Some review problems

Joshua Ruiter

April 23, 2019

Contents

1 Projectives and injectives

1.1 R-mod has enough projectives an injectives

1.1.1 Enough projectives

Proposition 1.1. *Let R be a commutative ring with unity. The category of R-modules has enough projectives.*

Proof. Let M be an R-module. Then M is a quotient of a free R-module F, for example, take the free module generated by a set of generators for M. So we have a surjection $F \to M$. Since F is free, it is also projective. □

1.1.2 Enough injectives

Many of the definitions and lemmas in this section follow Sections 15.53 and 15.54 of the Stacks Project, see `https://stacks.math.columbia.edu/tag/01D8`.

Lemma 1.2. *An abelian group is injective (in the category of abelian groups) if and only if it is divisible.*

Proof. (Injective $\implies$ divisible) Let Q be an injective abelian group. Let $q \in Q$, and consider the map $\mathbb{Z} \to Q, 1 \mapsto q$. Since Q is injective, the following diagram can be completed to a homomorphism $\phi : \frac{1}{n}\mathbb{Z} \to Q$.

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z} \arrow[r, hook] \arrow[d, "1\mapsto a"'] & \frac{1}{n}\mathbb{Z} \arrow[dl, dotted, "\phi"] \\
 & Q &
\end{tikzcd}$$

For any $n \in \mathbb{Z}$ and any $q \in Q$, we get $n\phi\left(\frac{1}{n}\right) = \phi(1) = q$, so the map $n : Q \to Q$ is surjective, hence Q is divisible.

(Divisible $\implies$ injective) Let Q be a divisible abelian group, and suppose we have the diagram below. We need to construct h making the diagram commute.

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "g"'] & C \arrow[dl, dotted, "h"] \\
 & Q &
\end{tikzcd}$$

Consider the set $\mathcal{S}$ of pairs (B, h_B) where $A \subset B \subset C$ and $h_B : B \to Q$ is a lift making the following diagram commute.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[r, hook] \arrow[dl, "h_B"] & C \\
Q & &
\end{tikzcd}$$

We give $\mathcal{S}$ a partial order by $(B, h_B) \leq (B', h_{B'})$ when $B \subset B'$ and $h_{B'}|_B = h_B$.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[r, hook] \arrow[dl, "h_B"] & B' \arrow[r, hook] \arrow[dll, "h_{B'}"] & C \\
Q
\end{tikzcd}$$

We want to apply Zorn's lemma to $\mathcal{S}$, so we need to show that any ascending chain has an upper bound. Let (B_i, h_{B_i}) be an ascending chain.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B_1 \arrow[r, hook] \arrow[dl, "h_{B_1}"] & B_2 \arrow[r, hook] \arrow[dll, "h_{B_2}"] & \cdots \\
Q
\end{tikzcd}$$

Then an upper bound is given by$(\widetilde{B}, h_{\widetilde{B}})$ where $\widetilde{B}$ is the subgroup generated by $\bigcup_i B_i$ and the map $h_{\widetilde{B}}$ is defined by $h_{\widetilde{B}}(b) = h_B(b)$ for $b \in B$. Thus Zorn's lemma applies to $\mathcal{S}$, so there is a maximal element $(B_{\max}, h_{B_{\max}})$.

If we can show that $B_{\max} = C$, and then we are done. To do this, it is sufficient to show that for any pair (B, h_B) such that $B \neq C$, there is $(B', h_{B'}) \in \mathcal{S}$ with $B \subsetneq B'$, since if we do this, then if $B_{\max} \neq C$, there is a larger subgroup strictly containing $B_{\max}$ with an extension, contradicting maximality of $B_{\max}$, and resulting in the conclusion that $B_{\max} = C$.

Now we show that if $(B, h_B) \in \mathcal{S}$ with $B \neq C$, there exists $(B', h_{B'}) \in \mathcal{S}$ with $B \subsetneq B'$ and $h_{B'}|_B = h_B$. Let $(B, h_B) \in \mathcal{S}$ with $B \neq C$ and choose $c \in C \setminus B$, and let $B_c = B + c = B + \mathbb{Z}c \subset B$ be the subgroup generated by B and c.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[r, hook, "\neq"] \arrow[dl, "h_B"] & B_c \arrow[r, hook] & C \\
Q
\end{tikzcd}$$

We consider two cases:

1. There does not exist $n \in \mathbb{Z}_{\geq 1}$ such that $nc \in B$.

2. There exists $n \in \mathbb{Z}_{\geq 1}$ such that $nc \in B$.

In case (1), $B_c = B + \mathbb{Z}c = B \oplus \mathbb{Z}c$, and h_B can be extended to $h_{B_c} : B_c \to Q$ by $h_{B_c}|_B = h_B$ and $h_{B_c}(c) = 0$. (Or set $h_{B_c}(c)$ to be anything, it doesn't have to be zero.) Thus B_c is a strictly larger extension than B.

In case (2), let $n \in \mathbb{Z}_{\geq 1}$ be the smallest integer so that $nc \in B$. Finally, we use the fact that Q is divisible to choose $q \in Q$ such that $nq = h_B(nc)$. Consider the map $\pi : B \oplus \mathbb{Z} \to B_c, (b, m) \mapsto b + mc$, which fits into the exact sequence

$$0 \to \ker \pi \to B \oplus \mathbb{Z}c \xrightarrow{\pi} B_c \to 0$$

and (via the first isomorphism theorem) induces an isomorphism $(B \oplus \mathbb{Z}c)/\ker \pi \cong B_c$. Now consider the map

$$\widetilde{h} : B \oplus \mathbb{Z} \to Q \qquad \widetilde{h}(b, m) = h_B(b) + mq$$

If $(b, m) \in \ker \pi$ so that $b + mc = 0$, then $-mc \in B$, so $|m| \geq n$ and n divides m (by minimality of n), so $m = nt$ for some $t \in \mathbb{Z}$, and then

$$\widetilde{h}(b, m) = h_B(b) + mq = h_B(-mc) + mq = h_B(-tnc) + tnq = t(-h_B(nc) + nq) = 0$$

This shows that $\ker \pi \subset \ker \widetilde{h}$. Thus $\widetilde{h}$ factors through $(B \oplus \mathbb{Z}c)/\ker \pi \cong B_c$ to give a map $h_{B_c} : B_c \to Q$ satisfying $h_{B_c}(b + mc) = h_B(b) + mq$ and in particular $h_{B_c}(b + 0c) = h_B(b)$, so h_{B_c} extends h_B.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[r, hook, "\neq"] \arrow[dl, "h_B"] & B_c \arrow[r, hook] \arrow[dll, "h_{B_c}"] & C \\
Q & & &
\end{tikzcd}$$

□

Remark 1.3. The proof given above that an injective abelian group is divisible also holds in the category of finitely generated abelian groups, since the groups used, $\mathbb{Z}$ and $\frac{1}{n}\mathbb{Z}$, are both finitely generated. That is to say, an injective object in the category of finitely generated abelian groups must be divisible.

Remark 1.4. The simplest examples of divisible abelian groups are $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$, so these are injective $\mathbb{Z}$-modules. Note that there are no finite abelian groups which are divisible.

The next goal is to prove the following.

Theorem 1.5. *Let R be a ring. The category of R-modules has enough injectives.*

Definition 1.6. Let R be a ring and M an R-module. We define $M^\vee = \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. We view $M^\vee$ as an R-module via the action

$$(r \cdot \phi)(m) = \phi(r \cdot m)$$

where $r \in R, m \in M, \phi \in M^\vee$, and $r \cdot m$ is the action of R on M.

We view $\operatorname{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z}) = M \mapsto M^\vee$ as a contravariant functor from the category of R-modules to itself. Note that because $\mathbb{Q}/\mathbb{Z}$ is divisible, it is an injective abelian group, so the functor $\operatorname{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ is exact (as a functor from abelian groups to abelian groups), so it is an exact functor from R-mod to itself.

Definition 1.7. Let M be an R-module. The **evaluation map** is

$$\operatorname{ev} : M \to (M^\vee)^\vee \qquad m \mapsto (\phi \mapsto \phi(m)) \qquad \operatorname{ev}(m)(\phi) = \phi(m)$$

Definition 1.8. Let R be a ring and M an R-module. The free module on M is

$$F(M) = \bigoplus_{m \in M} R[m]$$

with the accompanying surjection

$$F(M) \to M \qquad \sum_i r_i[m_i] \mapsto \sum_i r_i m_i$$

We think of $M \mapsto (F(M) \to M)$ as a functor from R-mod to the arrow category of R-mod.

Definition 1.9. Let R be a ring and M an R-module. Set $J(M) = (F(M^\vee))^\vee$.

Remark 1.10. Note that as an abelian group, $J(M)$ is torsion because $\mathbb{Q}/\mathbb{Z}$ is torsion.

Theorem 1.11. *Let R be a ring and M an R-module.*

1. The evaluation map $\mathrm{ev} : M \to (M^\vee)^\vee$ is injective.
2. There is a (canonical) embedding $M \hookrightarrow J(M)$.
3. $R^\vee$ is an injective R-module.
4. $J(M)$ is an injective R-module.
5. The category of R-modules has enough injectives.

Proof. (1) We show that if $x \in M$ and $x \neq 0$, then $\mathrm{ev}(x) \neq 0$. Equivalently, we need to show that there is $\phi \in M^\vee = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ such that $\mathrm{ev}(x)(\phi) = \phi(x) \neq 0$. Let $x \in M, x \neq 0$. Let $M' \subset M$ be the abelian subgroup generated by x (NOT the R-submodule generated by x, this is not the same thing). Then there is a nonzero map $\psi : M' \to \mathbb{Q}/\mathbb{Z}$ which does not vanish on x (for example, if $nx = 0$, send x to $\frac{1}{n}$). Then because $\mathbb{Q}/\mathbb{Z}$ is an injective abelian group, this extends to a map $\widetilde{\psi} : M \to \mathbb{Q}/\mathbb{Z}$ which does not vanish on x.

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] \arrow[d, "\psi"] & M \arrow[dl, dotted, "\widetilde{\psi}"] \\
& \mathbb{Q}/\mathbb{Z} &
\end{tikzcd}$$

Then $\mathrm{ev}(x)(\widetilde{\psi}) = \widetilde{\psi}(x) \neq 0$. Hence ev is injective.

(2) Consider the canonical surjection $F(M^\vee) \to M^\vee$. Apply the contravariant, exact functor $(-)^\vee$ to obtain $(M^\vee)^\vee \to (F(M^\vee))^\vee = J(M)$. Since $(-)^\vee$ is exact, the surjection becomes an injection. Thus we have injections

$$M \xrightarrow{\mathrm{ev}} (M^\vee)^\vee \to J(M)$$

which is to say, M embeds into $J(M)$.

(3) Let N be an R-module. As some people would say,

$$\mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) = \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z})$$

However, I think that it's sloppy to write an equality here. What this really means is that there is a natural isomorphism of R-modules

$$\mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) \to \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z}) \qquad \phi \mapsto \Big(n \mapsto \phi(n)(1)\Big)$$

with inverse given by

$$\mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) \qquad \psi \mapsto \Big(n \mapsto \big(1 \mapsto \psi(n)\big)\Big)$$

(details left unchecked by me, the author). By "natural isomorphism," I mean that this is furthermore an isomorphism of functors

$$(-)^\vee = \mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) = \mathrm{Hom}_R(-, R^\vee)$$

(once again, details left unchecked). Therefore since $(-)^\vee$ is exact, $\mathrm{Hom}_R(-, R^\vee)$ is exact, so $R^\vee$ is injective.

(4) Note that we have an isomorphism of R-modules

$$J(M) = (F(M^\vee))^\vee = \mathrm{Hom}_{\mathbb{Z}}\left(\bigoplus_{\phi \in M^\vee} R[\phi], \mathbb{Q}/\mathbb{Z}\right) \cong \prod_{\phi \in M^\vee} \mathrm{Hom}_{\mathbb{Z}}(R[\phi], \mathbb{Q}/\mathbb{Z}) \cong \prod_{\phi \in M^\vee} R^\vee$$

Since a product of injective objects is injective and $R^\vee$ is injective by (3), this product is injective.

(5) This is immediate from (2) and (4). □

1.1.3 Baer's criterion

Another approach (such as that in Dummit and Foote [1]) to showing that the category R-mod has enough injectives uses Baer's criterion, which we give below.

Proposition 1.12 (Baer's criterion)**.** *Let R be a ring and Q an R-module. Then Q is injective (in the category of R-modules) if and only if for every left ideal $I \subset R$ any R-module homomorphism $\phi : I \to Q$ can be extended to an R-module homomorphism $\widetilde{\phi} : R \to Q$.*

Proof. Proposition 36 of Dummit and Foote [1]. □

1.2 Projectives and injectives in some subcategories of abelian groups

Proposition 1.13. *The category of finitely generated abelian groups has enough projectives, but not enough injectives. (In fact, there are no nonzero injective objects at all in this category).*

Proof. Every finitely generated abelian group A is a finite direct sum of cyclic groups,

$$A \cong \mathbb{Z}^r \oplus \bigoplus_i \mathbb{Z}/n_i\mathbb{Z}$$

Then A is a quotient of a a free module on the same number of generators by sending a generator for each infinite cyclic summand to a generator for the corresponding cyclic summand of A. That is, we have the surjection

$$\mathbb{Z}^r \oplus \textstyle\bigoplus_i \mathbb{Z} \xrightarrow{\mathrm{Id}^r \oplus \pi} \mathbb{Z}^r \oplus \textstyle\bigoplus_i \mathbb{Z}/n_i\mathbb{Z}$$

where π sends the generator of the ith summand $\mathbb{Z}$ to the generator of $\mathbb{Z}/n_i\mathbb{Z}$. Hence there are enough projectives.

Now suppose A is an injective object in the category of finitely generated abelian groups. By remark 1.3, A is divisible. However, there are no divisible finitely generated abelian groups, except the trivial group. □

Proposition 1.14. *The category of torsion abelian groups has enough injectives, but not enough projectives.*

Proof. First, we show that there are enough injectives. Let M be a torsion abelian group. Then we have an embedding $M \to J(M)$, and by Theorem 1.11, $J(M)$ is injective. Note that the torsion subgroup of a divisible group is divisible, and that M lands in the torsion subgroup of $J(M)$, so M embeds into an injective object.

