NOTE ON KATZ–MAZUR. I.

MINGCHEN XIA

Contents

1. Introduction

This is the author's personal note when reading Katz–Mazur. Use at your own risk.

The goal is

(1) Emphasize the parts that I find interesting and provide more details.
(2) Correct the typos.
(3) Use the language of stacks as much as possible.

2. Katz–Mazur Chapter 1

2.1. **Section 1.4.** In this section, the essential concept of Drinfeld structure comes in.

Let C/S be a smooth commutative S-group scheme of relative 1. The most important examples are elliptic curves and $\mathbb{G}_m$.

In the book, $C(S)$ denotes the set of sections of $C \to S$. It is *not* the set of morphisms $S \to C$ as schemes. A point $P \in C(S)$ can be identified with an effective relative Cartier divisor $[P]$ on C/S. By the definition of group schemes, $C(S)$ is a commutative group.

Definition 2.1. A point $P \in C(S)$ has *exact order* $N \in \mathbb{Z}_{>0}$ if $D := [P] + [2P] + \cdots + [NP]$ is a subgroup scheme of C/S.

To understand the exact meaning of this definition, let us spell out the scheme $D = [P] + [2P] + \cdots + [NP]$ more explicitly. As an effective divisor, the associated ideal sheaf is given by

$$\mathcal{O}_C(-[P] - [2P] - \cdots - [NP]) = \mathcal{O}_C(-[P]) \cdots \mathcal{O}_C(-[NP]) \,.$$

The product is taken in the sheaf of rings $\mathcal{O}_C$.

In general, D is just a closed subscheme of C (relative to S). There is no guarantee that D is a subgroup scheme. So the assumption means that D is closed under addition and inversion.

Date: November 9, 2022.

ex:Frob **Example 2.2.** *When $p = 0$ on S (i.e. S is a $\mathbb{F}_p$-scheme), take $P = 0 \in C(S)$. Then*

$$D := [P] + [2P] + \cdots + [p^n P] = p^n[0] \,.$$

Namely, the ideal sheaf of D is $\mathcal{O}_C(-[0])^{p^n}$. It acquires a groups structure by viewing D as the kernel of $F^n_{C/S}$, where $F_{C/S} : C \to C^{(p)}$ is the relative Frobenius. To see this, recall that the effect of the relative Frobenius is to raise the coordinates to the p-th power, so the ideal sheaf of the kernel of $F^n_{C/S}$ is noting but $\mathcal{O}_C(-[0])^{p^n} = \mathcal{O}(-D)$.

In particular, $0 \in C(S)$ has exact order p^n for any $n \geqslant 0$.

Observe that the rank of the finite group scheme D is N. As C is commutative, it follows that D is killed by N. (The non-commutative case seems to be open up to now (2022)). In particular, P is killed by N. As a consequence, there is an obvious homomorphism of S-group schemes:

{eq:ZNZtoD}
$$\underline{\mathbb{Z}/N\mathbb{Z}} \to D \tag{2.1}$$

In fact, by adjunction, this map is the same as a homomorphism of abstract groups $\mathbb{Z}/N\mathbb{Z} \to D(S)$. The latter is given by sending 1 to P.

The map (2.1) is *not* always an isomorphism, as is clear in Example 2.2.

More generally, one can always define (2.1) from a point $P \in C(S)$ killed by N. When N is invertible in S, (2.1) is an isomorphism iff P has exact order N.

We already see a clear distinction between characteristic p dividing the level in equation and other characteristics. In moduli problems, sometimes we handle other characteristics first and extend to char p by flatness. The flatness does not come for free, we usually have to establish the flatness of certain moduli spaces at first.

2.2. **Section 1.5.** This section concerns a generalization of Section 1.4. Fix an abstract Abelian group A and a smooth commutative S-group scheme C of relative dimension 1.

Definition 2.3. An *A-structure* on C/S is a homomorphism $\phi : \overline{A} \to C$ of group schemes over S such that

$$D := \sum_{a \in A} [\phi(a)]$$

(with ϕ viewed as $A \to C(S)$ by adjunction) is a closed subgroup scheme of C/S.

We call D the A-subgroup of C/S generated by ϕ and ϕ an A-generator of G.

