Complete discrete valuation rings and local fields. (cf. Chap I of [**1**]) Let A be a commutative ring. These are equivalent.

a. A is a noetherian local ring and its maximal ideal is generated by a single non-nilpotent element.

b. A is a noetherian, integrally closed, integral domain possessing a unique ($\neq 0$) prime ideal.

c. A is a principal ideal domain possessing a unique ($\neq 0$) prime ideal.

d. A is an integral domain; its field of fractions K possesses a "discrete valuation homomorphism" , i.e., a surjective homomorphism

$$v : K^* \to \mathbf{Z}$$

such that if we make the convention that $v(0)$, the valuation of 0, is equal to $+\infty$ we have $v(x+y) \geq \min(v(x), v(y))$ for all $x, y \in K$; and moreover, A is the subset of elements of K with non-negative valuation.

e. A possesses a nonnilpotent element $\pi \in A$ such that every nonzero element $a \in A$ may be written *uniquely* as

$$a = u\pi^n,$$

where $u \in A^*$ is a unit of A, and $n \geq 0$.

f. (Definition) A is a discrete valuation ring, DVR for short.

Some notes: The field of fractions, K, together with its valuation homomorphism, is called a **discrete valued field**. The quotient field $k := A/m_A = A/\pi A$ is called the residue field of A, also "of the discrete valued field K". Any element $\pi \in K$ satisfying the properties of **e.** is called a *uniformizer* or a *local parameter* for the discrete valued field K and is a generator of m_A, the maximal ideal of A. The uniformizers are precisely the set of elements with valuation equal to 1. This terminology is suggested by the geometric examples of DVR's, i.e., where A is the local ring at a smooth k-rational point x of an algebraic curve X over a field k, in which case a "local parameter" in the above sense is nothing more than a rational function on X which provides a local parameter for X about the point x.

We will deal mainly with *complete* discrete valuation rings. The process of completion of a DVR can be thought of either "from the perspective of A", or "from the perspective of K".

For the former, we consider the topology on A where a sub-base of open ideals is given by the powers of the maximal ideal (or, for that matter, we could just say: by all non-zero ideals) and form the completion

$$\hat{A} := \text{proj. lim. } A/m_A^n,$$

and view $\hat{A}$ as a topological ring. One notes that the natural ring homomorphism $A \to \hat{A}$ is an imbedding since $\cap_{n=1}^{\infty} m_A^n = \{0\}$, and one proves that $\hat{A}$ is again a DVR, and that the

imbedding $A \to \hat{A}$ extends to an imbedding $K \to \hat{K}$ of the respective fields of fractions, which preserve discrete valuation homomorphisms.

For the latter, we just complete the discrete valued field K via a metric derived from the valuation homomorphism v ($\|x\| = \exp(v(x))$ will do) imbedding K in its completion $K \to \hat{K}$, note that the valuation v extends to a valuation $\hat{v}$ on $\hat{K}$, and define the DVR $\hat{A}$ to be the elements of $\hat{K}$ with nonnegative valuation, as in **d.** above.

"Non-archimedean" local fields of characteristic 0. We will be principally interested in complete DVR's $A = \hat{A}$ with field of fractions $K = \hat{K}$ and residue field k, where K is of characteristic 0 and k is finite. The latter condition is equivalent to requiring that the complete DVR A is compact, or that the complete discrete valued field K is locally compact. The topology on K determines its valuation homomorphism, for the elements of A are precisely those elements which are "power-bounded" (i.e., the set of all of their powers are contained in a compact subset of K) and, for example, the maximal ideal m_A is the subset of K consisting of those elements whose powers converge to 0. In our discussion below we will use the term **local field** to refer to a complete discrete valued field K of characteristic 0 with finite residue field k (giving short shrift to the local fields $\mathbf{R}$, $\mathbf{C}$, and fields of positive characteristic).

How do we get local fields? First, an arbitrary finite extension L/K of a local field is again a local field (cf. Prop. 3 of section 2 of Chap I of [**1**]) and the topology on L is simply the topology it inherits as a finite dimensional vector space of the complete field K. Given a prime number p, any local field (of our sort) with residue field of characteristic p is a finite extension field of the field of p-adic numbers,$\mathbf{Q}_p$, and conversely, it foollows from the above that any finite field extension $K/\mathbf{Q}_p$ is a local field. But also, you can start with a number field $F/\mathbf{Q}$, consider its ring of integers $\mathcal{O}_F \subset F$ (i.e., the integral closure of $\mathbf{Z}$ in F), choose a prime ideal $P \subset \mathcal{O}_F$, and form the complete DVR

$$\mathcal{O}_{F,P} := \text{proj. lim. } \mathcal{O}_F/P^n,$$

denoting its (discrete valued) field of fractions F_P. Any of our local fields comes from such a construction (**Exercise:** show this, as an application of "Krasner's principle").

Galois extensions of local fields. Let L/K be a finite Galois extension of local fields with Galois group G. Denote by $A \subset K$ and $B \subset L$ the associated discrete valuation rings, and $\ell = B/m_B$, and $k = A/m_A \subset \ell$ the respective residue fields. Let g denote the (cyclic) Galois group of the residue field extension

$$g := \text{Gal } (\ell/k).$$

We have an exact sequence (defining the subgroup $I \subset G$):

$$0 \to I \to G \to g \to 0.$$

The Galois group G stabilizes $B \subset L$ and $m_B \subset B$ and therefore induces an action on ℓ which fixes k. This gives the homomorphism $G \to g$. Will prove surjectivity by the elementary "Galois theoretic argument". The subgroup $I \subset G$, the **inertia group** of the extension L/K, consists then of the elements of G which induce the identity automorphism on ℓ. Letting $K^{\mathrm{ur}} = L^I \subset L$ be the fixed field of L we have that K^{ur}/K is the maximal unramified extension of K contained in L; the residue field of K^{ur} is ℓ and Gal (K^{ur}/K) is isomorphic to g. The extension K/K^{ur} is totally ramified. We get an exact sequence:

$$1 \to I \to G \to g \to 1.$$

We get a finer analysis of G (more specifically of the inertia subgroup $I \subset G$) by considering the "lower index" filtration:

Definition. Let $i \geq 0$. define the **i-th ramification subgroup** $G_i \subset G$ to be the set of all elements $\alpha \in G$ such that α induces the *identity* automorphism on B/m_B^{i+1}.

Note that $G_0 = I$ and by convention one sometimes puts $G_{-1} := G$. We have defined a decreasing filtration of normal subgroups of G:

$$\ldots G_{n+1} \subset G_n \ldots G_1 \subset G_0 = I \subset G.$$

Will explain the canonical inclusion $G_0/G_1 \subset k^*$ and the noncanonical inclusions $G_i/G_{i+1} \subset k^+$ for $i > 0$.

Denote, provisionally, $P := G_1$, and $\Delta := I/P = G_0/G_1 \subset \ell^*$, the **wild** and **tame** parts of the inertia group, and note that Λ is a finite cyclic group of order dividing $q-1$ where $q = \mathrm{card}\ (\ell)$, while P is a pro-p-group, for $p =$ the characteristic of ℓ. Put $K^{tame} := L^P$, the **maximally tamely ramified subextension of** L/K and denote, provisionally, $T := G/P = \mathrm{Gal}\ (K^{tame}/K)$.

We have the exact sequences:

$$1 \to P \to I \to \Delta \to 1,$$

and

$$1 \to \Delta \to T \to g \to 1.$$

Since Δ is a cyclic group of order prime to the order of P, there is a (noncanonical) lifting $\Delta \to I$ expressing I as a semi-direct product of Δ by P.

"Functorial" construction of unramified extensions. (cf. sections 5,6 of Chap I of [**1**]). Let p be a prime number, and k a finite field of characteristic p, recall the Witt vector construction which associates to any perfect ring R in characteristic p, its ring $W(R)$ of "Witt vectors".

$$R \mapsto W(R) := \{(a_0, a_1, a_2, \ldots) \mid a_j \in R\ \},$$

with "universal $p^{-\infty}$-polynomials" (cf. loc. cit.) defining a ring structure on $W(R)$.

When $k = \mathbf{F}_p$, $W(\mathbf{F}_p)$ is canonically isomorphic to the ring $\mathbf{Z}_p$ of p-adic integers, and the correspondence is simply: $a = \{(a_0, a_1, a_2, \ldots)\} \in W(\mathbf{F}_p) \longleftrightarrow \sum_{n=0}^{\infty} a_n p^n \in \mathbf{Z}_p$.

More generally, when k is a finite field, $W(k)$ is a complete DVR with residue field canonically isomorphic to k, the reduction map being given by $\{(a_0, a_1, a_2, \ldots)\} \mapsto a_0 \in k$. The DVR is "absolutely unramified" in the sense that $p \in W(k)$ is a uniformizer. An important property of this construction, for us, is that given any complete DVR A with field of fractions K of characteristic 0, and with finite residue field k, there is a canonical ring homomorphism $W(k) \to A$ such that composition with the projection to the residue field $A \to k$ is the canonical reduction homomorphism $W(k) \to k$ described above. This ring homomorphism is an injection, and A is a free $W(k)$-module of rank $e =$ the absolute ramification index of A. Moreover, we have that A may be obtained from $W(k)$ by the adjunction of a single element $\pi \in A$, which is a uniformizer of A satisfying an "Eisenstein equation" over $W(k)$, i.e., an equation of the form:

$$\pi^e + a_1 \pi^{e-1} + \ldots + a_e = 0,$$

where all the coefficients a_j are divisible by p in $W(k)$ and the constant term a_e is not divisible by p^2.

Projective limits of the groups of units of finite fields.

First, let us review some basic facts about profinite groups which are topologically singly generated. Let Γ be such a group (which is easily seen to be abelian). Let $\gamma \in \Gamma$ be a topological generator. Writing

$$\Gamma = \text{proj. lim. } \Gamma/N$$

where $N \subset \Gamma$ runs through all open subgroups (of finite index) in Γ, one sees that for each $N \subset \Gamma$, the element γ projects to a generator of the group G/N, and these groups are therefore all cyclic. Moreover, any projective limit of a projective system of finite cyclic groups with surjective homomorphisms, is a group Γ such as the above. We have that Γ itself is the completion of the cyclic group $< \gamma > \subset \Gamma$ with respect to the topology on $< \gamma >$ induced from Γ.

