ABELIAN VARIETIES OVER FINITE FIELDS: PROBLEM SET 0

Instructions: The goal of this problem set is to get familiar with the theory of finite fields. Problems marked ($\star$), ($\star\star$), and ($\star\star\star$) denote beginner, intermediate, and advanced problems, respectively. For the computational problems (⌨) you may use CoCalc or MAGMA's online calculators.

Not all finite rings are finite fields.

Problem 1 ($\star$)

(1) Consider the ring $\mathbb{Z}/12\mathbb{Z}$ of integers modulo 12 (the hours in the clock). Describe the group of units[a] $(\mathbb{Z}/12\mathbb{Z})^\times$. What do you notice about the non-invertible elements?
(2) Define the Euler totient function $\varphi\colon \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ by
$$\varphi(n) := \#\{1 \le m \le n : \gcd(m,n) = 1\}.$$
Show that $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.
(3) Show that φ is multiplicative, i.e., that $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $\gcd(m,n) = 1$.
(4) Show that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number. In this case, we denote the field $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$.

[a] The group of units $R^\times$ of a ring R is the set of $x \in R$ such that there exists some $y \in R$ satisfying $xy = 1$.

In the next problem we are going to establish some standard facts about finite fields.

Problem 2 ($\star$)

(1) Let F be a finite field; that is, a ring with finitely many elements such that $F^\times = F - \{0\}$. Show that the subring of F generated by the multiplicative identity is isomorphic to $\mathbb{F}_p$, for some prime p. This prime is the characteristic of F.
(2) Suppose F has characteristic p. Show that $\#F = p^n$ for some positive integer n.[a]
(3) Consider $F^\times = F - \{0\}$, the group of units in F. Suppose $\#F = p^n$, show that the elements in $F^\times$ are exactly the roots of the polynomial $x^{p^n-1} - 1$ in F. Conclude that the elements in $F^\times$ sum up to zero.
(4) By the fundamental theorem of finitely generated abelian groups, we can write $F^\times \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$, where $d_1 \mid d_2 \mid \cdots \mid d_r$. Therefore, every element in $F^\times$ also satisfies the polynomial $x^{d_r} - 1$. Conclude from this that $r = 1$ and $F^\times$ is cyclic.
(5) Let α be a generator of the multiplicative group $F^\times$. Let $\mathbb{F}_p[\alpha]$ denote the subring in F generated by $\mathbb{F}_p$ and α. Show that $F = \mathbb{F}_p[\alpha]$. Use this to show that any two finite fields with the same cardinality are isomorphic.[b]
(6) Now we investigate the Galois group of the field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$. Show that the map $\mathrm{Frob}_p : \beta \mapsto \beta^p$ is a ring isomorphism from $\mathbb{F}_{p^n}$ to itself, fixing $\mathbb{F}_p$. The automorphism Frob_p is called the p-Frobenius automorphism. What is the order of Frob_p?
(7) Now, let $f(x)$ be the minimal polynomial of α over $\mathbb{F}_p$. Show that $\mathbb{F}_p[\alpha] \cong \mathbb{F}_p[x]/(f)$. Conclude that f must have degree n. What does this tell us about the size of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$?
(8) Show that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a cyclic group generated by the p-Frobenius automorphism.

[a] Hint: there are several ways to solve this. One way is to use the fundamental theorem of finitely generated abelian groups. Alternatively, you can use that F is a vector space over $\mathbb{F}_p$.
[b] Remark: Up to isomorphism, there is a unique finite field of size p^n. We use $\mathbb{F}_{p^n}$ to denote the finite field of size p^n.

As we just learned, we can understand finite fields concretely by looking at the minimal polynomials defining the field extensions over their prime fields. For instance, the following problem gives two different ways of thinking about $\mathbb{F}_8$.

Problem 3 ($\star$)
Show that the polynomials $f(x) = x^3 + x^2 + 1$ and $g(y) = y^3 + y + 1$ are irreducible over the field $\mathbb{F}_2$. Describe explicitly an isomorphism between the fields $F := \mathbb{F}_2[x]/(f)$ and $G := \mathbb{F}_2[y]/(g)$. These two polynomials give an explicit description of $\mathbb{F}_8$.

The next problem characterizes inclusion relations between finite fields.

Problem 4 ($\star$)
Let m, n be positive integers. Show that $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m \mid n$. If this is the case, evaluate the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$.

The observation in the next problem is the starting point of Artin-Schreier theory.

Problem 5 ($\star\star$)
Let F be a field of characteristic p. Show that $f(x) = x^p - x - a \in F[x]$ is irreducible unless $a = b^p - b$, for some $b \in F$. Show also that if it is irreducible, then $F[x]/(f)$ is a Galois extension of F and the Galois group is cyclic of order p. Conversely, any Galois extension of F of order p is the splitting field of such a polynomial $f(x)$.

