Topics in Number Theory

Lectures delivered by Sug Woo Shin
Notes by Holden Lee

Fall 2012, MIT

Last updated Thu. 9/6/2012

Contents

Introduction

Sug Woo Shin taught a course (18.787) on Topics in Number Theory at MIT in Fall 2012. These are my "live-TEXed" notes from the course. The template is borrowed from Akhil Mathew.

Please email corrections to `holden1@mit.edu`.

Lecture 1
Thu. 9/6/12

Course website: `http://math.mit.edu/~swshin/Fall12-18787`

§1 Overview

In this course, we will cover abelian varieties and p-divisible groups, also known as Barsotti-Tate groups. We first build some basic knowledge and apply it to some interesting problems in number theory. Our main reference is Abelian Varieties, by Mumford. We will

1. *classify* abelian varieties over finite fields $\mathbb{F}_p$ and algebraic closures of finite fields $\overline{\mathbb{F}_p}$ (Honda-Tate Theory). We will also classify p-divisible groups up to isogeny (Dieudonné, Manin).

   With some more work, we can get classification up to isomorphism.

   Studying a variety over finite fields helps us understand abelian varieties over global fields, because when we study a global problem, one way to get information is to reduce modulo a prime and study over the variety over the special fiber.

2. go from characteristic p ($\mathbb{F}_p$) to characteristic 0 (e.g. $\mathbb{Q}_p$) using *deformations*.

   - The Serre-Tate Theorem will tell us that deformations of abelian varieties are basically deformations of p-divisible groups.
   - The theory of Grothendieck-Messing will reduce deformations of p-divisible groups to some linear algebra.

To understand abelian varieties and p-divisible groups, we first need to understand group schemes. An abelian variety is a special type of group scheme, while a p-divisible group is an inductive limit of group schemes.

§2 Review: Yoneda Lemma and T-valued points

This is not part of the lecture. I include this section as a reference.

2.1 The Yoneda Lemma

Lemma 1 (Yoneda Lemma)**:** lem:yoneda Let $\mathcal{C}$ be a locally small category. Let h_A denote the functor $\mathrm{Hom}(\bullet, A) : \mathcal{C} \to (\mathrm{Sets})$ and h^A denote the contravariant functor $\mathrm{Hom}(A, \bullet)$ (i.e. it is a functor $\mathcal{C}^{\mathrm{op}} \to (\mathrm{Sets})$).

1. (Covariant version) Let F be functor from $\mathcal{C}$ to (Sets). As functors $(\mathrm{Set})^{\mathcal{C}} \times \mathcal{C} \to (\mathrm{Set})$, we have $\mathrm{Nat}(h^A, F) \cong F(A)$. ($F$ is in $(\mathrm{Set})^{\mathcal{C}}$, A is in $\mathcal{C}$, and $\mathrm{Nat}(h^A, F) \cong F(A)$ is a set.)

2. (Contravariant version) Let F be a contravariant functor from $\mathcal{C}$ to (Sets). As functors $(\mathrm{Set})^{\mathcal{C}^{\mathrm{op}}} \times \mathcal{C} \to (\mathrm{Set})$, we have $\mathrm{Nat}(h_A, F) \cong F(A)$.

Corollary 2 (Yoneda Embedding)**:** cor:yoneda

1. The embedding $h^\bullet : \mathcal{C}^{\mathrm{op}} \to (\mathrm{Set})^{\mathcal{C}}$ given by sending $A \mapsto h^A = \mathrm{Hom}_{\mathcal{C}}(A, \bullet)$ is fully faithful. (The morphism $f : A \to B$ gets sent to $f \circ \bullet$.)
2. The embedding $h_\bullet : \mathcal{C} \to (\mathrm{Set})^{\mathcal{C}^{\mathrm{op}}}$ given by sending $A \mapsto h_A = \mathrm{Hom}_{\mathcal{C}}(\bullet, A)$ is fully faithful. (The morphism $f : A \to B$ gets sent to $\bullet \circ f$.)