To get an example of the above, suppose we have a projective system of finite cyclic groups $\{C_n\}_{n \in \mathbf{N}}$ and such that if n a multiple of m, we have a connecting homomorphism of our projective system, $C_n \to C_m$, and suppose that these connecting homomorphisms are all surjections. Then $\Gamma :=$ proj. lim. C_n is a group such as we have been discussing, i.e., a profinite group which is topologically singly generated. If, for some prime number p, the orders of C_n are all relatively prime to p, and every number relatively prime to p divides the order of some C_n, then an application of the Chinese Remainder Theorem gives that the corresponding group Γ is isomorphic to

$$\prod_{\ell \neq p} \mathbf{Z}_\ell,$$

the product being taken over all prime numbers ℓ different from p. Now let us apply this to the following situation. Let k be a finite field of cardinality $q = p^f$ imbedded in an algebraic closure $\bar{k}$. For each $n \geq 1$, let k_n/k be the (cyclic, Galois) extension contained in $\bar{k}$. Put $w_n = |k_n^*| = q^n - 1$, and consider the projective system of finite cyclic groups $C_n := k_n^*$, with connecting homomorphisms (when n is a multiple of m) $k_n^* \to k_m^*$ given by norm mappings. Since these norm mappings (i.e., , for finite field extensions) are surjective and since the orders of the C_n's have the property described in the previous paragraph, if we put (provisionally) $\Delta_k :=$ proj. lim. k_n^*, with the projective limit compiled via the norm mappings, we have:

$$\Delta_k \approx \prod_{\ell \neq p} \mathbf{Z}_\ell,$$

and we also have a natural continuous action of the Galois group $g = \mathrm{Gal}\,(\bar{k}/k)$ on Δ_k. The reason for the symbol $\approx$ is that we do not have any canonical isomorphism between the two topological groups displayed above. Nevertheless, we can make up for this by noting that if $k \subset k' \subset \bar{k}$, then there is indeed a canonical identification $\Delta_k' \cong \Delta_k$ equivariant, in the evident sense, with actions of Galois groups. In particular, we have a canonical identification,

$$\Delta_k \cong \Delta_{\mathbf{F}_p},$$

for any finite field $k \subset \bar{\mathbf{F}}_p$. The g-module $\Delta_{\mathbf{F}_p}$ depends, evidently, on the choice of algebraic closure $\bar{\mathbf{F}}_p$, but is often denoted

$$\Delta_{\mathbf{F}_p} = \prod_{\ell \neq p} \mathbf{Z}_\ell(1),$$

the "(1)" in the notation of the right-hand side telling us that the Galois group g as it acts on the left-hand side, while the rest of the notation reminds us of the isomorphy type of $\Delta_{\mathbf{F}_p}$ as topological group. We should remember that when we adopt this notation, we have converted the group action which is written multiplicatively on the left-hand side to a group action which we write additively on the right-hand side/ For later purposes, get ready for the notation $\mathbf{Z}_\ell(1)$ for a *single* given prime $\ell \neq p$, which will refer to the projection to the ℓ-adic completion of the topological g-module $\Delta_{\mathbf{F}_p}$.

"Functorial" construction of tamely ramified extensions. Fix an algebraic closure $\bar{\mathbf{F}}_p$ of $\mathbf{F}_p$, and for a finite subfield, $k \subset \bar{\mathbf{F}}_p$, consider the absolutely unramified extension $W(k)$ of $\mathbf{Z}_p = W(\mathbf{F}_p)$. If $W(k)^*$ denotes the (topological) group of units of the ring $W(k)$, we have an exact sequence

$$0 \to 1 + pW(k) \to W(k)^* \to k^* \to 0.$$

Since the group $1+pW(k)$ (under multiplication) is a pro-p-group, and k^* is a (finite cyclic) group of order prime to p this exact sequence splits canonically; equivalently, we have a unique homomorphism $\tau : k^* \to W(k)^*$ lifting the projection homomorphism $W(k)^* \to k^*$ usually referred to as the "Teichmŭller lifting" and concretely described as follows: for

$\bar{a} \in k$, choose any lifting $a \in W(k)$ and define $\tau(\bar{a})$ to be the limit of the Cauchy sequence a^{q^n} as n tends to ∞. it follows that if $\mu(W(k))$ denotes the group of units in the complete DVR $W(k)$, i.e., the torsion subgroups of $W(k)^*$, we have $\mu(W(k)) \cong k^*$, and in particular, $W(k)$, and its field of fractions, K, contain a primitive $q-1$-st root of unity, where q is the cardinality of k.

We now are in a position to apply the classical theory of "Kummer extensions" to construct a tamely ramified, totally ramified, extension L/K (cf. Lang's Algebra). We will do this by extracting an w-th root of the uniformizer p. That is, we form the field extension $L = K[X]/(X^w - p)$ and let $\pi \in L$ denote the image of X. You check that L/K is indeed a Kummer extension, cyclic of degree w, with Galois group canonically isomorphic to $\mu(W(k)) \cong k^*$. Moreover, the ring of integers in L is given by $W(k)[\pi]$ and π is a uniformizer.

– Here draw the various field extensions and Galois groups involved –

From this we see that Gal $(L/\mathbf{Q}_p)$ is canonically isomorphic to the semi-direct product of Gal $(k/\mathbf{F}_p)$ by k^*, the action of Gal $(k/\mathbf{F}_p)$ on k^* being the natural action.

Passage to the limit with tamely ramified extensions. We let K_n denote the field of fractions of $W(\bar{\mathbf{F}}_{p^n})$, $K_\infty := \cup_{n=1}^\infty K_n$ denote the field of fractions of $W(\bar{\mathbf{F}}_p)$. Let L_n denote the tamely ramified extension of K_n we have just constructed, and $L_\infty := \cup_{n=1}^\infty L_n$ the union of them all.

– Here, again, draw the various field extensions and Galois groups involved –

From this we see that if $T :=$ Gal $(L_\infty/\mathbf{Q}_p)$, then we have an exact sequence,

$$1 \to \prod_{\ell \neq p} \mathbf{Z}_\ell(1) \to T \to g \to 1,$$

where the action of g on $\prod_{\ell \neq p} \mathbf{Z}_\ell(1)$ is the natural action and, moreover, there is a continuous lifting of g to T so that T is isomorphic to the semi-direct product of g by $\prod_{\ell \neq p} \mathbf{Z}_\ell(1)$ (with the natural action).

The structure of T : Here is a convenient "generators-and-relations" view of the profinite group T. Choose (unnaturally, of course) a topological generator τ of the group $\prod_{\ell \neq p} \mathbf{Z}_\ell(1)$, and recall that we have our canonical generator $\phi =$ "Frobenius" of the group g. We have that the pair of elements $\{\tau, \phi\}$ form a system of topological generators of T, and conjugation by ϕ on $\Delta_{\mathbf{F}_p}$ is given by the natural action, i.e., we have the formula:

$$\phi \tau \phi^{-1} = \tau^p.$$

The profinite group T may be thought of as isomorphic to the "largest" profinite group on two generators $\{\tau, \phi\}$ satisfying the single relation $\phi \tau \phi^{-1} = \tau^p$.

Exercise: Describe all continuous representations of T into $\mathrm{GL}_2(\mathbf{Z}_\ell)$ where ℓ is a prime number different from p.

Open subgroups of T : Recall that p is a prime number, and $T := \mathrm{Gal}\,(L_\infty/\mathbf{Q}_p)$ is the Galois group of L_∞, the maximal tamely ramified extension of $\mathbf{Q}_p$. Moreover, we have been studying the exact sequence

$$1 \to \prod_{\ell \neq p} \mathbf{Z}_\ell(1) \to T \to \hat{\mathbf{Z}} \to 1,$$

where here we have done the confusing thing of writing the group law of the two flanking groups in the above exact sequence "additively", and yet we will continue, of course, to think of the group law in the noncomuutative group T as being written "multiplicatively". The action of the element 1 in $\hat{\mathbf{Z}}$ on $\prod_{\ell \neq p} \mathbf{Z}_\ell(1)$ (via first lifting this element to an element $\phi \in T$, and then considering the conjugation action $x \mapsto \phi x \phi^{-1}$ is multiplication by p). The above exact sequence splits (noncanonically), and in fact, any element $\phi \in T$ which lifts $1 \in \hat{\mathbf{Z}}$ effects such a splitting. Any such element $\phi \in T$ will be called "a Frobenius element". Fix such a "Frobenius element" ϕ, and recall that T may then be described as *the* profinite group on two generators $\{\tau, \phi\}$ satisfying only the one relation

$$(*) \qquad \phi\tau\phi^{-1} = \tau^p.$$

Clearly any element of T can be uniquely represented as a product $\alpha \cdot \beta$ where α is in the closed subgroup of T generated by τ and β is in the closed subgroup of T generated by ϕ. For any pair of positive integers e, f, with e not divisible by p, consider the closed subgroup $T_{e,f} \subset T$ generated by ϕ^f and τ^e. These generators clearly satisfy the relation

$$\phi^f \cdot \tau^e \cdot \phi^{-f} \;=\; (\tau^e)^q,$$

where $q = p^f$, and $T_{e,f}$ is *the* profinite group admitting as presentation those two generators and that one relation.

Exercise: Show that the $T_{e,f}$ (for all positive integers e not divisible by p, and positive integers f) comprise *all* open subgroups of T of finite index, and the open normal subgroups of finite index are precisely those $T_{e,f}$ where e divides p^f. In case $T_{e,f}$ is normal, show that the finite group $T/T_{e,f}$ is a semi-direct product of the cyclic group $\mathbf{Z}/f\mathbf{Z}$ by a cyclic group C_e of order e, where, if we write the group law on C_e multiplicatively, the action of the generator $1 \in \mathbf{Z}/f\mathbf{Z}$ on C_e is via "raising to the $q = p^f$-th power".

The representation theory of T and its subgroups. Let, then F be a local field (an "LF", say, which will play the lowly role of a field of scalars) and V a finite dimensional vector space over F admitting a (continuous) F-linear T-action.

