CMI-HIMR SUMMER SCHOOL: EXERCISES

JOHN VOIGHT

1. Lecture 1: over finite fields

Problem 1.1.

(a) Describe an efficient algorithm that takes as input an irreducible polynomial $f(T) \in \mathbb{Z}[T]$ and decides if $f(T)$ is a cyclotomic polynomial (i.e., if $f(T)$ is the minimal polynomial of a primitive root of unity).

(b) How many ways can you compute $f^{\otimes r}(T)$, given $f(T) \in 1+T\mathbb{Z}[T]$? What way is the most efficient (in theory or in practice)?

Problem 1.2. In each part of this exercise, the polynomial $c(T)$ is the (inverse) characteristic polynomial of Frobenius for an abelian variety A over $\mathbb{F}_q$. For each part, compute:

- the degree $k = [\mathbb{F}_{q^k} : \mathbb{F}_q]$ of the minimal extension such that all geometric endomorphisms of A are defined over $\mathbb{F}_{q^k}$, i.e., $\operatorname{End}(A^{\mathrm{al}}) = \operatorname{End}(A_{\mathbb{F}_{q^k}})$;
- the structure of the endomorphism algebras $\operatorname{End}(A_{\mathbb{F}_{q^d}})_{\mathbb{Q}}$ for all $d \mid k$.

(i) $c(T) = 1 - 7T + 22T^2 - 35T^3 + 25T^4$.

(ii) $c(T) = 1 - 2T + 2T^2$.

(iii) $c(T) = 1 + T^2 + 9T^4$

(iv) $c(T) = 1 - 4T^2 + 16T^4$

Check your work at `http://abvar.lmfdb.xyz/Variety/Abelian/Fq/`. What is the most exotic endomorphism algebra you can find? (And please share any comments you have on the display—or anything else!)

Do you notice a feature in common between (c) and (d) that generalizes?

Problem 1.3. Let A be an abelian variety over $\mathbb{F}_q$ and let $c(T) \in 1 + T\mathbb{Z}[T]$ be the characteristic polynomial of Frobenius. Factor

$$c(T) = \prod_{i=1}^{t} h_i(T)^{m_i} \in \mathbb{Q}[T]$$

with each $h_i(T)$ irreducible. Show that

$$\dim_{\mathbb{Q}} \operatorname{End}(A)_{\mathbb{Q}} = \sum_{i=1}^{t} m_i^2 \deg h_i(T).$$

[Hint: Factoring $c(T) = \prod_i (1 - z_i T)$*, we have* $\dim_{\mathbb{Q}} \operatorname{End}(A)_{\mathbb{Q}} = \#\{(i,j) : z_i z_j = q\}$*.]*

Date: 24–27 June 2019.

2. Lecture 2: over complex numbers

Problem 2.1. At a terminal prompt on your laptop, ssh into toby via

`ssh cmihimr@toby.dartmouth.edu`

with password given to you in lecture.

(a) Confirm the numerical endomorphism algebra computed in lecture, as follows.

```
cmihimr@toby:~$ magma
[...]
> QQ := RationalsExtra(200);
> _<x> := PolynomialRing(QQ);
> X := HyperellipticCurve(x^5-x^4+4*x^3-8*x^2+5*x-1);
> B, desc := HeuristicEndomorphismAlgebra(X : Geometric := true);
> B;
[*
    Associative Algebra of dimension 4 with base ring Rational
    Field,
    [ (1 0 0 0), (-1  0  0  1), (-1  1  0 -1), (0 0 1 1) ],
    [ M_2 (RR) ]
*]
> desc;
[* [* [* II,
        [ -1, 1 ],
        2, 6, 1
    *] *],
    [ 1, 1 ],
    [ M_2 (RR) ]
*]
> bl, Bquat := IsQuaternionAlgebra(B[1]);
> Discriminant(Bquat);
6
> Bquat;
Quaternion Algebra with base ring Rational Field,
defined by i^2 = 2, j^2 = -3/4
> GeoEndoRep := GeometricEndomorphismRepresentation(X);
> F<w> := BaseRing(GeoEndoRep[1][1]);
> F;
Number Field with defining polynomial x^4 + 1 over the Rational Field
> GeoEndoRep;
[...]
```

(b) What is the numerical endomorphism algebra of the curve $y^2 = x^5 + x^3 + x$? *[Hint: this is the curve with LMFDB label* 9216.a.36864.1*.]*

(c) Try some other examples at `https://github.com/edgarcosta/endomorphisms/blob/master/examples/Buttons.m`.