Remark:

- A category is **locally small** if homomorphisms between any two objects form a set.
- $(\mathrm{Set})^{\mathcal{C}^{\mathrm{op}}}$ is the category of *contravariant functors* $\mathcal{C} \to (\mathrm{Set})$.
- $\mathrm{Hom}(A, B)$ has just the structure of a set.
- $\mathrm{Nat}(G, F)$ denotes the set of natural transformations between G and F.
- A functor Φ is **fully faithful** if $\Phi_{A,B} : \mathrm{Hom}(A, B) \to \mathrm{Hom}(\Phi(A), \Phi(B))$ is bijective for any objects A and B. This basically means that Φ embeds the first category into the second, and there aren't any "extra" maps between embedded objects that are present in B but not A.
- We say a functor $F : \mathcal{C} \to (\mathrm{Set})$ is **representable** if $F \cong h^A$ for some A (and ditto for the contravariant case).

Proof of Corollary 1. We show (2) of the lemma implies (2) of the corollary; (1) is entirely analogous. Set $F = h_B$ to get

$$\mathrm{Nat}(h_A, h_B) \cong h_B(A).$$

Now a natural transformation is just a morphism in the functor category, so $\mathrm{Nat}(h_A, h_B) = \mathrm{Hom}_{(\mathrm{Set})^{\mathcal{C}^{\mathrm{op}}}}(h_A, h_B)$, and by definition $h_B(A) = \mathrm{Hom}(A, B)$, so we get

$$\mathrm{Hom}_{(\mathrm{Set})^{\mathcal{C}^{\mathrm{op}}}}(h_A, h_B) \cong \mathrm{Hom}(A, B).$$

This is exactly the condition to be fully faithful. $\square$

One way to think of this is that an object is determined by how other objects map into it.[1]

[1] As mentioned here `http://mathoverflow.net/questions/3184/philosophical-meaning-of-the-yoneda-lemma/3223#3223`, if one thinks of objects of a category as particles and morphisms as ways to smash one particle into another particle, then the Yoneda lemma says that it is possible to determine the identity of a particle by smashing other particles into it.

2.2 T-valued points

Definition 3: Let X and T be objects in a locally small category. Define the set of **T-valued points** of X to be

$$T(X) := \mathrm{Hom}(T, X).$$

In many cases we can think of "T-valued points" as a generalization of "points" of X. For example, suppose T is a singleton set $\{\cdot\}$ and X is a set, then a T-valued point is just a point of X.

The main application to algebraic geometry can be seen through the following example.

Example 4: ex:T-points Let R be an integral domain and V a variety over R. Let $T = \mathrm{Spec}(R)$ and X be the scheme corresponding to V. Then the T-points of X are exactly the points of V.

To see this, it's sufficient just to consider the affine case. Suppose $V \in R^n$ is defined by $f_1, \ldots, f_m$. By Lemma 5, to give a morphism

$$T = \mathrm{Spec}(R) \to X = \mathrm{Spec}\left(\frac{R[x_1, \ldots, x_n]}{(f_1, \ldots, f_m)}\right)$$

is the same as giving a R-algebra homomorphism

$$\frac{R[x_1, \ldots, x_n]}{(f_1, \ldots, f_m)} \to R,$$

which is just an assignment

$$(x_1, \ldots, x_n) \mapsto (a_1, \ldots, a_n) \text{ such that } f_i(x_1, \ldots, x_n) = 0 \text{ for some } i,$$

i.e. a point of V.

Lemma 5 (cf. Hartshorne, II, Exercise 2.4)**:** lem:spec-fff Let R be a ring. Then Spec is a fully faithful contravariant functor from the category of R-algebras to schemes over $\mathrm{Spec}(R)$.