Claim: Given any compact group Γ acting continuously as a group of F-linear automorphisms of V, there exists an $\mathcal{O}_F$-lattice$\Omega \subset V$ which is stabilized by the action of Γ. Any such representation is equivalent (over F) to a representation given by a continuous homomorphism $\rho : \Gamma \to \mathrm{GL}_d(\mathcal{O}_F)$, where $d = \dim_F(V)$.

So, equivalently, V is equipped with a pair of operators $\tau, \phi : V \to V$ which preserve an $\mathcal{O}_F$-lattice in V, and which satisfy the formula $\phi\tau\phi^{-1} = \tau^p$. Consider the operator $\tau : V \to V$. Suppose that $v \in V$ is a (nonzero, of course) eigenvector for τ with eigenvalue $\lambda \in F$. For integers $n \geq 0$, put $v_n := \phi^{-n}(v)$ and calculate using the relation $(*)$ to find that v_n is an eigenvector for τ with eigenvalue $\lambda^{p^n} \in F$. Since we have assumed that V is finite-dimensional, τ can only have a finite number of distinct eigenvalues, giving that $\lambda^{p^n} = \lambda^{p^m}$ for some pair of integers $n \neq m$, i.e., any eigenvalue λ of τ is a $(p-1)p^\nu$-th root of unity for some ν. It follows that any eigenvalue of τ is, in fact, a $(p-1)$-st root of unity, for τ is in the closed subgroup generated by τ^{p^ν}. We have shown, therefore, that the operator τ^{p-1} is unipotent (i.e., is equal to the operator $I + N$, where I is the identity and N is a nilpotent operator on V).

Exercise: What is the analogous statement for the subgroup $T_{e,f}$?

The representation theory of the Galois groups.

Now we consider $G_{\mathbf{Q}_p} := \mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$, and recall the exact sequence

$$1 \to P \to G_{\mathbf{Q}_p} \to T \to 1.$$

If $K/\mathbf{Q}_p$ is a finite extension field, with $G_K \subset G_{\mathbf{Q}_p}$ its Galois group (equivalently: $G_K = \{g \in G_{\mathbf{Q}_p} \mid g(x) = x \text{ for all } x \in K\}$) let $I_K := I \cap G_K$, where $I \subset G_{\mathbf{Q}_p}$ is the inertia subgroup. Put $P_K := G_K \cap P$ and $T_K :=$ the image of G_K in T, so that $T_K = T_{e,f}$ where f is the absolute residue degree of K and e is the absolute tame (i.e., prime to p) ramification index of K. We will refer to the image of I_K in T_K as the **tame inertia subgroup** of T_K.

We have the exact sequences

$$1 \to P_K \to G_K \to T_K \to 1.$$

Exercise for people who know Class Field Theory. Consider the infinite-dimensional vector space $V_K := \mathrm{Hom}_{cont}(P_K, \mathbf{Q}_p)$ of continuous group-homomorphisms of P_K to the additive group of p-adic numbers, $\mathbf{Q}_p$. The natural action of T_K on P_K induces a representation of T_K on the $\mathbf{Q}_p$-vector space V_K. Can you describe this infinite-dimensional representation?

Definition. Let F be a local field (an "LF") of residual characteristic different from p, and V a finite dimensional vector space over F. Then a continuous G_K-action on V is called **semi-stable** if every element of I acts unipotently on V. It is called **potentially semi-stable** if there is a finite extension field L/K of K such that the restriction of the G_K-action on V to G_L is semi-stable.

Proposition. (Grothendieck) Every continuous G_K representation on a finite-dimensional vector space over a local field F of residual characteristic different from p is potentially semi-stable.

Proof. Let $\mathcal{O}_F$ be the ring of integers of F, and k_F its the residue field . Let ℓ be the characteristic of k_F so that by assumption we have $\ell \neq p$. Let us take the view that our representation is given by a continuous homomorphism (of locally compact groups) $\rho : G_K \to \mathrm{GL}_d(\mathcal{O}_F)$ for some positive integer d, which is legitimate, given the "Claim" above. Make a preliminary finite extension K'/K so that the image of the restriction $\rho' : G_{K'} \to \mathrm{GL}_d(\mathcal{O}_F)$ is contained in the kernel of the residual homomorphism $\mathrm{GL}_d(\mathcal{O}_F) \to \mathrm{GL}_d(k_F)$. Changing notation (from K' to K) we may simply assume, now, that the image of ρ is contained in the kernel of the residual homomorphism, which is a pro-ℓ-group. Since there are no nontrivial continuous homomorphisms of a pro-p-group to a pro-ℓ-group, the pro-p-group P_K is contained in the kernel of the homomorphism ρ; i.e., ρ is induced from a representation of T_K. But, after our discussion above, any finite-dimensional representation of T_K has the property that there is a finite field extension L/K such that the tame inertia subgroup of L in T_L acts via unipotent elements. It follows then that the restriction of ρ to G_L is semi-stable.

Putting further squeezes on the continuous representations of G_K on finite dimensional vector spaces over local fields F, where the residual characteristics of K and F are different.

Let ℓ be the residue characteristic of F, and, as always, p the residue characteristic of K. I'm running out of convenient letters for prime numbers, but let r be a prime number different from p and ℓ, and let T_ℓ denote the quotient group of T that you get when you divide by the (normal, closed) subgroup of T given by $\prod_{r\neq p,\ell} \mathbf{Z}_\ell(1)$:

$$\prod_{r\neq p,\ell} \mathbf{Z}_\ell(1) \subset \prod_{r\neq p} \mathbf{Z}_r(1) \subset T.$$

We have that T_ℓ is a semi-direct product of the profinite completion of $\mathbf{Z}$ with a chosen generator being given by the Frobenius element $\phi \in g$) by the free ℓ-adic group on one generator, $\mathbf{Z}_\ell(1)$. As before, for $K/\mathbf{Q}_p$ a finite extension, define the analogous quotient group, $T_{\ell,K}$, of G_K. The argument given in the Proposition above proves, in fact, that any continuous representation ρ of G_K on a finite-dimensional vector space over F has the property that there is a finite field extension L/K such that the restriction of ρ to G_L factors through the quotient group, $T_{\ell,L}$ and the image of the inertia group of L acts unipotently.

Galois cohomology. This is a new section, so we let: $K =$ any field, K_s/K a separable algebraic closure of K. Put $G_K := \mathrm{Gal}(K_s/K) = \lim \mathrm{Gal}(L/K)$ where the projective limit is taken over all finite Galois extensions L/K in K_s. We view G_K as a compact topological group given its profinite ("Krull) topology.

Definition. An abelian group M together with a linear G_K-action on it is called a **Galois module over** K (cf. Serre: "topological" G_K-module) if

$$M = \bigcup M^H,$$

where H runs through all open normal subgroups of G_K.

One might make the distinction here between *Galois modules* and *étale abelian sheaves* over $\mathrm{Spec}(K)$ – the categories of these being, in fact, equivalent. Given an étale abelian sheaf $\mathcal{F}$, you get a G_K module $M_{\mathcal{F}} := \mathcal{F}(K_s)$ with its natural G_K-action.

$$H^q(G_K, M) = \text{ind. lim.} H^q(G_K/H, M^H),$$

where H runs through all open normal subgroups of G_K. If we think of M as coming from an étale abelian sheaf $\mathcal{F}$ we may write these as the étale cohomology groups $H^q(\mathrm{Spec}\ K, \mathcal{F})$.

$$H^0(G_K, M) = M^{G_K} = \mathrm{Hom}_{G_K}(\mathbf{Z}, M),$$

and, of course, if $M = M_{\mathcal{F}}$ we can think of this as $\mathcal{F}(K)$.

Example. When $G = G_k = \hat{\mathbf{Z}}$: e.g., k finite. $\phi \in G_k$ a topological generator corresponding to $1 \in \hat{\mathbf{Z}}$. run through the theory– G_k-module M is an abelian group M with an automorphism each of whose orbits are finite. We have

$$0 \to M^G \to M \to M \to M_G \to 0.$$

Gives cohomology. Snake lemma. If M is finite, then Euler characteristic is 0. Cup-product. With the natural mappings

$$M^G \otimes N^G \to (M \otimes N)^G,$$
$$M^G \otimes N_G \to (M \otimes N)_G.$$
$$H^1(G_k, \mathbf{Q}/\mathbf{Z}) = \mathbf{Q}/\mathbf{Z}.$$

This gives duality: If M, N are pontriagin dual, i.e., we have a perfect pairing

$$M \otimes N \to \mathbf{Q}/\mathbf{Z},$$

then we have a perfect pairing.

$$H^i(G, M) \otimes H^{1-i}(G, N) \to H^1(G, \mathbf{Q}/\mathbf{Z}) = \mathbf{Q}/\mathbf{Z}.$$

Low-dimensional cohomology of groups. Let G be a profinite topological group, and M a discrete G-module. We have

$$H^j(G; M) = \varinjlim H^j(G/H; M^H) = \varinjlim \mathrm{Ext}^j_{\mathbf{Z}[G/H]}(\mathbf{Z}, M^H),$$

where $H \subset G$ runs through all open subgroups (of finite index) in G.

Dimension 0 : We have $H^0(G;M) = M^G$ this equality being, by most treatments, the very *definition* of H^0, and the higher H^j's are the right-derived functors attached to the left-exact functor $M \mapsto M^G$. Perhaps the thing to notice here, if anything, is that the topology of G doesn't affect $H^0(G;M)$.

