Plan of the "Mazur seminar"

There will be several background talks, to be followed by talks working through the first half of Mazur's *Rational isogenies of prime degree*. Since we are single-mindedly focused on Ogg's conjecture and not the more general question of classifying prime-degree isogenies between elliptic curves over $\mathbf{Q}$ (i.e., we are only studying such isogenies whose kernel is constant as a Galois-module), there are many technical issues that arise for Mazur but are not relevant for our immediate purposes.

When we turn to Mazur's heftier IHES paper that develops a general machine for studying the arithmetic of modular curves and Jacobians, we will need to deal with delicate issues such as bad reduction of Jacobians, quasi-finite flat group schemes, etc. However, for the first part of the seminar we may safely set aside such concerns (granting the existence of the rank-zero Eisenstein quotient of Jacobians, a fact whose proof will emerge when we study Mazur's IHES paper). This summary focuses exclusively on the *Rational isogenies* paper; a separate summary will be prepared when we are close to finishing this paper and are in position to study the other paper.

This schedule leaves approximately 3 weeks at the end of the term, so that gives some extra room in case some talks required extra time, etc.

Talk 1. We will begin with an overview of Kubert's paper, ignoring large parts that are irrelevant to Mazur's proof of Ogg's conjecture. In essence, this paper explains both the natural motivation for Ogg's conjecture as well as the elimination of many possible counterexamples, reducing the problem to showing that $X_1(p)$ has no non-cuspidal $\mathbf{Q}$-rational points for $p \geq 17$. The key points are the following. First, it should be explained how one finds explicit algebraic models for the genus-zero modular curves and universal elliptic curves over them as in Table 3 (p. 217) of Kubert's paper, say for the cases of $\mathbf{Z}/5\mathbf{Z}$ and/or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ as representative samples. In principle, these methods give a direct construction of these modular curves as fine moduli schemes (say over $\mathbf{Q}$). Second, it should also be briefly indicated why $X_0(N)$ has genus 1 for

$$N \in \{11, 14, 15, 20, 21, 24, 27, 49\}$$

and (say for $X_0(14)$) how we see that the $\mathbf{Q}$-rational points are supported in the cusps. Finally, it should be explained why $X_1(16)$ and $X_0(35)$ have no non-cuspidal $\mathbf{Q}$-rational points.

(In view of the fact that Mazur eliminates all possible primes except for $2, 3, 5, 7, 11, 13$, it also needs to be proved that $X_1(N)$ has no non-cuspidal $\mathbf{Q}$-rational points for

$$N \in \{11, 13, 14, 15, 16, 18, 20, 21, 24, 25, 27, 35, 49\}$$

and that the torsion subgroups $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/10\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z}$ cannot occur. The preceding $X_0(N)$-results rule out all $X_1(N)$'s in the above list except for $N \in \{13, 18, 25\}$; these will be treated in a later talk. It is a simple exercise with the Galois-equivariant Weil pairing to see that for any elliptic curve E over $\mathbf{Q}$ with $E[2](\mathbf{Q}) = E[2](\overline{\mathbf{Q}})$, any quotient E' of E by a point of order 2 contains a Galois-stable cyclic subgroup of order 4. Thus, if either $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/10\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z}$ were to occur then we would get a non-cuspidal $\mathbf{Q}$-rational point on $X_0(20)$ and $X_0(24)$, and the preceding results show this to be impossible.)

Talk 2. A fundamental technique in Mazur's paper is the use of finite flat group schemes over discrete valuation rings. These arise in two contexts: specialization as torsion-points in abelian varieties, and in p-divisible groups whose connected component computes a formal group on an abelian scheme. The purpose of this talk is simply to explain background related to these results: examples of finite flat group schemes, relations with Galois modules, Cartier duality, the meaning of a short exact sequences, and a discussion of the meaning of Raynaud's theorem (Proposition 1.1), and (in the complete case) the relation between finite flat group schemes and formal groups in mixed characteristic (needed for Corollary 1.1). Emphasis should be placed on examples of both explicit and theoretical nature (such as the failure of Raynaud's theorem for high ramification, the Néron-Ogg-Shafarevich criterion, the functorial interpretation of connected components, and torsion on elliptic curves and abelian varieties with and without good reduction). The proof of Raynaud's theorem will be done later when we get to the IHES paper, but give a direct proof in the special case of maps from a constant cyclic group.