Now we show that there are not enough projectives [1]. To show there are not enough projectives, we show that there is no projective which surjects onto $\mathbb{Z}/2\mathbb{Z}$. Suppose there is a projective object P with a map $\phi : P \to \mathbb{Z}/2\mathbb{Z}$ and an element $x \in P$ so that $\phi(x) = 1$. For $k \geq 1$, we have the quotient map $\pi : \mathbb{Z}/2^k\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}, 1 \mapsto 1$. Since P is projective, there is a lift $\widetilde{\phi} : P \to \mathbb{Z}/2^k\mathbb{Z}$ with $\widetilde{\phi}(x) = 1$.

$$\begin{tikzcd}
& P \arrow[d, "\phi"] \arrow[dl, dotted, "\widetilde{\phi}"'] & \\
\mathbb{Z}/2^k\mathbb{Z} \arrow[r, "\pi"'] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

Note that any element of $\mathbb{Z}/2^k\mathbb{Z}$ which maps to 1 under π is a generator, since it is coprime to 2^k. In particular, $\widetilde{\phi}(x)$ is a generator of $\mathbb{Z}/2^k\mathbb{Z}$, so $x \in P$ has order at least 2^k. Since k was arbitrary, this shows that x has arbitrarily large order so x is not torsion, which is impossible since P is a torsion group. Thus P does not exist. □

[1] In fact, there are no nontrivial projective objects in this category, but the proof given here https://math.stackexchange.com/questions/1038786/existence-of-projectives-in-the-category-of-torsion-abelian-groups requires some knoweldge about Prufer groups, so we omit it. This proof is also given at that source, in the original question.

1.3 Computations of Ext groups

Review check. Outline the process of computing $\mathrm{Ext}^n_R(A, B)$ using projective an injective resolutions.

Remark 1.15. We recall the outline of computing Ext groups via projective and injective resolutions. Let R be a ring and let A, B be R-modules. Given a projective resolution of A

$$\cdots \to P_1 \to P_0 \to A \to 0$$

we apply the contravariant functor $\mathrm{Hom}_R(-, B)$ and drop the A term to obtain a chain complex

$$0 \to \mathrm{Hom}_R(P_0, B) \to \mathrm{Hom}_R(P_1, B) \to \cdots$$

The ith homology of this chain complex is $\mathrm{Ext}^i_R(A, B)$. Alternatively, one may being with an injective resolution of B,

$$0 \to B \to I_0 \to I_1 \to \cdots$$

and apply the covariant functor $\mathrm{Hom}_R(A, -)$ and drop the B term to obtain a chain complex

$$0 \to \mathrm{Hom}_R(A, I_0) \to \mathrm{Hom}_R(A, I_1) \to \cdots$$

The ith homology of this chain complex is also $\mathrm{Ext}^i_R(A, B)$.

The following computations of Ext groups are all examples, exercises, or theorems from Dummit and Foote [1].

Proposition 1.16. *Let A be an abelian group. Then*

$$\mathrm{Ext}^i_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \cong \begin{cases} {}_mA & i = 0 \\ A/mA & i = 1 \\ 0 & i \geq 2 \end{cases}$$

Proof. We have a projective resolution of $\mathbb{Z}/m\mathbb{Z}$

$$0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$$

Then we apply the contravariant functor $\mathrm{Hom}_{\mathbb{Z}}(-, A)$ and drop the $\mathbb{Z}/m\mathbb{Z}$ term to obtain a chain complex depicted below. Using the canoncial isomorphism $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \cong A$ via $\phi \mapsto \phi(1)$, we get an isomorphism of chain complexes.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \arrow[r, "m"] \arrow[d, "\cong"] & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & A \arrow[r, "m"] & A \arrow[r] & 0
\end{tikzcd}$$

Thus $\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \cong {}_mA$ and $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \cong A/mA$, and the higher ext groups vanish. □

Proposition 1.17. *Let m, d be integers with $d|m$, and let A be an abelian group of exponent m (aka A is a $\mathbb{Z}/m\mathbb{Z}$-module). Then*

$$\operatorname{Ext}^i_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/d\mathbb{Z}, A) = \begin{cases} {}_dA & i = 0 \\ {}_{m/d}A/dA & i = 1, 3, \dots \\ {}_dA/(m/d)A & i = 2, 4, \dots \end{cases}$$

Proof. We begin with a projective (free) resolution of $\mathbb{Z}/d\mathbb{Z}$ (in the category of $\mathbb{Z}/m\mathbb{Z}$-modules).

$$\cdots \xrightarrow{m/d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{m/d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/d\mathbb{Z} \longrightarrow 0$$

The map π is the quotient map $1 \mapsto 1$, whose kernel is generated by m/d, which justifies exactness at the first $\mathbb{Z}/m\mathbb{Z}$ term. Exactness at the other terms is clear.

Then we apply the contravariant functor $\operatorname{Hom}_{\mathbb{Z}/m\mathbb{Z}}(-, A)$ and drop the $\mathbb{Z}/d\mathbb{Z}$ term to obtain the upper chain complex depicted below. Using the isomorphism $\operatorname{Hom}_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \cong A$, we get an isomorphism of chain complexes.

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Hom}_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \arrow[r, "d"] \arrow[d, "\cong"] & \operatorname{Hom}_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \arrow[r, "m/d"] \arrow[d, "\cong"] & \operatorname{Hom}_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \arrow[r, "d"] \arrow[d, "\cong"] & \cdots \\
0 \arrow[r] & A \arrow[r, "d"] & A \arrow[r, "m/d"] & A \arrow[r, "d"] & \cdots
\end{tikzcd}$$

The ith homology of this periodic chain complex is $\operatorname{Ext}^i_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/d\mathbb{Z}, A)$, so we read off exactly the homology as claimed. □

Lemma 1.18. *$\mathbb{Z}/m\mathbb{Z}$ is an injective $\mathbb{Z}/m\mathbb{Z}$-module.*

Proof. By Baer's criterion 1.12, it suffices to show that for any ideal $I \subset \mathbb{Z}/m\mathbb{Z}$ and any $\mathbb{Z}/m\mathbb{Z}$-linear map $I \to \mathbb{Z}/m\mathbb{Z}$, there is an extension $\widetilde{\phi} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. An ideal of $\mathbb{Z}/m\mathbb{Z}$ is a subgroup of the form $n\mathbb{Z}/m\mathbb{Z}$. Any such subgroup can be written as $d\mathbb{Z}/m\mathbb{Z}$ where $d = \gcd(n, m)$, in particular, $d|m$.

Suppose we have $\phi : d\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. By linearity, ϕ is determined by $\phi(d)$. Since d has order m/d, it must be mapped to something of order m/d, so it is mapped to something in the subgroup $d\mathbb{Z}/m\mathbb{Z}$ (since finite cyclic groups have a unique subgroup of each divisor order), so $\phi(d) = kd$. Then we extend ϕ to $\mathbb{Z}/m\mathbb{Z}$ by setting $\widetilde{\phi}(1) = k$. □

Proposition 1.19. *Let m, d be integers with $d|m$, and let A be an abelian group of exponent m (aka A is a $\mathbb{Z}/m\mathbb{Z}$-module). Let $\widehat{A} = \operatorname{Hom}_{\mathbb{Z}/m\mathbb{Z}}(A, \mathbb{Z}/m\mathbb{Z})$ be the dual group of A. Then*

$$\operatorname{Ext}^i_{\mathbb{Z}/m\mathbb{Z}}(A, \mathbb{Z}/d\mathbb{Z}) = \begin{cases} {}_d\widehat{A} & i = 0 \\ {}_{m/d}\widehat{A}/d\widehat{A} & i = 1, 3, \dots \\ {}_d\widehat{A}/(m/d)\widehat{A} & i = 2, 4, \dots \end{cases}$$

Proof. By the previous lemma 1.18, $\mathbb{Z}/m\mathbb{Z}$ is an injective $\mathbb{Z}/m\mathbb{Z}$-module. Thus the following is an injective resolution of $\mathbb{Z}/d\mathbb{Z}$ (in the category of $\mathbb{Z}/m\mathbb{Z}$-modules).

$$0 \to \mathbb{Z}/d\mathbb{Z} \hookrightarrow \mathbb{Z}/m\mathbb{Z} \xrightarrow{d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{m/d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{m/d} \cdots$$

Then we apply the covariant functor $\operatorname{Hom}_{\mathbb{Z}/m\mathbb{Z}}(A, -)$ and drop the first term to obtain the chain complex below. We omit the subscript $\mathbb{Z}/m\mathbb{Z}$ for Hom.

$$0 \longrightarrow \operatorname{Hom}(A, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{d} \operatorname{Hom}(A, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{m/d} \operatorname{Hom}(A, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{d} \cdots$$

From this, we read off the necessary homology. □

Remark 1.20. A finite abelian group is (non-canonically) isomorphic to its dual, but an infinite abelian group need not be.

1.3.1 Injectives and projectives

Proposition 1.21. *Let Q be an injective R-module. Then $\operatorname{Ext}^n_R(A, Q) = 0$ for all R-modules A and all $n \geq 1$.*

Proof. We have the somewhat trivial injective resolution of Q

$$0 \to Q \to Q \to 0$$

Then we apply the contravariant functor $\operatorname{Hom}_R(A, -)$ and drop the first term to obtain the even more trivial chain complex

$$0 \to \operatorname{Hom}_R(A, Q) \to 0$$

whose ith homology is $\operatorname{Ext}^i_R(A, Q)$. Thus $\operatorname{Ext}^0_R(A, Q) = \operatorname{Hom}_R(A, Q)$ (as always), and higher Ext groups vanish. □

Example 1.22. For $R = \mathbb{Z}$, we know that injective is equivalent to divisible. So as examples of the above we obtain

$$\operatorname{Ext}^n_{\mathbb{Z}}(A, \mathbb{Q}) = 0 \qquad \operatorname{Ext}^n_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) = 0$$

for all $n \geq 1$ and all abelian groups A.

Proposition 1.23. *Let P be a projective R-module. Then $\operatorname{Ext}^n_R(P, A) = 0$ for all R-modules A and all $n \geq 1$.*

Proof. We have the somewhat trivial projective resolution of P

$$0 \to P \to P \to 0$$

Then we apply the covariant functor $\operatorname{Hom}_R(-, A)$ and drop the first term to obtain the even more trivial chain complex

$$0 \to \operatorname{Hom}_R(P, A) \to 0$$

whose ith homology is $\operatorname{Ext}^i_R(P, A)$. Thus $\operatorname{Ext}^0_R(P, A) = \operatorname{Hom}_R(P, A)$ as always, and higher Ext groups vanish. □

Example 1.24. For $R = \mathbb{Z}$ (or any PID), we know that projective is equivalent to free. So from the above we obtain

$$\operatorname{Ext}^n_{\mathbb{Z}}(\mathbb{Z}^k, A) = 0$$

for all $n, k \geq 1$ and all abelian groups A.

Proposition 1.25. *Let A, B be abelian groups. Then $\operatorname{Ext}^n_{\mathbb{Z}}(A, B) = 0$ for all $n \geq 2$.*

Proof. Recall that for abelian groups, injective is equivalent to divisible, and recall that a quotient of a divisible group is divisible. We know that $\mathbb{Z}$-mod has enough injectives, so choose an embedding $B \hookrightarrow Q$ with Q injective/divisible. Then the quotient Q/B is also divisible, to it is injective. Thus we have an injective resolution

$$0 \to B \to I \to I/B \to 0$$

Then we apply the covariant functor $\operatorname{Hom}_{\mathbb{Z}}(A, -)$ and drop the B term to obtain a chain complex whose ith homology is $\operatorname{Ext}^i_{\mathbb{Z}}(A, B)$.

$$0 \to \operatorname{Hom}_{\mathbb{Z}}(A, I) \to \operatorname{Hom}_{\mathbb{Z}}(A, I/B) \to 0$$

We can't say very much about Ext^0 and Ext^1, but we can read off from this that $\operatorname{Ext}^n_{\mathbb{Z}}(A, B) = 0$ for $n \geq 2$. □

Proposition 1.26. *Let A be a torsion abelian group. Then*

$$\operatorname{Ext}^i_{\mathbb{Z}}(A, \mathbb{Z}) = \begin{cases} 0 & i = 0, i \geq 2 \\ \operatorname{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) & i = 1 \end{cases}$$

Proof. We have an injective resolution of $\mathbb{Z}$

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

Then we apply the covariant functor $\operatorname{Hom}_{\mathbb{Z}}(A, -)$ and drop the $\mathbb{Z}$ term to obtain a chain complex whose ith homology is $\operatorname{Ext}^i_{\mathbb{Z}}(A, \mathbb{Z})$.

$$0 \to \operatorname{Hom}_{\mathbb{Z}}(A, \mathbb{Q}) \to \operatorname{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) \to 0$$

Because A is torsion and $\mathbb{Q}$ is torsion free, $\operatorname{Hom}_{\mathbb{Z}}(A, \mathbb{Q}) = 0$. Thus the 0th homology is zero, the first homology is $\operatorname{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$, and the higher homology groups vanish. □

1.3.2 Extensions and Ext

Theorem 1.27. *There is an isomorphism between $\operatorname{Ext}^1_R(A, B)$ and the group of isomorphism classes of extensions $0 \to B \to E \to A \to 0$.*

Example 1.28. We know that $\operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ by Proposition 1.16. By the previous theorem, this means that there are exactly p inequivalent extensions

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E \to \mathbb{Z}/p\mathbb{Z} \to 0$$

We now give concrete descriptions of these p extensions. As for any two groups, there is the trivial split extension

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$$

where the left map is inclusion into the left factor and the right map is projection onto the right factor (the choice of which factor does not change the equivalence class of this extension). For nontrivial extensions, we have the following $p-1$ extensions.

$$\begin{array}{c}
0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{p} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\text{mod } p} \mathbb{Z}/p\mathbb{Z} \to 0 \\
0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{2p} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\text{mod } p} \mathbb{Z}/p\mathbb{Z} \to 0 \\
\vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{(p-1)p} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\text{mod } p} \mathbb{Z}/p\mathbb{Z} \to 0
\end{array}$$

It is clear that none of these is equivalent to the trivial extension, since $\mathbb{Z}/p^2\mathbb{Z} \not\cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, so to know that we have found a representative for every equivalence class, it suffices to show that these $p-1$ extensions are all inequivalent. Suppose we have an equivalence as below with $m, n \in \{1, \ldots, p-1\}$.

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r, "mp"] \arrow[d, "\mathrm{Id}"] & \mathbb{Z}/p^2\mathbb{Z} \arrow[r, "\text{mod } p"] \arrow[d, "\theta", "\cong"'] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, equal, "\mathrm{Id}"] & 0 \\
0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r, "np"] & \mathbb{Z}/p^2\mathbb{Z} \arrow[r, "\text{mod } p"] & \mathbb{Z}/p\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

Commutativity of the right square gives $\theta(1) \equiv 1 \bmod p$, so $\theta(1) = 1 + kp$ for some k. Then commutativity of the left square gives

$$np \equiv \theta(mp) \equiv mp\theta(1) \equiv mp(1+kp) \equiv mp + mkp^2 \equiv mp \qquad \text{mod } p^2$$

Since $m, n < p$, this implies $m = n$.

Remark 1.29. Dummit and Foote do the same example where they describe the p distinct extension of $\mathbb{Z}/p\mathbb{Z}$ by itself, except that they write the nontrivial extensions as

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{p} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{n \text{ mod } p} \mathbb{Z}/p\mathbb{Z} \to 0$$

where the left map is the inclusion $1 \mapsto p$ and the right map is $x \mapsto nx \bmod p$. As above, this gives $p-1$ inequivalent extensions for $n \in \{1, \ldots, p-1\}$.