Example 4 is the most intuitive example. However, the power of the viewpoint of $X(T)$ is that we can consider more generalized points. For instance, letting R be a field k,

- a $\mathrm{Spec}(k[t])$ point is a one-parameter family of k-points, and
- a $\mathrm{Spec}\left(\frac{k[t]}{(t^2)}\right)$ point is a k-point with a Zariski tangent vector.

The Yoneda Embedding tells us that we can identify a scheme X with the **functor of points** $h_X(\bullet) = X(\bullet)$—i.e. with $X(T)$, the T-points of X, as T ranges over all schemes—without losing any information. A functor $X \to Y$ becomes a natural transformation $h_X = X(\bullet) \to h_Y = Y(\bullet)$, i.e. maps of sets $X(T) \to Y(T)$ for each T, that are functorial over T.

§3 Group schemes

3.1 Definition of group schemes

We will define group schemes over a fixed scheme S.

Definition 6: Let S be a scheme. Define (Sch/S), the category of S**-schemes**, as follows.

- The objects are schemes T with a structure map to S, $\begin{array}{c} T \\ \downarrow \\ S \end{array}$.
- The morphisms are

$$\mathrm{Hom}\left(\begin{array}{c} T \\ \downarrow f \\ S \end{array}, \begin{array}{c} T' \\ \downarrow f' \\ S \end{array} \right) = \left\{ g : \begin{tikzcd} T \arrow[rr, "g"] \arrow[dr, "f"'] & & T' \arrow[dl, "f'"] \\ & S & \end{tikzcd} \text{ commutes} \right\}$$

  called S-morphisms.

For short we'll write $\mathrm{Hom}_S(T, T')$, the maps f, f' being implicit.

We now apply the philosophy of the previous section: to study X we study $h_X = X(\bullet)$. If $X \in (\mathrm{Sch}/S)$ we get canonically

$$\begin{aligned} h_X : (\mathrm{Sch}/S) &\to (\mathrm{Sets}) \\ T &\mapsto \mathrm{Hom}_S(T, X). \end{aligned}$$

Since T and X are S-schemes, we define the T-points of X to be $X(T) := \mathrm{Hom}_S(T, X)$. The functor h_X sends

$$(T \xrightarrow{f} T') \mapsto (\mathrm{Hom}_S(T, X) \xleftarrow{h_X(f) = \bullet \circ f} \mathrm{Hom}_S(T', X)).$$

The Yoneda Embedding 2 tells us that $h_\bullet$ is a fully faithful contravariant functor

$$\begin{aligned} h_\bullet : (\mathrm{Sch}/S) &\to \mathrm{Fun}^{\mathrm{op}}((\mathrm{Sch}/S), (\mathrm{Sets})) = (\mathrm{Sets})^{(\mathrm{Sch}/S)^{\mathrm{op}}} \\ X &\mapsto h_X. \end{aligned}$$

We say $h \in \mathrm{Fun}^{\mathrm{op}}((\mathrm{Sch}/S), (\mathrm{Sets}))$ is **representable** (by the scheme X) if $h \cong h_X$.

We have several equivalent definitions for a group scheme. The Yoneda Embedding gives the equivalence of the 2nd and 3rd definitions.

Definition 7: A **group scheme** G over S' any of the following three equivalent objects.

1. a group object in (Sch/S), i.e. it is $(G, \widetilde{h_G})$ where $G \in$ (Sch/S) and the following commutes:

$$\begin{tikzcd}
(\mathrm{Sch}/S) \arrow[rr, "\widetilde{h_G}"] \arrow[dr, "h_G"'] & & (\mathrm{Gps}) \arrow[dl, "\text{forgetful}"] \\
& (\mathrm{Set}) &
\end{tikzcd}$$

2. (G, h_G) equipped with the following maps of sets
   - e_T (identity): $\{\cdot\} \to G(T)$
   - i_T (inverse): $G(T) \to G(T)$
   - m_T (multiplication): $G(T) \times G(T) \to G(T)$.

   such that $G(T)$ is a *group* under these operations, namely,

   (a) (Associativity) The following commutes:

$$\begin{tikzcd}
G(T) \times G(T) \times G(T) \arrow[r, "{(m_T,\mathrm{id})}"] \arrow[d, "{(\mathrm{id},m_T)}"] & G(T) \times G(T) \arrow[d, "m_T"] \\
G(T) \times G(T) \arrow[r, "m_T"'] & G(T).
\end{tikzcd}$$

   Note: This represents associativity because going clockwise we get $(xy)z$ and going counterclockwise we get $x(yz)$.

