w_\nu^2 + c_1v_\nu^2 \text{ with } x_\nu, y_\nu, t_\nu \in \mathbb{Q}_\nu^\times.$$

Choose $x, y \in \mathbb{Q}^\times$ close enough to x_ν, y_ν so that $x \in x_\nu(\mathbb{Q}_\nu^\times)^2$ and $y \in y_\nu(\mathbb{Q}_\nu^\times)^2$. By continuity, we can also guarantee that $t := ax^2 + by^2 \in t_\nu(\mathbb{Q}_\nu^\times)^2$.

Hence, $\langle -t, a_1, b_1, c_1\rangle$ is isotropic for $\nu \in S$. By definition of S, it's also isotropic for all $\nu \notin S$ since $\langle a_1, b_1, c_1\rangle$ is. By the $n = 4$ case, we conclude that $\langle -t, a, b, c\rangle$ is isotropic over $\mathbb{Q}$, i.e. t represented by $a_1z^2 + b_1w^2 + c_1v^2$. Thus, we have a global solution (x, y, z, w, v) over $\mathbb{Q}$. ■

2.6.2 Integral quadratic forms

Recall 2.6.4. Let k be a field. A **quadratic space** (V, f) over k is a pair of a finite-dimensional vector space V along with a **quadratic form** f, i.e. a function $f : V \to k$ satisfying

(1) $f(\lambda v) = \lambda^2 f(v)$

[19] Since $u(\mathbb{Q}_p) = 4$ for all p, all 5-dimensional forms are isotropic over all non-arch completions, so doing $n = 5$ will secretly suffice for doing $n \geq 5$

(2) $\langle v, w\rangle := f(v+w) - f(v) - f(w)$ is bilinear.

Equivalently, if you choose a basis $x_1, \ldots, x_n$ of V, then f is a degree 2 homogeneous polynomial in the x_i's.

Example. $f(x,y) = aX^2 + bXY + cY^2$ is a quadratic form in 2 variables (i.e. of dimension 2).

Over $\mathbb{Z}$, we can really just make the same definition.

Definition 2.6.5. A **quadratic space over** $\mathbb{Z}$ is a pair (M, f) of a finite free $\mathbb{Z}$-module $M \cong \mathbb{Z}^{\oplus n}$ and a function $f : M \to \mathbb{Z}$ as before. Again, after choosing a basis for M, f is simply a homogeneous degree 2 polynomial w/ $\mathbb{Z}$-coefficients.

How are these different from quadratic spaces over fields?

- Before, we said our quadratic forms should be non-degenerate, i.e. that the associated pairing should be perfect. This is no longer a reasonable assumption when working integrally, i.e. shouldn't assume $\langle -, -\rangle : M \times M \to \mathbb{Z}$ is a perfect paring.

  Example. $f(X,Y) = X^2 + Y^2$ is a simple and well-studied integral quadratic form. The associated bilinear form here is not non-degenerate in the above sense (is not unimodular). This has bilinear form w/ associated matrix
  $$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$
  which is not invertible.

  Recall 2.6.6. Over a field, non-degenerate $\iff$ $\det(\langle -, -\rangle) \in k^\times$. The same holds over $\mathbb{Z}$, non-degenerate $\iff$ $\det(\langle -, -\rangle) \in \mathbb{Z}^\times = \{\pm 1\}$.

- $\det(\langle -, -\rangle)$ depends on the basis of the vector space, but only up to square of units. Hence, over $\mathbb{Z}$, $\det(\langle -, -\rangle) \in \mathbb{Z}$ is a well-defined integer since $(\mathbb{Z}^\times)^2 = 1$.

To get started studying these things, let's specialize to the first non-trivial case.

2.6.3 Binary quadratic forms

Say $f(X,Y) = aX^2 + bXY + cY^2$. The matrix for $\langle -, -\rangle$ will then be
$$\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$$
with determinant
$$\det \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} = 4ac - b^2.$$

This is a familiar value (almost), so we define the **discriminant** of a quadratic form with associated matrix B to be $D := -\det B$.

We won't consider quadratic forms with 0 discriminant, so we get a dichotomy

- $D > 0 \iff f_{\mathbb{R}}$ is *indefinite*, i.e. f takes both positive and negative values.

- $D < 0 \iff f_{\mathbb{R}}$ is *definite*, i.e. f's values are always positive or always negative.

  In this case, we can arrange all values to be > 0 by changing f by a sign.

  Warning 2.6.7. f and $-f$ are not isomorphic, but it's clear that understanding one will allow you to understand the other.

Fact. If $D > 0 \iff$ the orthogonal group $O_f(\mathbb{Z})$ is infinite, while $D < 0 \iff O_f(\mathbb{Z})$ is finite.

When we work over $\mathbb{Z}$, it is a good idea to use a finite form of equivalence than isomorphism, called **strict isomorphism** (or **strict equivalence**). We have $f \sim g$, the two are strictly isomorphic, iff they are related by an invertible linear change of variables w/ determinant 1.

2.7 Lecture 12 (7/27): Reduction theory

... of positive definite binary integral quadratic forms (title continued).

Recall 2.7.1. A binary quadratic form is a polynomial of the form

$$f(X,Y) = aX^2 + bXY + cY^2 \text{ where } a,b,c \in \mathbb{Z}.$$

As shorthand, we'll also denote this as $f = \langle a,b,c \rangle$.

Warning 2.7.2. This conflicts with our previous notation where angled brackets denoted diagonal forms. Not every form is diagonalizable over $\mathbb{Z}$, so we drop this old notation.