2 Cohomology of cyclic groups

2.1 Cohomology of finite cyclic group

Proposition 2.1. *Let G be a finite cylic group with generator σ and let A be a G-module. Then*

$$H^i(G,A) = \begin{cases} A^G & i=0 \\ \ker N_G/(\sigma-1)A & i=1,3,\dots \\ A^G/N_GA & i=2,4,\dots \end{cases}$$

Proof. Let $N_G = \sum_{g\in G} g$ be the norm element of G. Consider the following free (and projective) resolution of $\mathbb{Z}$ as a trivial G-module.

$$\begin{tikzcd} \cdots \arrow[r, "\sigma-1"] & \mathbb{Z}[G] \arrow[r, "N_G"] & \mathbb{Z}[G] \arrow[r, "\sigma-1"] & \mathbb{Z}[G] \arrow[r, "\epsilon"] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

Now apply (contravariant) $\mathrm{Hom}_{\mathbb{Z}[G]}(-,A)$ and drop the $\mathbb{Z}$ term to obtain a chain complex whose ith homology is $H^i(G,A)$.

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \arrow[r, "(\sigma-1)_*"] & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \arrow[r, "(N_G)_*"] & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \arrow[r, "(\sigma-1)_*"] & \cdots \end{tikzcd}$$

Now we use the standard isomorphism (for any ring R) that $\mathrm{Hom}_R(R,A) \cong A$ via $\phi \mapsto \phi(1)$. Applying this to each term of the previous chain complex, we obtain an isomorphic chain complex with isomorphic homology.

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \arrow[r, "(\sigma-1)_*"] \arrow[d, "\cong"] & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \arrow[r, "(N_G)_*"] \arrow[d, "\cong"] & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \arrow[r, "(\sigma-1)_*"] \arrow[d, "\cong"] & \cdots \\ 0 \arrow[r] & A \arrow[r, "\sigma-1"] & A \arrow[r, "N_G"] & A \arrow[r, "\sigma-1"] & \cdots \end{tikzcd}$$

Then noting that the kernel of $\sigma-1$ is precisely A^G, we read off from this bottom chain complex the cohomology.

$$H^i(G,A) = \begin{cases} A^G & i=0 \\ \ker N_G/(\sigma-1)A & i=1,3,\dots \\ A^G/N_GA & i=2,4,\dots \end{cases}$$

□

Proposition 2.2. *Let G be a finite cyclic group with generator σ and let A be a G-module. Then*

$$\widehat{H}^i(G,A) = \begin{cases} \ker N_G/(\sigma-1)A & i=\dots,-3,-1,1,3,\dots \\ A^G/N_GA & i=\dots-2,0,2,4,\dots \end{cases}$$

Proof. The previous proposition (2.1) already verified this for $i \geq 1$. For $i=-1,0$, these are the right Tate cohomology groups essentially by definition of Tate cohomology in degrees

$-1, 0$. For $i \leq -2$, we just need to compute the homology, which we do using the same tactics as in Proposition 2.1. We start with the same projective resolution of $\mathbb{Z}$,

$$\cdots \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

then apply (covariant) $- \otimes_{\mathbb{Z}[G]} A$ and drop the $\mathbb{Z}$ term. Similar to before, we have very convenient isomorphisms.

$$\begin{tikzcd}
\cdots \arrow[r, "\sigma-1\otimes\mathrm{Id}_A"] & \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \arrow[r, "N_G\otimes\mathrm{Id}_A"] \arrow[d, "\cong"] & \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \arrow[r, "\sigma-1\otimes\mathrm{Id}_A"] \arrow[d, "\cong"] & \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \arrow[r] \arrow[d, "\cong"] & 0 \\
\cdots \arrow[r, "\sigma-1"] & A \arrow[r, "N_G"] & A \arrow[r, "\sigma-1"] & A \arrow[r] & 0
\end{tikzcd}$$

From this, we read off the homology $\widehat{H}^i(G, A) = H_{-i-1}(G, A)$ for $i \leq -2$, and it exactly what we claimed. □

2.2 $H^1(\mathrm{GL}_2(\mathbb{F}_p), \mathbb{F}_p^2)$

Proposition 2.3. *Let p be a prime, and consider $M = \mathbb{F}_p^2$ (viewed as column vectors) with the standard action from $\mathrm{GL}_2(\mathbb{F}_p)$ (by left matrix multiplication). For any subgroup $G \subset \mathrm{GL}_2(\mathbb{F}_p)$, $H^1(G, M)$ has order 1 or order p. If $p = 2$, then the order is 1.*

Proof. Let $G_p \subset G$ be a Sylow p-subgroup. Note that since the order of $\mathrm{GL}_2(\mathbb{F}_p)$ is $(p^2 - p)(p^2 - 1) = p(p-1)^2(p+1)$, any Sylow p-subgroup has order p or 1.

Because $pM = 0$, $H^1(G, M)$ is a p-torsion group. Since $\mathrm{Res} : H^1(G, M) \to H^1(G_p, M)$ is injective on the p-primary component (Corollary 1.8.24 of Sharifi [6]), this says that $\mathrm{Res} : H^1(G, M) \to H^1(G_p, M)$ is injective.

If $G_p = 0$, then $H^1(G, M) = H^1(G_p, M) = 0$ and there is nothing to prove, so suppose G_p has order p. Since all p-Sylow subgroups are conjugate, G_p is conjugate in $\mathrm{GL}_2(\mathbb{F}_p)$ to the cyclic unipotent subgroup U generated by

$$u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Then $G_p \cong U$ so $H^1(G_p, M) \cong H^1(U, M)$. So to show that $H^1(G, M)$ has order 1 or p, it suffices to show that $H^1(U, M)$ has order 1 or p (since the restriction map embeds $H^1(G, M)$ into $H^1(G_p, M) \cong H^1(U, M)$). Since U is fintie cyclic (of order p), by the computation of Tate cohomology for finite cyclic groups,

$$H^1(U, M) \cong \ker N/(u-1)M$$

where $N = 1 + u + \cdots + u^{p-1} \in \mathrm{Mat}_2(\mathbb{F}_p)$ is the norm map. For p odd,

$$N = \sum_{k=0}^{p-1} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p & \frac{p(p-1)}{2} \\ 0 & p \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

For $p = 2$,

$$N = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

So for p odd, $\ker N = \mathbb{F}_p^2$, and for p even, $\ker N = \mathbb{F}_p = \mathbb{F}_p e_1$, generated (as a U-module) by $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. The other part we need for $H^1(U, M) \cong \ker N/(u-1)M$ is $(u-1)M$, which is $\mathbb{F}_p e_1$. Thus we obtain

$$H^1(U, M) = \begin{cases} 0 & p = 2 \\ \mathbb{F}_p & p > 2 \end{cases}$$

□

Remark 2.4. The previous proof says a little bit more than the proposition asserts. It says that if p is odd and $G \subset \mathrm{GL}_2(\mathbb{F}_p)$ is a Sylow p-subgroup (so it has order p), then $H^1(G, M) \cong \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.

It also says that if p does not divide the order of $G \subset \mathrm{GL}_2(\mathbb{F}_p)$, then $H^1(G, M) = 0$, since $G_p = 0$ and $H^1(G_p, M) = 0$. On the other hand, if p does divide the order of G, all the proof tells us is that $H^1(G, M)$ embeds into $H^1(G_p, M) = \mathbb{Z}/p\mathbb{Z}$, so $H^1(G, M)$ may be zero or $\mathbb{Z}/p\mathbb{Z}$, we don't know for sure. Perhaps other methods exist to sharpen this, but this proof does not accomplish this.

2.3 Cohomology of infinite cyclic group

Lemma 2.5. *Let G be a group and let $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ be the augmentation map,*

$$\epsilon\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \qquad a_g \in \mathbb{Z}$$

The kernel of ϵ is equal to the ideal $I_G \subset \mathbb{Z}[G]$ generated by elements $g - 1$ for $g \in G$.

Proof. It is clear that for $g \in G$, $\epsilon(g-1) = 0$ so $I_G \subset \ker \epsilon$. Conversely, if $x = \sum a_g g \in \ker \epsilon$, then

$$0 = \epsilon\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \implies \sum_{g \in G} a_g g = \sum_{g \in G} a_g (g - 1)$$

so $x \in I_G$. □

Proposition 2.6. *Let G be an infinite cyclic group with generator σ. Then*

$$0 \to \mathbb{Z}[G] \xrightarrow{\sigma - 1} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

is a free resolution of $\mathbb{Z}$ as trivial $\mathbb{Z}[G]$-module. Thus

$$H^i(G, A) = \begin{cases} A^G & i = 0 \\ A/(\sigma - 1)A & i = 1 \\ 0 & i \geq 2 \end{cases}$$

Proof. It is clear that ϵ is surjective. To verify injectivity, suppose $x = \sum_{g\in G} a_g g = \sum_{i\in\mathbb{Z}} a_i\sigma^i \in \ker(\sigma - 1)$. Since $\sigma x - x = 0$, all the coefficients of x must be the same. Since x can have only finitely many nonzero coefficients, they must all be zero. Regarding exactness at the middle term, in the language of the previous lemma, $\ker\epsilon = I_G$. Since G is cyclic, I_G is generated by $\sigma - 1$, which is to say, I_G is the image of $\sigma - 1$, so the sequence is exact.

From this resolution, we apply $\mathrm{Hom}_{\mathbb{Z}[G]}(-, A)$ and drop the $\mathbb{Z}$ term to obtain a complex whose homology is $H^i(G, A)$. We also have canonical isomorphisms $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \cong A$, which gives an isomorphic complex whose homology is easier to read off.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \arrow[r, "(\sigma-1)_*"] \arrow[d, "\cong"] & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & A \arrow[r, "\sigma-1"] & A \arrow[r] & 0
\end{tikzcd}$$

From the bottom complex, we read off

$$H^i(G, A) = \begin{cases} \ker(\sigma - 1) = A^G & i = 0 \\ A/(\sigma - 1)A & i = 1 \\ 0 & i \geq 2 \end{cases}$$

□

3 Brauer groups of cyclic extensions

3.1 Relative Brauer group of cyclic extension

Proposition 3.1. *Let L/K be a finite cyclic Galois extension. Then* $\operatorname{Br}(L/K) \cong K^\times / \operatorname{N}_K^L(L^\times)$.

Proof. We use the isomorphism $\operatorname{Br}(L/K) \cong H^2(\operatorname{Gal}(L/K), L^\times)$. Since $\operatorname{Gal}(L/K)$ is finite cyclic, by the computation of Tate cohomology for finite cyclic groups,

$$H^2(\operatorname{Gal}(L/K), L^\times) \cong \widehat{H}^0(\operatorname{Gal}(L/K), L^\times) \cong (L^\times)^{\operatorname{Gal}(L/K)}/N_G L^\times$$

By Galois theory, $(L^\times)^{\operatorname{Gal}(L/K)} = K^\times$. Also, the group norm N_G coincides with the field norm N_K^L,

$$N_G(\alpha) = \left(\sum_{\sigma \in G} \sigma\right)(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) = \operatorname{N}_K^L(\alpha)$$

so

$$\operatorname{Br}(L/K) \cong K^\times / \operatorname{N}_K^L(L^\times)$$

□

3.2 $\operatorname{Br}(\mathbb{R})$ and $\operatorname{Br}(\mathbb{F}_q)$ via cohomology

Proposition 3.2. $\operatorname{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$*.*

Proof. The separable closure of $\mathbb{R}$ is the algebraic closure $\mathbb{C}$, so $\operatorname{Br}(\mathbb{R}) = \operatorname{Br}(\mathbb{R}^{\text{sep}}/\mathbb{R}) = \operatorname{Br}(\mathbb{C}/\mathbb{R})$. Since $\mathbb{C}/\mathbb{R}$ is finite cyclic (order 2, generated by complex conjugation), by Proposition 3.1,

$$\operatorname{Br}(\mathbb{R}) \cong \mathbb{R}^\times / \operatorname{N}_{\mathbb{R}}^{\mathbb{C}}(\mathbb{C}^\times)$$

The norm map in this case is $x + iy \mapsto x^2 + y^2$, so the image is $\mathbb{R}_{>0}$. Thus

$$\operatorname{Br}(\mathbb{R}) \cong \mathbb{R}^\times/\mathbb{R}_{>0} \cong \mathbb{Z}/2\mathbb{Z}\langle -1 \rangle$$

□

Proposition 3.3. $\operatorname{Br}(\mathbb{F}_q) = 0$*.*

Proof. The absolute Brauer group is the union of all the relative Brauer groups of finite Galois extensions. Also, $\mathbb{F}_q$ has a unique (up to isomorphism) extension of degree n, which we denote $\mathbb{F}_{q^n}$.

$$\operatorname{Br}(\mathbb{F}_q) = \bigcup_{n \geq 1} \operatorname{Br}(\mathbb{F}_{q^n}/\mathbb{F}_q)$$

Thus it suffices to show that $\operatorname{Br}(\mathbb{F}_{q^n}/\mathbb{F}_q) = 0$. The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is finite cyclic Galois, so by Proposition 3.1,

$$\operatorname{Br}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{F}_q^\times / \operatorname{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\mathbb{F}_{q^n})$$

Using the fact that norm maps are surjective for finite fields, this quotient is zero. □

3.3 $\operatorname{Br}(\mathbb{R})$ and $\operatorname{Br}(\mathbb{F}_q)$ via central simple algebras

Proposition 3.4. *Any central division algebra over $\mathbb{R}$ is isomorphic to the Hamilton quaternions. Consequently,* $\operatorname{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$.