   (b) (Inverse)

$$\begin{tikzcd}
& G(T) \times G(T) \arrow[dr, "m_T"] & \\
G(T) \arrow[ur, "{(\mathrm{id},i_T)}"] \arrow[r, "\text{structure}"] \arrow[dr, "{(i_T,\mathrm{id})}"'] & G(S) \arrow[r, "e_T"] & G(T) \\
& G(T) \times G(T) \arrow[ur, "m_T"'] &
\end{tikzcd}$$

   Note: The top, middle, and bottom give xx^{-1}, e, and $x^{-1}x$, respectively, so commutativity gives $xx^{-1} = e = x^{-1}x$.

   (c) (Identity) Let $e'_T : G(T) \to G(T)$ be the composition of the structure map with $e : G(S) \to G(T)$.

$$\begin{tikzcd}
& G(T) \times G(T) \arrow[dr, "m_T"] & \\
G(T) \arrow[ur, "{(\mathrm{id},e'_T)}"] \arrow[rr, "\mathrm{id}"] \arrow[dr, "{(e'_T,\mathrm{id})}"'] & & G(T) \\
& G(T) \times G(T) \arrow[ur, "m_T"'] &
\end{tikzcd}$$

Note: This gives $x \cdot e = x = e \cdot x$.

and these group operations are *functorial*, namely for all $T \xrightarrow{f} T'$ in (Sch/S),

- $$\begin{tikzcd} \{\cdot\} \arrow[r, "e_T"] \arrow[dr, "e_{T'}"'] & G(T) \\ & G(T') \arrow[u, "h_G(f)"'] \end{tikzcd}$$

- $$\begin{tikzcd} G(T) \arrow[r, "i_T"] & G(T) \\ G(T') \arrow[u, "h_G(f)"] \arrow[r, "i_{T'}"] & G(T') \arrow[u, "h_G(f)"'] \end{tikzcd}$$

- $$\begin{tikzcd} G(T) \times G(T) \arrow[r, "i_T"] & G(T) \\ G(T') \times G(T') \arrow[u, "h_G(f)"] \arrow[r, "i_{T'}"] & G(T') \arrow[u, "h_G(f)"'] \end{tikzcd}$$

3. (G, e, i, m) where $G \in (\mathrm{Sch}/S)$,

$$\begin{aligned} e &: S \to G \\ i &: G \to G \\ m &: G \times G \to G \end{aligned}$$

and we have the analogues of the group laws in the 2nd definition, but with fiber product instead of product and with e, i, m instead of e_T, i_T, m_T.

(a) (Associativity)

$$\begin{tikzcd} G \times_S G \times_S G \arrow[r, "(m,\mathrm{id})"] \arrow[d, "(\mathrm{id},m)"] & G \times_S G \arrow[d, "m"] \\ G \times_S G \arrow[r, "m"'] & G. \end{tikzcd}$$

(b) (Inverse)

$$\begin{tikzcd} & G \times_S G \arrow[dr, "m"] & \\ G \arrow[ur, "(\mathrm{id},i)"] \arrow[r, "\text{structure}"] \arrow[dr, "(i,\mathrm{id})"'] & S \arrow[r, "e"] & G \\ & G \times_S G \arrow[ur, "m"'] & \end{tikzcd}$$

(c) (Identity) Let $e' : G \to G$ be the composition of the structure map with $e : S \to G$.