Problem 2.2. Read section 43.4 and do exercise 43.1 in the book at `http://quatalg.org`.

Problem 2.3. In this exercise, we explore the use of the lattice basis reduction algorithms to recognize algebraic numbers and find linear relations among complex numbers.

Equip $\mathbb{R}^n$ with the standard inner (dot) product $\langle\, ,\, \rangle$ and induced norm $\| \|^2$, the measure of size. We consider finitely generated subgroups $L \subset \mathbb{R}^n$, so $L = \sum_i \mathbb{Z}x_i$ with $x_i \in \mathbb{R}^n$ linearly independent over $\mathbb{R}$. We suppose that there is a black box (labelled "LLL") that returns short vectors (vectors of small norm) in L, and we don't ask any questions right now what is happening in the box.

Let $a \in \mathbb{R}$ be given to D decimal digits. Suppose that a is algebraic and satisfies a polynomial $f(x) \in \mathbb{Z}[x]$ of degree $d \geq 1$ (not necessarily monic) that we want to guess. Consider the subgroup $L \subseteq \mathbb{R}^{d+2}$ with $\mathbb{Z}$-span the rows of the matrix $A \in \mathrm{Mat}_{(d+1)\times(d+2)}(\mathbb{Z})$ whose first $(d+1) \times (d+1)$ submatrix is the identity matrix and whose last column has entries

$$10^D, \lfloor 10^D a \rfloor, \lfloor 10^D a^2 \rfloor, \ldots, \lfloor 10^D a^d \rfloor.$$

Let $c = (c_0, c_1, \ldots, c_d, c_{d+1}) \in L$ be a short vector returned by the black box.

(a) Let $f(x) = c_0 + c_1 x + \cdots + c_d x^d$. Show (without working too hard!) that $f(a) \approx c_{d+1}/10^D$ is small; conclude $f(x)/c_d$ is a good candidate for the minimal polynomial of a.

(b) Generalize the above procedure to work for $a \in \mathbb{C}$.

(c) Generalize the above procedure to take as input $z_1, \ldots, z_d \in \mathbb{C}$ and gives as output small $c_1, \ldots, c_d \in \mathbb{Z}$ such that $\sum_{i=1}^d c_i z_i$ is small.

(d) Interpret the previous part as computing short vectors in the integer (row) kernel of a matrix $P \in \mathrm{Mat}_{d\times 1}(\mathbb{C})$, and generalize this to work for arbitrary $P \in \mathrm{Mat}_{d\times e}(\mathbb{C})$.

3. Lecture 3: over number fields

Problem 3.1. Let $X\colon y^2 = f(x)$ be a nice hyperelliptic curve over a number field F of genus g (so that $\deg f(x) = 2g+1, 2g+2$), and let $A := \mathrm{Jac}(X)$ be its Jacobian. Then

$$\omega_1 := \frac{\mathrm{d}x}{y}, \dots, \omega_g := x^{g-1}\frac{\mathrm{d}x}{y}$$

is an F-basis of regular differentials.

Let $P_0 = (0, y_0) \in X(F)$ be a non-Weierstrass point (i.e., $y_0 \neq 0$) and let

$$\widetilde{P_0} = (x, \sqrt{f(x)}) \in X(F[[x]])$$

be the formal lift of P_0, where $\sqrt{f(x)} = y_0 + O(x)$.

Let $\alpha \in \mathrm{End}(A)$ and let $M = (m_{i,j})_{i,j}$ be the tangent representation of α with respect to (the dual of) this basis. Recall the map

$$\alpha_X\colon X \dashrightarrow \mathrm{Sym}^g(X)$$

defined by

$$\alpha_X(P) = \{Q_1, \dots, Q_g\} \quad \text{if } \alpha([P]-[P_0]) = [Q_1 + \dots + Q_g - gP_0].$$

Let

$$\alpha_X(\widetilde{P_0}) = \{\widetilde{Q_1}, \dots, \widetilde{Q_g}\}$$

and let $x_j = x(\widetilde{Q_j})$. Then

$$(*) \qquad \sum_{j=1}^{g} x_j^{i-1}\frac{\mathrm{d}x_j}{\sqrt{f(x_j)}} = \sum_{j=1}^{g} m_{i,j}x^{j-1}\frac{\mathrm{d}x}{\sqrt{f(x)}} \in F^{\mathrm{al}}[[x^{1/\infty}]] \quad \text{for all } i = 1, \dots, g.$$

in the Puiseux series ring.

