Characters of finite abelian groups

(Apostol, sections 6.4 - 6.7.)

Part 0.

Goal: to study Dirichlet characters, which are nonzero $\mathbb{C}$-valued homomorphisms on the group of units (invertible elements) mod k $(k \in \mathbb{Z}_+)$.

Ultimately, we'll build a "Dirichlet L series" $L(s, \chi)$ from each Dirichlet character χ, for a given k, and will use these series to study primes in the arithmetic progression

$$k+h,\ 2k+h,\ 3k+h,\ \ldots \qquad \text{for } (h,k)=1.$$

Part I. Some basics on $\mathbb{Z}/k\mathbb{Z}$.

Recall: For $k \in \mathbb{Z}^+$ and $k\mathbb{Z}$ the subgroup $\{kj : j \in \mathbb{Z}\}$ of $\mathbb{Z}$, we know that the quotient group $\mathbb{Z}/k\mathbb{Z}$ is a commutative ring with unity. Here, if $\overline{h}$ denotes the element $h + k\mathbb{Z}$ $= \{h + kj : j \in \mathbb{Z}\}$ of $\mathbb{Z}/k\mathbb{Z}$, then by definition we have

$$\overline{h} + \overline{l} = \overline{h+l},$$
$$\overline{h} \cdot \overline{l} = \overline{hl} \qquad (h, l \in \mathbb{Z}).$$

The zero in $\mathbb{Z}/k\mathbb{Z}$ is $\overline{0}$; the unity is $\overline{1}$.

Also, if we define $S_k = \{\overline{n} : 0 \le n < k\}$, then we have $\mathbb{Z}/k\mathbb{Z} = S_k$.

Proof: the elements of S_k are distinct, since $\overline{n_1} = \overline{n_2} \Rightarrow n_1 - n_2$ is a multiple of k, and for

$0 \le n_1, n_2 < k$, this implies that $n_1 = n_2$. Moreover, $n \in \mathbb{Z} \Rightarrow n = kq + r$ for some $q, r \in \mathbb{Z}$ and $0 \le r < k$. So $\overline{n} = \overline{r}$; i.e. $\overline{n}$ belongs to the set S_k. $\square$

So $|\mathbb{Z}/k\mathbb{Z}| = k$.

Let $(\mathbb{Z}/k\mathbb{Z})^*$ denote the group of units (invertible elements under multiplication) in $\mathbb{Z}/k\mathbb{Z}$. Note that

$$(\mathbb{Z}/k\mathbb{Z})^* = \{\overline{h} \in \mathbb{Z}/k\mathbb{Z} : (h,k) = 1\}.$$

Proof: $\overline{h} = h + k\mathbb{Z} \in (\mathbb{Z}/k\mathbb{Z})^*$
$\iff \exists\, l \in \mathbb{Z} : \overline{h}\,\overline{l} = \overline{1} \iff \exists\, l \in \mathbb{Z} : \overline{hl - 1} = \overline{0} \iff \exists\, l \in \mathbb{Z} : hl - 1 \in k\mathbb{Z} \iff \exists\, l, j \in \mathbb{Z} : hl - 1 = kj \iff (h,k) = 1$. $\square$

So $|(\mathbb{Z}/k\mathbb{Z})^*| = \varphi(k)$.

<u>Part II.</u> Groups generated by subgroups and elements.

Until further notice, G is a finite abelian group, and e is the identity in G.

<u>Definition</u>: If G' is a proper subgroup of G and $a \in G \setminus G'$, then the <u>indicator</u> h of a in G' is defined by

$$h = \min\{m \in \mathbb{Z}_+ : a^m \in G'\}.$$

Note that h exists since, if a has order n in G, then $a^n = e \in G'$.

Theorem 6.6.

Let G' be a proper subgroup of G; let $a \in G \setminus G'$ have indicator h in G'. Then the set

$$G'' = \{ xa^l : x \in G' \text{ and } 0 \le l < h \}$$

is a subgroup of G, of order $|G'| \cdot h$.

Proof

(a) Closure: if xa^l and $ya^m \in G$ then, since G is abelian,

$$(xa^l)(ya^m) = xya^{l+m}.$$

Write $l+m = hq+r$ with $q, r \in \mathbb{Z}$ and $0 \le q < h$. Then

$a^{l+m} = a^{hq+r} = (a^h)^q a^r = za^r$ for some $z \in G'$, since $a^h \in G'$. So

$(xa^m)(ya^l) = xyza^r$ is in G'', since $xyz \in G'$ (as G' is a group) and $0 \le r < h$.

(b) Closure under inverses: Let $x \in G'$ and $0 \le l < h$: we construct an inverse in G'' of xa^l, as follows.

If $l = 0$, then x^{-1} is the inverse of xa^l, and $x^{-1} \in G'$, so $x^{-1} \in G''$. So assume $l \ne 0$: so $0 < l < h$, which implies $0 < h-l < h$. Now let $y = x^{-1}a^{-h}$: since $x, a^h \in G'$, we have $y \in G'$. So $ya^{h-l} \in G''$. Moreover

$$(xa^l)(ya^{h-l}) = xa^l \cdot x^{-1}a^{-h}a^{h-l} = xx^{-1}a^{l-h+h-l} = e.$$

So G'' is closed under inverses.

(c) The order of $|G''|$.

Again, G'' is the set of products of the form xa^{l} with $x \in G'$ and $0 \le l < h$. If we can show that all such products are distinct, we'll be done.

Suppose
$$xa^{l} = ya^{m} \qquad \text{for } x, y \in G', \ 0 \le l, m < h.$$

Then
$$xy^{-1} = a^{m-l}, \text{ so } a^{m-l} \in G'. \text{ Since } G' \text{ is a group,}$$
$a^{l-m} \in G'$ as well.

So $a^{|l-m|} \in G'$, so $|l-m| = 0$ or $|l-m| \ge h$, by minimality of h.

$|l-m| \ge h$ is impossible since $0 \le l, m < h$. So $|l-m| = 0$, so $l = m$. But then
$$xa^{m} = ya^{m}, \text{ so } x = y.$$

So the products are distinct. $\square$

Part III. Characters on G.

Definition: a character f on G is a homomorphism $f: G \to \mathbb{C}$ that's not the zero function.

Theorem 6.7.

If f is a character on G, then:

(a) $f(e) = 1$.
(b) $f(a)$ is a root of unity $\forall a \in G$.

Proof.

(a) Choose $c \in G$ with $f(c) \neq 0$. Then $f(c) = f(ce) = f(c)f(e)$, so $f(e) = 1$.

(b) Let n be the order of a in G. Then

$$1 = f(e) = f(a^n) = f(a)^n,$$

so $f(a)$ is an n^{th} root of unity.