Proof. Let D be a central division algebra over $\mathbb{R}$ with $d^2 = \dim_{\mathbb{R}} D$. Then D contains a maximal subfield K with $\dim_{\mathbb{R}} K = d$. Since the only nontrivial finite extension of $\mathbb{R}$ is $\mathbb{C}$, $K = \mathbb{C}$ and $d = 2$, so $\dim_{\mathbb{R}} D = 4$. Now consider the $\mathbb{R}$-algebra homomorphisms

$$\begin{aligned} \mathbb{C} &\to D \qquad z \mapsto z \\ \mathbb{C} &\to D \qquad z \mapsto \overline{z} \end{aligned}$$

By the Skolem-Noether theorem, these are conjugate, so there exists $j \in D^\times$ such that $jzj^{-1} = \overline{z}$ for all $z \in \mathbb{C}$. In particular, $jij^{-1} = -i$ or we may write this as $ji = -ij$, so j does not commute with $\mathbb{C}$, so j is not in $\mathbb{C}$. Now observe that

$$j^2 z j^{-2} = -(-z) = z$$

so j^2 commutes with $\mathbb{C}$. Since $j^2 \in D^\times$ is a unit, $\mathbb{C}(j^2)$ is a field, but there are no nontrivial finite extensions of $\mathbb{C}$, so $j^2 \in \mathbb{C}$. Since we have

$$j^2 = j(j^2)j^{-1} = \overline{j^2}$$

we also get $j^2 \in \mathbb{R}$. Since $j^2 \in \mathbb{R}$ but $j \notin \mathbb{R}$, j^2 must not be a positive real, since positive reals have square roots in $\mathbb{R}$. Thus $j^2 < 0$. Now up to rescaling, we may assume that $j^2 = -1$, by replacing j with $\frac{j}{\sqrt{|j^2|}}$. Finally, we claim that $1, i, j, ij$ is an $\mathbb{R}$-basis of D. Since $\dim_{\mathbb{R}} D = 4$, it suffices to show that they are linearly independent. Suppose there are $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that

$$\alpha + \beta i + \gamma j + \delta ij = \alpha + \beta i + (\gamma + \delta i)j = 0$$

If one of γ, δ is nonzero, then we may rearrange the above into

$$j = -\frac{\alpha + \beta i}{\gamma + \delta i}$$

which implies $j \in \mathbb{C}$, which we know to be false (since j does not commute with i). So $\gamma = \delta = 0$, which implies $\alpha + \beta i = 0$, which implies $\alpha = \beta = 0$. Thus $1, i, j, ij$ are linearly independent, so they form a basis of D. So D has a presentation

$$D = \langle 1, i, j, ij \mid i^2 = j^2 = -1, ij = -ji \rangle$$

which is precisely the usual presentation of the Hamilton quaternions, so D is isomorphic to the Hamilton quaternions.

Since nonzero elements of $\operatorname{Br}(\mathbb{R})$ correspond to isomorphism classes of central division algebras over $\mathbb{R}$, this shows that there is exactly one such isomorphism class, so there is exactly one nonzero element in $\operatorname{Br}(\mathbb{R})$. Thus it must be the group with two elements, $\mathbb{Z}/2\mathbb{Z}$. □

Proposition 3.5. *Any finite division ring is a field. Consequently,* $\operatorname{Br}(\mathbb{F}_q) = 0$.

Proof. Let D be a finite division ring of characteristic p, so D is a central division algebra over $\mathbb{F}_q$ for some $q = p^n$. Let $d^2 = \dim_{\mathbb{F}_q} D$. If $d = 1$, then D is a field and we are done, so suppose $d > 1$. Then D contains a maximal subfield P with $\dim_{\mathbb{F}_q} P = d > 1$. By the Skolem-Noether theorem, any two maximal subfields $P \subset D$ are conjugate, which is to say, for any two maximal subfields P, P', there exists $\sigma \in D^\times$ such that

$$P' = \sigma P \sigma^{-1}$$

Thus if we fix a maximal subfield $P \subset D$ (with $\dim_{\mathbb{F}_q} P = d$), the orbit of P under conjugation gives all maximal subfields of D. Since any element of $D^\times$ is contained in some maximal subfield of D, it follows that

$$D = \bigcup_{\sigma \in D^\times} \sigma P \sigma^{-1} \qquad D^\times = \bigcup_{\sigma \in D^\times} \sigma P^\times \sigma^{-1}$$

The second equality asserts that the finite group $D^\times$ is equal to the union of all conjugates of a given subgroup $P^\times$, but by a standard lemma in group theory, this is impossible if $P^\times$ is a proper subgroup. So we reach a contradiction, and conclude that d cannot be greater than 1, so $d = 1$ and $D = \mathbb{F}_q$ is a finite field.

Since any nonzero element of $\mathrm{Br}(\mathbb{F}_q)$ corresponds to a central division algebra over $\mathbb{F}_q$ of dimension > 1, the fact that there are no such division algebras implies that $\mathrm{Br}(\mathbb{F}_q) = 0$. □

4 $\mathbb{Z}_p$ and $\mathbb{Q}_p$

Throughout this section, let p be a prime.

Remark 4.1. Recall that a p-adic integer $x \in \mathbb{Z}_p$ has a unique expansion

$$x = \sum_{k=0}^{\infty} a_k p^k = a_0 + a_1 p + a_2 p^2 + \cdots$$

where $0 \leq a_i \leq p-1$. It is a unit (is in $\mathbb{Z}_p^\times$) if and only if $a_0 \neq 0$.

Lemma 4.2. *The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ has dense image. That is, if $x \in \mathbb{Z}_p$ and $n \geq 1$, there exists $\alpha \in \mathbb{Z}$ with $0 \leq \alpha \leq p^n - 1$ such that $|x - \alpha|_p \leq p^{-n}$.*

Proof. Using the expansion of above, write $x = a_0 + a_1 p + a_2 p^2 + \cdots$, then set $\alpha = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$. Then it is clear that $0 \leq \alpha \leq p^n - 1$ and using the nonarchimedean triangle inequality we get

$$|x - \alpha|_p = |a_n p^n + a_{n+1} p^{n+1} + \cdots|_p \leq \max_{i \geq n} |a_i p^i| = |p^n| = p^{-n}$$

□

4.1 p-adic units $\mathbb{Z}_p^\times$

Remark 4.3. From the previous unique description via expansions, it is clear that the following sequence is exact.

$$0 \to p^n \mathbb{Z}_p \hookrightarrow \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z} \to 0$$

where the right map is the "truncation" map

$$a_0 + a_1 p + a_2 p^2 + \cdots \mapsto a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$$

Thus from the first isomorphism theorem we obtain

$$\mathbb{Z}_p / p^n \mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

More generally, for $m \leq n$ we have a truncation map $p^m \mathbb{Z}_p \to \mathbb{Z}/p^{n-m}\mathbb{Z}$ with kernel $p^n \mathbb{Z}_p$ fitting into an exact sequence

$$0 \to p^n \mathbb{Z}_p \to p^m \mathbb{Z}_p \to \mathbb{Z}/p^{n-m}\mathbb{Z} \to 0$$

inducing an isomorphism

$$p^m \mathbb{Z}_p / p^n \mathbb{Z}_p \cong \mathbb{Z}/p^{n-m}\mathbb{Z}$$

The first version was just the case $m = 0$.

Definition 4.4. Let $U_0 = \mathbb{Z}_p^\times$ and for $n \geq 1$, set

$$U_n = 1 + p^n \mathbb{Z}_p = \left\{ 1 + a_n p^n + a_{n+1} p^{n+1} + \cdots \in \mathbb{Z}_p^\times \right\}$$

Note that U_n is a subgroup of $\mathbb{Z}_p^\times$, and that there is a filtration

$$\mathbb{Z}_p^\times \supset 1 + p\mathbb{Z}_p \supset 1 + p^2 \mathbb{Z}_p \supset \cdots \qquad U_0 \supset U_1 \supset U_2 \supset \cdots$$

Lemma 4.5. *There are exact sequences*

$$\begin{tikzcd} 1 \arrow[r] & 1 + p\mathbb{Z}_p \arrow[r, hook] & \mathbb{Z}_p^\times \arrow[r, "\text{mod } p"] & (\mathbb{Z}/p\mathbb{Z})^\times \arrow[r] & 1 \\ 1 \arrow[r] & 1 + p^n\mathbb{Z}_p \arrow[r, hook] & \mathbb{Z}_p^\times \arrow[r, "\text{mod } p^n"] & (\mathbb{Z}/p^n\mathbb{Z})^\times \arrow[r] & 1 \\ 1 \arrow[r] & 1 + p^{n+1}\mathbb{Z}_p \arrow[r, hook] & 1 + p^n\mathbb{Z}_p \arrow[r, "1+p^n x \mapsto x \text{ mod } p"] & \mathbb{Z}/p\mathbb{Z} \arrow[r] & 1 \end{tikzcd}$$

[2] *for $n \geq 1$ which induce isomorphisms*

$$U_0/U_1 \cong (\mathbb{Z}/p\mathbb{Z})^\times \qquad U_0/U_n \cong (\mathbb{Z}/p^n\mathbb{Z})^\times \qquad U_n/U_{n+1} \cong \mathbb{Z}/p\mathbb{Z}$$

Proof. Exactness is obvious by inspection, and the isomorphisms are immediate from the first isomorphism theorem. □

Definition 4.6. For $x \in \mathbb{Q}_p$, the p**-adic exponential** function is

$$\exp(x) = \sum_{n=0}^\infty \frac{x^n}{n!}$$

and the p**-adic logarithm** is

$$\log(1+x) = \sum_{n=1}^\infty (-1)^{n+1} \frac{x^n}{n}$$

Note that at this point, these are both formal power series, but the next lemma determines their respective domains of convergence.

Lemma 4.7. *Let $f(x) = \sum_{n=0}^\infty a_n x^n \in \mathbb{Q}_p[[x]]$. Define*

$$r_f = \left(\limsup |a_n|_p^{1/n} \right)^{-1}$$

Then $f(x)$ converges for $|x|_p < r_f$ and diverges for $|x|_p > r_f$.

Proof. Proposition 4.3.1 of Gouvea [3]. Gouvea also gives a criterion for convergence on the "boundary" $|x|_p = r_f$ which is not included here. □

Lemma 4.8. *The p-adic logarithm and exponential have the following properties.*

[2] The first sequence is redudant, as it is a special case of the second, but we include it anyway.

1. *For $f(x) = \log(1+x)$, $r_f = 1$, so the domain of $\log(1+x)$ is $p\mathbb{Z}_p$ and the domain of $\log(x)$ is $1 + p\mathbb{Z}_p$.*

2. *For $f(x) = \exp(x)$, $r_f = p^{-1/(p-1)}$, so the domain of $\exp(x)$ is*

$$\begin{cases} p\mathbb{Z}_p & p \geq 3 \\ 4\mathbb{Z}_2 & p = 2 \end{cases}$$

3. *Whenever there is convergence, the following identities hold.*

$$\begin{aligned} \log(ab) &= \log a + \log b \\ \exp(a+b) &= (\exp a)(\exp b) \\ \exp \log a &= a \\ \log \exp a &= a \end{aligned}$$

Proof. Section 4.5 of Gouvea [3]. In particular, Lemma 4.5.1, Proposition 4.5.3, Lemma 4.5.5, Proposition 4.5.7, Proposition 4.5.8 □

Proposition 4.9. *If $p \geq 3$, then we have isomorphisms*

$$\mathbb{Z}_p \cong p\mathbb{Z}_p \underset{\log}{\overset{\exp}{\rightleftarrows}}_{\cong} 1 + p\mathbb{Z}_p = U_1$$

In the case $p = 2$ we have isomorphisms

$$\mathbb{Z}_2 \cong 4\mathbb{Z}_2 \underset{\log}{\overset{\exp}{\rightleftarrows}}_{\cong} 1 + 4\mathbb{Z}_2 = U_2$$

Proof. The isomorphisms given by exp and log follow from the previous lemma 4.8. The isomorphism $\mathbb{Z}_p \cong p\mathbb{Z}_p$ is given by $x \mapsto px$, and similarly $\mathbb{Z}_2 \cong 4\mathbb{Z}_2$ via $x \mapsto 4x$. See Proposition 4.5.9 of Gouvea [3] for more on this. □

Remark 4.10. Let p be odd. Under the isomorphism $\log : 1 + p\mathbb{Z}_p \to p\mathbb{Z}_p$, the subgroup $U_n = 1 + p^n\mathbb{Z}_p \subset 1 + p\mathbb{Z}_p$ on the left side has image $p^n\mathbb{Z}_p$ on the right side, so the p-adic logarithm gives an isomorphism

$$U_n = 1 + p^n\mathbb{Z}_p \cong p^n\mathbb{Z}_p$$

Proposition 4.11 (Structure of $\mathbb{Z}_p^\times$)**.**

$$\mathbb{Z}_p^\times \cong \begin{cases} U_1 \times (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^\times & p \geq 3 \\ U_2 \times (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}_2 \times \{\pm 1\} & p = 2 \end{cases}$$

Proof. In light of the isomorphisms from Proposition 4.9, the first and second exact sequences of Lemma 4.5 give exact sequences below.

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}_p \cong U_1 \arrow[r, hook] & \mathbb{Z}_p^\times \arrow[r] & (\mathbb{Z}/p\mathbb{Z})^\times \arrow[r] & 0 & p \geq 3 \\ 0 \arrow[r] & \mathbb{Z}_2 \cong U_2 \arrow[r, hook] & \mathbb{Z}_2^\times \arrow[r] & (\mathbb{Z}/4\mathbb{Z})^\times \cong \{\pm 1\} \arrow[r] & 0 & \end{tikzcd}$$

We claim that these are split exact. For the $p = 2$ sequence, simply use the embedding

$$\{\pm 1\} \hookrightarrow \mathbb{Z}^\times \hookrightarrow \mathbb{Z}_2^\times$$

Splitting of the other sequence is more involved, so we omit some details. Basically, it suffices to find $(p-1)$st roots of unity in $\mathbb{Z}_p^\times$, since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$.

Consider $f(x) = x^{p-1} - 1 \in \mathbb{Z}[x] \subset \mathbb{Z}_p[x]$. Over $\mathbb{F}_p$, this splits completely into $p-1$ distinct linear factors, and the derivative is $\overline{f'}(x) = (p-1)x^{p-2} \neq 0$, so by Hensel's lemma, all of the simple roots lift to roots in $\mathbb{Z}_p$. Thus $\mathbb{Z}_p$ contains all $(p-1)$st roots of unity.

See Corollary 4.5.10 of Gouvea [3] for some more details. Once the sequences split, we obtain exactly the claimed isomorphisms. □

Corollary 4.12 (Structure of $\mathbb{Q}_p^\times$)**.**

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times \cong \begin{cases} \mathbb{Z} \times \mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^\times & p \geq 3 \\ \mathbb{Z} \times \mathbb{Z}_2 \times (\mathbb{Z}/4\mathbb{Z})^\times & p = 2 \end{cases}$$

Proof. Any element of $\mathbb{Q}_p^\times$ can be written uniquely as $p^n u$ where $u \in \mathbb{Z}_p^\times$, so we get an isomorphism

$$\mathbb{Q}_p^\times \to \mathbb{Z} \times \mathbb{Z}_p^\times \qquad p^n u \mapsto (n, u)$$

The rest is immediate from the structure of $\mathbb{Z}_p^\times$. □

4.2 Completions of $\mathbb{Q}$ are non-isomorphic

Remark 4.13. From the structure of $\mathbb{Q}_p^\times$ given in Corollary 4.12, and the fact that $\mathbb{Z}$ and $\mathbb{Z}_p$ are torsion-free, the torsion subgroup of $\mathbb{Q}_2$ is $(\mathbb{Z}/4\mathbb{Z})^\times$ and for $p \geq 3$ the torsion subgroup of $\mathbb{Q}_p^\times$ is $(\mathbb{Z}/p\mathbb{Z})^\times$. That is to say, the only roots of unity in $\mathbb{Q}_2$ are ± 1, and for $p \geq 3$ the only roots of unity in $\mathbb{Q}_p^\times$ are $(p-1)$st roots of unity.