Carry out the computation of this lift in a simple example (avoiding Puiseux series), as follows. Let $f(x) = x^5 + x + 1$ and $P_0 = (0,1)$.

(a) To warm up, compute $\widetilde{P_0} = (x, \sqrt{f(x)}) = (x, 1 + O(x))$ to order $O(x^3)$.

(b) Consider $\alpha = -2$ (the endomorphism given by multiplication by -2), with $M = \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}$. Writing

$$x_j = c_{j,1}x + O(x^2)$$

for $j = 1, 2$, plug into (*) and solve for $c_{j,1}$, then repeat to compute x_j to order $O(x^3)$. [What unusual thing happens for $\alpha = 2$?]

(c) Continuing in this way, we can fit a divisor. Confirm this and check your work:

```
cmihimr@toby:~$ magma
[...]
> _<x> := PolynomialRing(Rationals());
> X := HyperellipticCurve(x^5+x+1);
> P0 := X ! [0,1];
> not IsWeierstrassPlace(Place(P0));
> M := Matrix(Rationals(), [[-2,0],[0,-2]]);
> bl, D := DivisorFromMatrixAmbientSplit(X, P0, X, P0, M);
> _<y1,y2,x1,x2> := Ambient(D);
> D;
```

```
[...]
> InitializedIterator(X,X,M, 4);
[...]
```

Plug in your branches into this (g*d awful) divisor to confirm that it vanishes. Compare this with `CantorFromMatrixAmbientSplit`.

(d) Perform multiplication by -2 directly on the Jacobian with a universal point and compare with (c), as follows:

```
> KX<xX,yX> := FunctionField(X);
> XKX := ChangeRing(X,KX);
> PX := XKX![xX,yX];
> P0 := XKX![0,1];
> AKX := Jacobian(XKX);
> -2*AKX![PX,XKX!P0];
[...]
```

Problem 3.2. In this exercise, we verify that the curve

$$X\colon y^2 + (x^3 + x + 1)y = -x^5$$

529.a.529.1 (a model for the modular curve $X_0(23)$) with $A := \mathrm{Jac}(X)$ has

$$\mathrm{End}(A)_{\mathbb{Q}} = \mathrm{End}(A^{\mathrm{al}})_{\mathbb{Q}} = \mathbb{Q}(\sqrt{5}).$$

(a) Using Frobenius polynomials as in Lecture 1, show that $\mathrm{End}(A)_{\mathbb{Q}}$ is a field contained in $\mathbb{Q}(\sqrt{5})$.

```
> QQ := RationalsExtra(100);
> _<x> := PolynomialRing(QQ);
> _<T> := PolynomialRing(Integers());
> X := HyperellipticCurve([-x^5,x^3+x+1]);
> X;
Hyperelliptic Curve defined by y^2 + (x^3 + x + 1)*y = -x^5
over Rational Field
> EulerFactor(X,2);
4*T^4 + 2*T^3 + 3*T^2 + T + 1
[...]
```

(b) As in Lecture 2, compute that the numerical endomorphism algebra is indeed $\mathbb{Q}(\sqrt{5})$, endomorphisms all defined over $\mathbb{Q}$, with numerical endomorphism α with representation

$$M = \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix}$$

interpreting `HeuristicEndomorphismLattice`

(c) Verify this endomorphism following https://github.com/edgarcosta/endomorphisms/blob/master/examples/puiseux/Talk1.m.

(d) Confirm this by a Hecke field computation as follows:

```
> S := CuspForms(23);
> BaseField(Newforms(S)[1][1]);
Number Field with defining polynomial $.1^2 + $.1 - 1 over the
```

Rational Field

Problem 3.3. Throughout this exercise, we use the following notation. Let $X \colon y^2 = f(x)$ be a nice hyperelliptic curve over a number field F with $\deg f(x)$ odd, and let $A := \mathrm{Jac}(X)$ be its Jacobian. Let $\mathrm{Gal}(f)$ be the Galois group of a splitting field of f realized as a permutation group on the set $\mathcal{R}$ of roots of f.