Recall that the discriminant of $f = \langle a,b,c \rangle$ is $D_f = b^2 - 4ac$.

Assumption. We assume that the corresponding real quadratic form $f_{\mathbb{R}}$ is positive definite. Equivalently, $f(X,Y) > 0$ unless $(X,Y) = (0,0)$. Also equivalently, $D_f < 0$ and $a, c > 0$.

From now on, *form* means 'positive definite integral (binary) quadratic form'.

Recall 2.7.3. We say $f \sim g \iff$ related by an invertible integral change of variables w/ det $= 1$. Concretely, $f(\alpha X + \beta Y, \delta X + \gamma Y) = g(X,Y)$ for some

$$\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Remark 2.7.4. $f \sim g \implies D_f = D_g$ but the converse does not hold. In fact, we have the following chain of implications

$$f \sim g \implies f \simeq g \implies f_{\mathbb{Z}_p} \simeq g_{\mathbb{Z}_p} \forall p \implies f_{\mathbb{Q}} \simeq g_{\mathbb{Q}} \text{ and } D_f = D_g$$

and none of the above can be reversed in general.

For $D < 0$, we will be interested in studying the set

$$X_D := \{\text{strict equiv. classes of forms } f \text{ w/ } D_f = D\}.$$

Definition 2.7.5. When $f_{\mathbb{Z}_p} \simeq g_{\mathbb{Z}_p}$ for all p, we say f and g are in the same **genus**. For more than two variables, the discriminant is too coarse an invariant to be super useful, so instead one prefers to think in terms of forms of the same genus.

Question 2.7.6. *For which D is X_D nonempty?*

Answer. Note we need $D = b^2 - 4ac$ for some a, b, c, so $D \equiv b^2 \pmod 4$ so $D \equiv 0, 1 \pmod 4$. Conversely, if $D \equiv 0 \pmod 4$, may use $f = X^2 - \frac{D}{4}Y^2$ has $D_f = D$ (remember $D < 0$). If $D \equiv 1 \pmod 4$, then $f = X^2 + XY + \frac{1-D}{4}Y^2$ has $D_f = D$.

The forms given in the answer above are called the **principal forms of discriminant** D.

Question 2.7.7. *Why is it natural to group forms by D?*

Here's one answer

Theorem 2.7.8. *Let $D < 0$ w/ $D \equiv 0, 1 \pmod 4$. Let $p > 2$ be prime. Then, p can be represented by some form of discriminant D if and only if $\left(\frac{D}{p}\right) = 1$, i.e. D is a square mod p.*

Proof. ($\Longrightarrow$) Assume $p = aX^2 + bXY + cY^2$. Looking at p-adic valuations, *not* both $X, Y \equiv 0 \pmod p$. Thus, $(\overline{X}, \overline{Y}) \neq (0, 0) \in \mathbb{F}_p^2$. Extend $(\overline{X}, \overline{Y})$ to a basis of $\mathbb{F}_p^{\oplus 2}$ and calculate $D \pmod p$ in this basis. The matrix will look like $\begin{pmatrix} 0 & b \\ b & c \end{pmatrix}$ so $b^2 \equiv D \pmod p$, so D is a square mod p.

($\Longleftarrow$) If D is a square mod p, then it's a square mod $4p$ since p is odd (and D is a square mod 4 always). Hence, can write $D = b^2 + 4p(-c)$, so $D = D_f$ where $f = pX^2 + bXY + cY^2$. ■

Remark 2.7.9. The equation $\left(\frac{D}{p}\right) = +1$ can be rewritten as a congruence condition on $p \pmod D$ by Quadratic reciprocity.

Example. Say $D = -4 = D_{X^2+Y^2}$. Then,

$$\left(\frac{-4}{p}\right) = +1 \iff p \equiv 1 \pmod 4.$$

Corollary 2.7.10. *If $\#X_D = 1$, then if f is any form of discriminant D, we have that p is represented by $f \iff \left(\frac{D}{p}\right) = +1 \iff$ some congruence condition on p holds.*

(Above holds even replacing strict equivalence w/ regular equivalence)

Here's the first big thing we want to prove.

Theorem 2.7.11. *For all $D < 0$, X_D is finite.*

It's cardinality will be denoted h_D and called the **class number** of D. In fact, given D, one can explicitly find finitely many forms $f_1, \ldots, f_{h_D}$ representing all strict equiv classes of forms of disc D.

The basic idea is to try and make a and b as small as possible. We'll do this using 2 kinds of changes of variables

(1) $(X, Y) \mapsto (Y, -X)$, i.e. $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. This transforms

$$\langle a, b, c \rangle \mapsto \langle c, -b, a \rangle.$$

(2) $(X, Y) \mapsto (X + kY, Y)$, i.e. $\begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^k$ with $k \in \mathbb{Z}$. This sends

$$\langle a, b, c \rangle \mapsto \langle a, b + 2ak, c' \rangle$$

(the exact value of c' is not important to us).

Definition 2.7.12. A form $\langle a, b, c\rangle$ is **reduced** if

$$|b| \leq a \leq c.$$

Moreover, if $|b| = a$ or $a = c$, then we require $b \geq 0$.