Proposition 4.14. *The fields $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \ldots$ are all pairwise non-isomorphic (as abstract fields).*

Proof. According to the following table comparing the torsion subgroup of the multiplicative group, none of $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3$ is isomorphic to $\mathbb{Q}_5, \mathbb{Q}_5, \ldots$ and none of $\mathbb{Q}_5, \mathbb{Q}_7, \ldots$ are isomorphic to each other.

K	Torsion in $K^\times$
$\mathbb{R}$	$\mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\}$
$\mathbb{Q}_2$	$\mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\}$
$\mathbb{Q}_3$	$\mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\}$
$\mathbb{Q}_p$, $p \geq 5$	$\mathbb{Z}/(p-1)\mathbb{Z}$

So it remains to check that $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3$ are pairwise non-isomorphic. For this, we consider the invariant $K^\times / K^{\times 2}$.

K	$K^\times / K^{\times 2}$	$\lvert K^\times / K^{\times 2} \rvert$
$\mathbb{R}$	$\mathbb{R}/\mathbb{R}_{>0} \cong \mathbb{Z}/2\mathbb{Z}$	2
$\mathbb{Q}_2$	$(\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z})/2 \cong (\mathbb{Z}/2\mathbb{Z})^3$	8
$\mathbb{Q}_3$	$(\mathbb{Z} \times \mathbb{Z}_3 \times \mathbb{Z}/2\mathbb{Z})/2 \cong (\mathbb{Z}/2\mathbb{Z})^2$	4

Note that $\mathbb{Z}_3/2 = 0$ because 2 is a unit in $\mathbb{Z}_3$. Since these are all distinct, none of these are isomorphic either. □

Remark 4.15. Let p be an odd prime. One interesting consequence of $|\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}| = 4$ is that $\mathbb{Q}_p$ has exactly three quadratic field extensions (in a fixed algebraic closure), because any quadratice field extension is formed by adjoining a square root of a non-square.

4.3 The group of units $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic

Proposition 4.16. *Let p be an odd*[3] *prime and $n \in \mathbb{Z}_{\geq 1}$. The group of units $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic.*

Proof. By Lemma 4.5,

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times/U_n = \mathbb{Z}_p^\times/(1 + p^n\mathbb{Z}_p)$$

Using Proposition 4.11,

$$\mathbb{Z}_p^\times \cong U_1 \times (\mathbb{Z}/p\mathbb{Z})^\times$$

Since $U_n \subset U_1$, in the quotient $\mathbb{Z}_p^\times/U_n \cong (U_1 \times (\mathbb{Z}/p\mathbb{Z})^\times)/U_n$ the U_n lives entirely in the U_1 component, so

$$\mathbb{Z}_p^\times/U_n \cong (U_1 \times (\mathbb{Z}/p\mathbb{Z})^\times)/U_n \cong (U_1/U_n) \times (\mathbb{Z}/p\mathbb{Z})^\times$$

By Remark 4.10, $U_n \cong p^n\mathbb{Z}_p$, so

$$U_1/U_n = \frac{1 + p\mathbb{Z}_p}{1 + p^n\mathbb{Z}_p} \cong \frac{p\mathbb{Z}_p}{p^n\mathbb{Z}_p} \cong \mathbb{Z}/p^{n-1}\mathbb{Z}$$

The final isomorphism comes from Remark 4.3. Putting this together, we obtain

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong U_1/U_n \times (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/p^{n-1}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times$$

Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$, the product on the right is a product of cyclic groups of relatively prime orders, so it is cyclic. □

[3] This does fail for $p = 2$ for at least some values of n. As a counterexample, $(\mathbb{Z}/8\mathbb{Z})^\times$ is order four, but not cyclic, since $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$.

5 Inflation-restriction sequence

5.1 Statement of Inflation-restriction sequence, proof of exactness for first 3 terms

Proposition 5.1. *Let G be a group, let $N \subset G$ be a normal subgroup, and let A be a G-module. Then the following sequence is exact.*

$$0 \longrightarrow H^1(G/N, A^N) \xrightarrow{\mathrm{Inf}} H^1(G, A) \xrightarrow{\mathrm{Res}} H^1(N, A) \longrightarrow H^2(G/N, A^N) \xrightarrow{\mathrm{Inf}} H^2(G, A)$$

Remark 5.2. An incomplete proof of the above is given in Theorem 4.1.20 of Rosenberg [5]. A confusing proof is given in Proposition 3.3.16 of Gille & Szamuely [2]. A proof utilizing spectral sequences is given in Proposition 6.8.2 and Remark 6.8.3 of Weibel [7]. See below for a proof of exactness for just the first three terms, following Theorem 1.8.10 of Sharifi [6].

Remark 5.3. We recall the description of Inf in terms of cocycles. Let G be a group with a normal subgroup N and let A be a G-module. For a cocycle $\phi : G/N \to A^N$ and for $g \in G$, we have a cocycle in $Z^1(G, A)$ described by

$$\widetilde{\mathrm{Inf}}(\phi) : G \to A \qquad \widetilde{\mathrm{Inf}}(\phi)(g) = \phi(\overline{g})$$

where $\overline{g} = gN$ is the image of g in G/N. That is to say, there is a map

$$\widetilde{\mathrm{Inf}} : Z^1(G, A) \to Z^1(G/N, A^N) \qquad \phi \mapsto (g \mapsto \phi(\overline{g}))$$

In these terms, $\mathrm{Inf}[\phi] = [\widetilde{\mathrm{Inf}}(\phi)]$. The previous equality is represented by the following commutative square, where the vertical arrows are quotient maps.

$$\begin{tikzcd}
Z^1(G/N, A^N) \arrow[r, "\widetilde{\mathrm{Inf}}"] \arrow[d] & Z^1(G, A) \arrow[d] \\
H^1(G/N, A^N) \arrow[r, "\mathrm{Inf}"] & H^1(G, A)
\end{tikzcd}$$

Remark 5.4. We recall the description of Res in terms of cocycles. Let G be a group with a subgroup N and let A be a G-module. The literal function restriction map

$$Z^1(G, A) \to Z^1(N, A) \qquad \psi \mapsto \psi|_H$$

induces Res, which is to say $\mathrm{Res}[\psi] = [\psi|_N]$. We represent this with the following commutative square, where vertical arrows are quotient maps.

$$\begin{tikzcd}
Z^1(G, A) \arrow[r, "\psi \mapsto \psi|_N"] \arrow[d] & Z^1(N, A) \arrow[d] \\
H^1(G, A) \arrow[r, "\mathrm{Res}"] & H^1(N, A)
\end{tikzcd}$$

Proposition 5.5. *Let G be a group and $N \subset G$ a normal subgroup, and let A be a G-module. Then the following sequence is exact.*

$$0 \longrightarrow H^1(G/N, A^N) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(N, A)$$

Proof. First, we show Inf is injective (which gives exactness at the first term). Let $[\phi] \in H^1(G/N, A^N)$ with representative cocycle ϕ such that $[\phi] \in \ker \text{Inf}$, so $\text{Inf}[\phi] = [\widetilde{\text{Inf}}(\phi)] = 0 \in H^1(G, A)$. That is, $\widetilde{\text{Inf}}(\phi)$ is a coboundary, which in degree one means that there exists $a \in A$ so that for all $g \in G$,

$$\widetilde{\text{Inf}}(\phi)(g) = \phi(\overline{g}) = (g - 1)a$$

In particular, for $n \in N$,

$$0 = \phi(\overline{n}) = (n - 1)a$$

so $a \in A^N$. Then reusing the previous equality, we have $a \in A^N$ such that

$$\phi(\overline{g}) = (g - 1)a = (\overline{g} - 1)a$$

which is exactly the condition for ϕ to be a coboundary. Thus $[\phi] = 0$, and Inf is injective.

Now we need exactness at $H^1(G, A)$. We can easily get $\text{im Inf} \subset \ker \text{Res}$ by showing that $\text{Res} \circ \text{Inf} = 0$. Let $[\phi] \in H^1(G/N, A^N)$ with representative cocycle ϕ. Then

$$\text{Res} \circ \text{Inf}[\phi] = \text{Res}[\widetilde{\text{Inf}}(\phi)] = [\widetilde{\text{Inf}}(\phi)|_N]$$

But just as a cocycle, $\widetilde{\text{Inf}}(\phi)|_N$ is zero, because for $n \in N$,

$$\widetilde{\text{Inf}}(\phi)|_N(n) = \phi(\overline{n}) = \phi(1) = 0$$

[4] Thus $\text{Res} \circ \text{Inf} = 0$. Now we need to show $\ker \text{Res} \subset \text{im Inf}$. Let $[\alpha] \in \ker \text{Res} \subset H^1(G, A)$, with representative cocycle $\alpha \in Z^1(G, A)$. Since $\text{Res}[\alpha] = [\alpha|_N] = 0$, $\alpha|_N$ is a coboundary, so there exists $a \in A$ such that for all $n \in N$, $\alpha(n) = (n - 1)a$. Define

$$\beta : G \to A \qquad \beta(g) = \alpha(g) - (g - 1)a$$

This is defined so that for $n \in N$,

$$\beta(n) = \alpha(n) - (n - 1)a = 0$$

Note that $\beta \in Z^1(G, A)$, since it differs from the cocylce α by a coboundary $(g - 1)a$, which also means $[\beta] = [\alpha] \in H^1(G, A)$. Also, for $g \in G, n \in N$,

$$\beta(gn) = g\beta(n) + \beta(g) = \beta(g)$$

[4] Note that a cocycle vanishes on the identity. This follows from the cocycle relation: $\phi(x) = \phi(1x) = 1\phi(x) + \phi(1) \implies \phi(1) = 0$.

so β factors through G/N, meaning that there is a map $\overline{\beta}$ making the following diagram commute, which is to say, $\overline{\beta}(\overline{g}) = \beta(g)$.

$$\begin{tikzcd}
G \arrow[r, "\beta"] \arrow[d] & N \\
G/N \arrow[ur, "\overline{\beta}"'] &
\end{tikzcd}$$

Also, for $g \in G, n \in N$,

$$\begin{aligned} n\beta(g) &= n\beta(g) + \beta(n) = \beta(ng) \\ &= \beta(gg^{-1}ng) = g\beta(g^{-1}ng) + \beta(g) = \beta(g) \end{aligned}$$

the last equality uses normality of N to say that $g^{-1}ng \in N$. Thus the image of β lands in A^N, so $\overline{\beta} \in H^1(G/N, A^N)$. Finally, it is immediate that $\widetilde{\mathrm{Inf}}(\overline{\beta}) = \beta$, so

$$\mathrm{Inf}[\,\overline{\beta}\,] = [\widetilde{\mathrm{Inf}}(\overline{\beta})] = [\beta] = [\alpha]$$

proving $\ker \mathrm{Res} \subset \mathrm{im}\,\mathrm{Inf}$. □

5.2 $H^1(G, M)$ for G profinite, M discrete, torsion free, finitely generated

Remark 5.6. Let G be a profinite group. Recall that a subgroup is open if and only if it is closed and of finite idex.

$$\{\text{open subgroups}\} = \{\text{closed subgroups of finite index}\}$$

Additionally, a closed subset of a compact set is compact, and since G is Hausdorff, a compact set is closed. Thus

$$\{\text{closed subgroups}\} = \{\text{compact subgroups}\}$$

$$\{\text{open subgroups}\} = \{\text{closed subgroups of finite index}\} = \{\text{compact subgroups of finite index}\}$$

Proposition 5.7. *Let G be a profinite group and M a discrete G-module which is torsion free and finitely generated as an abelian group. Then $H^1(G, M)$ is finite.*

Proof. Let $m_1, \dots, m_n$ be a set of generators for M. Set $G_i = \mathrm{stab}(m_i)$. Since M is a discrete module, G_i is open in G. Then set

$$G_M = \bigcap_{i=1}^{n} G_i$$

and note that G_M is also open, since it is a finite intersection of open sets. G_M acts trivially on generators of M, so it acts trivially on all of M. Consider the conjugation action of G on its set of subgroups.

$$G \times \{\text{subgroups } H \subset G\} \to \{\text{subgroups } H \subset G\} \qquad g \cdot H = gHg^{-1}$$

For the subgroup G_M, the stabilizer of this action is the normalizer $\text{stab}(G_M) = N_G(G_M)$, and the orbit is the set of conjugate subgroups. Because G_M is open, it has finite index, and because $G_M \subset N_G(G_M)$, the normalizer also has finite index. By the orbit-stabilizer theorem, the size of the orbit is equal to the index of the stabilizer, so the size of the orbit is finite, which is to say, G_M has finitely many conjugate subgroups. Thus we have a finite intersection

$$N = \bigcap_{g \in G} g G_M g^{-1}$$

so N is a finite index open subgroup. It is clear that N is normal, and that N acts trivially on M, so $M^N = M$. Since N acts trivially on M, the decomposition $M \cong \oplus\mathbb{Z}$ is a decomposition of N-modules, so

$$H^1(N, M) = H^1(N, \oplus\mathbb{Z}) \cong \bigoplus H^1(N, \mathbb{Z}) \cong \text{Hom}_{\text{cts}}(N, \mathbb{Z})$$

Since N is an open subgroup of a finite index in a profinite group, it is also compact, so the image of N under a continuous homomorphism $N \to \mathbb{Z}$ is a compact subgroup of $\mathbb{Z}$, which is to say, it is trivial. Thus $\text{Hom}(N, \mathbb{Z}) = 0$, so $H^1(N, M) = 0$. Now consider the first three nonzero terms of the Inflation-Restriction sequence.

$$0 \longrightarrow H^1(G/N, M^N) \longrightarrow H^1(G, M) \longrightarrow H^1(N, M) = 0$$

By exactness, $H^1(G, M) \cong H^1(G/N, M^N) = H^1(G/N, M)$. Recall that G/N is finite, so from the restriction-corestriction sequence, we know that $H^1(G/N, M)$ is torsion of exponent dividing $|G/N|$. Since M is finitely generated, $H^1(G/N, M)$ is finitely generated. Thus $H^1(G/N, M)$ is a torsion and finitely generated abelian group, so it is finite. Thus $H^1(G, M)$ is also finite. □

6 Merkurjev-Suslin theorem

6.1 Construction of Galois symbol

Review check. Outline the process of constructing the Galois symbol map $h^n_{K,m} : K^M_n(K) \to H^n(G_K, \mu_m^{\otimes n}$, assuming $\operatorname{char} K$ is coprime to m.

Remark 6.1. Let K be a field and let m be a positive integer such that m is coprime to the characteristic of K, so that the group of mth roots of unity μ_m lives in a separable closure K^{sep}. Let $G_K = \operatorname{Gal}(K^{\text{sep}}/K)$ be the absolute Galois group of K. Recall from Kummer theory that in this situation, there is an isomorphism

$$K^\times/K^{\times m} \cong H^1(G_K, \mu_m)$$

We may also view this as a surjection $K^\times \to H^1(G_K, \mu_m)$ with kernel $K^{\times m}$.

$$0 \to K^{\times m} \hookrightarrow K^\times \to H^1(G_K, \mu_m) \to 0$$

The isomorphism may be described explicitly in terms of elements as follows. For $a \in K^\times$, the class of $a \in K^\times/K^{\times m}$ corresponds to the Kummer cocycle $\chi_a \in H^1(G_K, \mu_m)$, where

$$\chi_a : G_K \to \mu_m \qquad \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$$

where α is any mth root of a. For details behind this, such as why χ_a is well defined, or why it is a cocycle, see Proposition 4.3.6 of Gille & Szamuley [2] or Proposition 2.5.8 of Sharifi [6].