Recall (from Exercise 2.1 of Adam Morgan's course) that as Gal_F-modules we have an isomorphism $A(F^{\mathrm{al}})[2] \simeq \mathbb{F}_2[\mathcal{R}]_{\Sigma=0}$ where $\mathbb{F}_2[S]$ is the permutation module on S over $\mathbb{F}_2$ and Σ is the formal sum-of-coordinates map.

Suppose $\mathrm{Gal}(f)$ acts transitively on $\mathcal{R}$ (equivalently, $f(x)$ is irreducible).

(a) Let $S \leq \mathrm{Gal}(f)$ be the stabilizer subgroup fixing a chosen root, well-defined up to conjugacy in $\mathrm{Gal}(f)$. Consider the ring

$$\mathrm{End}_{\mathbb{F}_2[\mathrm{Gal}(f)]}(\mathbb{F}_2[\mathcal{R}])$$

of $\mathbb{F}_2$-linear maps $\phi\colon \mathbb{F}_2[\mathcal{R}] \to \mathbb{F}_2[\mathcal{R}]$ that commute with the action of $\mathrm{Gal}(f)$. Show that $\dim_{\mathbb{F}_2} \mathrm{End}_{\mathbb{F}_2[\mathrm{Gal}(f)]}(\mathbb{F}_2[\mathcal{R}])$ is equal to the number of orbits of S acting on $\mathcal{R}$. Conclude that $\mathrm{Gal}(f)$ acts 2-transitively on $\mathcal{R}$ if and only if $\dim_{\mathbb{F}_2} \mathrm{End}_{\mathbb{F}_2[\mathrm{Gal}(f)]}(\mathbb{F}_2[\mathcal{R}]) = 2$. *[Hint: any such ϕ is determined by where it sends the chosen root.]*

(b) Observe that the restriction of $\mathrm{End}(A)$ acting on $A(F^{\mathrm{al}})[2]$ is isomorphic as a ring to $\mathrm{End}(A) \otimes \mathbb{F}_2 \cong \mathrm{End}(A)/2\,\mathrm{End}(A)$.

(c) Show that if $\mathrm{Gal}(f)$ acts 2-transitively on $\mathcal{R}$ then $\mathrm{End}(A) \simeq \mathbb{Z}$.

Let $K \supseteq F$ be the minimal (finite Galois) extension such that $\mathrm{End}(A_K) = \mathrm{End}(A^{\mathrm{al}})$. The group $\mathrm{Gal}(K \mid F)$ acts faithfully on $B := \mathrm{End}(A^{\mathrm{al}})_{\mathbb{Q}}$ by $\mathbb{Q}$-linear automorphisms, so $\mathrm{Gal}(K \mid F) \hookrightarrow \mathrm{Aut}_{\mathbb{Q}}(B)$ as groups.

(d) Suppose $\deg f(x) = p \geq 3$ is prime and $\mathrm{Gal}(f) \cong C_p \rtimes C_{p-1}$ is the affine linear group of order $p(p-1)$. Suppose also that B is a quadratic field (over $\mathbb{Q}$). Prove that $K = F(\sqrt{d})$, where $d = \mathrm{disc}(f)$ is the discriminant of f. *[Hint: consider the action of $\mathrm{Gal}_{\mathbb{Q}(\sqrt{d})}$ on $\mathcal{R}$.]*

(e) For each of the following polynomials, compute $\mathrm{End}(A^{\mathrm{al}})_{\mathbb{Q}}$ and its field of definition using (d), and then confirm this using a numerical or rigorous computation:
   (i) $f(x) = x^5 - 14x^3 - 84x^2 + 81x - 28$
   (ii) $f(x) = x^5 - 5x^3 + 5x - 4$
   (iii) $f(x) = x^5 - 4x^3 - 46x^2 - 44x - 194$

4. Lecture 4: classification

Problem 4.1. List all possibilities for the $\mathbb{R}$-algebra $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{R}$ if A is an abelian surface over a number field. Find an example of as many of these possibilities as you can find in the LMFDB.

Problem 4.2. Do Exercise 3.7 in the book at `http://quatalg.org`.

Problem 4.3. Do Exercise 8.11.