Dimension 1 : Here

$$H^1(G;M) = \lim_{\rightarrow} H^1(G/H;M^H) = \cup H^1(G/H;M^H),$$

the limit/and/union being again taken over all open subgroups H (of finite index) in G. The point here is that the groups $H^1(G/H;M^H)$ are subgroups of $H^1(G;M)$. More about this in a moment. A basic interpretation of H^1 is as follows: $H^1(G;M) \cong$ the quotient group of (continuous) crossed homomorphisms from G to M modulo the subgroup of "principal crossed homomorphisms". If $N \subset G$ is a closed normal subgroup, consider the basic exact sequence:

$$0 \rightarrow H^1(G/N, M^N) \rightarrow H^1(G,M) \rightarrow H^1(N,M)^{G/N}.$$

Here the mappings are the natural mappings, and

Exercise. Prove the exactness by directly appealing to the crossed-homomorphisms interpretation. The basic exact sequence is really the beginning of the Spectral Sequence

$$E_2^{p,q} = H^p(G/N, H^q(N,M)) \Rightarrow H^{p+q}(G;M).$$

In particular, we can extend the basic exact sequence above to an exact sequence

$$0 \rightarrow H^1(G/N, M^N) \rightarrow H^1(G,M) \rightarrow H^1(N,M)^{G/N} \rightarrow H^2(G/N, M^N).$$

Cup products for "low dimensions" : For A a commutative ring, and A-modules M_1, M_2 endowed with A-linear discrete G-module structures, we have functorial cup products

$$H^i(G,M_1) \otimes_A H^j(G,M_2) \rightarrow H^{i+j}(G, M_1 \otimes_A M_2).$$

In particular, when $i = 0$ and $j = 1$, this computes to be the evident homomorphism if you interpret H^1 as crossed homomorphisms (**Exercise:** What is that evident homomorphism? And when $i = 1$ and $j = 1$, ...

Interpretations of Galois cohomology in dimension 1 : torsors. Let M be now a finite Galois module over a field K. The cohomology group $H^1(G_K, M)$ can be interpreted as the group of isomorphism classes of "M-torsors". To define the notion of M-torsor, we will be considering finite G_K**-sets** T: these are, by definition, (finite) sets equipped with continuous G_K-action, i.e., equipped with an action which factors through a finite quotient group of G_K.

Definition. Let M be a finite G_K-module. An M**-torsor** is a G_K-set T, together with a G_K-equivariant action of the abelian group M on the set T, i.e. , a mapping

$\alpha : M \times T \to T$ which satisfies the standard rules for an action. Moreover, we require that the action α makes M act principally and transitively on T and and the action satisfies the rule: $\alpha(gm, gt) = g\alpha(m \cdot t)$ for all $g \in G_K$, $m \in M$, and $t \in T$.

Exercise: For finite G_K-modules M, establish a canonical isomorphism between $H^1(G, M)$ and the set of isomorphism classes of M-torsors.

Remark: Torsors over algebraic groups. Lang's Theorem.

Interpretations of Galois cohomology in dimension 1 : descent theory. Explain the notion of twisting by a 1-cocycle, and connect $H^1(G_K, \underline{Aut}(E))$ with twists of E, for various kinds of E. Brauer-Severi varieties. Explain Hilbert's Theorem 90 this way.

Tate Local Duality. Local Class Field theory gives the canonical identification

$$H^2(G_K,\ \mu(\bar{\mathbf{K}})) \equiv \mathbf{Q}/\mathbf{Z}.$$

For fun, a quick check that the tame version of this is true. That is. for $\ell \neq p$, we have:

$$H^1(I_\ell,\ \mu_\ell(\bar{\mathbf{K}})) \equiv \mathbf{Q}_\ell/\mathbf{Z}_\ell,$$

and use the basic Spectral Sequence to deduce that

$$H^2(G_K,\ \mu_{\ell^\infty}(\bar{\mathbf{K}})) \equiv \mathbf{Q}_\ell/\mathbf{Z}_\ell.$$

Define the Cartier dual of the module M to be $M^* := \mathrm{Hom}_{\mathbf{Z}}(M, \mu)$. Suppose that M is finite. Then

Theorem. (Tate Local Duality):

$$H^i(G_K, M) \times H^{2-i}(G_K, M^*) \to H^2(G_K, \mu) = \mathbf{Q}/\mathbf{Z}$$

is a perfect pairing in the sense that (a) the cohomology groups $H^*(G_K, M)$ and $H^*(G_K, M^*)$ are all finite and the pairing is perfect. In particular, the only nonzero dimsensions of cohomology are for $i = 0, 1, 2$.

The most important pairing occurs in the "middle dimension":

$$H^1(G_K, M) \times H^1(G_K, M^*) \to \mathbf{Q}/\mathbf{Z}.$$

Cheating Example: Put $M = \mathbf{Z}/N\mathbf{Z}$ with trivial G_K-action. Then

$$H^1(G_K, M) = \mathrm{Hom}_{\mathrm{cont.}}\ (G_K, \mathbf{Z}/N\mathbf{Z}),$$

and

$$H^1(G_K, M^*) = H^1(G_K, \mu_N) = K^*/K^{*N},$$

(by Kummer theory, so: the pairing gives an isomorphism

$$\mathrm{Hom}_{\mathrm{cont.}}\ (G_K, \mathbf{Z}/N\mathbf{Z}) \equiv \mathrm{Hom}\ (K^*/K^{*N}, \mathbf{Q}/\mathbf{Z}).$$

From this we deduce a natural isomorphism

$$G_K^{\mathrm{ab}}/G_K^{\mathrm{ab}N} \equiv K^*/K^{*N},$$

and these isomorphisms are compatible for N increasing "multiplicatively" and they compile to give (in the projective limit) the local class field theory isomorphism $G_K^{\mathrm{ab}} \to \hat{K}^*/K^{*N}$ (where the hat refers to profinite completion).

Applying the basic exact sequence.

$$0 \to H^1(G_k, M^{I_k}) \to H^1(G_K, M) \to H^1(I_K, M)^{G_k} \to 0.$$

If M is unramified, then this reads:

$$0 \to H^1(G_k, M) \to H^1(G_K, M) \to \mathrm{Hom}_{G_k}\ (I_K)^{\mathrm{ab}}, M) \to 0.$$

If M is unramified and of cardinality a power of a prime number $\ell \neq p$, then

$$\mathrm{Hom}_{G_k}\ ((I_K)^{\mathrm{ab}}, M) = \mathrm{Hom}_{G_k}\ \mathbf{Z}_\ell(1), M) = M(-1)^{G_k},$$

giving the following evaluation of the basic exact sequence

$$0 \to H^1(G_k, M) \to H^1(G_K, M) \to M(-1)^{G_k} \to 0,$$

and, of course

$$0 \to H^1(G_k, M^*) \to H^1(G_K, M^*) \to M^*(-1)^{G_k} \to 0,$$

but since $M^*(-1) = M^\wedge$ (Pontrjagin duality) we have

$$0 \to H^1(G_k, M^*) \to H^1(G_K, M^*) \to (M^\wedge)^{G_k} \to 0.$$

Remark. There are two ways of doing this (see [Milne] Ch. 1).

The *finite* and *singular* parts of 1-dimensional cohomology. Axiomatized version

Applying the basic exact sequence.

Let K be an "LF" as usual, with residue field k of characteristic p, $\bar{K}/K$ an algebraic closure and $G_K = \mathrm{Gal}\,(\bar{K}/K)$. Let M be a finite abelian group with a continuous G_K-action. Let's examine the basic exact sequence:

$$(*) \qquad 0 \to H^1(G_k, M^{I_k}) \to H^1(G_K, M) \to H^1(I_K, M)^{G_k} \to 0,$$

and let us "evaluate" this sequence in even more down-to-earth terms in special instances:

1. If M is of order prime to p, and the G_K action on M is tamely ramified. Then the wild ramification group $P_K \subset I_K$ acts trivially on M; therefore G_K acts through the tame quotient T_K and I_K acts through the quotient group $\Delta_K = I_K/P_K$, which fits in the exact sequence:

$$0 \to \Delta_K \to T_K \to G_k \to 0.$$

Under our hypotheses, the natural homomorphism induces an isomorphism of cohomology groups $H^1(\Delta_K, M) \cong H^1(I_K, M)$ (for we have an exact sequence $0 \to H^1(\Delta_K, M^{P_K}) \to H^1(I_K, M) \to H^1(P_K, M)$ and the last of these groups vanishes).

Therefore our basic sequence $(*)$ becomes:

$$(**) \qquad 0 \to H^1(G_k, M^{\Delta_k}) \to H^1(G_K, M) \to H^1(\Delta_K, M)^{G_k} \to 0.$$

Since both G_k and Δ are canonically $\hat{\mathbf{Z}} = \prod_\ell \mathbf{Z}_\ell$ and $\prod_{\ell \neq p} \mathbf{Z}_\ell(1)$ respectively, we may make use of the canonical isomorphism evaluating H^1 of such a group (call it C) acting continuously on a finite abelian goup N,

$$C \otimes H^1(C, N) \cong N_C$$

to evaluate the flanking terms in this exact sequence as:

$$0 \to (M^{\Delta_K})_{G_k} \to H^1(G_K, M) \to (M_{\Delta_K}(-1))^{G_k} \to 0.$$

Here we should explain the "(-1)" carefully.

Let's compare this evaluation with Tate Local Duality. So, let us consider the Cartier Dual of M,

$$M^* = \mathrm{Hom}\,(M, \mu(\bar{K})) = M^\wedge \otimes \mathrm{Ta}(\mu(\bar{K})).$$

Here $M^\wedge$ is the pontrjagin dual of M; i.e., $M^\wedge = \mathrm{Hom}\,(M, \mathbf{Q}/\mathbf{Z})$, and $\mathrm{Ta}(\mu(\bar{K})$ is the Tate module of $\mu(\bar{K})$; i.e., the module such that there is a canonical isomorphism

$$\mathrm{Ta}(\mu(\bar{K})) \otimes \mathbf{Q}/\mathbf{Z} \cong \mu(\bar{K}).$$

So we have the exact sequences:

$$0 \to (M^{\Delta_K})_{G_k} \to H^1(G_K, M) \to (M_{\Delta_K}(-1))^{G_k} \to 0.$$

$$0 \to ((M^*)^{\Delta_K})_{G_k} \to H^1(G_K, M^*) \to ((M^*)_{\Delta_K}(-1))^{G_k} \to 0.$$

To compare these more easily, let us pontrjagin-dualize the first exact sequence,

$$0 \to [(M_{\Delta_K}(-1))^{G_k}]^\wedge \to [H^1(G_K, M)]^\wedge \to [(M^{\Delta_K})_{G_k}]^\wedge \to 0.$$

Exercise. Unravelling the definitions, and using the standard properties of pontrjagin duality, find the tautological isomorphisms

$$(1) \qquad \alpha : ((M^*)^{\Delta_K})_{G_k} \qquad \cong \qquad [(M_{\Delta_K}(-1))^{G_k}]^\wedge,$$

and

$$(2) \qquad \beta : ((M^*)_{\Delta_K}(-1))^{G_k} \qquad \cong \qquad [(M^{\Delta_K})_{G_k}]^\wedge.$$

Proposition. The Tate Duality Isomorphism $H^1(G_K, M^*) \cong [H^1(G_K, M)]^\wedge$ restricts to an isomorphism $((M^*)^{\Delta_K})_{G_k} \cong [(M_{\Delta_K}(-1))^{G_k}]^\wedge$, and induces an isomorphism on the quotient groups, $((M^*)_{\Delta_K}(-1))^{G_k} \cong [(M^{\Delta_K})_{G_k}]^\wedge$.