Definition 6.2. Let R be a ring and M be an R-module. We use the notation $M^{\otimes n}$ for the n-fold tensor product $M \otimes_R \cdots \otimes_R M$ with n factors. (In what follows, we will always have $R = \mathbb{Z}$, but this notation makes sense more generally.)

Definition 6.3. Let $K, m, K^{\text{sep}}, \mu_m, G_K$ be as above. For $n \in \mathbb{Z}_{\geq 2}$, Consider the cup product (all tensor products over $\mathbb{Z}$)

$$H^1(G_K, \mu_m)^{\otimes n} \xrightarrow{\cup} H^n(G_K, \mu_m^{\otimes n})$$

Combining this with the surjections $K^\times \to H^1(G_K, \mu_m)$, we obtain a homomorphism

$$\partial^n : (K^\times)^{\otimes n} \to H^n(G_K, \mu_m^{\otimes n})$$

Remark 6.4. Recall the general fact that for two positive integers a, b,

$$\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/\gcd(a,b)\mathbb{Z}$$

Iterating this, we obtain

$$\mu_m^{\otimes n} = \mu_m \otimes \cdots \otimes \mu_m \cong \mathbb{Z}/m\mathbb{Z} \otimes \cdots \otimes \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \cong \mu_m$$

So for the target of ∂^n we have $H^n(G_K, \mu_m^{\otimes n}) \cong H^n(G_K, \mu_m)$. Despite this, we still often write the tensor product.

Proposition 6.5. *Let ∂^n be the map defined above. If $a_1, \ldots, a_n \in K^\times$ such that $a_i + a_j = 1$ for some pair $i \neq j$, then $\partial^n(a_1 \otimes \cdots \otimes a_n) = 0$.*

Proof. Lemma 4.6.2 and Proposition 4.6.1 in Gille & Szamuley [2]. Maybe I'll include this later, maybe it isn't important to know the details here. □

Definition 6.6. Let K, ∂^n, etc. be as above. The nth **Milnor K-group** $K_n^M(K)$ is the quotient of $(K^\times)^{\otimes n}$ by the ideal generated by elements $a_1 \otimes \cdots \otimes a_n$ for which some pair i, j we have $a_i + a_j = 1$. By definition, ∂^n vanishes on this ideal, and induces a homomorphism

$$h^n_{K,m} : K_n^M(K) \to H^n(G_K, \mu_m^{\otimes n})$$

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{ker} \arrow[r] & (K^\times)^{\otimes n} \arrow[r, "\{\ldots\}"] \arrow[d, "\partial^n"'] & K_n^M(K) \arrow[r] \arrow[dl, "h^n_{K,m}"] & 0 \\
& & H^2(G_K, \mu_m^{\otimes n}) & &
\end{tikzcd}$$

The class of $a_1 \otimes \cdots \otimes a_n \in (K^\times)^{\otimes n}$ in the quotient $K_n^M(K)$ is denoted by $\{a_1, \ldots, a_n\}$ and is called a **symbol**. The map $h^n_{K,m}$ is the **Galois symbol** map.

6.2 Statement of Merkurjev-Suslin theorem in terms of cyclic algebras

Review check. State the Merkurjev-Suslin theorem for a field K containing a primitive mth root of unity in terms of $\mathrm{Br}(K)$ and cyclic algebras.

Definition 6.7. Let K be a field containing a primitive mth root of unity ω. For $a, b \in K^\times$, the **cyclic algebra** $(a, b)_\omega$ is given by the presentation

$$\langle x, y \mid x^m = a, y^m = b, xy = \omega yx \rangle$$

Note that $\dim_K (a, b)_\omega = m^2$, with a K-basis given by products $x^i y^j$ for $0 \leq i, j \leq m - 1$.

Theorem 6.8 (Merkerjev-Suslin, Theorem 2.5.7 on page 41 of Gille & Szamuely [2])**.** *Let K be a field containing a primitive mth root of unity ω. The a central simple K-algebra A whose class has order dividing m in $\mathrm{Br}(K)$ is Brauer equivalent to a tensor product of cyclic algebras.*

$$[A] = (a_1, b_1)_\omega \otimes_K \cdots \otimes_K (a_i, b_i)_\omega$$

That is, the m-torsion subgroup ${}_m\mathrm{Br}(K) \subset \mathrm{Br}(K)$ is generated by cyclic algebras.

Remark 6.9. Every field has a primitive square root of unity (namely -1), so the case $m = 2$ says that the 2-torsion of $\mathrm{Br}(K)$ for any field K is generated by quaternion algebras. (This is pointed out in Theorem 1.5.8 of Gille & Szamuely [2].)

6.3 Statement of Merkurjev-Suslin theorem in terms of Galois symbol

Review check. State the Merkurjev-Suslin theorem in general for any field K, in terms of the Galois symbol $h^2_{K,m} : K_2^M(K) \to H^2(G_K, \mu_m^{\otimes 2})$.

Theorem 6.10 (Merkurjev-Suslin theorem, Theorem 4.6.6 on page 132 of Gille & Szamuely [2])**.** *Let K be a field and m a positive integer which is invertible in K. For $n = 2$, the Galois symbol map is a surjection*

$$h^2_{K,m} : K_2^M(K) \twoheadrightarrow H^2(G_K, \mu_m^{\otimes 2})$$

with kernel $mK_2(M)$, so it induces an isomorphism

$$K_2^M(K)/m \cong H^2(G_K, \mu_m^{\otimes 2})$$

Remark 6.11. The previous theorem is a special case of the much more general Voevodsky-Rost theorem (published 2000), formerly known as the Bloch-Kato conjecture. It says that $h^n_{K,m}$ is an isomorphism for all $n \geq 0$, not just $n = 2$. Note that the case $n = 0$ is trivial, and $n = 1$ is just the isomorphism

$$K_1(K)/m = K^\times / K^{\times m} \cong H^1(G_K, \mu_m)$$

of Kummer theory. The case $n = 2$ (above) was proven by Merkurjev-Suslin in 1982.

Remark 6.12. Let K be a field and let m be a positive integer which is coprime to the characteristic of K. Let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the absolute Galois group. From remark 6.4, we have an isomorphism

$$H^2(G_K, \mu_m^{\otimes 2}) \cong H^2(G_K, \mu_m)$$

From Kummer theory, we have an isomorphism

$$H^2(G_K, \mu_m) \cong {}_m \mathrm{Br}(K)$$

Combining these with the isomorphism of the Merkurjev-Suslin theorem, we obtain

$$K_2^M(K)/m \cong {}_m \mathrm{Br}(K)$$

Remark 6.13. Here is a large diagram attempting to summarize the various objects and maps involved in the above statements. The map δ is one of the isomorphisms from Kummer theory, coming from the connecting homomorphism of a LES.

The vertical sequence involving $K_2^M(K)$ is exact by definition of $K_2^M(K)$. The first horizontal row is exact by definition of kernel. The inclusion of $\langle u \otimes (1-u) \rangle$ into $\ker \partial^2$ is the content of Proposition 6.5. Exactness of the second horizontal row is the content of the

Merkurjev-Suslin theorem.

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & & \langle u \otimes (1-u) \mid u \in K^\times \rangle \arrow[d, hook] \arrow[dl, hook] & & \\
0 \arrow[r] & \ker \partial^2 \arrow[r, hook] & K^\times \otimes K^\times \arrow[r, "\partial^2"] \arrow[d, two heads] & H^1(G_K, \mu_m) \otimes H^1(G_K, \mu_m) \arrow[d, "\cup"] & \\
0 \arrow[r] & mK_2^M(K) \arrow[r, hook] & K_2^M(K) \arrow[r, two heads, "h^2_{K,m}"] \arrow[d] & H^2(G_K, \mu_m^{\otimes 2}) \arrow[r] \arrow[d, "\cong"] & 0 \\
 & & 0 & H^2(G_K, \mu_m) \arrow[d, "\cong \text{ Kummer theory}"] & \\
 & & & {}_m\operatorname{Br}(K) &
\end{tikzcd}$$

6.4 Connection between the two versions

Definition 6.14. Let L/K be a cyclic Galois extension of order m, and fix an isomorphism $\chi : \operatorname{Gal}(L/K) \to \mathbb{Z}/m\mathbb{Z}$. Let $b \in K^\times$, and let $\sigma = \chi^{-1}(1)$. The **cyclic algebra** (χ, b) is the algebra with the following presentation. It is generated as an L-algebra by L and an element y, satisfying

$$y^m = b \qquad \sigma(\lambda) = y^{-1}\lambda y, \ \ \forall \lambda \in L$$

Remark 6.15. If K contains a primitive mth root of unity ω, then there is an isomorphism $(\chi, b) \cong (a, b)_\omega$ [5] which justifies the double use of the term "cyclic algebra." See Corollary 2.5.5 of Gille & Szamuely [2].

Proposition 6.16. *Let K be a field, fix separable closure K^{sep}, and let $G_K = \operatorname{Gal}(K^{\text{sep}}/K)$. Let L/K be a cyclic Galois extension of degree m contained in K^{sep}, and let $G = \operatorname{Gal}(L/K)$. Fix an isomorphism*

$$\chi : G \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z}$$

Then define

$$\widetilde{\chi} : G_K \to \mathbb{Z}/m\mathbb{Z} \qquad \sigma \mapsto \chi(\sigma|_L)$$

Let $\delta : H^1(G_K, \mathbb{Z}/m\mathbb{Z}) \to H^2(G_K, \mathbb{Z})$ be the coboundary map of the LES associated to

$$0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$$

Then consider the cup product map

$$H^2(G_K, \mathbb{Z}) \otimes H^0(G_K, K^{\text{sep}\,\times}) \xrightarrow{\cup} H^2(G_K, K^{\text{sep}\,\times})$$

[5] There are details about what a anc χ should be to make this work, but we omit these.

Fix $b \in K^\times$. Under the isomorphism

$$H^2(G_K, K^{\mathrm{sep}\,\times}) \cong \mathrm{Br}(K)$$

the element $\delta(\widetilde{\chi}) \cup b$ correpends to the Brauer class of the cyclic algebra (χ, b).

Proof. Proposition 4.7.3 of Gille & Szamuley [2]. □

Proposition 6.17. *Let K be a field and let m be a positive integer which is coprime to the characteristic of K, and suppose K contains a primitive mth root of unity ω. Let $a, b \in K^\times$. Under the isomorphism*

$$K_2^M(K)/m \cong {}_m\mathrm{Br}(K)$$

of remark 6.12, the element $\{a, b\}$ corresponds to the Brauer class of the cyclic algebra $(a, b)_\omega$. That is, $h^n_{K,m}\{a, b\}$ is Brauer equivalent to $(a, b)_\omega$.

Proof. Proposition 4.7.1 of Gille & Szamuely [2]. □

Remark 6.18. The tensor product $K^\times \otimes K^\times$ is generated by simple tensors $a \otimes b$, so the quotient $K_2^M(K)$ is generated by the images of these, that is, $K_2^M(K)$ is generated by symbols $\{a, b\}$. Thus the previous proposition says that ${}_m\mathrm{Br}(K)$ is generated by cyclic algebras $(a, b)_\omega$. That is to say, the Galois symbol version of Merkurjev-Suslin 6.10 implies the cyclic algebra version of Merkurjev-Suslin 6.8.

7 K_2 of a field

Theorem 7.1 (Matsumoto). *Let K be a field. $K_2(K)$ is generated by symbols $\{u, v\}$ for $u, v \in K^\times$ subject to the relations*

$$\begin{aligned} \{uv, w\} &= \{u, w\}\{v, w\} \\ \{u, vw\} &= \{u, v\}\{u, w\} \\ \{u, 1-u\} &= 1 \end{aligned}$$

for $u, v, w \in K^\times$. Note that the last relation only makes sense for $u \neq 1$.

Remark 7.2. If we write $K_2(K)$ additively instead of multiplicatively, the previous relations become

$$\begin{aligned} \{uv, w\} &= \{u, w\} + \{v, w\} \\ \{u, vw\} &= \{u, v\} + \{u, w\} \\ \{u, 1-u\} &= 0 \end{aligned}$$

Lemma 7.3. *Symbols satsify the relations*

$$\begin{aligned} \{\alpha_1^m, \alpha_2, \ldots, \alpha_n\} &= \{\alpha_1, \ldots, \alpha_n\}^m && \text{for all } m \in \mathbb{Z} \\ \{\alpha_1, \ldots, \alpha_n\} &= 1 && \text{if } \alpha_i = 1 \text{ for some } i \end{aligned}$$

Proof. The first is an immediate consequence of multiplicativity. The second is a consequence of the first, as

$$\begin{aligned} \{\ldots, 1, \ldots\} = \left\{\ldots, xx^{-1}, \ldots, \right\} &= \{\ldots, x, \ldots\}\left\{\ldots, x^{-1}, \ldots\right\} \\ &= \{\ldots, x, \ldots\}\{\ldots, x, \ldots\}^{-1} = 1 \end{aligned}$$

□

7.1 K_2 of a finite field is trivial

Proposition 7.4. *Let $\mathbb{F}_q$ be the finite field with q elements.*

1. *If q is odd, there exists $u \in \mathbb{F}_q^\times$ such that u and $1-u$ are both not squares.*
2. *If α is a generator of $\mathbb{F}_q^\times$, then $\{\alpha, \alpha\}$ is trivial.*
3. *For any $u, v \in \mathbb{F}_q^\times$, $\{u, v\}$ is trivial.*
4. *$K_2(\mathbb{F}_q)$ is trivial.*

Proof. (1) Note that $\mathbb{F}_q^\times$ is cyclic of order $q-1$. Let α be a generator. Since $q-1$ is even, half of the elements of $\mathbb{F}_q^\times$ are squares $(1, \alpha^2, \alpha^4, \ldots, \alpha^{q-3})$ and half are not squares $(\alpha, \alpha^3, \ldots, \alpha^{q-2})$. Consider the bijection

$$\mathbb{F}_q \to \mathbb{F}_q \qquad u \mapsto 1-u$$

This maps 0 to 1 and 1 to 0, so we have a bijection

$$\mathbb{F}_q \setminus \{0,1\} \to \mathbb{F}_q \setminus \{0,1\} \qquad u \mapsto 1-u$$

Suppose there is no u such that u and $1-u$ are both not squares. Then under this bijection, all of the $\frac{q-1}{2}$ non-squares get mapped to squares. But one of the squares in $\mathbb{F}_q^\times$ is 1, so there are only $\frac{q-1}{2}-1$ squares in $\mathbb{F}_q \setminus \{0,1\}$, so this is impossible. Thus there does exist $u \in \mathbb{F}_p^\times$ such that $u, 1-u$ are both not squares.