Theorem 2.7.13 (Gauss, Disquisitiones Arithmeticae)**.** *Every form is strictly equivalent to a unique reduced form.*

According to Tate, if you read Gauss' first proof of quadratic reciprocity in here, then it is essentially the same as Tate's calculation of $K_2(\mathbb{Q})$ and deduction of Hilbert and quadratic reciprocity from it

Proof. Let's first do existence, $f \sim \langle a, b, c\rangle$ where we've chosen a representative for which $a \geq 0$ is minimal. First note that $c \geq a$ (otherwise, can use first move to swap them). Then use the second move to make sure $|b| \leq a$ (can force $-a < b \leq a$). If $|b| = a$, then $a = b$ (look at parenthetical) so $b \geq 0$. If $a = c$, can use first move (swap a, c and negate b) to ensure $b \geq 0$. This finishes existence.

Now uniqueness. We need to show no two reduced forms can be strictly equivalent. The key claim is that if f is reduced, then a is the least positive value of f. Once you know this, show that when the a's are the same, any move between them has to be a move of type 2, and then show you must have $k = 0$. ■

Remark 2.7.14. Given f, how do you find $f' \sim f$ with f' reduced? Either make a smaller by a move of type 1 or make b smaller by a move of type 2.

Fact. The matrices $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ generate $\mathrm{SL}_2(\mathbb{Z})$.

Corollary 2.7.15. *X_D is finite.*

Proof. The set of reduced f with $D_f = D$ is finite. Any such $f = \langle a, b, c\rangle$ satisfies

$$|b| \leq a \leq c \text{ and } |D| = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2,$$

so you must have $|b| \leq a \leq \sqrt{|D|/3}$. Hence, there are only finitely many possible values for (a, b). Given (a, b), you can solve for c, so we win. ■

Corollary 2.7.16. *If $f_1, \ldots, f_h$ is the list of reduced forms of discriminant D, then $h = h_D$.*

Example ($D = -4$)**.** We know $0 < a \leq \sqrt{4/3}$ so $a = 1$. Also $|b| \leq a$, so $b \in \{-1, 0, 1\}$. Actually, $b \in \{0, 1\}$ by the border case condition. At the same time, $b^2 - 4c = -4$, so $b^2 \equiv 0 \pmod 4$, so b is even. Hence, we must have $b = 0$. So the only reduced form of discriminant -4 is $\langle 1, 0, 1\rangle$, i.e. $f = X^2 + Y^2$.

Remark 2.7.17. The forms

$$X^2 - \frac{D}{4}Y^2 \text{ and } X^2 + XY + \frac{1-D}{4}Y^2$$

from before are reduced.

Remark 2.7.18. $h_D = 1$ is rare. In fact, there are only 9 square-free values of D for which this holds, $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$ (theorem of Heegner).

Not quite right as stated. Issue is difference between d and $D = \mathrm{disc}(\mathbb{Q}(\sqrt{d}))$

2.8 Lecture 13 (7/28): Ideal Class Group

2.8.1 Last time

Studied strict equivalence classes of integral, positive-definite binary quadratic forms of fixed discriminant $D \equiv 0, 1 \pmod 4$. We saw that the set of strict equivalence classes is finite (using reduction theory).

Today we'll do something a little different. We'll give a different perspective on this finite set essentially by linearizing the problem. We'll relate binary quadratic forms over $\mathbb{Z}$ to certain linear data over a ring $\mathscr{O}_F$ attached to a quadratic extension $F = \mathbb{Q}(\sqrt{D})$ of $\mathbb{Q}$.

Warning 2.8.1. What we'll do is very specific to the case at hand, degree 2 forms in 2 variables over $\mathbb{Z}$.

Assumption. In order for things to work out especially nicely, we'll assume from now on that D is a **fundamental discriminant**, i.e. if $D \equiv 0 \pmod 4$ then $D/4$ is square free, and if $D \equiv 1 \pmod 4$ then D is square free.

You can make things work outside this case with just a little more work.

Observation 2.8.2. Say $D = -4$ so we're considering $f = X^2 + Y^2$. In $\mathbb{Z}[i]$, this becomes a difference of squares

$$X^2 + Y^2 = (X + iY)(X - iY) = \alpha\overline{\alpha} = N(\alpha) \text{ for } \alpha = X + iY \in \mathbb{Z}[i].$$

Thus, numbers of the form $X^2 + Y^2$ are norms of elements of $\mathbb{Z}[i]$. In particular, we see from this that this set of numbers is closed under multiplication. Specifically, one sees that (assuming I did the math right)

$$(x^2 + y^2)(z^2 + w^2) = (xz - yw)^2 + (yz + xw)^2.$$

Slogan. Binary quadratic forms arise from norm functions.

2.8.2 Rings of Integers

Let $D < 0$ be a fundamental discriminant, and let $K = \mathbb{Q}(\sqrt{D}) = \left\{a + b\sqrt{D} : a, b \in \mathbb{Q}\right\}$. We would first like a subring $\mathscr{O}_K \subset K$ analogous to $\mathbb{Z} \subset \mathbb{Q}$.

Theorem 2.8.3. *For $\alpha \in K$, TFAE:*

(1) The subring $\mathbb{Z}[\alpha] \subset K$ generated by α is f.g. as a $\mathbb{Z}$-module.

(2) α is the root of a monic polynomial with integer coefficients.

(3) The polynomial $(T - \alpha)(T - \overline{\alpha}) \in \mathbb{Q}[T]$ actually lies in $\mathbb{Z}[T]$, i.e. $\mathrm{Tr}(\alpha), \mathrm{Nm}(\alpha) \in \mathbb{Z}$ where $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$ and $\mathrm{Nm}(\alpha) = \alpha\overline{\alpha}$.

We set of α satisfying these conditions is our definition of the **ring of integers** $\mathscr{O}_K \subset K$.

