

Solutions to all or part of
Sheet 1 received from:

Lenos	Bartlett
Petracca	Ranacher-Tur
Vank	Sektnan.
Birkbeck	

Q4. Some people got misled
by a typo in the notes:

$$\dim M_k(\Gamma) = (k-1)(g-1) + \frac{k}{2} \infty$$

for Γ neat (not $(k-1)(g-2)$.)

Q5. can be done w/o using explicit
formula for $\dim M_k(\Gamma(S))$

Q10. See recent Arxiv preprints
by Nadim Rustom.

Q11. There's a unique index 2 subgroup
and it works. (contains $\Gamma(2)$)

Q12. Very nice argument: can show
 $\Gamma_0(N)$ is free on 3 generators
- stabilizes at $0, \infty$ and 1 other
This gives a source of index N subgroups
 $\forall N \nexists X(N) \rightarrow X_0(N)$ unramified everywhere
 $\Rightarrow g(X(N)) = 1$.

Some properties of functors + representable functors

C category ("locally small" - means
between any 2 objs are a set).

$\text{Hom}(X, -)$ is a functor $C \rightarrow \text{Set}$;
denote it by h^X . ("covariant Hom-functor")

A functor $F: C \rightarrow \text{Set}$ is representable
if \exists of functors $F \cong h^X$ some $X \in \text{Ob}(C)$.
How do we specify the isomorphism $F \cong h^X$?

Note $h^X(X)$ has a canonical elt:
 id_X . Need to know a corresponding elt of
 $F(X)$, as $h^X(X) \cong F(X)$.

Having specified a $\varphi \in F(X)$ canon. to id_X ,
this determines an elt of $F(Y)$ for every hom
 $\alpha: X \rightarrow Y$: take $F(\alpha)(\varphi)$.

Prop 3.2.1 (Yoneda's Lemma)

This construction is a bijection
(not "transformations") $\xrightarrow{\sim} F(X)$

for any $F: \underline{\text{Sets}} \rightarrow \text{Sets}$ and $X \in \text{Ob}(\mathcal{C})$.

(Have discussed covariant functors,
but we get the same for contravariant
functors by replacing \mathcal{C} with \mathcal{C}^{op})

So if F is representable, the bijection
 $F(Y) \cong h^X(Y)$ is determined by
a $\varphi \in F(X)$; we are saying that
for every $Y \in \text{Ob}(\mathcal{C})$ and $y \in F(Y)$,
 $\exists!$ hom $\alpha: X \rightarrow Y$ st $\alpha(\varphi) = y$.
We say " (X, φ) represents F ".
 φ is an essential part of the data!

Examples ($\mathcal{C} = \text{Ring}$)

$\cdot F(R) = R$. ("forgetful functor")

Represented by
 $(\mathbb{Z}[T], T)$

$(\forall R \text{ ring}, r \in R, \exists! \alpha: \mathbb{Z}[T] \rightarrow R \text{ st } \alpha(T) = r)$

$\cdot F(R) = R^\times$

Represented by
 $(\mathbb{Z}[T, T^{-1}], T)$.

$\cdot F(R) = \{n^{\text{th}} \text{ roots of 1 in } R\}$
rep by $(\mathbb{Z}[T]/(T^n - 1), T)$.

(Comment: "primitive n^{th} roots of 1"
isn't a functor on Ring .)

A non-example

$F(R) = (\text{squares in } R)$.

This is not representable.

Pf: Suppose F is represented by
 (A, α) , some ring A and $a \in A$,
with $a \neq b$ some $b \in A$.

Then for any ring S and elt $s \in S$ of
 $\exists! \text{ hom } A \xrightarrow{\alpha} S \text{ st } \alpha(a) = s$.
 s is a square.

But: take $S = \mathbb{Z}[T]$, $s = T^2$
So $\exists! \alpha: A \rightarrow \mathbb{Z}[T]$ with $\alpha(a) = T^2$
 $\Rightarrow \alpha(b) \in \{\pm T\}$

Let $\sigma: S \rightarrow S$ be $T \mapsto -T$.
 $\sigma(s) = s$.

So $\sigma \circ \alpha \in \text{Hom}(A, S)$ also sends
 $a \mapsto s$, but $\sigma \circ \alpha \neq \alpha$ as
 $\sigma \circ \alpha(b) \neq \alpha(b)$.
This contradicts uniqueness of α . \square

Moral of this example:
Automorphisms are bad
for representability

§ 3.3 Elliptic curves over general base schemes.

"elliptic curves over S ", S a scheme.

Definition 3.3.1 Let S be a scheme.
 An ell. curve/ S is a scheme Σ with a morphism $\Sigma \xrightarrow{\pi} S$ (an S -scheme) st
 π is flat + proper, + all fibres are smooth genus 1 curves, given with a section " \mathcal{O} ": $S \rightarrow \Sigma$.

Example In Silverman's book, there is the equation

$$Y^2 + XY = X^3 - \left(\frac{36}{j-1728}\right)X - \left(\frac{1}{j-1728}\right)$$

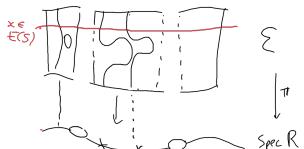
Associated homogeneous cubic

$$Y^2Z + XYZ = X^3 - (\dots)XZ^2 - (-)Z^3$$

 is a subscheme of \mathbb{P}^2/R , R the ring
 $\mathbb{Z}[\sqrt{j}, (\sqrt{j-1728})^3]$

This is an ell. curve / $\text{Spec } R$.
 (discriminant is $\Delta = \frac{4}{(j-1728)^3}$).