(2) Let α be a generator of $\mathbb{F}_q^\times$. Note that since the symbol is anti-commutative,

$$\{\alpha,\alpha\}^2 = 1$$

Also note that

$$\{\alpha,\alpha\}^{q-1} = \left\{\alpha^{q-1},\alpha\right\} = \{1,\alpha\} = 1$$

If q is even (so $q-1$) is odd, this says that $\{\alpha,\alpha\}$ to an odd and even power are trivial, so it must be trivial. If q is odd, by (1) we can choose $u \in \mathbb{F}_q^\times$ such that $u, 1-u$ are both not squares, so $u = \alpha^i, 1-u = \alpha^j$ with i,j odd. Then

$$1 = \{u, 1-u\} = \left\{\alpha^i, \alpha^j\right\} = \{\alpha,\alpha\}^{ij}$$

so once again $\{\alpha,\alpha\}$ to an odd power (namely ij) is trivial. Since it also squares to 1, it is trivial.

(3) Let $u, v \in \mathbb{F}_q^\times$. Then write them as powers of a generator $u = \alpha^i, v = \alpha^j$. Then by the symbol relations,

$$\{uv\} = \left\{\alpha^i, \alpha^j\right\} = \{\alpha,\alpha\}^{ij}$$

which is trivial by (2).

(4) This is immediate from (3) and the fact that symbols generate $K_2(K)$ for any field K. □

7.2 K_2 of algebraically closed field is uniquely divisible

Review check. Show that if K is an algebraically closed field, then $K_n^M(K)$ is uniquely divisible.

Proposition 7.5. *Let F be a field and $m \in \mathbb{Z}_{\geq 1}$ such that $F^\times = F^{\times m}$, and also suppose that* either $\operatorname{char} F = m$ *or the group of mth roots of unity $\mu_m \subset F^{\text{sep}}$ is contained in F. Then $\mathrm{K}_n^M F$ is uniquely m-divisible.*

Proof. Define

$$f_m : \prod_{i=1}^n F^\times \to \mathrm{K}_n^M F \qquad (\alpha_1, \ldots, \alpha_n) \mapsto \{\beta_1, \alpha_2, \ldots, \alpha_n\}$$

where $\beta_1 \in F^\times$ satisfies $\beta_1^m = \alpha_1$. To verify that this is well defined, suppose $\gamma_1 \in F^\times$ is also an mth root of α_1, $\gamma_1^m = \alpha_1$. Then

$$\left(\beta_1\gamma_1^{-1}\right)^m = \beta_1^m\gamma_1^{-m} = \alpha_1\alpha_1^{-1} = 1$$

so $\beta_1\gamma_1^{-1} = \zeta$ is an mth root of unity. Now choose $\beta_2 \in F^\times$ so that $\alpha_2 = \beta_2^m$. Then using Lemma 7.3 a few times,

$$\begin{aligned}
\{\beta_1, \alpha_2, \ldots, \alpha_n\} &= \{\gamma_1\zeta, \alpha_2, \ldots, \alpha_n\} \\
&= \{\gamma_1, \alpha_2, \ldots, \alpha_n\}\{\zeta, \alpha_2, \ldots, \alpha_n\} \\
&= \{\gamma_1, \alpha_2, \ldots, \alpha_n\}\{\zeta, \beta_2^m, \ldots, \alpha_n\} \\
&= \{\gamma_1, \alpha_2, \ldots, \alpha_n\}\{\zeta, \beta_2, \ldots, \alpha_n\}^m \\
&= \{\gamma_1, \alpha_2, \ldots, \alpha_n\}\{\zeta^m = 1, \beta_2, \ldots, \alpha_n\} \\
&= \{\gamma_1, \alpha_2, \ldots, \alpha_n\}
\end{aligned}$$

Thus f_m is well defined. Now we claim that f_m is an n-symbolic map. It is clear that f_m is multiplicative with respect to the arguments $\alpha_2, \ldots, \alpha_n$. It is also multiplicative with respect to the 1st argument, since if $\beta_1^m = \alpha_1, (\beta_1')^m = \alpha_1'$, then $(\beta_1\beta_1')^m = \alpha_1\alpha_1'$ and so

$$\begin{aligned}
f_m(\alpha_1\alpha_1', \alpha_2, \ldots, \alpha_n) &= \{\beta_1\beta_1', \ldots, \alpha_n\} \\
&= \{\beta_1, \ldots, \alpha_n\}\{\beta_1', \ldots, \alpha_n\} \\
&= f_m(\alpha_1, \ldots, \alpha_n) f_m(\alpha_1', \ldots, \alpha_n)
\end{aligned}$$

If $\alpha_i + \alpha_j = 1$ for some $i \neq j$, and $i, j \neq 1$, then it is clear from the definition of f that $f_m(\alpha_1, \ldots, \alpha_n) = 1$. If $\alpha_1 + \alpha_j = 1$ for some $j \neq 1$, choose β_1 so that $\beta_1^m = \alpha_1$, and then we need to consider the cases (1) $\operatorname{char} F = m$ and (2) $\mu_m \subset F$ separately. In case (1) where $\operatorname{char} F = m$, we get

$$\alpha_j = 1 - \alpha_1 = 1 - \beta_1^m = (1 - \beta_1)^m$$

hence

$$f_m(\alpha_1, \ldots, \alpha_j, \ldots) = \{\beta_1, \ldots, (1-\beta_1)^m, \ldots\} = \{\beta_1, \ldots, 1 - \beta_1, \ldots\}^m = 1$$

since $\beta_1 + (1 - \beta_1) = 1$. So in case (1), f_m has the Steinberg property. In case (2), let $\zeta \in F$ be a primitive mth root of unity. Then

$$\alpha_j = 1 - \alpha_1 = 1 - \beta_1^m = \prod_{k=1}^{m}(1 - \zeta^k\beta_1)$$

Note that

$$1 = \left\{\zeta^k\beta_1, \ldots, 1 - \zeta^k\beta_1, \ldots\right\} = \left\{\zeta^k, \ldots, 1 - \zeta^k\beta_1, \ldots\right\}\left\{\beta_1, \ldots, 1 - \zeta^k\beta_1, \ldots\right\} \tag{7.1}$$

$$\implies \left\{\beta_1, \ldots, 1 - \zeta^k\beta_1, \ldots\right\} = \left\{\zeta^k, \ldots, 1 - \zeta^k\beta_1, \ldots\right\}^{-1} \tag{7.2}$$

Then using equation 7.2

$$\begin{aligned}
f_m(\alpha_1, \ldots, \alpha_j, \ldots) &= \left\{\beta_1, \ldots, \prod_k (1 - \zeta^k\beta_1), \ldots\right\} \\
&= \prod_k \left\{\beta_1, \ldots, 1 - \zeta^k\beta_1, \ldots\right\} = \prod_k \left\{\zeta^k, \ldots, 1 - \zeta^k\beta_1, \ldots\right\}^{-1}
\end{aligned}$$

Now choose δ_k so that $\delta_k^m = 1 - \zeta^k \beta_1$. Then we continue our equalities.

$$
\begin{aligned}
f_m(\alpha_1, \ldots, \alpha_j, \ldots) &= \prod_k \{\zeta^k, \ldots, \delta_k^m, \ldots\}^{-1} = \prod_k \{\zeta^k, \ldots, \delta_k, \ldots, \}^{-m} \\
&= \prod_k \{(\zeta^k)^m, \ldots, \delta_k, \ldots\}^{-1} = \prod_k \{1, \ldots, \delta_k, \ldots, \}^{-1} = \prod_k 1 = 1
\end{aligned}
$$

So in case (2), f_m has the Steinberg property. Hence in either case, f_m is an n-symbolic map, and induces the group homomorphism

$$
\widetilde{f}_m : \mathrm{K}_n^M F \to \mathrm{K}_n^M F \qquad \{\alpha_1, \ldots, \alpha_n\} \mapsto \{\beta_1, \ldots, \alpha_n\}
$$

where $\beta_1^m = \alpha_1$, which is inverse to m-power-map, since

$$
(\widetilde{f}_m \circ m) \{\alpha_1, \ldots, \alpha_n\} = \widetilde{f}_m \{\alpha_1, \ldots, \alpha_n\}^m = \widetilde{f}_m \{\alpha_1^m, \ldots, \alpha_n\} = \{\alpha_1, \ldots, \alpha_n\}
$$

Thus $\mathrm{K}_n^M F$ is uniquely m-divisible. □

Corollary 7.6. *Let F be an algebraically closed field. Then $\mathrm{K}_n^M F$ is uniquely divisible.*

Proof. Since F is algebraically closed, it contains mth roots of unity for all $m \geq 1$. Hence by Proposition 7.5, is uniquely m-divisible for all $m \geq 1$, so it is uniquely divisible. □

8 Algebraic number theory

8.1 Number fields

8.1.1 Galois, totally real, totally imaginary

Proposition 8.1. *Let K be a number field with $K/\mathbb{Q}$ Galois. Then K is totally real or totally imaginary.*

Proof. Suppose K is not totally imaginary, so there is an embeddings $K \hookrightarrow \mathbb{R}$. Let $\widetilde{K}$ denote the image of K in $\mathbb{R}$. Since $\widetilde{K}/\mathbb{Q}$ is Galois, any embedding $\widetilde{K} \hookrightarrow \mathbb{C}$ which fixes $\mathbb{Q}$ induces an automorphism of $\widetilde{K}$, which is to say, the image is $\widetilde{K}$. Any embeddings $K \hookrightarrow \mathbb{C}$ factors as an isomorphism $K \cong \widetilde{K}$ composed with an embedding $\widetilde{K} \hookrightarrow \mathbb{C}$. So any embeddings $K \hookrightarrow \mathbb{C}$ (which necessarily fixes $\mathbb{Q}$) has image $\widetilde{K} \subset \mathbb{R}$. □

8.1.2 A criterion for roots of unity

Definition 8.2. An **algebraic integer** is an element α of the algebraic closure of $\mathbb{Q}$ whose monic minimal polynomial over $\mathbb{Q}$ has integer coefficients. The **degree** of α is the degree of the minimal polynomial, or equivalently, the degree of the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$.

Proposition 8.3 (Milne [4] Proposition 5.5)**.** *Let $m, M \in \mathbb{Z}_{\geq 1}$. The set of algebraic integers α such that*

1. $\deg \alpha \leq m$
2. $|\alpha'| < M$ *for all conjugates* α' *of* α

is finite. [6]

Proof. The first condition says that α is a root of a monic irreducible polynomial $f \in \mathbb{Z}[x]$ with $\deg f \leq m$. The conjugates α' of α are precisely the other roots of f (in $\mathbb{Q}^{\text{alg}}$), and the coefficients of f can all be expressed in terms of these roots. Thus all coefficients of f have absolute value bounded by some linear scaling of M. Thus there are only finitely many possible values for the finitely many coefficients, so there are finitely many polynomials of which α could be a root, and these polynomials each have finitely many roots. So there are only finitely many such α's. □

Proposition 8.4. *Let α be an algebraic integer such that for all embeddings $\sigma : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$, $|\sigma(\alpha)| = 1$. Then α is a root of unity.* [7]

Proof. Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α and let $d = \deg f = \deg \alpha$. Let $\alpha = \alpha_1, \ldots, \alpha_d$ be the roots of f in $\mathbb{C}$, so these are the possible values of $\sigma(\alpha)$ for embeddings $\sigma : \mathbb{Q} \to \mathbb{C}$, so by hypothesis, $|\alpha_i| = 1$.

$$f(x) = \prod_{i=1}^{d} (x - \alpha_i)$$

[6] Here absolute value means the extended archimedean absolute value, which is to say, the restriction of complex norm.

[7] As in the previous proposition, by absolute value we mean complex norm.

Now we note that for any n, α^n is a root of

$$g_n(x) = \prod_{i=1}^{d} (x - \alpha_i^n)$$

and we also note that $g_n(x) \in \mathbb{Z}[x]$. Thus α^n has degree $\leq d$. The conjugates of α^n are $\alpha_1^n, \ldots, \alpha_d^n$ which by hypothesis have absolute value (complex norm) 1.

$$|\alpha_i^n| = |\alpha_i|^n = 1^n = 1$$

Thus the set $\{\alpha^1, \alpha^2, \alpha^3, \ldots\}$ is contained in the set of all algebraic inegers β such that $\deg \beta \leq d$ and $|\beta'| < 2$ for all conjugates, so by Proposition 8.3, it is a finite set. That is, $\alpha^n = \alpha$ for some $n > 1$, so $\alpha^{n-1} = 1$, which is to say, α is a root of unity. □

8.1.3 Existence of finite extension which kills class group

Proposition 8.5. *Let K be a number field. Then there exists a finite extension L/K such that every ideal of $\mathcal{O}_K$ becomes principle in $\mathcal{O}_L$.*

Proof. Let $m = |\operatorname{Cl}(\mathcal{O}_K)|$, and choose representative ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$. Since m is the order of $\operatorname{Cl}(\mathcal{O}_K)$, $\mathfrak{a}_i^m = 1$, which is to say, $\mathfrak{a}_i^m$ is principle, so there exists $a_i \in \mathcal{O}_K$ such that $\mathfrak{a}_i^m = (a_i)$.

For each i, let $\alpha_i = a_i^{1/m}$ be an mth root of a_i in an algebraic closure of K, and let $L = K(\alpha_1, \ldots, \alpha_m)$ be the finite algebraic extension generated by all the α_i. Then in $\operatorname{Cl}(\mathcal{O}_L)$, $\mathfrak{a}_i^m = (a_i) = (\alpha_i^m) = (\alpha_i)^m$. By unique factorization of ideals in Dedekind domains, this implies $\mathfrak{a}_i = (\alpha_i)$. □

8.1.4 Fundamental unit for real quadratic number fields

Theorem 8.6 (Dirichlet Unit Theorem)**.** *Let K be a number field with r_1 real embeddings and r_2 pairs of complex conjugate embeddings. Then*

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r_1 + r_2 - 1}$$

Remark 8.7. In the case of a quadratic extension $K = \mathbb{Q}(\sqrt{d})$ with d a square-free integer, the unit theorem says

1. If $d > 0$, there are two real embeddings so $r_1 = 2$ and no complex embeddings so $r_2 = 0$. Since K embeds in $\mathbb{R}$, the only roots of unity are ± 1, so the unit theorem gives

$$\mathcal{O}_K^\times \cong \{\pm 1\} \times \mathbb{Z}$$

2. If $d < 0$, there are no real embeddings so $r_1 = 0$ and there is one pair of complex conjugate embeddings so $r_2 = 1$. So $\mathcal{O}_K$ has no torsion free part.

$$\mathcal{O}_K^\times \cong \mu(K)$$

Even more precisely, if $d = -1$, then $\mu(K) = \mathbb{Z}/4\mathbb{Z}$, but if $d \leq -2$, $\mu(K) = \{\pm 1\}$.