Why is this a reasonable definition? Intuitively, we're trying to say α has no denominator. Think about **(1)** above. If α had a denominator, then it's powers would have worse and worse denominators and there'd be no way the subring it generated would be finite over $\mathbb{Z}$.

Exercise. Explicitly describe $\mathscr{O}_K$. Show that it is a free $\mathbb{Z}$-module of rank 2 w/ generators

(1) $1, \sqrt{D}/2$ if $D \equiv 0 \pmod 4$

(2) $1, (1-\sqrt{D})/2$ if $D \equiv 1 \pmod 4$

Remark 2.8.4. Say we have $\alpha \in \mathscr{O}_K$. Then, depending on $D \mod 4$, we have

$$\alpha = X + \frac{\sqrt{D}}{2}Y \text{ or } \alpha = X + \frac{1-\sqrt{D}}{2}Y$$

with $X, Y \in \mathbb{Z}$. Observe that

$$N(\alpha) = X^2 - \frac{D}{4}Y^2 \text{ or } X^2 + XY + \frac{1-D}{4}Y^2$$

exactly gives our fundamental forms of discriminant D.

What about all the other ones? Before answer this, a couple of prelims

2.8.3 Some prelimes

About $N : \mathscr{O}_K \to \mathbb{Z}$ We start by briefly discussing the norm map.

Lemma 2.8.5. *Let $\alpha \in \mathscr{O}_K$. Then (recall $\mathscr{O}_K \simeq \mathbb{Z}^{\oplus 2}$ as $\mathbb{Z}$-modules),*

$$N(\alpha) = \alpha\overline{\alpha} = \det\left((-)\cdot\alpha : \mathscr{O}_K \to \mathscr{O}_K\right) = \#\mathscr{O}_K/\alpha\mathscr{O}_K$$

(Need $\alpha \neq 0$ for last equality).

(first second equality, the characteristic poly of the multiplication map is the minimal polynomial of α. For the last equality, use structure theorem for modules over PID to assume map is given by a diagonal matrix)

Example. Suppose $\alpha = n \in \mathbb{Z} \subset \mathscr{O}_K$. Then, $N(n) = n\overline{n} = nn = n^2$. Similarly, the multiplication by n map $(-)\cdot n : \mathscr{O}_K \to \mathscr{O}_K$ is diagonal w/ entries (n, n), so has determinant $\det\begin{pmatrix} n & \\ & n \end{pmatrix} = n^2$. Finally, $\mathscr{O}_K/n\mathscr{O}_K \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ has size n^2.

Corollary 2.8.6. *If $I \subset \mathscr{O}_K$ is a nonzero ideal (i.e. and $\mathscr{O}_K$-submodule), then $\#\mathscr{O}_K/I \subset \infty$.*

We can extend this norm map to ideals.

Definition 2.8.7. If $I \neq 0$ is an ideal in $\mathscr{O}_K$, then $N(I) := \#(\mathscr{O}_K/I)$.

Fact. $N(IJ) = N(I)N(J)$

Basis-free approach to strict eq of BQF's Say $f(X, Y) = aX^2 + bXY + cY^2$ is a binary quadratic form. We can view it as an abstract quadratic form $f : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$, i.e. $f(\lambda m) = \lambda^2 f(m)$ and $f(m+n) - f(m) - f(n)$ bilinear for $m, n \in \mathbb{Z} \oplus \mathbb{Z}$. Now that we're in this abstract setting, might as well just write $f : M \to \mathbb{Z}$ where M is some free $\mathbb{Z}$-module of rank 2.

Remark 2.8.8. Usual equivalence (using $\mathrm{GL}_2(\mathbb{Z})$) of binary quadratic forms now becomes: $f : M \to \mathbb{Z}$ and $f' : M' \to \mathbb{Z}$ are isomorphic if there's an iso $\alpha : M \to M'$ so that

$$\begin{tikzcd}
M \arrow[rr, "\alpha"] \arrow[dr, "f"'] & & M' \arrow[dl, "f'"] \\
& \mathbb{Z} &
\end{tikzcd}$$

commutes.

To get strict equivalence, we'll consider *oriented*[20] free $\mathbb{Z}$-modules of rank 2 equipped w/ a quadratic form.

Now, to every BQF $f(X,Y) = aX^2 + bXY = cY^2$, there is an oriented free $\mathbb{Z}$-module of rank 2 w/ quadratic form. Strict equivalences of BQF's exactly match up with oriented isomorphisms of these guys. In fancy language, this gives an equivalence of groupoids.

To get from an abstract oriented free $\mathbb{Z}$-module of rank 2 equipped w/ a quadratic form to a concrete binary quadratic form, just choose a basis (preferably one that's positively oriented).

Example. Consider $N : \mathscr{O}_K \to \mathbb{Z}$ the norm map. We can orient this by

(1) standard orientation on $\mathbb{C}$ if $D \equiv 0 \pmod 4$

(2) opposite orientation if $D \equiv 1 \pmod 4$

These correspond to our principal forms

2.8.4 BQFs and Class groups

Definition 2.8.9. Let $I \subset \mathscr{O}_K$ be a nonzero ideal. Define

$$\begin{aligned} f : \quad I &\longrightarrow \quad \mathbb{Z} \\ \alpha &\longmapsto \frac{N(\alpha)}{N(I)} \in \mathbb{Z} \end{aligned}.$$

Why is this an integer? Recall $N(\alpha) = \#\mathscr{O}_K/\alpha\mathscr{O}_K$ and $N(I) = \#\mathscr{O}_K/I$. Since $\alpha \in I$, $\mathscr{O}_K/\alpha\mathscr{O}_K \twoheadrightarrow \mathscr{O}_K/I$, so $f(\alpha) = \#I/\alpha\mathscr{O}_K \in \mathbb{Z}$.