Talk 3. Néron models pervade Mazur's paper, and we do need to consider bad reduction in the context of elliptic curves (for Mazur's other paper, bad reduction in higher relative dimension will also arise). This talk

should address the following topics: definition of smoothness and abelian schemes, Néron mapping property and component groups, and semistable reduction theorem. Treat the examples of elliptic curves with good and bad reduction as well as relative Jacobians of proper smooth curves (including discussion of general facts about Jacobians and their tangent spaces along identity). Also address the relationship between the minimal Weierstrass model of an elliptic curve and its Néron model.

Talk 4. The link between the moduli spaces and the group schemes arises from a consideration of arithmetic models of modular curves (and Jacobians of these curves). This talk should explain the meaning of a moduli space, say with the example of projective space and the functorial definition of the Plücker embedding, some indications of how $Y_1(N)$ is constructed as a scheme over $\mathbf{Z}[1/N]$ (for $N \geq 5$), how $X_1(N)$ and $X_0(N)$ are made over $\mathbf{Z}[1/N]$, and why these are smooth. Despite the absence of a universal family of elliptic curve over $X_1(N)$ and $X_0(N)$, indicate how we can still construct Hecke correspondences, Atkin-Lehner involution, and Hecke endomorphisms of Jacobians (see §2(a)–(c)). Also discuss why points of $X_1(N)$ have semistable reduction, and show that these constructions recover weight-2 cusp forms at level N.

Talk 5. One loose end from Talk 1 is the triple of higher-genus curves $X_1(N)$ for $N = 13, 18, 25$. The study of these cases rests on a technique of Mazur and Tate that handled $X_1(13)$. This curve has genus 2, and Mazur–Tate combine Ogg's analysis of the torsion-subgroup of $J_1(13)$ with H^1's on the fppf and étale sites to carry out a descent-analysis to prove $J_1(13)(\mathbf{Q})$ has rank zero.

This talk should explain the Mazur–Tate paper, and if time permits it should also address Kubert's variant on this to treat either of the non-prime levels $N = 18$ or $N = 25$ (probably $N = 18$ is a better choice). In view of the techniques used by Mazur and Tate, this talk should also include a brief discussion of Ogg's analysis of the torsion, as well as an example-based explanation of what fppf and étale cohomology mean, including the interpretation of H^1 via torsors (and the application of this to compute an fppf H^1 with coefficients in a finite étale group scheme). It should also be explained how an exact sequence of abelian sheaves naturally arises from exact sequences of smooth commutative group schemes, since Mazur–Tate use cohomology sequences attached to such short exact sequences.

Talk 6. We are now in position to study Mazur's paper. The first task is the material in §1, but much of it can be ignored since we are only aiming to prove Ogg's conjecture (and not the other things in this paper). The only results we require are Propositions 1.1 and 1.2, and Corollary 1.1. Since Proposition 1.1 has already been discussed, the task at hand is Proposition 1.2 and Corollary 1.1 (in good reduction case). Explain the proof of Proposition 1.2 without Mazur's gratuitious appeal to algebraic spaces, instead arguing via duality of abelian schemes (so it is necessary to explain/prove the torsion criterion for exactness of a 3-term complex of abelian schemes). Then use this to prove Corollary 1.1 in the good reduction case, via Raynaud's theorem and the relationship between the formal group and the connected components of the p-power torsion levels. If time permits, explain the interesting example of Serre for $p = 2$.

Throughout this discussion, K should be taken to be the fraction field of a complete discrete valuation ring with mixed characteristic $(0, p)$ and absolute ramification degree $< p - 1$; finiteness of $[K : \mathbf{Q}_p]$ plays no logical role and so should not be assumed.