—-(Give proof)—-

1. If M is unramified (but no condition on its order) then the basic exact sequence reads:

$$0 \to H^1(G_k, M) \to H^1(G_K, M) \to \mathrm{Hom}_{G_k}\ (I_K)^{\mathrm{ab}}, M) \to 0.$$

The *finite* and *singular* parts of 1-dimensional cohomology. If we are in either caser **1.** or **2.** above, let us give alternate notation for the two flanking groups in the basic exact sequence (*). Put:

$$H^1_f(G_K, M) := H^1(G_k, M),$$

and

$$H^1_s(G_K, M) := H^1(I_K, M)^{G_k},$$

and I will refer to these groups, respectively, as the **finite part** and the **singular part** of $H^1_f(G_K, M)$, so that we can rewrite our basic exact sequence as:

$$0 \to H^1_f(G_K, M) \to H^1(G_K, M) \to H^1_s(G_K, M) \to 0,$$

and we have that Tate Duality, puts the finite part of $H^1(G_K, M)$ in pontrijagin duality with the singular part of $H^1(G_K, M^*)$, and, of course, vice versa.

Structured modules. Let K be an "LF", and M a finite continuous G_K-module. Recall that a **finite/singular** structure on M is simply a choice of subgroup, which we will denote $H^1_f(G_K, M)$ and call the **finite part**, of $H^1(G_K, M)$. We denote the quotient group

$$H^1_s(G_K, M) := H^1(G_K, M)/H^1_f(G_K, M),$$

and refer to $H^1_s(G_K, M)$ as the **singular part** of $H^1(G_K, M)$. In particular, to give a finite/singular structure on M is the same as giving an exact sequence,

$$0 \to H^1_f(G_K, M) \to H^1(G_K, M) \to H^1_s(G_K, M) \to 0.$$

Recall further our

Definition: If the residue characteristic of K does not divide the order of M and the wild-ramification subgroup $P_K \subset G_K$ act trivially on M, by the **standard finite/singular structure on** M we mean the "basic exact sequence",

$$0 \to H^1(G_k, M^{I_K}) \to H^1(G_K, M) \to H^1(I_K, M)^{G_k} \to 0.$$

(So, the standard f/s structure on M has finite part $H^1_f(G_K, M) := H^1(G_k, M^{I_K})$ and singular part $H^1_s(G_K, M) := H^1(I_K, M)^{G_k}$.)

Example: If the residue characteristic of K does not divide the order of M and M is an unramified G_K-module, meaning that the inertia subgroup $I_K \subset G_K$ acts trivially on M, then the standard finite/singular structure on M is given by

$$0 \to H^1(G_k, M) \to H^1(G_K, M) \to \mathrm{Hom}(I_K, M)^{G_k} \to 0.$$

Now let F be a Number Field (i.e., of finite degree over $\mathbf{Q}$) and if v is a place of F, let F_v be the completion of F at v. For simplicity of notation, if nothing else, first fix $\bar{F}/F$ and algebraic closure of the global field F, and then, for each place v of F, choose an extension $\bar{F}_v/\bar{F}$ and imbedding $F_v \hookrightarrow \bar{F}_v$ such that $\bar{F}_v$ is the algebraic closure of F_v. Letting $G := G_F = \mathrm{Gal}(\bar{F}/F)$, and for places v, $G_v := G_{F_v} = \mathrm{Gal}(\bar{F}_v/F_v)$ we get closed imbeddings $G_v \hookrightarrow G$, giving us a specific choice of decomposition subgroup for each place v. We will sometimes write $H^j(F, M)$ for the cohomology group $H^j(G, M) = H^j(G_F, M)$, and similarly for the local Galois cohomology groups $H^j(F_v, M) = H^j(G_v, M) = H^j(G_{F_v}, M)$.

Definition. A **structured** (finite) Galois module over F is a (continuous) G-module M, together with a rule σ which assigns to each place v of F a f/s structure on $H^1(G_v, M)$ such that for almost all places v the f/s structure is "standard".

Remark. Given a finite Galois module M over F, it may be the underlying Galois module for many possible *structures* σ. Given two structures σ_1 and σ_2 on M let us say that σ_1 is more stringent than σ_2 if, for all places v, the finite part of $H^1(G_v, M)$ for the structure σ_1 is contained in the finite part of $H^1(G_v, M)$ for the structure σ_2.

Basic Example. Let M be a finite Galois module over F. If S is a finite set of places large enough so that every place $v \neq S$ has the property that it is non-archimedean, the residue characteristic of v is prime to $|M|$ and M is unramified at v, define the structure σ_S on the Galois module M to be given as follows. For all $v \neq S$ we take $H^1_f(G_v, M)$ to be the standard structure (which, since the action of G on M is unramified at v, is simply $H^1_f(G_v, M) = H^1(G_{k_v}, M)$, where k_v is the residue field of F_v). For $v \in S$ we take the the least stringent f/s structure; i.e., $H^1_f(G_v, M) = H^1(G_v, M)$. Denote by M_S the Galois module M equipped with the structure σ_S.

Definition. The **Cartier dual** M^* of a structured (finite) Galois module M over F is the Cartier dual of M as G_F-module equipped with f/s structure such that for each place v, Tate Local Duality (which establishes a Pontrjagin duality between $H^1(G_v, M)$ and $H^1(G_v, M^*)$) puts $H^1_f(G_v, M)$ and $H^1_s(G_v, M^*)$ in Pontrjagin duality, and also puts $H^1_s(G_v, M)$ and $H^1_f(G_v, M^*)$ in Pontrjagin duality.

Remark. By what we have already proved in class, M^* with f/s structures for all v, as just defined, is a structured module. That is, for almost all v its structure is standard. If we fix our Galois module M and have two structures σ_1 and σ_2 on M, the first more stringent than the second, the corresponding dual structures σ_1^* and σ_2^* on M^* will have the property that σ_1^* is less stringent than σ_2^*.

Let M be a structure Galois module over F, and $h \in H^1(G, M)$.

Proposition. For almost all places v, the image of h under restriction mapping

$$\mathrm{res}_v : H^1(G, M) \to H^1(G_v, M)$$

lies in $H^1_f(G_v, M)$.

The way to prove this. Let L/F be a finite Galois extension that effaces the cohomology class h; i.e., such that h is in the kernel of the restriction homomorphism $H^1(F, M) \to H^1(L, M)$, and therefore in the image of $H^1(\mathrm{Gal}(L/F), M) \to H^1(F, M)$. Now just do the right diagram-check to see that $\mathrm{res}_v(h) \in H^1_f(G_v, M)$ for all non-archimedean places v of F which are of residual characteristic prime to $|M|$ and are unramified in the finite extensions L/F.

Define the **singular restriction** homomorphism, call it $\mathrm{res}_{s,v}$, as the composition

$$\mathrm{res}_{s,v} : H^1(G, M) \to H^1(G_v, M) \to H^1_s(G_v, M).$$

It follows from the above Proposition that for any given $h \in H^1(G, M)$ the image of h under the singular restriction homomorphism $\mathrm{res}_{s,v}$ is zero for almost all places v. We get a homomorphism which we can call **the singular restriction homomorphism**,

$$\bigoplus_v \mathrm{res}_{s,v} : H^1(G, M) \quad \to \quad \bigoplus_v H^1_s(G_v, M).$$

Definition. Let M be a structured Galois module over F. Define the **finite part** of $H^1(G,M)$, denoted $H^1_f(G,M)$, to be the kernel of the singular restriction homomorphism above. Define the **singular part** $H^1_s(G,M)$ to be the quotient of $H^1(G,M)$ by $H^1_f(G,M)$, giving us an exact sequence for global Galois cohomology:

$$0 \to H^1_f(G,M) \to H^1(G,M) \to H^1_s(G,M) \to 0,$$

and an injective homomorphism,

$$H^1_s(G,M) \hookrightarrow \bigoplus_v H^1_s(G_v,M).$$

Some notes. Of course, this whole set-up depends upon the choice of *structure* on the structured Galois module M. For example, if M is the structured module denoted M_S as described above, and if the G-action on M is trivial, then

$$H^1_f(G,M_S) = \mathrm{Hom}(G^{\mathrm{ab}}_{F,S}, M),$$

where $G^{\mathrm{ab}}_{F,S}$ is the Galois group of the maximal abelian extension of F unramified outside S.

In the literature, you will find definitions of the *finite part* of cohomology, usually for a specific choice of structure (see the hand-out of last Thursday for some discussion of this). The finite part, $H^1_f(G,M)$, of global cohomology is also sometimes referred to as a "generalized Selmer group". We'll see why, soon. We will sometimes refer to an element h in $H^1_f(G,M)$ as a "Selmer element". To keep the balance between nomenclature for $H^1_f(G,M)$ and $H^1_s(G,M)$ one might call $H^1_s(G,M)$ the "Kolyvagin group" and its elements "Kolyvagin elements" (although these would be neologisms). Note that by definition, given any element $h \in H^1_f(G,M)$, and any place v, we have $\mathrm{res}_v(h) \in H^1_f(G_v,M)$. If $c = (\cdots, c_v, \cdots) \in \bigoplus_v H^1_s(G_v,M)$, by the **support** of c, denoted $\mathrm{supp}(c)$, let us mean the set of places v for which $c_v \neq 0$.

