Introduction to Characters

Travis Scholl

April 23, 2015

Abstract

*These notes were taken from a course by Ralph Greenburg in Spring 2015 [Gre15] on counting points on varieties over finite fields. It also overlaps with [Ser12, Ch. VI] and [Was97]. Any mistakes should be due to me.

1 Characters

This section will define the basic objects required for studying characters. Much of this theory can be generalized but for simplicity we will stick to the "hands on" approach.

Definition 1.1. Let A be a finite abelian group. The *dual* of A to be the group $\widehat{A} = \mathrm{Hom}(A, \mathbb{C}^*)$, that is the group of homomorphisms $A \to \mathbb{C}^*$. This is also called the *Pontryagin dual.* Elements $\chi \in \widehat{A}$ are examples of *characters.* In this group the trivial character χ_0 is the map sending A to 1.

Exercise 1.2. Prove that

(a) Let $\chi \in \widehat{A}$. Show the image $\chi(A)$ is contained in the set of roots of unity:

$$\chi(A) \subseteq \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}.$$

(b) For any fixed A, there exists an isomorphism $\widehat{A} \cong A$.

(c) There is a canonical isomorphism $\widehat{\widehat{A}} \cong A$, i.e. the "double dual" functor is naturally isomorphic to the identity functor on the category of finite abelian groups.

Hint. Use the structure theorem for finite abelian groups. If A is a product of cyclic groups $\mathbb{Z}/n\mathbb{Z}$, then maps out of A are uniquely determined by where a generator in each component go. Notice that there is a unique cyclic subgroup of order n in $\mathbb{C}^*$.

Definition 1.3. Let $\mathcal{F}_A$ denote the vector space of $\mathbb{C}$-valued functions on A. Note that $\widehat{A} \subset \mathcal{F}_A$. We give an inner product to $\mathcal{F}_A$ by defining

$$\langle f, g \rangle = \frac{1}{|A|} \sum_{a \in A} f(a)\overline{g(a)}$$

Remark 1.4. The inner product defined in Definition 1.3 can also be interpreted as an integral. We could instead write $\int_A f_1 \overline{f_2} d\mu_A$ where μ_A is a normalized Haar measure on A. In this case this just means any singleton $\{a\}$ has measure $\frac{1}{|A|}$ so that the measure of A is normalized to 1.

Exercise 1.5. Show $\dim_{\mathbb{C}} \mathcal{F}_A = |A|$.

Hint. Note that $\mathcal{F}_A$ is arbitrary set-theoretic functions. So they are uniquely defined only by their value on each point in A.

Theorem 1.6 (*Fourier Series*)**.** *The elements $\chi \in \widehat{A}$ form an orthogonal basis for $\mathcal{F}_A$.*

If $f \in \mathcal{F}_A$ then $f = \sum_{\chi \in \widehat{A}} c_\chi \chi$.

Remark 1.7. This should remind of you Fourier series you might have seen in analysis. Just note that the map $\mathbb{R} \to \mathbb{C}^*$ given by $x \mapsto e^{2\pi i n x}$ for some fixed $n \in \mathbb{Z}$ is a character. Use this to compare with the standard Fourier series.

Before proving Theorem 1.6, we first prove a very helpful lemma.

Lemma 1.8. *If $\chi \in \widehat{A}$ then*

$$\frac{1}{|A|} \sum_{a \in A} \chi(a) = \begin{cases} 1 & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

Proof. Let d be the order of χ so that $\chi^d = \chi_0$. Then $\chi(A)$ is exactly the d^{th} roots of unity (each with multiplicity $|A|/d$). The sum of the dth roots of unity is 0 unless $d = 1$, in which case $\chi = \chi_0$ and we have $\sum_{a \in A} \chi(a) = |A|$. ◻

Proof of Theorem 1.6. By Exercise 1.5 it is sufficient to show that the χ are orthogonal since then they will form an independent set of the same size as the dimension.