Give I the orientation it inherits from $\mathscr{O}_K$, i.e.

(1) counterclockwise in $\mathbb{C}$ if $D \equiv 0 \pmod 4$

(2) the opposite if $D \equiv 1 \pmod 4$

Theorem 2.8.10.

(1) *f is a quadratic form of discriminant D.*

(2) *Every quadratic form of discriminant D is strictly equivalent to $f_I : I \to \mathbb{Z}$ for some ideal I.*

(3) *For $\mathbb{Z}$-module iso $\varphi : I \xrightarrow{\sim} J$, TFAE*

- ***(a)*** *φ is an iso of oriented quadratic forms*

$$(I, f_I) \xrightarrow{\sim} (J, f_J)$$

- ***(b)*** *φ is an $\mathscr{O}_K$-linear iso*

- ***(c)*** *There exists $\alpha \in K$ s.t. φ is given by multiplication by α.*

[20] i.e. a choice of "positive" basis of $\bigwedge^2 M$ ($2 = \operatorname{rank} M$)

2.9 Lecture 14 (7/29)

Note 6. 5 minutes late (missed first page)

Sounds like still recapping stuff from yesterday, so if you want a reminder, just scroll up...

Today we want to prove the theorem from the end of last time.

Theorem 2.9.1. *Let $F = \mathbb{Q}(\sqrt{D})$ with D a fundamental discriminant.*

(1) *f_I is a positive definite binary quadratic form of discriminant D.*

(2) *Every pos. def. BQF of discriminant D is strictly equivalent to $f_I : I \to \mathbb{Z}$ for some ideal I.*

(3) *For $\mathbb{Z}$-module iso $\varphi : I \xrightarrow{\sim} J$, TFAE*

- ***(a)*** *φ is an iso of oriented quadratic forms*

$$(I, f_I) \xrightarrow{\sim} (J, f_J)$$

- ***(b)*** *φ is an $\mathscr{O}_F$-linear iso*
- ***(c)*** *There exists $\alpha \in F^\times$ s.t. φ is given by multiplication by α.*

Proof. **(1)** f_I is positive definite of discriminant D. We saw this already when $I = \mathscr{O}_F$.

Lemma 2.9.2. *If $M \simeq \mathbb{Z} \oplus \mathbb{Z}$ and $f : M \to \mathbb{Z}$ is a BQF of disc D, then for any finite index subgroup $M' \subset M$, the map $f' : M' \to \mathbb{Z}$, $f'(m) = \frac{f(m)}{[M:M']}$, is also a BQF of discriminant D.*

This lemma further breaks into two claims.

Claim 2.9.3. *If F is a BQF, then $D_{\lambda f} = \lambda^2 D_f$.*

(Multiples matrix by λ so scales determinant by λ^2)

Claim 2.9.4. *If f is a BQF and $M' \subset M$ is a finite-index subgroup, then $D_{f|_{M'}} = [M : M']^2 D_f$.*

For this one, use (e.g. from structure theorem of f.g. modules over a PID) that there exists a basis e, f of M and numbers $n, m \in \mathbb{N}$ such that ne, mf is a basis of M'. Then, $[M : M'] = nm$ and the bilinear form now has matrix $\begin{pmatrix} n^2a & nmb \\ nmc & m^2d \end{pmatrix}$ so det scaled by $(nm)^2$.

(2) Consider some $f = aX^2 + bXY + cY^2$ with $a, b, c \in \mathbb{Z}$ and $D = b^2 - 4ac$. Note that $b^2 \equiv 0 \pmod 4$, so $D \equiv 0 \pmod 4 \iff b$ even. In any case, we see that $(b + \sqrt{D})/2 \in \mathscr{O}_F$. Consider the $\mathbb{Z}$-submodule of $\mathscr{O}_F$ spanned by a and $(b \pm \sqrt{D})/2$, where we use $+$ if $D \equiv 0 \pmod 4$ and $-$ if $D \equiv 1 \pmod 4$. Note that these are $\mathbb{Z}$-linearly independent so they form a $\mathbb{Z}$-basis. Also note that the submodule I they generate is an ideal; just need to check that it's closed under multiplication by

$$\frac{\sqrt{D}}{2} \text{ if } D \equiv 0 \pmod 4 \text{ or } \frac{1 - \sqrt{D}}{2} \text{ if } D \equiv 1 \pmod 4.$$

This is just to get the orientations right, not super important

Now note that $N(I) = a$ since $\mathscr{O}_F$ has basis $\left\langle 1, \frac{b \pm \sqrt{D}}{2} \right\rangle$ so $\mathscr{O}_F / I \simeq \mathbb{Z}/a\mathbb{Z}$. Finally, we claim that $f = f_I$, i.e. that

$$f_I\left(Xa + Y\left(\frac{b \pm \sqrt{D}}{2}\right)\right) = aX^2 + bXY + cY^2.$$

Just compute

$$f_I\left(Xa+Y\left(\frac{b\pm\sqrt{D}}{2}\right)\right)=\frac{N\left(Xa+Y\left(\frac{b\pm\sqrt{D}}{2}\right)\right)}{a}=\frac{a^2X^2+abXY+(?)Y^2}{a}=aX^2+bXY+cY^2$$

(the ? above is annoying to compute, but we don't have to since we know the discriminant, so the answer is determined already by the first two coefficients)

(3) Say $I, J \subset \mathscr{O}_F$ are non-zero ideals w/ a $\mathbb{Z}$-linear iso $\varphi : I \xrightarrow{\sim} J$.