When working over finite fields, one encounters many interesting counting problems, such as the following three.

Problem 6 ($\star\star$)
Let q be a prime power, and let d be a positive integer. Show that the average number of roots in $\mathbb{F}_q$ of a degree-d monic polynomial over $\mathbb{F}_q$ is 1. That is:

$$\frac{1}{\#(\text{degree } d \text{ monic polynomials in } \mathbb{F}_q[x])} \cdot \sum_{\substack{f \in \mathbb{F}_q[x] \\ \text{degree } d, \text{ monic}}} \#(\text{roots of } f \text{ in } \mathbb{F}_q) = 1.$$

For the next problem, you might want to check out `SageMath`'s reference manual to get familiar with the commands related to finite fields and/or matrices.

Problem 7 ($\star\star$)
(1) Let q be a prime power, and let $\mathrm{GL}_n(\mathbb{F}_q)$ denote the group of $n \times n$ invertible matrices with entries in $\mathbb{F}_q$. Show that

$$\#\mathrm{GL}_n(\mathbb{F}_q) = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

(2) ⌨ Use your favorite computer algebra system to write a computer program that verifies this formula.

Problem 8 ($\star\star$)
Let q be a prime power. Show that an irreducible polynomial $f \in \mathbb{F}_q[x]$ is a factor of $x^{q^n} - x$ if and only if $\deg f \mid n$. Show that $x^{q^n} - x$ factors as the product of all monic irreducible polynomials of degrees dividing n. Let $N(q, r)$ be the number of monic irreducible polynomials of degree r, where $r \mid n$. Derive the formula

$$N(q, n) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$$

where μ is the Möbius function.[a]

[a] Hint: Google the Möbius inversion formula.

The following problem uses some basic concepts from complex analysis. It might be helpful to keep in mind the Riemann zeta function, and the algebraic similarities between the rings $\mathbb{Z}$ and $\mathbb{F}_q[x]$ (see [Ros02]).

Problem 9 ($\star\star$)
Let q be a prime power. The zeta function of the polynomial ring $\mathbb{F}_q[x]$[a], denoted by $\zeta_{\mathbb{F}_q[x]}(s)$, is defined by the infinite series

$$\zeta_{\mathbb{F}_q[x]}(s) := \sum_{\substack{f \in \mathbb{F}_q[x] \\ f \text{ monic}}} \frac{1}{|f|^s},$$

where $|f| := \#\, \mathbb{F}_q[x]/(f)$.

(1) Show that $\zeta_{\mathbb{F}_q[x]}(s)$ converges absolutely to a holomorphic function in the half-plane $\mathrm{Re}(s) > 1$.
(2) Show that $\zeta_{\mathbb{F}_q[x]}(s)$ has an expression as an infinite product indexed by irreducible monic polynomials in $\mathbb{F}_q[x]$.
(3) Show that $\zeta_{\mathbb{F}_q[x]}(s)$ has an analytic continuation to $\mathbb{C} - \{1\}$ with a simple pole at $s = 1$. Calculate the residue at this pole.
(4) Define $\xi_{\mathbb{F}_q[x]}(s) := q^{-s}(1 - q^{-s})^{-1}\zeta_{\mathbb{F}_q[x]}(s)$ and note that $\xi_{\mathbb{F}_q[x]}(s) = \xi_{\mathbb{F}_q[x]}(1 - s)$.

[a] Remark: This is also the zeta function of the affine line $\mathbb{A}^1_{\mathbb{F}_q} := \mathrm{Spec}\, \mathbb{F}_q[x]$.

There are interesting relations between quadratic residues of different finite fields, as suggested by the following problem.

Problem 10 ($\star\star$)
Let p be an odd prime number.

(1) Given $a \in \mathbb{F}_p^\times$, write $(a/p) = 1$ if a is a square in $\mathbb{F}_p$ and write $(a/p) = -1$ if not. Show that $(\,\cdot\,/p) : \mathbb{F}_p^\times \to \{\pm 1\}$ is a surjective homomorphism.
(2) Let $\varphi : \mathbb{F}_p^\times \to \{\pm 1\}$ be a surjective homomorphism. Show that $\varphi = (\,\cdot\,/p)$.
(3) Show that $(a/p) = a^{(p-1)/2}$ for every $a \in \mathbb{F}_p^\times$.
(4) Show that $(-1/p) = 1$ if and only if $p \equiv 1 \bmod 4$.
(5) Show that $(2/p) = 1$ if and only if $p \equiv \pm 1 \bmod 8$.
(6) ($\star\star\star$) Let ℓ be an odd prime distinct from p. Prove the quadratic reciprocity law:

$$(p/\ell)(\ell/p) = (-1)^{(p-1)(\ell-1)/4}.$$

In the following three problems, we build the algebraic closure of a finite field, and introduce its absolute galois group.