A closed subgroup scheme $G \subseteq C$ is an A-subgroup if it is finite locally free over S of rank $|A|$ and fppf locally it admits an A-generator.

It is obvious that a point of exact order N is the same as a $\mathbb{Z}/N\mathbb{Z}$-structure.

As before, if $|A|$ is invertible in S, then the natural morphism $\phi : \overline{A} \to D$ is an isomorphism.

The most important situation for the future is the following:

Example 2.4. *Take $A = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Assume that C/S is an elliptic curve. Then an A-structure on C is called a* Drinfeld level N-structure *on*

C/S. The images of $(1,0)$ and $(0,1)$ in $C(S)$ are known as the Drinfeld basis*.*

2.3. **Section 1.6.** Fix an abstract Abelian group A and a smooth commutative S-group scheme C of relative dimension 1.

Lemma 2.5. *Let $A = \mathbb{Z}/N_1\mathbb{Z}\times\cdots\times\mathbb{Z}/N_r\mathbb{Z}$. Then the presheaf $\mathcal{H}\mathrm{om}_{S\text{-group}}(\underline{A}, C)$ on $\mathrm{Sch}_{/S}$ is represented by $C[N_1] \times_S \cdots \times_S C[N_r]$.*

Proof. In more concrete terms, we are claiming that for any S-scheme T, we have

$$\mathrm{Hom}_{S\text{-scheme}}\left(T, C[N_1] \times_S \cdots \times_S C[N_r]\right) = \mathrm{Hom}_{T\text{-group}}(\underline{A}, C_T) = \mathrm{Hom}_{\mathrm{group}}(A, C(T))\,.$$

We compute the left-hand side:

$$\begin{aligned}\mathrm{Hom}_{S\text{-scheme}}\left(T, C[N_1] \times_S \cdots \times_S C[N_r]\right) &= \prod_{i=1}^{r} \mathrm{Hom}_{S\text{-scheme}}\left(T, C[N_i]\right) \\ &= \prod_{i=1}^{r} \mathrm{Hom}_{\text{Abelian group}}(\mathbb{Z}/N_i\mathbb{Z}, C(T)) = \mathrm{Hom}_{\mathrm{group}}(A, C(T))\,.\end{aligned}$$

□

Corollary 2.6. *The functor $\mathrm{Sch}_{/S} \to \mathcal{S}\mathrm{et}$ sending T to the set of A-structures on C_T/T is representable.*

This functor is denoted by $A\text{-}\mathrm{Str}(C/S)$. In fact, we have an obvious closed immersion

$$A\text{-}\mathrm{Str}(C/S) \hookrightarrow \mathcal{H}\mathrm{om}_{S\text{-group}}(\underline{A}, C)$$

as being a subgroup scheme is clearly a closed condition.

Note that $A\text{-}\mathrm{Str}(C/S)$ is of finite presentation. If N denotes the exponent of A, suppose that $[N] : C \to C$ is finite, then $A\text{-}\mathrm{Str}(C/S) \to S$ is finite.

If N is invertible in S, then $A\text{-}\mathrm{Str}(C/S)$ is étale over S. To see this, take a thickening $T_0 \hookrightarrow T$ of S-schemes and an A-structure $\phi_0 : A \to C(T_0)$ on C_{T_0}/T_0. But as N is the exponent of A, ϕ_0 factors through $A \to C[N](T_0)$. So the lifting can be carried out using the fact that $C[N]$ is étale (as N is invertible on S).

ex:ZNZ **Example 2.7.** *We will write $\mathbb{Z}/N\mathbb{Z}\text{-}\mathrm{Str}(\mathbb{G}_m/\operatorname{Spec}\mathbb{Z})$ as $\mu_N^\times$. It can be regarded as the structure of N-th primitive roots of unity.*

Corollary 2.8. *Let G be a closed subgroup scheme of C that is finite locally free over S of rank $|A|$.*

The functor $\mathrm{Sch}_{/S} \to \mathcal{S}\mathrm{et}$ sending T to the set of A-generators on G_T is representable.

This functor is denoted by $A\text{-}\mathrm{Gen}(G/S)$. Again, it is clear that we have a closed immersion

$$A\text{-}\mathrm{Gen}(C/S) \hookrightarrow \mathcal{H}\mathrm{om}_{S\text{-group}}(\underline{A}, C)\,.$$

When G/S is finite étale, so is $A\text{-}\mathrm{Gen}(C/S)$, as it is nothing but the isomorphism functor between $\underline{A}$ and G as S-group schemes.