$$\begin{tikzcd}
 & G \times_S G \arrow[dr, "m"] & \\
G \arrow[ur, "(\mathrm{id}, e')"] \arrow[rr, "\mathrm{id}"] \arrow[dr, "(e', \mathrm{id})"'] & & G(T) \\
 & G \times_S G \arrow[ur, "m"'] &
\end{tikzcd}$$

Proof of equivalence. The 1st and 2nd definition are equivalent: In the 2nd definition, the first set of conditions simply say $G(T)$ is a group, and the second set of conditions say that $\widetilde{h_G}$ is a functor; i.e. it sends the scheme morphism f to a group homomorphism $\widetilde{h_G}(f)$.

The 2nd and 3rd definitions are equivalent: We go between G to $G(T)$ by the Yoneda embedding. h_G sends fiber products of schemes to products of sets. $\square$

We can understand group schemes as *schemes* with group axioms on schemes, or as *functors of points* with group axioms on the set of T-points for each T.

3.2 Examples of group schemes

Let $G = \operatorname{Spec} A$ and $S = \operatorname{Spec} R$. Suppose A is an R-algebra, so there is a natural structure map $G \to S$. We have by Lemma 5 that Spec is a contravariant fully faithful functor from (R-algebras) to ($\mathrm{Sch}/\operatorname{Spec} R$):

$$\begin{tikzcd}
(\text{rings}) \arrow[r, "\mathrm{Spec}"] & (\mathrm{Sch}) \\
(R\text{-algebras}) \arrow[u, hook] \arrow[r, "\text{f.f.}", "\mathrm{Spec}"'] & (\mathrm{Sch}/\operatorname{Spec} R) \arrow[u, hook]
\end{tikzcd}$$

(Note the categories on the bottom are not full subcategories of the top.) As Lemma 5 says, S-morphisms between schemes over $\operatorname{Spec} R$ are nothing but R-algebra homomorphisms in the opposite direction, so we can be more concrete. So giving $G = \operatorname{Spec} A$ a group scheme structure, i.e. giving e, i, m for G, amounts to giving R-algebra maps (note $\operatorname{Spec}(A \otimes_R A) = \operatorname{Spec} A \times_{\operatorname{Spec} R} \operatorname{Spec} A$)

$$\begin{aligned}
e &: A \to R \\
i &: A \to A \\
m &: A \to A \otimes_R A.
\end{aligned}$$

such that R-algebra version of (a), (b), and (c) hold. (Just invert all the arrows in (a), (b), and (c), and replace the rings with schemes. A satisfying these axioms is called a **Hopf algebra**.)

We can give some common, concrete examples of group varieties.

Example 8: Define the additive group scheme $\mathbb{G}_{a,\operatorname{Spec} R}$ as follows. (First we consider the 3rd definition.) Let $A = R[t]$ and let $\mathbb{G}_{a,\operatorname{Spec} R} = \operatorname{Spec} A$ be the scheme with e, i, and m induced by the R-algebra homomorphisms

$$\begin{aligned} e &: R[t] \to R & f &\mapsto f(0) \\ i &: R[t] \to R[t] & f &\mapsto f(-t) \\ m &: R[t] \to R[t'] \otimes_R R[t''] \cong R[t', t''] & f &\mapsto f(t' + t'') \end{aligned}$$

For instance, for $R = k$, on points the group operation is just addition. Indeed, the map m gives $\operatorname{Spec} R[t', t''] \to \operatorname{Spec} R[t]$ that sends the ideal $(t' - a, t'' - b)$ to $m^{-1}((t' - a, t'' - b)) = (t - (a + b))$, i.e. sends the point (a, b) to the point $a + b$.

Now consider $\mathbb{G}_{a,\operatorname{Spec} R}(\operatorname{Spec} R')$ where R' is a R-algebra. Using the 2nd definition, $\mathbb{G}_{a,\operatorname{Spec} R}(\operatorname{Spec} R')$ consists of maps $\operatorname{Spec} R' \to \operatorname{Spec} R[t]$—i.e. maps $R[t] \to R'$, which together with the group axioms, means

$$\mathbb{G}_{a,\operatorname{Spec} R}(\operatorname{Spec} R') = (R', +).$$

(Check this.)