The pairing. Let M be a structured (finite) Galois module over F and let M^* be its Cartier dual. Define a pairing (which we will denote $(h,c) \mapsto < h,c >$):

$$H^1_f(G,M) \otimes \bigoplus_v H^1_s(G_v,M^*) \to \mathbf{Q}/\mathbf{Z}$$

by the rule:

If $h \in H^1_f(G,M)$ and $c = (\cdots, c_v, \cdots) \in \bigoplus_v H^1_s(G_v,M^*)$, then

$$< h,c > := \sum_v < \mathrm{res}_v(h), c_v >_v = \sum_{v \in \mathrm{supp}(c)} < \mathrm{res}_v(h), c_v >_v,$$

where $< , >_v$ refers to the Pontrjagin pairing between $H^1_f(G_v,M)$ and $H^1_s(G_v,M^*)$.

Given any element $c \in \bigoplus_v H^1_s(G_v, M^*)$ we may view c as giving a homomorphism $H^1_f(G, M) \to \mathbf{Q}/\mathbf{Z}$ ($h \mapsto < h, c >$) and we sometimes call this homomorphism by the same letter c; i.e., $c(h) := < h, c >$. We also write, for any place v, $h_v := \mathrm{res}_v(h)$, and $c_v(h) := < \mathrm{res}_v(h), c_v > = < h_v, c_v >$, so that, all in all, we have lots of way of writing the above pairing; e.g.,

$$c(h) = \sum_{v \in \mathrm{supp}(c)} c_v(h_v).$$

Proposition. The above pairing vanishes on the subgroup

$$H^1_f(G, M) \otimes H^1_s(G, M^*) \subset H^1_f(G, M) \otimes \bigoplus_v H^1_s(G_v, M^*).$$

That is, given a (Kolyvagin element) $c \in H^1_s(G, M^*)$ and $h \in H^1_f(G, M)$, we have the relation:

$$\sum_{v \in \mathrm{supp}(c)} c_v(h_v) = 0.$$

The way to prove this. This comes directly from the piece of Global Class Field Theory that we reviewed last Thursday.

The point of view to adopt about all this. Any Kolyvagin element $c \in H^1_s(G, M^*)$ imposes some *local condition* (at places v in its support) that must be satisfied by all Selmer elements $h \in H^1_f(G, M)$.

For example: If the support of $c \neq 0$ is concentrated at exactly one place v_o, then any Selmer element h must have the property that $h_{v_o} \in \mathrm{Ker}(c_{v_o}) \subset H^1_f(G_{v_o}, M)$. Here is a way of thinking about the local condition detected by this Kolyvagin element c: It tells us that we may *strengthen* the f/s structure on the Galois module M, without changing the finite part of its (1-dimensional) cohomology. That is, let us define M' to be the structured module whose underlying Galois module is M again, whose f/s structure for all places $v \neq v_o$ is equal to the f/s structure on M, but on v_0 we place a more stringent f/s structure on the G_{v_o}-module M by setting:

$$H^1_f(G_{v_o}, M') := \mathrm{Ker}\{c_{v_o} : H^1_f(G_{v_o}, M) \to \mathbf{Q}/\mathbf{Z}\} \subset H^1_f(G_{v_o}, M).$$

The above discussion gives us that the finite part of the 1-dimensional cohomology of the more stringent structure M' is *equal* to the finite part of the 1-dimensional cohomology of M. Now this is already a curiously favorable state of affairs, because if we are trying to to show that $H^1_f(G, M)$ is small, we have (by constructing the Kolyvagin element c) that

$$H^1_f(G, M') = H^1_f(G, M),$$

where M' is more stringent than M, and there is nothing to stop us from trying to do this again inductively, to force the finite cohomology to satisfy more and more stringent local

conditions by finding further Kolyvagin elements for these increasingly stringent structures. In the most extreme cases one then shows that $H^1_f(G,M)$ satisfies such stringent conditions that it is forced to vanish, or else it is generated by specifically constructed cohomology classes. The efficacy of this method is determined by our ability to manufacture Kolyvagin elements with good control over their local components. This appraoch, combined with the following two further ideas is the underlying philosophy behind Kolyvagin's method:

1. It is possible, at times, to judiciously enlarge the base field F without losing too much of the Selmer group, but this larger base field gives us an even better chance of constructing Kolyvagin elements.

2. In various different contexts, one can find well-behaved collections of objects (these are the **Euler systems** of algebraic cycles, Heegner points, circular units, elements in algebraic K-groups, etc.) which produce the desired Kolyvagin elements in cohomology.

Proposition. Let M be a finite structure Galois module over F. Then $H^1_f(G,M)$ is finite.

Outline of Proof. Let S be a finite set of places large enough so that every place $v \neq S$ has the property that the residue characteristic of v is prime to $|M|$, M is unramified at v, and the f/s structure of M at v is standard. Let M_S be the underlying Galois module M over F, equipped with the structure σ_S as described under the rubric of "**Basic Example**" above. Since $H^1_f(G,M) \subset H^1_f(G,M_S)$, it suffices to prove finiteness of $H^1_f(G,M)$ when $M = M_S$.

For this, let L/F be the "splitting field for the G_F-action on M" ;, i.e., L/F is a finite Galois extension such that the action of G_F on M factors through a faithful action of $\mathrm{Gal}(L/F)$ on M. Now let T be the set of places of L which lie over the places of F in S. Denote by M_T the G_L Galois module with M as underlying G_L-module, with the structure σ_T.

Lemma 1. $H^1_f(G_L,M_T) = \mathrm{Hom}(G^{\mathrm{ab}}_{L,T},M)$ is finite.

Remark. There are two ways to prove this: via Class Field Theory, or, using less machinery: Kummer theory and the fact that the group of S-units in $\mathcal{O}_F$ is finitely generated .

Lemma 2. There is a natural injection of

$$\mathrm{Ker}\{H^1_f(G,M_S) \to H^1_f(G_L,M_T)\}$$

into $H^1(Gal(L/K),M)$.

Prove both of these as Exercises.

The Proposition follows from Lemmas 1 and 2 because $H^1(Gal(L/K),M)$ is (visibly) finite.

1. Kummer-theoretic analysis of $\mathrm{Hom}(G^{\mathrm{ab}}_{F,S},\mu_N)$**.**

Let $F/\mathbf{Q}$ be a field of finite degree, $\bar{F}/F$ an algebraic closure, S a finite set of places of F which contain all archimedean places, and $\mathcal{O}_{F,S} \subset F$ the sub-ring of S-integers of F. So, if S consists of the set of archmidean places, then $\mathcal{O}_{F,S} = \mathcal{O}_F$ is the ring of integers in F. Let $G_{F,S}$ be the Galois group of the maximal sub-extension of $\bar{F}/F$ which is unramified outside S. By the group of S-units of $\mathcal{O}_F$ we mean $\mathcal{O}_{F,S}^*$. By $\mathrm{Pic}(\mathcal{O}_{F,S})$ we mean the abelian group of isomorphism classes of $\mathcal{O}_{F,S}$-modules of finite type which are locally free of rank 1, the group-structure being given by tensor product.

We recall that $\mathcal{O}_{F,S}^*$ is a finitely generated abelian group, that $\mathrm{Pic}(\mathcal{O}_{F,S})$ is a finite abelian group, and that (fixing F, of course) if S is taken large enough, $\mathrm{Pic}(\mathcal{O}_{F,S})$ is trivial.

Fix N a positive integer, and assume that F contains $\mu_N(\bar{F})$, and that S contains all places of residual characteristic dividing N.

If M is the Galois module μ_N over F, then the G_F-action on M is trivial by the above hypothesis, and if M_S refers to M with its S-structure (recalling previous handouts) then

$$H^1_f(G_F, M_S) = \mathrm{Hom}(G^{\mathrm{ab}}_{F,S}, \mu_N).$$

Theorem. *The natural homomorphisms (which we will define in class) make*

$$0 \to \mathcal{O}_{F,S}^*/\mathcal{O}_{F,S}^{*N} \to \mathrm{Hom}(G^{\mathrm{ab}}_{F,S}, \mu_N) \to \mathrm{Pic}(\mathcal{O}_{F,S})[N] \to 0$$

exact.

Describe carefully the twist of an element of Pic by an element $\phi \in \mathrm{Hom}(G^{\mathrm{ab}}_{F,S}, \mu_N)$.

2. Cohomology of abelian varieties over finite and local fields.

Recall. *If N is a positive integer and A is an abelian variety (or a semi-abelian variety) over any field K, putting $M := A(\bar{K})[N]$ (which we also write as $A[N]$ for short) we have the Kummer sequence*

$$0 \to A(K)/NA(K) \to H^1(G_K, M) \to H^1(G_K, A(\bar{K}))[N] \to 0.$$

Theorem (Lang). *Let A be any connected smooth (commutative) algebraic group over the finite field k. Then $H^1(G_k, A(\bar{k})) = 0$.*

Corollary. *If N is a positive integer and A is an abelian variety (or a semi-abelian variety) over the finite field k, then the natural homomorphism coming from the Kummer sequence induces an isomorphism*

$$A(k)/NA(k) \cong H^1(G_k, A(\bar{k}))[N].$$

Proposition. *Let K be an "LF" and k its residue field. Let A be an abelian scheme over $\mathcal{O}_K$. Then the natural mapping induces an isomorphism of abelian groups*

$$A(\mathcal{O}_K) \cong A(K).$$

If N is a positive number not divisible by the characteristic of k, the natural mapping

$$A(K)/NA(K) \cong A(\mathcal{O}_K)/NA(\mathcal{O}_K) \to A(k)/NA(k)$$

is an isomorphism.