2.4. **Section 1.8 to Section 1.10.** Let $Z \to S$ be a finite locally free morphism (stacks-project [Stacks, Tag 02K9]) for rank N.

N points $P_1, \dots, P_N \in Z(S)$ is a *full set of sections* of Z/S if for any affine S-scheme $\operatorname{Spec} R$ and any $f \in H^0(Z_R, \mathcal{O})$, we have

{eq:charpol}

$$\det(T - f) = \prod_{i=1}^{N} (T - f(P_i)) \tag{2.2}$$

in $R[T]$.

What is $f(P_i)$? In fact, we may regard f as a morphism $Z_R \to \mathbb{A}^1_R$. Then on the functor of points, we have a map $Z_R(\operatorname{Spec} R) \to R$, but $Z_R(\operatorname{Spec} R) \supseteq Z(S)$, so we define $f(P_i) \in R$ as the image of P_i under this map.

In order to verify (2.2), it suffices to verify the constant term:

$$\operatorname{Nm}(f) = \prod_{i=1}^{N} f(P_i)$$

in R. This simply follows from the observation that the characteristic polynomial of f is the norm of $T - f$ if we change the base to $R[T]$.

It is easy to see that when $P_1, \dots, P_N$ are fixed, the condition of being a full set of sections is a closed condition on the target.

This notion is fairly trivial when Z/S is étale. In this case, it simply means that the map

$$S \coprod \cdots \coprod S \to Z$$

induced by $P_1, \dots, P_N$ is an isomorphism of S-schemes.

The notion of a full set of sections is useful because of the following theorem.

Theorem 2.9. *When Z is a closed subscheme of a smooth curve C/S, N given points $P_1, \dots, P_N \in Z(S)$ is a full set of sections iff $Z = [P_1] + \cdots + [P_N]$ as divisors on C/S.*

Proof. A standard reduction using EGA III allows us to assume $S = \operatorname{Spec} R$, where R is an Artinian local ring with algebraically closed residue field k. As Z is finite locally free over S, it is the disjoint union of local schemes $Z_1, \dots, Z_r$, where each Z_i contains exactly 1 closed point on the special fiber. As we are only interested in sections, one easily reduces to the case where Z is Artinian local as well. The closed point of Z is denoted by z.

As C is smooth, we have a non-canonical isomorphism

$$\hat{\mathcal{O}}_{C,z} \cong R[[X]]\,.$$

By Weierstrass preparation, we can write

$$Z \cong \operatorname{Spec} R[[X]]/(F(X)) \cong \operatorname{Spec} R[X]/(F(X))\,,$$

where $F(X) = X^N + \mathcal{O}(X^{N-1})$. We may assume that the coefficients of the lower order terms are in $\mathfrak{m}_R$.

Next we handle the closed subscheme $[P_1] + \cdots + [P_N]$ of C. It is defined by a polynomial $G(X) = (X - X(P_1)) \cdots (X - X(P_N))$ in $Z = \operatorname{Spec} R[X]/F(X)$. As $X - X(P_i) | F(X)$, $X(P_i) \in \mathfrak{m}_R$ (as can be seen after reduction mod $\mathfrak{m}_R$). Now the extrinsic condition $Z = [P_1] + \cdots + [P_N]$ becomes $F(X) = (X - X(P_1)) \cdots (X - X(P_N))$.

It is clear now Z and $[P_0] + \cdots + [P_N]$ are both supported on z. So in order to prove the equality, we may pass to the formal completion at z. The same reduction allows us to pass from the formal completion to $C = \mathbb{A}^1_S$.

The problem becomes simple algebra, which we omit. □

In particular, this theorem shows that A-structures depends only on the $|A|$-torsion points of an elliptic curve C/S. This is what one should expect from the classical theory of level structures (Igusa, Deligne–Rapoport...).