(**(b)** $\iff$ **(c)**) **(c)** $\implies$ **(b)** is clear. What about **(b)** $\implies$ **(c)**? We have $I \subset \mathscr{O}_F$ of finite index, so rationally we have $I_{\mathbb{Q}} = (\mathscr{O}_F)_{\mathbb{Q}} = F$, so φ rationalizes to an F-linear isomorphism $F \xrightarrow{\sim} F$, i.e. rationalizes to multiplication by some $\alpha \in F^\times$.

(**(a)** $\iff$ **(b)**, **(c)**) We start with **(c)** $\implies$ **(a)**. Write $\alpha = x/y$ with $x, y \in \mathscr{O}_F$, so we have $I \xrightarrow{\cdot\alpha} J$. We compose with multiplication by y:

$$\begin{tikzcd} I \arrow[r, "\cdot\alpha"'] \arrow[rr, bend left, "\cdot x"] & J \arrow[r, "\cdot y"'] & J' = Jy \end{tikzcd}.$$

Hence, we reduce to the case where $\alpha \in \mathscr{O}_F \setminus \{0\}$ (if x, y give oriented isos, then so does α). Note that $I \xrightarrow{\cdot\alpha} \alpha I$ preserves orientation since multiplication by any complex number does. To see that it preserves the form, observe that

$$f_{\alpha I}(\alpha x) = \frac{N(\alpha x)}{N(\alpha I)} = \frac{N(x)}{N(I)} = f_I(x)$$

using multiplicativity of the norm.

This just leaves **(a)** $\implies$ **(b)**. This is the hardest, but here's the key: given I, can single out the subring $\mathscr{O}_F \subset \mathrm{End}_{\mathbb{Z}}(I)$ intrinsically in terms of the quadratic form f_I. Why is this helpful? Say we have an (oriented) iso $\alpha : I \xrightarrow{\sim} J$ of quadratic forms. This induces an iso $\mathrm{End}_{\mathbb{Z}}(I) \simeq \mathrm{End}_{\mathbb{Z}}(J)$ via conjugation, but the key fact tells us that this must preserve the subring $\mathscr{O}_F$. Thus, α will induce an isomorphism (of rings) $\mathscr{O}_F \xrightarrow{\sim} \mathscr{O}_F$, but the only two such isos are id and complex conjugation. Hence, α is either $\mathscr{O}_F$-linear or $\mathscr{O}_F$-semilinear (i.e. $\alpha(\lambda x) = \overline{\lambda}\alpha(x)$). Only the first of these cases is orientation preserving, so we conclude that α is $\mathscr{O}_F$-linear.

How do we show this key fact?

Lemma 2.9.5. *Given $A : I \to I$ a $\mathbb{Z}$-linear map, then A is multiplication by some $\lambda \in \mathscr{O}_F$ if and only if*

(1)

$$\frac{\langle Ax, Ay\rangle}{\sqrt{f_I(Ax)f_I(Ay)}} = \frac{\langle x, y\rangle}{\sqrt{f_I(x)f_I(y)}}$$

and

(2)

$$\frac{f_I(Ax)}{f_I(x)} \in \mathbb{Z}$$

is a constant independent of x.

Note that the expression in **(1)** above is the angle between x and y, so **(1)** says that A preserves angles. Similarly, **(2)** says that it should scale norms of vectors by a constant factor. Note that, to prove this lemma, it will suffice to show that A is equal to multiplication by some λ for some $\lambda \in \mathbb{C}$ (λ root of characteristic polynomial of A then shows that it's in $\mathscr{O}_F$). Hence, we've reduced to

Claim 2.9.6. *An $\mathbb{R}$-linear map $\mathbb{C} \to \mathbb{C}$ is multiplication by some $\lambda \in \mathbb{C}$ iff it preserves angles and scales norms by a constant.*

This is easy to check.

■

Now let's see some consequences of the above theorem.

Fact. $\mathscr{O}_F$ is a Dedekind domain. We won't define this here, but know it entails

(1) Every nonzero ideal is uniquely a product of maximal ideals.

(2) An $\mathscr{O}_F$-module M is isomorphic to some nonzero ideal $\iff$ it's invertible under $\otimes_{\mathscr{O}_F}$, i.e. $\iff \exists N$ so that $M \otimes_{\mathscr{O}_F} N \simeq \mathscr{O}_F$.

Corollary 2.9.7. *There's a bijection*

$$\left\{ \begin{matrix} \textit{strict equiv classes of} \\ \textit{pos. def. BQF's of disc } D \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \textit{invertible } \mathscr{O}_F\textit{-modules} \\ \textit{up to isomorphism} \end{matrix} \right\} \simeq \left\{ \begin{matrix} \textit{nonzero ideals} \\ \textit{up to } \cdot\alpha, \alpha \in F^\times \end{matrix} \right\}$$

Note that the middle thing above is the Picard group $\operatorname{Pic}(\mathscr{O}_F)$ *and the one on the right is the ideal class group* $\operatorname{Cl}(\mathscr{O}_F)$.

In particular, there's a group structure on the set of strict equiv classes of pos. def binary quadratic forms of fixed discriminant D.

Remark 2.9.8. In above bijection, we say that isomorphisms line up, so also automorphisms line up. In particular, these SO_f's will be automorphisms of invertible modules. The automorphisms of invertible modules are the same as automorphisms of the ring, i.e. all multiplication by a unit, so $\mathrm{SO}_f \simeq \mathscr{O}_F^\times$.