Let $\chi_1, \chi_2 \in \widehat{A}$. By Exercise 1.2 we know the image of any $\chi \in \widehat{A}$ is contained in the roots of unity. Hence $\overline{\chi(a)} = \chi(a)^{-1}$ for any $a \in A$. Using this and the previous lemma we can write

$$\begin{aligned} \langle \chi_1, \chi_2 \rangle &= \frac{1}{|A|} \sum_{a \in A} \chi_1(a) \overline{\chi_2(a)} \\ &= \frac{1}{|A|} \sum_{a \in A} \chi_1(a) \left(\chi_2(a)\right)^{-1} \\ &= \frac{1}{|A|} \sum_{a \in A} \left(\chi_1 \chi_2^{-1}\right)(a) \\ &= \begin{cases} 1 & \text{if } \chi_1 = \chi_2 \\ 0 & \text{if } \chi_1 \neq \chi_2. \end{cases} \end{aligned}$$

◻

Theorem 1.6 gives an expansion of any element $f \in \mathcal{F}_A$ into a linear combination $\sum_{\chi \in \widehat{A}} c_\chi \chi$. But the coefficients c_χ in the theorem can be calculated via the inner product. Fix $\psi \in \widehat{A}$ and consider the inner product with ψ as follows

$$\begin{aligned} \langle f, \psi \rangle &= \left\langle \sum_{\chi \in \widehat{A}} c_\chi \chi, \psi \right\rangle \\ &= c_\chi \sum_{\chi \in \widehat{A}} \langle \chi, \psi \rangle \\ &= c_\psi \end{aligned}$$

which shows

$$c_\psi = \frac{1}{|A|} \sum_{a \in A} f(a) \psi^{-1}(a). \tag{1}$$

2 Gauss Sums

In the previous section we considered characters as group homomorphisms into $\mathbb{C}^*$. In this section we expand our objects from finite abelian groups A to finite fields $\mathbb{F}_q$ where q is some prime power. The extra structure allows us to talk about *additive characters* (homomorphisms on $\mathbb{F}_q$ with the additive structure) and *multiplicative characters* (homomorphisms on $\mathbb{F}_q^*$).

There is a natural action of $\mathbb{F}_q$ on $\widehat{\mathbb{F}_q}$. Given $b \in \mathbb{F}_q$ let $m_b : \mathbb{F}_q \to \mathbb{F}_q$ be the multiplication by b map. This is a group homomorphism with respect to the additive structure. Then for $\psi \in \widehat{\mathbb{F}_q}$ define $b \cdot \psi = \psi_b = \psi \circ m_b$. It's clear this is again a character.

Proposition 2.1. *Let ψ be a non-trival character in $\widehat{\mathbb{F}_q}$. For any $b_1, b_2 \in \mathbb{F}_q$, if $b_1 \neq b_2$ then $\psi_{b_1} \neq \psi_{b_2}$.*

Proof.

$$\begin{aligned} \psi_{b_1} = \psi_{b_2} \quad &\Leftrightarrow \quad \psi(b_1 a) = \psi(b_2 a) \quad \forall a \in \mathbb{F}_q \\ &\Leftrightarrow \quad \psi((b_1 - b_2)a) = 1 \quad \forall a \in \mathbb{F}_q \end{aligned}$$

Now $(b_1 - b_2)a$ varies over all of $\mathbb{F}_q$ since $b_1 \neq b_2$. Since ψ is non-trivial it follows that $\psi_{b_1} \neq \psi_{b_2}$. $\square$

Corollary 2.2. *For any non-trivial $\psi \in \widehat{\mathbb{F}_q}$ we have $\widehat{\mathbb{F}_q} = \{\psi_b \mid b \in \mathbb{F}_q\}$.*

Exercise 2.3. Prove Corollary 2.2.

Next we want to consider multiplicative characters, i.e. $\widehat{\mathbb{F}_q^*}$, and relate them to additive ones. Given $\chi \in \widehat{\mathbb{F}_q^*}$ we extend it to a map $\widetilde{\chi} : \mathbb{F}_q \to \mathbb{C}$ as follows. If $\chi \neq \chi_0$ then

$$\widetilde{\chi}(a) = \begin{cases} \chi(a) & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases}$$

and if $\chi = \chi_0$ then we extend it by

$$\widetilde{\chi_0}(a) = 1 \quad \forall a \in \mathbb{F}_q.$$

Warning 2.4. Note that $\widetilde{\chi_0}$ is extended differently! This will make things easier later. Also it's nice that it is still a constant function. Also be careful because $\widetilde{\chi}$ may not necessarily lie in $\widehat{\mathbb{F}_q}$ because it is not additive. However, $\widetilde{\chi}$ is still multiplicative so $\widetilde{\chi}(ab) = \widetilde{\chi}(a)\widetilde{\chi}(b)$ for all $a, b \in \mathbb{F}_q$.