Putting the above Corollary and Proposition together, we have a natural isomorphism (under the hypotheses of the proposition):

$$(*) \qquad A(K)/NA(K) \quad \cong \quad H^1(G_k, A(\bar{k})[N]).$$

Now note that under the above hypotheses the G_K-module $M := A(\bar{K})[N] \cong A(\bar{k})[N]$ is unramified, and that there is a nice computation for us to do! For we have two natural exact sequences with the same middle term: the *Kummer sequence*,

$$0 \to A(K)/NA(K) \to H^1(G_K, M) \to H^1(G_K, A(\bar{K}))[N] \to 0,$$

and the *Basic exact sequence*,

$$0 \to H^1(G_k, M) \to H^1(G_K, M) \to \mathrm{Hom}(I_K, M)^{G_k} \to 0.$$

Exercise. *Assume the hypotheses of the previous proposition. Show that (*) is compatible with the two injections in the the two exact sequences above, yielding an isomorphism between those two exact sequences (and once I learn more plaintex, I will actually be able to draw the relevant exact diagram).*

3. The *finite/singular* structure on the Galois module of N-torsion points of an abelian variety. Let K be any complete local field (with finite residue field k) and A an abelian variety over K. Let $N \geq 1$. Consider the finite G_K-module

$$M := A(\bar{K})[N].$$

Definition. *By the* **A.V.** *finite/singular structure on M we mean the finite/singular structure which has:*

$$H^1_f(G_K, M) := \mathrm{Im}\{A(K)/NA(K) \to H^1(G_K, M)\} = \mathrm{Ker}\{H^1(G_K, M) \to H^1(G_K, A(\bar{K}))\},$$

and (as would then follow):

$$H^1_s(G_K, M) \cong H^1(G_K, A(\bar{K}))[N].$$

Remark. *The* **A.V.** *finite/singular structure on M depends upon the abelian variety A and the isomorphism between M and the group of N-torsion in A.*

Proposition. *If N is a positive number not divisible by the characteristic of k, and if A is an abelian variety over K which has good reduction over k, and if $M = A(\bar{K})[N]$, M is an unramified G_K-module, and the A.V. finite/singular structure on M is equal to its standard finite/singular structure.*

If F is a number field, A an abelian variety over F, $N \geq 1$, and $M = A(\bar{F})[N]$ is the G_F-module of N-torsion in A, by the **A.V.** finite/singular structure on M we mean the rule that assigns to each place v of F the **A.V.** finite/singular structure on M when viewed as Galois module over G_{F_v}.

Proposition. *Let F be a number field, A an abelian variety over F, $N \geq 1$, and $M = A(\bar{F})[N]$. The* **A.V.** *finite/singular structure on M is a structure.*

Proof. This follows from the Exercise above, plus the fact that an abelian variety over a number field has good reduction for almost all places v.

4. Selmer and Shafarevich-Tate groups. Define these.

Proposition. *Let F be a number field, A an abelian variety over F, $N \geq 1$, and $M = A(\bar{F})[N]$ with its A.V. structure. Then*

$$H^1_f(G_F, M) \cong S_N(A/F),$$

where $S_N(A/F)$ is the N-Selmer group of A over F.

Deduce (as last Thursday)

Corollary. *The groups $A(F)/NA(F)$ and $\mathrm{Sha}(A/F)[N]$ are finite for any positive N.*

State the **Shafarevich-Tate Conjecture.** Interpretation of Sha as locally trivial torsors. Discuss L/K-forms, the (non-abelian) Galois module of Automorphisms of an algebraic variety, connections with torsors, and with (nonabelian) H^1. State the theorem of descent. Examples! Elliptic curves, curves of genus 1 over F with with a rational point in F_v for every place v. Consider the smooth plane cubic curve $E : x^3 + y^3 + 60z^3 = 0$. By work of Kolyvagin and Rubin, one knows that

$$\mathrm{Sha}_E \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}.$$

Noting that change of sign of ι corresponds to multiplying by -1 in Sha_E we see that there are, in toto, four "nontrivial" Σ's to find here and after some minor computations (cf [M]) one finds all of them again as smooth plane cubics:

$$\Sigma_1 : 3x^3 + 4y^3 + 5z^3 = 0$$

$$\Sigma_2 : 12x^3 + y^3 + 5z^3 = 0$$

$$\Sigma_3 : 15x^3 + 4y^3 + z^3 = 0$$

$$\Sigma_4 : 3x^3 + 20y^3 + z^3 = 0.$$

1. Automorphism groups, Isomorphism sets, and L/K-forms. Recall that if V is an algebraic variety over a field K then $\mathrm{Aut}_K(V)$ is the group of automorphisms (which are defined over K) of the K-variety V. If L/K is a Galois extension, with Galois group $G := \mathrm{Gal}(L/K)$, then $\mathrm{Aut}_L(V)$ has a natural G-action, i.e., there is a natural homomorphism of G into the group of group-automorphisms of $\mathrm{Aut}_L(V)$ (defined in the evident way).

By a **G-group** let us mean a group A together with a G-action in it.

By $\underline{\mathrm{Aut}}_L(V)$ let us mean the G-group $\mathrm{Aut}_L(V)$; i.e., it is the group $\mathrm{Aut}_L(V)$ taken together with its G-action.

If W is another K-variety, let $\mathrm{Isom}_K(W,V)$ be the set of K-isomorphisms from W to V, noting that it is either empty or else is a set-theoretic torsor with respect to the group $\mathrm{Aut}_K(V)$ (the operation being composition). There is also a natural G-action on $\mathrm{Isom}_K(W,V)$ By $\underline{\mathrm{Isom}}_L(W,V)$ let us mean the *G-set* $\mathrm{Isom}_L(W,V)$; i.e., it is the set $\mathrm{Isom}_L(W,V)$ taken together with its G-action.

So, if we assume $\mathrm{Isom}_L(W,V)$ to be nonempty, then $\underline{\mathrm{Isom}}_L(W,V)$ is a torsor with respect to $\underline{\mathrm{Aut}}_L(V)$ and the G-action on these respect the torsor structure; i.e., we have the formula

$$\gamma^g \alpha^g = (\gamma \cdot \alpha)^g,$$

for all $g \in G$, $\gamma \in \mathrm{Isom}_L(W,V)$, and $\alpha \in \mathrm{Aut}_L(V)$.

When we have a G-set X, which is a (set-theoretic) torsor over a G-group A such that the formula

$$\xi^g \alpha^g = (\xi \cdot \alpha)^g,$$

for all $\xi \in X$ and $\alpha \in A$, as above, let us say that (the G-set) X is a **G-action torsor** over (the G-group) A.

In summary, (if $\mathrm{Isom}_L(W,V)$ is nonempty) the G-set $\underline{\mathrm{Isom}}_L(W,V)$ is a G-action torsor over (the G-group) $\underline{\mathrm{Aut}}_L(V)$. We say that W is an **L/K-form of** V if $\mathrm{Isom}_L(W,V)$ is non-empty.

Note also that we may systematically insist upon extra structure for our algebraic varieties (e.g. a base point over K, or a reduction of the automorphism group by other means) and get an analogous theory.

2. Sets of isomorphism classes of L/K-forms, G-action torsors. Connection with 1-cohomology.

For simplicity, suppose that L/K is a *finite* Galois extension, and hence that $G = \mathrm{Gal}(L/K)$ is a finite group. We leave setting up the more general theory as an exercise (where L/K is an arbitrary, possibly infinite, Galois extension and its Galois group is given its Krull topology).

Definition 1. *Let V be a variety over K and L/K a Galois extension with group G, as above. Let $E(L/K,V)$ denote the pointed set of K-isomorphism classes of L/K-forms of V.*

The base point of $E(L/K,V)$ is given by V itself, the *trivial* L/K-form of V.

Definition 2. *Let A be a G-group. By $T(G;A)$ let us mean the pointed set of isomorphism classes of G-action torsors over A.*

The base point of $T(G;A)$ is given by A itself, viewed as G-action torsor over itself via its multiplication law.

Definition 3. *Let A be a G-group. By* Cross.Hom$(G;A)$ *let us mean the set of* **crossed homomorphisms** *from G to A, meaning the pointed set of maps $h : G \to A$ with the property that*

$$h(g_1 \cdot g_2) = h(g_1)^{g_2} \cdot h(g_2).$$

The trivial mapping $h(G) = 1 \in A$ is a crossed homomorphism, and provides the base point for the set Cross.Hom$(G;A)$. There is a natural action (not preserving base point) of the group A on the set Cross.Hom$(G;A)$ by the formula,

$$(\alpha \cdot h)(g) = \alpha^g \cdot h(g) \cdot \alpha^{-1},$$

making Cross.Hom$(G;A)$ naturally an A-set.

Definition 4. *By $H^1(G;A)$ we mean the pointed set defined as the quotient of* Cross.Hom$(G;A)$ *with respect the equivalence relation given by its A-action; i.e., $H^1(G;A)$ is the orbit-set of* Cross.Hom$(G;A)$ *under this A-action.*

The base point of $H^1(G;A)$ is the orbit of the trivial crossed homomorphism.

Exercises :

1. When A is abelian, show that the above definition of $H^1(G;A)$ coincides with the group-cohomology definition (the base point corresponding to the origin of the group structure in $H^1(G;A)$).

2. In complete generality, (recalling what we did on Thursday last) show that there is a natural isomorphism of pointed sets

$$T(G;A) \cong H^1(G;A).$$

3. In complete generality, (recalling what we did on Thursday last) show that there is a natural injection

$$E(L/K,V) \hookrightarrow T(\mathrm{Gal}(L/K); \underline{\mathrm{Aut}}_L(V)) \cong H^1(\mathrm{Gal}(L/K); \underline{\mathrm{Aut}}_L(V)).$$

4. Suppose that $n \geq 1$ and that K is a field of characteristic not dividing n containing a primitive n-th root of 1. Let $G(X)$ be a polynomial (say with no multiple roots) and consider the plane curve $V : Y^n = G(X)$, and its collection of *twists* $V_D : DY^n = G(X)$, for D ranging through the nonzero elements of K. The curves V_D are L/K-twists of V for $L = K(D^{1/n})$. Think through the above theory, in the context of these examples.

3. Algebraic geometric torsors.

Let K be a field and K_s/K a separable closure. If V is a variety over K let $\bar{V}$ denote its pullback to K_s,; i.e., $\bar{V}$ is obtained from V by extension of scalars to K_s, and if $f : V \to W$ is a mapping over K, let $\bar{f} : \bar{V} \to \bar{W}$ be the mapping induces after extension of scalars to K_s. Let Γ be an algebraic group over K, and

$$\mu : \Gamma \times \Gamma \to \Gamma$$

the group multiplication mapping.