Definition 8.8. For a real quadratic number field $\mathbb{Q}(\sqrt{d})$ with $d > 0$, a generator for the infinite cyclic factor of $\mathcal{O}_K^\times$ is called a **fundamental unit**. It is traditionally denoted by ϵ.

Remark 8.9. Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic number field. The following is an algorithm for finding a fundamental unit.

1. If $d \equiv 2, 3 \bmod 4$, compute the sequence b^2d for $b = 1, 2, \ldots$.
$$d, 4d, 9d, 16d, \ldots$$
until b^2d differs from a square by ± 1. For the first b such that $b^2d = a^2 \pm 1$, the fundamental unit is $\epsilon = a + b\sqrt{d}$.

2. If $d \equiv 1 \bmod 4$, compute the same sequence b^2d for $b = 1, 2, \ldots$, until b^2d differs from a square by ± 4. For the first b such that $b^2d = a^2 \pm 4$, the fundamental unit is $\epsilon = \frac{1}{2}(a + b\sqrt{d})$.

We omit the reasons why this works for the moment. It's basically a brute force argument.

Problem 8.10. Find the fundamental unit for each of the following.

1. $\mathbb{Q}(\sqrt{7})$
2. $\mathbb{Q}(\sqrt{82})$
3. $\mathbb{Q}(\sqrt{5})$
4. $\mathbb{Q}(\sqrt{13})$

Solution. (1) This fits in the case $d \equiv 2, 3 \bmod 4$. The sequence b^2d is $7, 28, 63, \ldots$ and $63 = 64 - 1$, so the fundamental unit is $\epsilon = 8 + 3\sqrt{7}$.

(2) This fits in the case $d \equiv 2, 3 \bmod 4$. The sequence b^2d starts with 82 which already differs from a square by ± 1, so the fundamental unit is $\epsilon = 9 + \sqrt{82}$.

(3) This fits in the case $d \equiv 1 \bmod 4$. The first term of the sequence b^2d is 5 which already differs from the sqaure 1 by 4, so $a_1 = b_1 = 1$ and the fundamental unit is $\epsilon = \frac{1}{2}\left(1 + \sqrt{5}\right)$.

8.2 Local fields

8.2.1 Example ramification and residual degree calculations

Problem 8.11. For each of the following, compute the ramification and residual field degrees $e(L/K), f(L/K)$.

1. $K = \mathbb{Q}_5, L = \mathbb{Q}_5(\sqrt{2})$.
2. $K = \mathbb{Q}_5, L = \mathbb{Q}_5(\sqrt{5})$.
3. $K = \mathbb{Q}_3, L = \mathbb{Q}_3(\sqrt{2}, \zeta)$ where ζ is a primitive 3rd root of unity.

Solution.
(1) Normalize the discrete valuation on K so that $v_K(K^\times) = \mathbb{Z}$ and $v_L(L^\times) = \frac{1}{e}\mathbb{Z}$. Note that

$$N^L_K(\sqrt{2}) = \sqrt{2}(-\sqrt{2}) = -2$$

so

$$|\sqrt{2}|_L = |2|_K^{1/2} = 1$$

so $\sqrt{2} \in \mathcal{O}_L$. Thus there is an element of the residue field $k_L = \mathcal{O}_L/\mathfrak{m}_L$ which is a root of x^2-2. Since x^2-2 is irreducible over $k_K \cong \mathbb{F}_5$, the extension k_L/k_K has degree greater than 1, that is, $f > 1$. Since $ef = 2$, this forces $f = 2, e = 1$. Hence $\mathbb{Q}_5(\sqrt{2})$ is totally unramified over $\mathbb{Q}_5$.

(2) Normalize the discrete valuation on K so that $v_K(K^\times) = \mathbb{Z}$ and $v_L(L^\times) = \frac{1}{e}\mathbb{Z}$. Then

$$1 = v_L(5) = 2v_L(\sqrt{5}) \implies v_L(\sqrt{5}) = \frac{1}{2}$$

Thus $e \geq 2$, so $f = 1, e = 2$, and $\sqrt{5}$ is a uniformizer.

(3) Note that $[L : K] = 4$.

$$\begin{tikzcd}
& \mathbb{Q}_3(\sqrt{2},\zeta) \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}_3(\zeta) \arrow[dr, dash, "2"'] & & \mathbb{Q}_3(\sqrt{2}) \arrow[dl, dash, "2"] \\
& \mathbb{Q}_3 &
\end{tikzcd}$$

Note that ζ is a root of x^2+x+1 over $\mathbb{Q}_3$. By a similar argument as (1),

$$e^{\mathbb{Q}_3(\sqrt{2})}_{\mathbb{Q}_3} = 1 \qquad f^{\mathbb{Q}_3(\sqrt{2})}_{\mathbb{Q}_3} = 2$$

Regarding $\mathbb{Q}_3(\zeta)$, we observe that

$$\begin{aligned}
x^2+x+1 = (x-\zeta)(x-\zeta^2) &\implies 3 = (\zeta-1)(\zeta^2-1) \\
&\implies v_{\mathbb{Q}_3(\zeta)}(3) = 1 = v_L(\zeta-1) + v_L(\zeta^2-1)
\end{aligned}$$

Since $\zeta - 1, \zeta^2 - 1$ are Galois conjugates, they have equal valuation. Hence

$$v_L(\zeta-1) = \frac{1}{2}$$

so

$$e^{\mathbb{Q}_3(\zeta)}\mathbb{Q}_3 = 2 \qquad f^{\mathbb{Q}_3(\zeta)}_{\mathbb{Q}_3} = 1$$

Returning to our original diagram, we can write in the ramification and residual degrees we computed. Since all the extensions are degree 2, we can also deduce ramification and residual degrees for the upper extensions and the total extension L/K by multiplicativity in towers.

$$\begin{tikzcd}
& \mathbb{Q}_3(\sqrt{2},\zeta) \arrow[dl, dash, "{e{=}2,\ f{=}1}"'] \arrow[dr, dash, "{e{=}1,\ f{=}2}"] & \\
\mathbb{Q}_3(\zeta) \arrow[dr, dash, "{e{=}1,\ f{=}2}"'] & & \mathbb{Q}_3(\sqrt{2}) \arrow[dl, dash, "{e{=}2,\ f{=}1}"] \\
& \mathbb{Q}_3 &
\end{tikzcd}$$

By multiplicativity in towers,

$$e_K^L = f_K^L = 2$$

8.2.2 Hensel's lemma

Proposition 8.12 (Hensel's lemma, version 1)**.** *Let K be a complete nonarchimedean discretely valued field, with associated local ring $(\mathcal{O}_K, \mathfrak{m})$, and residue field $k = \mathcal{O}_K/\mathfrak{m}$. Let $f \in \mathcal{O}_K[x]$, and suppose there exist $g_1, h_1 \in \mathcal{O}_K[x]$ with g_1 monic and* $\gcd(g_1, h_1) = 1$ *such that*

$$\overline{f} = \overline{g_1 h_1} \in k[x] \qquad \text{(equivalently } f \equiv g_1 h_1 \bmod \mathfrak{m})$$

Then there exist $g, h \in \mathcal{O}_K[x]$ such that g is monic, $\overline{g} = \overline{g}_1, \overline{h} = \overline{h}_1$, and $f = gh$. That is, factorizations of polynomials over k lift to factorizations over $\mathcal{O}_K$, provided there are no common factors and one is monic.

Remark 8.13. This is hardly worth stating, but the "converse" of Hensel's lemma is obvious. If f factors in in $\mathcal{O}_K[x]$, then applying the quotient map $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{m}$ to the coefficients gives a factorization in $k[x]$.

Remark 8.14. In particular, we care about the case $K = \mathbb{Q}_p, \mathcal{O}_K = \mathbb{Z}_p, \mathfrak{m} = p\mathbb{Z}_p, k = \mathbb{F}_p$. In this case, Hensel's lemma says that if a polynomial $f(x) \in \mathbb{Z}_p[x]$ has a factorization $\bmod p$ into relatively prime factors, then that factorization comes from a factorization in $\mathbb{Z}_p$.

In particular, $\mathbb{Z} \subset \mathbb{Z}_p$, and this is where Hensel's lemma is often applied, at least in examples. Suppose we want to know if some polynomial equation $f(x) = 0$ with $f \in \mathbb{Z}[x]$ has a solution in $\mathbb{Q}_p$ or $\mathbb{Z}_p$. If we find a factorization of $\overline{f}$ with a monic, non-repeated linear factor $(x - a)$ where $a \in \mathbb{F}_p$, then that factorization lifts to a factorization of f in $\mathbb{Z}_p[x]$ so there is a lift of $\alpha \in \mathbb{Z}_p$ so that $\overline{\alpha} = a$ and $f(\alpha) = 0$. The next corollary says this more precisely.

Corollary 8.15 (Hensel's lemma, version 1, for $\mathbb{Q}_p$)**.** *Let $f(x) \in \mathbb{Z}_p[x]$. If $\overline{f}(x) \in \mathbb{F}_p[x]$ has a simple root a, that is, there exists $a \in \mathbb{F}_p$ such that $\overline{f}(a) = 0$ and $\overline{f'}(a) \neq 0$, then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\overline{\alpha} = a$.*

We also need another version of Hensel's lemma at one point later.

Proposition 8.16 (Hensel's lemma, version 2)**.** *Let K be a complete nonarchimedean discretely valued field, with associated local ring $(\mathcal{O}_K, \mathfrak{m})$. Let $f(x) \in \mathcal{O}_K[x]$ be monic. Suppose $a \in \mathcal{O}_K$ such that*

$$f'(a) \neq 0 \qquad |f(a)| < |f'(a)|^2$$

Then there exists a unique $\alpha \in \mathcal{O}_K$ such that $f(\alpha) = 0$ and

$$|a - \alpha| \leq \left| \frac{f(a)}{f'(a)} \right|$$

Proposition 8.17. *Let p be a prime.*

1. *If $p \geq 3$, then: $u \in \mathbb{Z}_p^\times$ is a square $\iff$ $\overline{u} \in \mathbb{F}_p^\times$ is a square.*

2. *If $p = 2$, then: $u \in \mathbb{Z}_2^\times$ is a square $\iff$ $u \equiv 1 \bmod 8$.*

Proof. ($1 \implies$) If $u = \alpha^2 \in \mathbb{Z}_p$ then $\overline{u} = \overline{\alpha}^2 \in \mathbb{F}_p^\times$.

($1 \impliedby$) Suppose $\overline{u} = a^2 \in \mathbb{F}_p$. Consider $f(x) = x^2 - u \in \mathbb{Z}_p[x]$. Then

$$\overline{f}(x) = x^2 - \overline{u} = x^2 - a^2 = (x - a)(x + a)$$

Note that $\overline{f'}(a) = 2a \neq 0$ since $p \geq 3$, so we can apply Corollary 8.15 to conclude that there is a root $\alpha \in \mathbb{Z}_p$ of f, so $u = \alpha^2$.

($2 \implies$) If $u = a^2 \in \mathbb{Z}_2$, then $\overline{u} \equiv \overline{a}^2 \bmod 8$.

($2 \impliedby$) Suppose $u^2 \equiv 1 \bmod 8$. Consider $f(x) = x^2 - u \in \mathbb{Z}_p[x]$. We want to apply version 2 of Hensel's lemma to $f(x)$ with $a = 1$. It is clear that $f'(1) = 2 \neq 0$. Since $u^2 - 1 \equiv 0 \bmod 8$,

$$|f(1)|_2 = |1 - u^2|_2 \leq \frac{1}{8} < \frac{1}{4} = \left(|2|_2\right)^2 = \left(|f'(1)|_2\right)^2$$

so the hypotheses are satisfied. Thus there exists $\alpha \in \mathbb{Z}_p$ such that $\alpha^2 - u = 0$, which is to say, u is a square in $\mathbb{Z}_2$. □

8.2.3 A concrete failure of the Hasse principle

Remark 8.18. The Hasse principle asserts that "global" information is related to "local" information, in the sense that existence of solutions in $\mathbb{Q}$ to some equation are related to existence of solutions in all local field completions of $\mathbb{Q}$, namely $\mathbb{Q}_p$ for all p and $\mathbb{R}$. This is exactly true in the case of quadratic forms - the Hass-Minkowsi theorem says that a quadratic form has a solution in $\mathbb{Q}$ if and only if there is a solution in every $\mathbb{Q}_p$ and a solution in $\mathbb{R}$. However, it fails for higher degree forms, as given by the following example.

Lemma 8.19. *Let p be an odd prime, and let a, b be quadratic non-residues mod p. Then ab is a quadratic residue mod p.*

Proof. If a, b are both non-residues, they both represent the same nontrivial class in $\mathbb{F}_p^\times / \mathbb{F}_p^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}$ (this isomorphism uses the fact that $p - 1$ is even). Then ab represents the trivial class, that is, $ab \in \mathbb{F}_p^{\times 2}$. □

Proposition 8.20. *The equation*

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$$

has a root in $\mathbb{Q}_p$ for all primes p and in $\mathbb{R}$, but no root in $\mathbb{Q}$.

Proof. It is clear that there is no root in $\mathbb{Q}$, since $2, 17$, and 34 are not squares, and it is clear that there are roots in $\mathbb{R}$. Since $17 \equiv 1 \bmod 8$, by Proposition 8.17, there is a root of $x^2 - 17$ in $\mathbb{Q}_2$.

Now let p be an odd prime. It suffices to show that at least one of $2, 17, 34$ is a square in $\mathbb{Q}_p$. By Proposition 8.17, if $u \in \mathbb{Q}_p^\times$ is a quadratic residue mod p, then it is a square in $\mathbb{Q}_p$. If either 2 or 17 is a quadratic residue mod p, we are done. If both are non-residues, then by Lemma 8.19, then $34 = (2)(17)$ is a quadratic residue, so it is a square in $\mathbb{Q}_p$. $\square$

Remark 8.21. The proof of the previous proposition actually yields an infinite family of equations for which the Hasse principle fails. For any prime of the form $p = 8k + 1$, and the proof above shows that

$$(x^2 - 2)(x^2 - p)(x^2 - 2p) = 0$$

has a solution in every $\mathbb{Q}_p$ and in $\mathbb{R}$ but no solutions in $\mathbb{Q}$.

References

[1] David S. Dummit and Richard M. Foote. Abstract algebra, third edition, 2004.

[2] Philippe Gille and Tamás Szamuely. Central simple algebras and group cohomology, 2006.

[3] Fernando Q. Gouvea. P-adic numbers, 1997.

[4] James S. Milne. Algebraic number theory (v3.07), 2017. Available at www.jmilne.org/math/.

[5] Jonathan Rosenberg. Algebraic k-theory and its applications, 1994.

[6] Romyar Sharifi. Group and galois cohomology. Available at http://math.ucla.edu/ sharifi/groupcoh.pdf.

[7] Charles A. Weibel. An introduction to homological algebra, 1994.