Example 9: Define the multiplicative group scheme $\mathbb{G}_{m,\operatorname{Spec} R}$ as follows. Let $A = R[t, t^{-1}]$; let $\mathbb{G}_{m,\operatorname{Spec} R}$ be the scheme with e, i, m induced by the R-algebra homomorphisms

$$\begin{aligned} e &: f \mapsto f(1) \\ i &: f \mapsto f(t^{-1}) \\ m &: f \mapsto f(t't''). \end{aligned}$$

(Note 1 is the multiplicative identity so we look at $f(1)$ not $f(0)$.)

From a different angle, we get

$$\mathbb{G}_{m,\operatorname{Spec} R}(\operatorname{Spec} R') = (R'^{\times}, \cdot).$$

(When we consider $\operatorname{Spec} R' \to \operatorname{Spec} R[t, t^{-1}]$, i.e. maps $R[t, t^{-1}] \to R'$, the image of t must be an invertible element.)

Remark: For any ring R, $\mathbb{G}_{a,\operatorname{Spec} R} \cong \mathbb{G}_{a,\operatorname{Spec} \mathbb{Z}} \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} R$, by defining an isomorphism on the level of points. The same is true for $\mathbb{G}_{m,\operatorname{Spec} R}$.

Example 10: To define the additive and multiplicative group schemes for general S, we need to use relative Spec.

$$\begin{aligned} \mathbb{G}_{a,S} &:= \underline{\operatorname{Spec}}(\mathscr{O}_S[t]) \\ \mathbb{G}_{m,S} &:= \underline{\operatorname{Spec}}(\mathscr{O}_S[t, t^{-1}]). \end{aligned}$$

with e, i, and m defined similarly. (See Hartshorne II.5 for review on $\mathscr{O}_S$ and `http://en.wikipedia.org/wiki/Spectrum_of_a_ring#Global_Spec` for review on relative spec. $\mathscr{O}_S[t]$

means replace the Spec $A(U)$ in the wikipedia definition by Spec $A(U)[t]$, and likewise for $\mathscr{O}_S[t, t^{-1}]$. We are basically cover $\mathscr{O}_S$ by affine schemes, constructing a polynomial algebra over each affine scheme, and patching them together.)

Define

$$\begin{aligned} \mathrm{GL}_{n,S}(T) &= \mathrm{GL}_n(\mathscr{O}_T(T)) \\ &= M_n(\mathscr{O}_T(T))^\times \end{aligned}$$

Taking $n = 1$, we recover the multiplicative group scheme: $\mathrm{GL}_{1,S} = \mathbb{G}_{m,S}$.

Example 11: Define

$$\mu_{n,S} = \underline{\mathrm{Spec}}\mathscr{O}_S[t]/(t^n - 1).$$

Here e, i, m are the same as for $\mathbb{G}_{m,S}$. Alternatively,

$$\mu_{n,S}(T) = \{x \in \mathscr{O}_T(T) : x^n = 1\}.$$

(The image of t should satisfy $t^n = 1$.)

Example 12: ? Define the constant group scheme as follows: let H be an absolute group. Define

$$\underline{H}(T) = \mathrm{Hom}(\pi_0(T), H) = \mathrm{Hom}_{\mathrm{cont}}(T, H)$$

where H is given the discrete topology in the last expression. ($\pi_0(T)$ means connected components of T.) Note $T \to T'$ gives $\underline{H}(T') \to \underline{H}(T)$. This gives us a group scheme.