By an **algebraic geometric torsor** over Γ let us mean an algebraic variety X over K, together with a mapping (defined over K)

$$\alpha : \Gamma \times X \to X,$$

(called the **Γ-action mapping**) such that there exists an isomorphism of K_s-varieties $u : \bar{\Gamma} \to \bar{X}$ such that $\bar{\alpha} \cdot (1 \times u) = u \cdot \bar{\mu}$; i.e., such that u identifies the multiplication law on $\bar{\Gamma}$ with the $\bar{\Gamma}$-action mapping. Call these pairs (X, α) **a.g. torsors for** Γ, for short.

Remark. When you give an a.g. torsor structure for Γ on an algebraic variety X you are giving a (particular kind of) homomorphism from $\Gamma(K_s)$ to $\mathrm{Aut}_{K_s}(X)$.

We say that an algebraic geometric torsor is **trivial** over K if u above can be defined over K; or equivalently, if there is a K-isomorphism between Γ and X bringing α to μ. It is equivalent to ask that X has a K-rational point. If (X, α) is an algebraic geometric torsor for Γ defined over K, and trivial over an extension field L/K, then X is an L/K-form of Γ, but we should be attentive to the difference in structures here. We have a mapping (of isomorphism classes of elements in the sets:

$$\{\text{a. g. torsors for } \Gamma_{/K} \text{ becoming trivial over } L\ \} \quad \mapsto \quad \{\ L/K\text{−forms of the algebraic variety } \ \Gamma\}.$$

Exercises.

5. Think through the nature of the above mapping. It is not necessarily one:one. Can you find an example?

6. Define the natural mapping (as quickly done in class on Thursday):

$$\{\text{iso.classes of a. g. torsors for } \Gamma_{/K} \text{ becoming trivial over } L\ \} \to H^1(\mathrm{Gal}(L/K); \Gamma(L)).$$

Hint: Choosing a point $x \in X(L)$ you can construct a specific 1-cocycle c_x (i.e., a crossed homomorphism $c_x : \mathrm{Gal}(L/K) \to \Gamma(L)$) by setting $c_x(g) :=$ that unique $\gamma \in \Gamma(L)$ such that $x^g = \gamma \cdot x$. Show that this does the trick.

7. Show that the mapping of Exercise **6.** is an injective mapping (of pointed sets).

Definition 5. *We shall say that $\Gamma_{/K}$ has the* **descent property for torsors** *if the mapping of Exercise* **6.** *is a bijection for all Galois field extensions L/K.*

4. Abelian varieties.

Theorem. *Let K be a field, and $\Gamma = A$ an abelian variety over K.) Then A has the descent property for torsors. We have a canonical identification between the set of isomorphism classes of a.g. torsors for A over K and $H^1(G_K, A(K_s))$.*

Remark. This is a serious theorem.

Exercises.

8. Noting that $H^1(G_K, A(K_s))$ has a natural (abelian) group structure, give a nice geometric definition of an *addition law* for a.g. torsors for A over K such that the natural isomorphism of the above theorem becomes an isomorphism of (abelian) groups.

9. Describe an involution of a.g. torsors over A which realizes the inversion mapping $a \mapsto -a$ with respect to the group structure discussed in Exercise **8.**

Second definition of the Shafarevich-Tate group.

Definition 6. *Let S be a set (any set, not necessarily finite) of places of a number field F, and let A be an abelian variety over F. By $\mathrm{Sha}_S(A/F)$ let us mean the set of isomorphism classes of a.g. torsors for A defined over F and trivial over F_v where v ranges through all places of F not contained in S. If S is empty, we call $\mathrm{Sha}_S(A/F)$ simply $\mathrm{Sha}(A/F)$.*

Theorem. *There is an exact sequence*

$$0 \to \mathrm{Sha}_S(A/F) \to H^1(G_F, A(\bar{F})) \to \prod_{v \notin S} H^1(G_{F_v}, A(\bar{F}_v));$$

i.e., the second definition is the same as the first definition!

5. Elliptic curves, and curves of genus 1. Let X be a smooth projective curve over K of genus 1. Let $E = \mathrm{jac}(X) = \mathrm{Pic}^0(X)$ denote the jacobian variety of X. Then E is an elliptic curve over K; i.e., it is an abelian variety of dimension 1 defined over K. Discuss $\mathrm{Pic}^n(X)$ for any $n \in \mathbf{Z}$.

Exercises:

10. Let K be a field of characteristic 0, X a smooth projective curve over K of genus 1, and $E = \mathrm{jac}(X)$. Give a careful discussion of the structure of the algebraic group $\underline{\mathrm{Aut}}(X)$ over K (this will depend upon whether $j(E) = 0$, $j(E) = 1728$, or $j(E) \neq 0, 1728$). Show that the component of the algebraic group $\underline{\mathrm{Aut}}(X)$ containing the identity element, call it $\underline{\mathrm{Aut}}^o(X)$, is isomorphic to E.

11. Show that the set of isomorphism classes of a.g. torsors for E over K is equal to the set of isomorphism classes of couples (X, ι) where X is a smooth projective curve over K, and $\iota : E \cong \underline{\mathrm{Aut}}^o(X)$, is an isomorphism of algebraic groups over K.

12. If the E-torsor (X, ι) corresponds to the cohomology class $\xi \in H^1(G_K; E(\bar{K}))$ compare (X, ι) to the E-torsor $\mathrm{Pic}^1(X)$, and in terms of this comparision and ξ, give a

formula for the cohomology class $\in H^1(G_K; E(\bar{K}))$ corresponding to the E-torsor $\mathrm{Pic}^n(X)$ (for any n).

6. Finding elements of $\mathrm{Sha}(E/F)$ **in projective space.** Let X be a smooth projective curve of genus 1 over a number field F, and let E denote its jacobian. We identify X with the E-torsor $X_1 := \mathrm{Pic}^1(X)$. Let $\xi \in H^1(G_K; E(\bar{K}))$ be the cohomology class corresponding to X_1 and let n be the order of ξ. Then $X_n = \mathrm{Pic}^n(X)$ has an F-rational point. Does X *also* possess a divisor of degree n defined over F? Let us analyze this question, by considering the exact sequence of G_F-modules,

$$0 \to \bar{F}(X)^*/\bar{F}^* \to \mathbf{Z}[X(\bar{F})] \to \mathrm{Pic}(X)(\bar{F}) \to 0,$$

and passing to G_F-cohomology, we have:

$$\mathbf{Z}[X(\bar{F})]^{G_F} \to \mathrm{Pic}(X)(F) \to H^1(G_F, \bar{F}(X)^*/\bar{F}^*).$$

To analyze the right-hand group, we make use of Hilbert's Theorem 90, and compute $H^1(G_F, \bar{F}(X)^*/\bar{F}^*)$ from the exact sequence of G_F-modules

$$0 \to \bar{F}^* \to 0 \to \bar{F}(X)^* \to 0 \to \bar{F}(X)^*/\bar{F}^* \to 0,$$

giving

$$H^1(G_F, \bar{F}(X)^*/\bar{F}^*) = \mathrm{Ker}\ \{\mathrm{Br}_F \to \mathrm{Br}_{F(X)}\ \}.$$

Now, if ξ is an element of $\mathrm{Sha}(E/F)[n]$, we have:

Theorem* .

$$\mathrm{Ker}\ \{\mathrm{Br}_F \to \mathrm{Br}_{F(X)}\ \} = 0.$$

Proof. Since $\mathrm{Br}_F \subset \bigoplus_v \mathrm{Br}_{F_v}$, it suffices to show that $\mathrm{Br}_{F_v} \to \mathrm{Br}_{F_v(X)}$ is injective for all places v of F. Let

$$X_v = X \times_{\mathrm{Spec}(F)} \mathrm{Spec}(F_v)$$

and using the theory in A. Grothendieck's "Le groupe de Brauer III. Exemples et Complements", we may factor $\mathrm{Br}_{F_v} \to \mathrm{Br}_{F_v(X)}$ through

$$\mathrm{Br}_{F_v} \to \mathrm{Br}_{X_v} \to \mathrm{Br}_{F_v(X)}$$

and, by Prop. 2.1 of loc. cit. (since X_v is a noetherian regular integral scheme of dimension 1) the second mapping in the diagram above is injective. Since X_v has an F_v-rational point, the first mapping has a right-inverse, and therefore is also injective.

Corollary 1. *If X is an everywhere locally trivial E-torsor corresponding to an element of order n in* $\mathrm{Sha}(E/F)$*, then there exists a divisor D on X of degree n and which is defined over F.*

Under the hypotheses (and conclusion) of Corollary 1, suppose that $n \geq 3$, and consider the invertible coherent sheaf $\mathcal{O}_X(D)$ of regular functions locally defined on X with poles bounded by D. Letting $\mathbf{P}^{n-1}$ denote the projective space (over F) dual to the projectivization of the vector space of global sections, $H^0(X, \mathcal{O}_X(D))$, denote by $\phi : X \hookrightarrow \mathbf{P}^{n-1}$ the natural imbedding derived from the linear system containing D, which identifies X with a curve of genus 1 over F, of degree n, in projective $(n-1)$-space.

Corollary 2. *If X is an E-torsor corresponding to an element of order n in* $\mathrm{Sha}(E/F)$*, then X is isomorphic, over F, to a "normally imbedded" curve of genus* 1*, of degree n in projective $(n-1)$-space.*

Idle question*. Fix $n \geq 3$. Consider the Chow variety, call it C_n of all (smooth) projective "normally imbedded" curve of genus 1, of degree n in projective $(n-1)$-space. Then C_n is a quasi-projective variety over $\mathbf{Q}$, with a standard (quasi-) projective imbedding. In terms of this standard imbedding, let

$$H : C_n(\bar{\mathbf{Q}}) \to \mathbf{R}^{\geq 0}$$

denote the classical (Weil) height function. Given an elliptic curve E over a number field F, by the **height**, $h(\sigma)$ of an element $\sigma \in \mathrm{Sha}(E/F)[n]$) let us mean the minimum of the heights (in the sense of the H just mentioned) of all the points in $C_n(F)$ which correspond to normally imbedded curves of genus 1, of degree n in projective $(n-1)$-space which are isomorphic over F to E-torsors representing the element σ. Of course, $h(\sigma) = h(-\sigma)$. Can we find a (good) upper bound for the values of h on $\mathrm{Sha}(E/F)[n]$ (depending, of course, on E, F, and n; or perhaps just on the absolute norm of the conductor of E, the absolute degree of F, and n) ?