Note that the extension $\widetilde{\chi}$ is a $\mathbb{C}$-valued function on $\mathbb{F}_q$ so that $\widetilde{\chi} \in \mathcal{F}_{\mathbb{F}_q}$. So we can apply Theorem 1.6 which says $\widetilde{\chi}$ can be written as a linear combination of the $\psi \in \widehat{\mathbb{F}_q}$. So by Corollary 2.2 we have

$$\widetilde{\chi} = \sum_{b \in \mathbb{F}_q} c_b \psi_b$$

for some fixed non-trivial $\psi \in \widehat{\mathbb{F}_q}$.

Exercise 2.5. Let $\chi \in \widehat{\mathbb{F}_q^*}$ and fix some non-trivial $\psi \in \widehat{\mathbb{F}_q}$. By above we can write $\widetilde{\chi} = \sum_{b \in \mathbb{F}_q} c_b \psi_b$.

(a) In the notation above, show

$$c_0 = \begin{cases} 0 & \text{if } \chi \neq \chi_0 \\ 1 & \text{if } \chi = \chi_0 \end{cases}$$

Hint. See Warning 2.4 and compute $\langle \widetilde{\chi}, \psi_0 \rangle$. The proof of Lemma 1.8 may be helpful.

(b) Show $\langle \widetilde{\chi}, \widetilde{\chi} \rangle = \sum |c_b|^2$.

Hint. Notice $\langle \cdot, \cdot \rangle$ is a Hermitian inner product on $\mathcal{F}_{\mathbb{F}_q}$.

Definition 2.6. A *Gauss sum* is the sum of a multiplicative character times an additive one. Specifically, given $\chi \in \widehat{\mathbb{F}_q^*}$ and $\psi \in \widehat{\mathbb{F}_q}$, then define the Gauss sum to be

$$\gamma(\chi, \psi) = \sum_{a \in \mathbb{F}_q} \widetilde{\chi}(a)\overline{\psi(a)}.$$

There are many cool things one can do with Gauss sums. Here is a small application where we compute the absolute value.

Theorem 2.7. *Let $\chi \in \widehat{\mathbb{F}_q^*}$ and $\psi \in \widehat{\mathbb{F}_q}$. If ψ and χ are non-trivial then $|\gamma(\chi, \psi)| = \sqrt{q}$.*

Proof. From Theorem 1.6 and Corollary 2.2 we can write $\widehat{\chi} = \sum_{b \in \mathbb{F}_q} c_b \psi_b$ for some coefficients $c_a \in \mathbb{C}$.

First we will show $|c_{b_1}| = |c_{b_2}|$ for any non-zero $b_1, b_2 \in \mathbb{F}_q$. Recall that $\widetilde{\chi}$ is multiplicative, so for any $b \neq 0$ in $\mathbb{F}_q$ we can write

$$\begin{aligned}
c_b &= \langle \widetilde{\chi}, \psi_b \rangle \\
&= \sum_{a \in \mathbb{F}_q} \widetilde{\chi}(a)\overline{\psi_b(a)} \\
&= \sum_{a \in \mathbb{F}_q} \widetilde{\chi}(ab)\widetilde{\chi}(b^{-1})\overline{\psi_1(ba)} \\
&= \sum_{a \in \mathbb{F}_q} \widetilde{\chi}(ab)\widetilde{\chi}(b^{-1})\overline{\psi_1(ba)} \\
&= \widetilde{\chi}(b^{-1}) \sum_{a \in \mathbb{F}_q} \widetilde{\chi}(ab)\overline{\psi_1(ba)} \\
&= \widetilde{\chi}(b^{-1}) \langle \widetilde{\chi}, \psi_1 \rangle \\
&= \widetilde{\chi}(b^{-1}) c_1
\end{aligned}$$

Since $\widetilde{\chi}(b^{-1})$ is a root of unity it follows $|c_b| = |c_1|$.

Now we can show $|c_b| = \frac{1}{\sqrt{q}}$. Using Exercise 2.5 we have

$$\langle \widetilde{\chi}, \widetilde{\chi} \rangle = \sum_{b \in \mathbb{F}_q} |c_b|^2 = (q-1)|c_1|^2$$

and as χ is a character for $\mathbb{F}_q^*$ we have

$$\begin{aligned}
1 = \langle \chi, \chi \rangle &= \frac{1}{|\mathbb{F}_q^*|} \sum_{a \in \mathbb{F}_q^*} \chi(a)\overline{\chi(a)} \\
&= \frac{1}{q-1} \sum_{a \in \mathbb{F}_q} \widetilde{\chi}(a)\overline{\widetilde{\chi}(a)} \\
&= \frac{q}{q-1} \langle \widetilde{\chi}, \widetilde{\chi} \rangle
\end{aligned}$$

Note: the two inner products above are for different character groups!