2.10 Lecture 15 (7/30): Dirichlet's class number formula

2.10.1 Loose ends from last time

Say $D < 0$ is a fundamental discriminant, and say $K = F = \mathbb{Q}(\sqrt{D})$. We arrived at a bijection

$$\left\{ \begin{matrix} \text{strict eq. classes of} \\ \text{pos. def. BQD of disc } D \end{matrix} \right\} \longleftrightarrow \{\text{nonzero ideals } I \subset \mathscr{O}_F\}_{/\sim}$$

where ideals $I \sim J$ iff there exists $\alpha \in F^\times$ s.t. $\alpha I = J$. In fact, this bijection was an equivalence of groupoids so gives

$$\mathrm{SO}_f(\mathbb{Z}) \simeq \mathrm{Aut}_{\mathscr{O}_K}(I) = \mathrm{Aut}_{\mathscr{O}_K}(\mathscr{O}_K) = \mathscr{O}_K^\times = \mu_K = \begin{cases} \{\pm 1\} & \text{if } D \neq -3, -4 \\ \mu_6 & \text{if } D = -3 \\ \mu_4 & \text{if } D = -4 \end{cases}$$

(above, μ_n is group of nth roots of unity).

A consequence of this is that the set of {strict equivalence classes of positive definite binary quadratic froms of discriminant D} has an abelian group structure. This helps explain some things...

Question 2.10.1. *Given $f, g > 0$ BQF of disc D, when is $f \simeq g$ (i.e.* GL_2*-equivalent)?*

Answer (exercise)**.** iff either $[f] = [g] \in \mathrm{Cl}(\mathscr{O}_F)$ (i.e. they're strictly equivalent) or $[f] = ([g])^{-1}$ in $\mathrm{Cl}(\mathscr{O}_F)$ (i.e. represented by conjugate ideals).

Warning 2.10.2. The equivalence relation $[f] \sim [f]^{-1}$ does not come from a normal subgroup, so the set of GL_2-equivalence classes does not have a natural group structure.

Question 2.10.3. *Given $f, g > 0$ BQF of disc D, when are f and g in the same genus (i.e. when $f_{\mathbb{Z}_p} \simeq g_{\mathbb{Z}_p}$ for all p)?*

Answer (difficult)**.** iff $[f] = [g] \cdot x^2$ for some $x \in \mathrm{Cl}(\mathscr{O}_F)$. Hence, the "genus class group" is simply $\mathrm{Cl}(\mathscr{O}_K)/2\,\mathrm{Cl}(\mathscr{O}_K)$.

This sort of genus classification better generalizes to higher forms.

2.10.2 Dirichlet's class number formula

To keep things simple, take p a prime $\equiv 3 \pmod 4$ and let $D = -p$.

Theorem 2.10.4 (**Dirichlet's class number formula**)**.** *Let $h_{-p} := \#\,\mathrm{Cl}(\mathscr{O}_{\mathbb{Q}(\sqrt{-p})})$ and let*

$$\mu_{-p} = \#\textit{roots of unity in } \mathbb{Q}(\sqrt{-p}) = \begin{cases} 2 & \textit{if } p \neq 3 \\ 6 & \textit{if } p = 3. \end{cases}$$

Then,

$$\frac{h_{-p}}{\mu_{-p}} = -\frac{1}{2p} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \cdot k.$$

Remark 2.10.5. It's not obvious that the RHS above lives in $\frac{1}{\mu_p}\mathbb{Z}$ or that it's positive, but both of these must be true given this formula.

Remark 2.10.6. h_{-p}/μ_{-p} is the "groupoid cardinality" of the ideal class groupoid. This is the groupoid (category) whose objects are ideals and whose morphisms (isomorphisms) are of the form $\cdot\alpha : I \xrightarrow{\sim} J$ with $\alpha \in F^\times$. In general, the **groupoid cardinality** of a groupoid $\mathcal{C}$ is

$$\#\mathcal{C} := \sum_{x \in \mathcal{C}/\simeq} \frac{1}{\#\,\mathrm{Aut}_{\mathcal{C}}(x)}.$$

Where does Dirichlet's formula come from? One needs to combine three ingredients related to the two below analytic functions.

- We start with the **Dedekind zeta function**

  $$\zeta_F(s) := \sum_{I \subset \mathscr{O}_F} \frac{1}{N(I)^s}$$

  (sum over nonzero ideals).

- We also need the **Dirichlet L-function** attached to a character $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ (e.g. $\chi = \left(\frac{\cdot}{p}\right)$) defined by

  $$L(s,\chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}.$$

Both of the above converge absolutely for $s > 1$.

The ingredients are

(1) $\zeta_F(s) = \zeta(s) L(s,\chi)$

This follows from comparing Euler products (use splitting behavior of primes in quadratic extensions).

(2) $\lim\limits_{s \to 1^+} (s-1)\zeta(s) = 1$. For $F = \mathbb{Q}(\sqrt{-p})$, one gets

$$\lim_{s \to 1^+} (s-1)\zeta_F(s) = \frac{2\pi}{\sqrt{p}} \cdot \frac{h_{-p}}{\mu_{-p}}.$$

(3) (exercise)

$$\lim_{s \to 1^+} L(s,\chi) = -\frac{\pi}{p^{3/2}} \sum_{k=1}^{p-1} \chi(k) k.$$

This series $L(s,\chi)$ actually is (conditionally) convergent as $s = 1$, so one could write the above as $L(1,\chi) = \mathit{blah}$.