Problem 11 ($\star\star\star$)
Recall that there exists an injective homomorphism $\mathbb{F}_{p^m} \to \mathbb{F}_{p^n}$ whenever $m \mid n$. Consider the set of finite fields $\{\mathbb{F}_{p^n}\}_{n \geq 1}$ together with the set of injective homomorphisms $\{\phi_{m,n} : \mathbb{F}_{p^m} \to \mathbb{F}_{p^n}\}$. Show that $\langle \{\mathbb{F}_{p^n}\}, \{\phi_{m,n}\} \rangle$ forms a direct system and its direct limit is the algebraic closure[a] of $\mathbb{F}_p$:

$$\varinjlim \mathbb{F}_{p^n} = \overline{\mathbb{F}}_p.$$

[a] Since each $\mathbb{F}_{p^n}$ is separable over $\mathbb{F}_p$, $\overline{\mathbb{F}}_p$ is also the separable closure of $\mathbb{F}_p$.

Problem 12 ($\star\star$)
Let $\overline{\mathbb{F}}_p$ be the algebraic closure of $\mathbb{F}_p$ constructed in the previous problem.

(1) We construct an sequence $(a_n)_{n\geq 1}$ as follows: write $n = n'p^{v_p(n)}$, where n' and p are coprime. Let x_n, y_n be such that $1 = n'x_n + p^{v_p(n)}y_n$. Let $a_n = n'x_n$.
   (a) Show that for $m \mid n$, we have $a_m \equiv a_n \bmod m$.
   (b) Show that there does not exist $a \in \mathbb{Z}$ such that $a \equiv a_n \bmod n$.

(2) Let $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ be the Galois group, and let $\mathrm{Frob}_p\colon \beta \mapsto \beta^p$ denote the p-Frobenius automorphism of $\overline{\mathbb{F}}_p$. Consider the element $\psi \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ defined by $\psi(\beta) := \mathrm{Frob}_p^{a_i}(\beta) = \beta^{p^{a_i}}$ if $\beta \in \mathbb{F}_{p^i}$. Show that ψ is not in the cyclic group $\langle \mathrm{Frob}_p \rangle$.

Problem 13 ($\star\star\star$)
Show that the absolute Galois group of a finite field is isomorphic (as a topological group) to the profinite completion of the integers: $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$. Conclude that $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is the closure of the cyclic group $\langle \mathrm{Frob}_q \rangle$, where $\mathrm{Frob}_q\colon \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q, \beta \mapsto \beta^q$ is the q-Frobenius automorphism.[a]

[a] A good reference to learn about infinite Galois theory is [Mil12, Chapter 7].

The following problem is a theorem attributed to Chevalley and Warning (see [Ser73]).

Problem 14 ($\star\star\star$)
Let q be a power of a prime number p. Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a polynomial in n variables with $\deg f < n$. Let V be the set of zeros of f in $\mathbb{F}_q^n$. Show that $|V| \equiv 0 \bmod p$. In particular, every quadratic form in at least 3 variables over $\mathbb{F}_q$ has a nontrivial zero.

The next problem requires some algebraic geometry.

Problem 15 ($\star\star\star$)
Let G be a finite p-group, and let k be an algebraically closed field of characteristic $\ell \neq p$. Suppose that G acts algebraically on n-dimensional affine space $\mathbb{A}_k^n$. In this problem, we will show that the action of G has a fixed point.[a]

(1) Do the case of $k = \overline{\mathbb{F}}_\ell$.
(2) General case: Since G is finite, we can find a subring $\Lambda \subset k$, finitely generated over $\mathbb{Z}$, over which the action of G is defined. Proceed by contradiction to reduce to the case of $k = \overline{\mathbb{F}}_\ell$.

[a] See Theorem 1.2 in Serre's: How to use finite fields for problems concerning infinite fields for the solution, and other interesting applications of finite fields!

References

[Mil12] James S. Milne, *Fields and Galois theory (v4.30)*, 2012, Available at www.jmilne.org/math/, p. 124.

[Ros02] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR 1876657

[Ser73] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. No. 7, Springer-Verlag, New York-Heidelberg, 1973, Translated from the French. MR 344216

[Ser09] Jean-Pierre Serre, *How to use finite fields for problems concerning infinite fields*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 487, Amer. Math. Soc., Providence, RI, 2009, pp. 183–193. MR 2555994