Think of this as a family of elliptic curves: one for every $j \neq 0, 1728$, varying in an "algebraic way".



For Σ/S as above, $E(S) =$
 $\text{Hom}_{S-\text{sch}}(S, \Sigma)$
 = Sections of $\pi: \Sigma \rightarrow S$.
 picking out a point on each fibre.

Warning If $P \in E(S)$ has order N , i.e.
 $NP = 0$ and $NP \neq 0$ for $0 < M < N$,
 it is not necessarily true that P_x has order
 N on Σ_x for any $x \in S$.
 (E.g. if $\Sigma/\text{Spec}(\mathbb{Z}_p)$, can have pts
 of order p reducing mod p to 0.)
 (at closed pt of $\text{Spec } \mathbb{Z}_p$)

Prop 3.3.2 If Σ/S is an ell. curve, then
 Σ has a Weierstrass equation locally on S .

That is, \exists covering $\coprod U_i \rightarrow S$
in Zariski top. st $\mathcal{E}|_{U_i}$ has a W.eq⁺ ν_i .

More precisely, we'll show the following:

$\omega_{S/\mathbb{A}^1} = \pi_* (\Omega_{\mathbb{P}^1_S})$ is an invertible sheaf on S ,

$\bigwedge_{i=1}^n$

and any local basis w of ω_{S/\mathbb{A}^1} (over some $U \subset S_{\text{reg}}$)

determines a W.eq⁺ over U . If ω is invertible on S ,
can do this in such a way that
 $w = \frac{-dx}{2y}$.

Proof (sketch)

The invertibility of $\pi_* (\Omega_{\mathbb{P}^1_S})$ comes from a calculation in "sheaf cohomology", cf.

p 53 of Mumford "Abelian Varieties"
- $R^i \pi_* (\Omega^i)$, zero for $i > 0$, invertible

Now, given U and w a basis of $\pi_* (\Omega_{\mathbb{P}^1_S})$ this gives a local parameter on E at O .

st $w = dt(1 + \text{higher order terms})$.

("local parameter adapted to w ")

$\pi_* (\mathcal{O}_E (2)) \stackrel{\text{loc}}{\sim} \text{free rank 2 over } U$

Assume $U = \text{Spec}(A)$
then $\pi_* \mathcal{O}_E (2) \cong A \cdot (1, x)$

where $x = \frac{1}{t^2} (1 + \dots)$

Similarly $\pi_* \mathcal{O}_E (3) \cong A \cdot (1, x, y)$

$y = \frac{1}{t^3} + \dots$

$\pi_* \mathcal{O}_E (4) \cong A \cdot (1, x, y, x^2)$

$S(0) = A \cdot (1, x, y, x^2, xy)$

$y^2 - x^3 \in \pi_* \mathcal{O}_E (5)$

so $y^2 - x^3 \in A \cdot (1, x, y, x^2, xy)$

and that's a Weierstrass eq⁺ over $A[x, y]$

Moreover $\frac{dx}{dt} = \frac{-2xT}{T^3} + \dots \quad \left. \begin{array}{l} \frac{dy}{dt} = \\ y = \end{array} \right\} \text{so } \frac{dy}{dx} \text{ mod } TAT$

(Don't have such a nice characterization
of the W.eq⁺ if ω not invertible on S .)

Defn 3.3.3 For S a scheme, $\alpha, \beta \in \Gamma(S, \mathcal{O}_S)$, let $E(\alpha, \beta)$ be subscheme of \mathbb{P}_S^1

def by

$$Y^2Z + \alpha XYZ + \beta YZ^2 = X^3 + \beta X^2Z.$$

and let $\Delta(\alpha, \beta) = -\beta^3(\alpha^4 - \alpha^3 + 8\alpha^2\beta - 36\alpha\beta + 16\beta^2 + 27\beta^3)$
be its discriminant.

If $\Delta(\alpha, \beta) \in \Gamma(S, \mathcal{O}_S^\times)$ this is an
ell. curve / S .

$$P = (0, 0, 1) \in E(S).$$

and we calculate

$$\begin{array}{ll} P = (\alpha : 0 : 1) & -P = (0 : \beta : 1) \\ 2P = (-\beta : \beta(\alpha-1) : 1) & -2P = (-\beta : 0 : 1) \\ 3P = (1-\alpha : \alpha-\beta-1 : 1) & -3P = (1-\alpha : (\alpha-1)^2 : 1) \\ \vdots & \vdots \end{array}$$

P does not have order 1, 2 or 3 in any fibre.

Prop 3.3.4 For any scheme S , E/S et. are
and $P \in E(S)$ st. $P, 2P, 3P \neq 0$ on any fibre.
 $\exists! \alpha, \beta \in \Gamma(S, \mathcal{O}_S)$ st. $\Delta(\alpha, \beta) \in \Gamma(S, \mathcal{O}_S^\times)$
and \exists a unique iso $E(\alpha, \beta) \xrightarrow{\sim} E$
mapping $(0, 0)$ to P .

Corollary: The pair
 $(\text{Spec } \mathbb{Z}[A, B, \Delta(A, B)], (E(A, B), (0, 0)))$
represents the functor

$\text{Sch}^{\text{opp}} \rightarrow \text{Set}$

$S \mapsto (\text{pairs } (E, P), E/S \text{ et. are,}$
 $P \in E(S) \text{ not of order 1, 2, 3}$
 $\text{in any fibre.})$