Combining these three ingredients says that

$$\frac{2\pi}{\sqrt{p}} \frac{h_{-p}}{\mu_{-p}} = \lim_{s \to 1^+} (s-1)\zeta_F(s) = \lim_{s \to 1^+} (s-1)\zeta(s) L(s,\chi) = L(1,\chi) \lim_{s \to 1^+} (s-1)\zeta(s) = -\frac{\pi}{p^{3/2}} \sum_{k=1}^{p-1} \chi(k) k,$$

so one now rearranges to win.

Ingredient **(3)** is on the problem set, so let's say something about the other two.

Ingredient (1) We start by recalling the Euler product of the Riemann-zeta function

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_p \left(\frac{1}{1 - p^{-s}} \right).$$

This is essentially a consequence of unique prime factorization. Since F has unique factorization of ideals into prime ideals, one analogously gets an Euler product

$$\zeta_F(s) = \sum_{I \neq 0} N(I)^{-s} = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

Each maximal ideal $\mathfrak{p}$ contains a unique rational prime p, so we can regroup this product according to which rational prime each $\mathfrak{p}$ contains.

Recall 2.10.7 (from pset)**.** Given a rational prime p, we say

- p splits $\iff (p) = \mathfrak{p}_1\mathfrak{p}_2 \iff \chi(p) = +1$
- p is inert $\iff (p)$ is a prime ideal in $\mathscr{O}_F \iff \chi(p) = -1$
- p ramifies $\iff (p) = \mathfrak{p}^2 \iff \chi(p) = 0$

So if p splits, we get two p-Euler factors

$$\frac{1}{1 - N(\mathfrak{p}_1)^{-s}} \cdot \frac{1}{1 - N(\mathfrak{p}_2)^{-s}} = \frac{1}{1 - p^{-s}} \frac{1}{1 - p^{-s}}.$$

If p is inert, then $N(p) = p^2$, so get

$$\frac{1}{1 - N(p)^{-s}} = \frac{1}{1 - p^{-2s}} = \frac{1}{1 - p^{-s}} \frac{1}{1 + p^{-s}}.$$

if p is ramified, then $N(\mathfrak{p}) = p$, so get

$$\frac{1}{1 - N(\mathfrak{p})^{-s}} = \frac{1}{1 - p^{-s}} \cdot 1.$$

In every case, we get the Euler factor from Riemann zeta along with a second term. In fact, one sees that

$$\zeta_F(s) = \zeta(s) \prod_p \frac{1}{1 - \chi(p)p^{-s}} = \zeta(s)L(s, \chi).$$

This is ingredient **(1)**.

Ingredient (2) We want to show that

$$\lim_{s \to 1^+} (s-1)\zeta_F(s) = \frac{2\pi}{\sqrt{p}} \cdot \frac{h_{-p}}{\mu_{-p}}.$$

We won't give full details, but hopefully can show where all these factors come from. The product formula/ingredient **(1)** came from a multiplicatively analysis of the zeta function. This will instead come from an additive analysis of it.

We partition ideals into their ideal classes. Let $I_1, I_2, \ldots, I_{h_{-p}}$ be representatives of the ideal class group. Hence,

$$\zeta_F(s) = \sum_{I \neq 0} \frac{1}{N(I)^s} = \sum_{i=1}^{h_{-p}} \left(\sum_{[I]=[I_i]} \frac{1}{N(I)^s} \right).$$

Note that it suffices to show all of these inner sums have a pole at $s = 1$ of residue $2\pi/(\mu_p\sqrt{p})$.

To keep life easy, we'll only explain what's going on for the principal ideal class $\mathscr{O}_F = I_1$, i.e. we'll show

$$\lim_{s\to 1^+}(s-1)\sum_{I=(\alpha):\alpha\in\mathscr{O}_K\setminus\{0\}}\frac{1}{N(\alpha)^s} = \frac{2\pi}{\mu_{-p}\sqrt{p}}.$$

Note that a generator of an ideal is only determined up to multiplication by units, so we can equivalently show that

$$\lim_{s\to 1^+}(s-1)\sum_{\alpha\in\mathscr{O}_K\setminus\{0\}}\frac{1}{N(\alpha)^s} = \frac{2\pi}{\sqrt{p}}.$$

At this point, we don't really care that $\mathscr{O}_K$ is the ring of integers of an imaginary quadratic field; we really only care that it's a lattice in the complex numbers.

Proposition 2.10.8. *For any full lattice $L \subset \mathbb{C}$ (i.e. $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ with ω_1, ω_2 linearly independent over $\mathbb{R}$),*

$$\lim_{s\to 1^+}(s-1)\sum_{\alpha\in L\setminus\{0\}}\frac{1}{N(\alpha)^s} = \frac{2\pi}{\mathrm{vol}(L)},$$

where $\mathrm{vol}(L)$ is the area of a fundamental parallelogram.

This can be proved very similarly to how one shows

$$\lim_{s\to 1^+}(s-1)\zeta(s) = 1.$$

The key claim is that you can approximate this sum by an integral, i.e. (something like)

$$\mathrm{vol}(L)\sum_{\alpha\in L\setminus\{0\}}\frac{1}{N(\alpha)^s} \sim \int_{\alpha\in\mathbb{C}}\frac{1}{N(\alpha)^s}\mathrm{d}x\mathrm{d}y.$$

Then you can actually compute this integral by integrating over circles $N(\alpha) = r$. The circles give a π factor and you just work things out and see the answer.

3 List of Marginal Comments

Index