Example 13: Let Γ be an abstract commutative group, and

$$G = \underline{\mathrm{Spec}} \underbrace{\mathscr{O}_S[\Gamma]}_{\text{group algebra}}.$$

(If S is an affine scheme, we just get the group algebra.) Here

$$\mathscr{O}_S[\Gamma] = \bigoplus_{\gamma \in \Gamma} \mathscr{O}_S \cdot \gamma.$$

Define

$$\begin{aligned} e &: \mathscr{O}_S[\Gamma] \to \mathscr{O}_S & \gamma &\mapsto 1 \\ i &: \mathscr{O}_S[\Gamma] \to \mathscr{O}_S[\Gamma] & \gamma &\mapsto \gamma^{-1} \\ i &: \mathscr{O}_S[\Gamma] \to \mathscr{O}_S[\Gamma] \otimes \mathscr{O}_S[\Gamma] & \gamma &\mapsto \gamma \otimes \gamma. \end{aligned}$$

Problem 1: Check that this is a group scheme.
Check that if $\Gamma = \mathbb{Z}/n\mathbb{Z}$ we get μ_n, and if $\Gamma = \mathbb{Z}$ we get $\mathbb{G}_m$.

3.3 Morphisms between group scheme

The natural next step is to define a notion of morphisms between group schemes. As we've said, the objects of (Gp/S) to be the group schemes over S. The morphisms are

$$\begin{aligned} &\mathrm{Hom}_{(\mathrm{Gp}/S)}(G, G') \\ := &\ \mathrm{Hom}(\widetilde{h_G}, \widetilde{h_{G'}}) \text{ in } \mathrm{Fun}((\mathrm{Sch}/S), (\mathrm{Gp})) \\ = &\left\{ \begin{tikzcd} G \arrow[rr] \arrow[dr] & & G' \arrow[dl] \\ & S & \end{tikzcd} : G(T) \to G'(T) \text{ is a group homomorphism, for every } T \in (\mathrm{Sch}/S) \right\} \end{aligned}$$

Definition 14: A **subgroup scheme** is a subscheme $H \subseteq G$ such that $H(T) \subseteq G(T)$ (subgroup) for all $T \in (\mathrm{Sch}/S)$. Equivalently, a subgroup scheme is (H, e_H, i_H, m_H) such that $H \subseteq G$, and the following commute:

$$\begin{tikzcd} S \arrow[r, "e_H"] \arrow[dr, "e_G"'] & H \arrow[d, hook] \\ & G \end{tikzcd} \qquad \begin{tikzcd} H \arrow[r, "i_H"] \arrow[d, hook] & H \arrow[d, hook] \\ G \arrow[r, "i_G"] & G. \end{tikzcd} \qquad \begin{tikzcd} H \times H \arrow[r, "m_H"] \arrow[d, hook] & H \arrow[d, hook] \\ G \times G \arrow[r, "m_G"] & G. \end{tikzcd}$$

We want to define kernels and cokernels. Cokernels are more difficult; let's do kernels first.

Definition 15: Let $G \xrightarrow{f} H$ be in (Gp/S). Define the kernel K/S to be the functor $K(\bullet)$ such that

$$K(T) = \ker(G(T) \xrightarrow{f(T)} H(T))$$

for all T/S.

Proof of well-definedness. It's not obvious that this functor is represented by a scheme! So let's call the functor $F(T) := \ker(G(T) \xrightarrow{f(T)} H(T))$ for now; we have to show there exists a scheme K such that $K(T) = F(T)$, i.e. we need to show F is represented by a scheme K. We do this by constructing K. Define $K := G \times_H S$, so we have the following diagram.

$$\begin{tikzcd} K \arrow[r] \arrow[d] & G \arrow[d, "f"] \\ S \arrow[r, "e_H"] & H \end{tikzcd}$$

Now take T-points and check that

$$K(T) = G(T) \times_{H(T)} S(T) = \left\{ g \in G(T) : f(g) = 1_{H(T)} \right\} = \ker f(T).$$

The first equality is from definition of the fiber product (Here, $\times_{H(T)}$ denotes the set-theoretic pullback). $\square$

Quotients are hard; we'll get to them later.