Talk 7. The arithmetic models of modular curves provide Hecke rings that act on Jacobians, as in Talk 4. Define the "new" quotient as in §2(b) over $\mathbf{Q}$ and explain the relationship between its cotangent space and the space of newforms of weight 2 at the same level. Prove Proposition 2.1, including explanations of the role of the Eichler-Shimura relations, multiplicity-one for newforms, and the reason why the number fields arising from newforms on $J_0(N)$ are totally real. Also discuss the definition of optimal quotients, and apply Proposition 2.1 to prove that such quotients of the Jacobian admit a compatible action by the Hecke ring (and indicate why optimality is crucial for this fact).

Talk 8. The relationship between q-expansions, both analytic and algebraic, is a vital tool in Mazur's study of Néron models of optimal quotients. We only require level-N modular curves over $\mathbf{Z}[1/N]$, so we can avoid the technical difficulties surrounding Grothendieck duality in the non-smooth case.

Give a careful definition of q-expansions algebraically in terms of Tate curve and a formal completion along a section ∞ over $\mathbf{Z}[1/N]$ (do define this section!), and at least provide a convincing sketch of the proof

that this definition agrees with analytic q-expansions, and explain the q-expansion principle in this good reduction situation. State Grothendieck-Serre duality for proper smooth curves, and prove that this duality is compatible with tangent/cotangent duality at the origin on the associated (relative) Jacobian; this is the real meaning of Lemma 2.1, and explain why it is so.

Talk 9. As an application of the algebraic theory of q-expansions, we are in position to prove a non-obvious property of the map from $X_0(N)_{/\mathbf{Z}[1/N]}$ to the Néron model $\mathscr{A}$ of an optimal quotient A of $J_0(N)_{/\mathbf{Q}}$ when the modular curve is mapped to its Jacobian by taking ∞ as the base point. As usual, we only work with N inverted, so all of the complications of bad fibers can be ignored. Discuss what it means to say that a map $f : X \to Y$ between finite-type schemes over a noetherian base S is a formal immersion along a section $x \in X(S)$, and show that if $f_1, f_2 : X \rightrightarrows Y$ are S-maps such that $f_1(x)|_Z = f_2(x)|_Z$ for some closed subscheme $Z \hookrightarrow S$, then $f_1(x)|_U = f_2(x)_U$ for an open subscheme $U \subseteq S$ around Z. Prove the following special case of Proposition 3.1: $X_0(N)_{/\mathbf{Z}[1/2N]} \to \mathscr{A}$ is a formal immersion along ∞ (Mazur proves a stronger result over $\mathbf{Z}[1/2m]$ where m is the product of the primes dividing N to order at least 2, but we shall ignore this), and deduce that when $p \nmid 2N$ then $X_0(N)(\mathbf{Z}_{(p)}) \to \mathscr{A}(\mathbf{Z}_{(p)})$ has ∞ as the only point over $0 \in \mathscr{A}(\mathbf{Z}_{(p)})$ whose reduction in $X_0(N)(\mathbf{F}_p)$ is $\infty \bmod p$. In the special case when N is prime, explain how to use the Atkin–Lehner involution to deduce the same property at the other cusp.

Talk 10. Now we reach the punchline. Define the Eisenstein quotient of $J_0(N)_{/\mathbf{Q}}$ for prime N (see pp. 95–98 in the IHES paper), and state the finiteness property for its Mordell–Weil group (Theorem 3.1, Ch. III in the IHES paper). Use this to prove that that if E is an elliptic curve over $\mathbf{Q}$ and C is a cyclic subgroup with prime order $N > 2$, then E has potentially good reduction at all odd primes (this is the special case of Corollary 4.3 with prime N, $K = \mathbf{Q}$, and any $p \neq 2$). Review how Mazur applies this to prove Ogg's conjecture. In whatever time remains, explain the definition and analysis of Manin constants (as in Corollary 4.1) in the special case of square-free N.