Example 2.10. *We continue Example 2.7. Observe that a $\mathbb{Z}/N\mathbb{Z}$-structure on $\mathbb{G}_m/\mathbb{Z}$ is the same as a homomorphism $\mathbb{Z}/N\mathbb{Z} \to \mathbb{G}_m(\mathbb{Z})$ that generates μ_N. Such a map is determined by the image of 1. That is, for any ring R,*

$$\mu_N^\times(R) = \left\{ \zeta \in R : T^N - 1 = \prod_{a=1}^{N} (T - \zeta^a) \in R[T] \right\} .$$

Here we used the algebraic Lemma 1.10.2.

Now observe that $\mu_N^\times$ is regular of dimension 1 and $\mu_N^\times \to \operatorname{Spec} \mathbb{Z}$ is finite locally free of rank $\phi(N)$. Over $\operatorname{Spec} \mathbb{Z}[1/N]$, it is a finite étale cover.

We can easily reduce to the case $N = p^n$. Outside p, the situation is almost clear, as μ_{p^n} is then non-canonically isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. As we know from the general story that $\mu_{p^n}^\times \to \operatorname{Spec} \mathbb{Z}$ is finite hence having closed image. It follows that $\mu_{p^n}^\times \to \operatorname{Spec} \mathbb{Z}$ is in fact surjective. The fiber over p consists of a single point, which is $\mathbb{F}_p$-rational (as $\mu_{p^n}(\mathbb{F}_p^{\mathrm{alg}})$ is so). We denote this point as q. We need to show that $\mathcal{O}_{\mu_{p^n}^\times, q}$ is regular. As it is at least 1-dimensional, it suffices to show that $\mathfrak{m}_{\mu_{p^n}^\times, q}$ is generated by a single element: $\zeta - 1$. This is an easy exercise in commutative algebra.

Finally the flatness of $\mu_N^\times \to \operatorname{Spec} \mathbb{Z}$ follows from miracle flatness.

In fact, with some more efforts, one can show that $\mu_N^\times = \operatorname{Spec} \mathbb{Z}[X]/(\Phi_N(X))$, where $\Phi_N(X)$ is the N-th cyclotomic polynomial.

2.5. **Section 1.11.** Fix a connected scheme S and a short exact sequence of finite flat commutative S-group schemes of finite presentation:

$$0 \to H \to G \to E \to 0$$

with E/S finite étale. Consider a finite Abelian group A such that $|A| = \operatorname{rank} G/S$. Let $\phi : A \to G(S)$ be a group homomorphism.

This section studies when ϕ is an A-generator of G/S (in the sense that $\phi(a)$ with $a \in A$ forms a full set of sections).

Observation: we have the following natural maps by adjunction

$$\underline{A} \to G \to E \,.$$

The kernel exists and is finite étale (as finite étale group schemes form an Abelian category). Recall that finite étale group schemes can be identified with $\pi_1^{\text{ét}}$-groups, so the kernel is constant, which is identified with $\underline{K}$ for some abstract subgroup $K \subseteq A$. Is it true that over a connected base, the finite subgroups (without assuming to be étale) of a finite constant group scheme are constant?

Then one finds easily the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & A & \longrightarrow & A/K & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H(S) & \longrightarrow & G(S) & \longrightarrow & E(S) & \longrightarrow & H^1_{fppf}(S,H) \end{array}$$

The answer to our question is given by

Proposition 2.11. *ϕ is an A-generator of G/S iff the following conditions are satisfied:*

(1) $|K| = \operatorname{rank} H/S$, $\phi : K \to H(S)$ is a K-generator of H/S.
(2) $|A/K| = \operatorname{rank} E/S$, $\phi : A/K \to E(S)$ is an E/S-generator of E/S.

It might be surprising that the étaleness of E is necessary.

3. Chapter 2

Results in this chapter are mostly very standard. I include a few remarks.

3.1. **Section 2.3.** On page 75, in order to show that $E[N]$ and $\underline{\mathbb{Z}/N\mathbb{Z}}$ étale locally, it is not necessary to know that the base scheme is normal. In fact, we could simply pass to the strict henselization of the base, where the problem is trivial.

References

stacks-project [Stacks] T. Stacks Project Authors. Stacks Project. http://stacks.math.columbia.edu. 2020.

Mingchen Xia, Department of Mathematics, Chalmers Tekniska Högskola, Göteborg
Email address, xiam@chalmers.se
Homepage, http://www.math.chalmers.se/~xiam/.