Together these inequalities show

$$|c_1| = \frac{1}{\sqrt{q}}$$

Now unwinding definitions we have

$$\begin{aligned}
\gamma(\chi, \psi) &= \sum_{a \in \mathbb{F}_q} \left(\sum_{b \in \mathbb{F}_q} c_b \psi_b(a) \right) \overline{\psi(a)} \\
&= \sum_{b \in \mathbb{F}_q} c_b \sum_{a \in \mathbb{F}_q} \psi_b(a) \overline{\psi(a)} \\
&= \sum_{b \in \mathbb{F}_q} c_b |\mathbb{F}_q| \langle \psi_b, \psi \rangle \\
&= c_1 q
\end{aligned}$$

which with above finishes the proof. □

Exercise 2.8. Find the absolute value of the Gauss sum $\gamma(\chi, \psi)$ in the following cases:

- $\chi = \chi_0$, $\psi \neq \psi_0$
- $\chi \neq \chi_0$, $\psi = \psi_0$
- $\chi = \chi_0$, $\psi = \psi_0$

Hint.

- 0
- 0
- q

3 A Theorem of Gauss

Another example of Gaussian sums comes from a theorem of Gauss.

Definition 3.1. Let p be an odd prime. Define a map $\mathbb{Z} \to \{-1, 0, 1\}$ by

$$a \mapsto \left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \nmid a \text{ and } a \text{ is a square mod } p \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is not a square mod } p \\ 0 & \text{if } p \mid a \end{cases}$$

It's not hard to see this is a non-trivial character on $\mathbb{F}_p^*$ extended to $\mathbb{F}_p$. It is called the *Legendre symbol.*

Now consider the map $\mathbb{F}_p \to \mathbb{C}*$ given by $a \mapsto e^{2\pi i a/p}$. It's not hard to see this is a non-trivial additive character of $\mathbb{F}_p$.

Theorem 3.2 (Quadratic Gauss Sum)**.**

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) e^{2\pi i a/p} = \begin{cases} \sqrt{p} & \textit{if } p \equiv 1 \mod 4 \\ \sqrt{-p} & \textit{if } p \equiv 3 \mod 4. \end{cases}$$

Proof. See [Ire13, Ch. 6]. □

4 Inflation and Restriction

Next we look at the relation between characters on groups and their quotient groups.

Let A be a finite abelian group and B a subgroup of A. Given a character $\chi \in \widehat{A/B}$ it extends to a character on $\widehat{A}$ by precomposing with the quotient map $A \to A/B$.

Definition 4.1. Let $\pi : A \to A/B$ be the canonical map and $\psi \in \widehat{A/B}$. Then the *inflation* of ψ is the map $\inf(\psi) = \psi \circ \pi \in \widehat{A}$. Note $\inf : \widehat{A/B} \to \widehat{A}$ is indeed a homomorphism.

Definition 4.2. Let $\chi \in \widehat{A}$. Then the *restriction* of χ is the map $\operatorname{res} B = \chi|_B \in \widehat{B}$. Note $\operatorname{res} : \widehat{A} \to \widehat{B}$ is indeed a homomorphism.

Exercise 4.3. Show $\inf : \widehat{A/B} \to \widehat{A}$ is injective and $\operatorname{res} : \widehat{A} \to \widehat{B}$ is surjective. Then prove we have an exact sequence

$$0 \longrightarrow \widehat{A/B} \xrightarrow{\inf} \widehat{A} \xrightarrow{\operatorname{res}} \widehat{B} \longrightarrow 0.$$

References

[Gre15] Ralph Greenberg. Math 583C: Counting Points on Varieties. Spring 2015.

[Ire13] K. Ireland. *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics. Springer New York, 2013.

[Ser12] J.P. Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics. Springer New York, 2012.

[Was97] L.C. Washington. *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics. Springer New York, 1997.

Travis Scholl
Department of Mathematics, University of Washington, Seattle WA 98195
email: tscholl2@uw.edu