Recall:
$(G,+)$ Abelian Group, $D \subseteq G$ difference set.
$\rightsquigarrow (G, \mathcal{B})$ $\mathcal{B} = \{g+D \mid g \in G\}$.
symmetric design

The Multiplier Theorem:
Goal: Construct difference sets / prove that they don't exist

Def'n: Let $(V, \mathcal{B})$ be a design.
An automorphism of $(V, \mathcal{B})$ is a permutation $\sigma: V \to V$ that induces a permutation of $\mathcal{B}$. That is to say, there exists a permutation $\tilde{\sigma}: \mathcal{B} \to \mathcal{B}$ s.t. $\tilde{\sigma}(\alpha) = \{\sigma(x) \mid x \in \alpha\}$.
(We assume $\mathcal{B}$ is just a set of sets, i.e. Don't worry about multisets)

Proposition:
Let $(V, \mathcal{B})$ be a design:
$V = \{x_1, \dots, x_v\}$, $\mathcal{B} = \{\alpha_1, \dots, \alpha_b\}$
Let $\sigma: V \to V$ and $\tilde{\sigma}: \mathcal{B} \to \mathcal{B}$ be permutations. Let N be the incidence matrix of $(V, \mathcal{B})$. Let P be the permutation matrix of σ and $\tilde{P}$ be the permutation matrix of $\tilde{\sigma}$.
Then, σ is the automorphism of $(V, \mathcal{B})$ with induced permutation $\tilde{\sigma}$ iff: $PN = N\tilde{P}^T$
Proof:
Check:
$(PN)_{ij} = \begin{cases} 1 & \text{if } \sigma^{-1}(x_i) \in \alpha_j \\ 0 & \text{o/w} \end{cases}$ and $(N\tilde{P}^T)_{ij} = \begin{cases} 1 & \text{if } x_i \in \tilde{\sigma}(\alpha_j) \\ 0 & \text{o/w} \end{cases}$

We are interested in the case where the design comes from a difference set $D \subseteq G$.

Example: For any $h \in G$, the map $\sigma(g) = h + g$ is an automorphism of (G, B)

Note: If (G, B) is a design coming from difference set $D \subseteq G$, then $\underset{\substack{\downarrow \\ 0+D}}{D} \in B$

Moreover, every block $D' \in B$ is also a difference set and gives rise to the same design.

Defn An integer $m \in \mathbb{Z}$ is a <u>multiplier</u> of (G, B) if $\sigma(g) = mg$ is an automorphism.

$$mg := \begin{cases} \underbrace{g + \cdots + g}_{m \text{ times}} & \text{if } m \geq 0 \\ \underbrace{-g-g-\cdots-g}_{m \text{ times}} & \text{if } m < 0 \end{cases}$$

Proposition:

If (G, B) comes from the difference set $D \subseteq G$, then TFAE:

(1) m is a multiplier for the design

(2) $mD \in B$.

(3) $mD = h + D$ for some $h \in G$

Proof:

(2) ⇒ (3) Easy

(1) ⇒ (2) Also easy

(3) ⇒ (1) Suppose $mD = h+D$. Consider $\sigma: G \to G$, $\sigma(g) = mg$

and $\tilde{\sigma}: B \to B$, $\tilde{\sigma}(\alpha) = m\alpha$ (equiv. $\tilde{\sigma}(g+D) = gm + h + D$)

$= \{\sigma(x) \mid x \in \alpha\}$

We need to show

(A) σ is a permutation

(B) $\tilde{\sigma}$ is —— " ——

(A): σ is a map from $V \to V$, so it suffices to show that σ is surjective. Let $x \in G$. Since D is a difference set, can write $x = g_1 - g_2$, $g_1, g_2 \in D$.

Also,

$x = \underbrace{(h+g_1)} - \underbrace{(h+g_2)}$, where $(h+g_1), (h+g_2) \in h+D = mD$

i.e. multiples of m.

$\therefore$ $h+g_1 \in mD \subseteq \text{Image}(\sigma)$ and likewise with $h+g_2$.

So, x is the difference of elements in image(σ) and this is a subgroup of G, this implies $x \in \text{image}(\sigma)$. So, σ is surjective.

(B): It suffices to show that $\tilde{\sigma}$ is injective. Suppose

$\tilde{\sigma}(g+D) = \tilde{\sigma}(g'+D) \Rightarrow mg + \underbrace{h+D} = mg' + \underbrace{h+D}$

Since symmetric designs are simple, this implies that these 2 blocks must be the same $\therefore$ ~~blocks~~

$\Rightarrow mg + h = mg' + h \Rightarrow mg = mg' \Rightarrow \sigma(g) = \sigma(g')$

Proof:

And since $\bar{\tau}$ is a permutation (by (A)), $s=s'$. This proves $\tilde{\delta}$ is injective.

$\square$

Example: (Fano Plane)

$G = \mathbb{Z}/7$, $D = \{0, 1, 3\}$

Claim: 2 is a multiplier.

This is because:

$$2D = \{0, 2, 6\} = 6 + D$$

is a block of the design.

Claim: 3 is not a multiplier.

This is because:

$$3D = \{0, 3, 2\} \notin \mathcal{B}.$$

Note: We could also use $D' = \{1, 2, 4\}$ to construct the Fano Plane and

$$2D' = \{2, 4, 1\} = D'.$$

← Super easy to see that 2 is a multiplier.

In this case, we say that D' is fixed by the multiplier 2.

Theorem:
Let (G, B) be a design from a difference set: ~~...~~
(i) For every multiplier m, there is a block $D \in B$ s.t. $mD = D$
(ii) If $\gcd(v,k)=1$, then $\exists D \in B$ s.t. $mD = D$ for every multiplier m.

Proof:
(i) Let $\sigma(g) = mg$ and $\tilde{\sigma}(\alpha) = m\alpha$. $\sigma: G \to G$, $\tilde{\sigma}: B \to B$. Assuming m is a multiplier, σ is an automorphism with induced permutation $\tilde{\sigma}$.

In terms of matrices:
$$PN = N\tilde{P}^T$$
Since (G, B) is a symmetric design, N is invertible,
$$\tilde{P}^T = N^{-1}PN$$
So, P, $\tilde{P}^T$ are similar and have the same eigenvalues.
$\therefore$ σ and $\tilde{\sigma}$ have the same cycle type
Now, σ has a fixed point: $\sigma(0)=0$, so $\tilde{\sigma}$ has a fixed point, i.e. $\exists D \in B$ s.t. $\tilde{\sigma}(D) = mD = D$.

(ii) Let $\varphi: B \to G$ be the map $\varphi(\alpha) = \sum_{g \in \alpha} g$
Claim: If $\gcd(v,k)=1$, then φ is a bijection
Proof: (Exercise)
Then, take $D = \varphi^{-1}(0)$ and check that $mD = D$ for every multiplier m. $\square$

Putting this all together:
Upshot is that constructing difference sets with a given multiplier m is easy.

WLOG, we can assume that D is fixed by the multiplier. Then, D must be a union of orbits of the map $g \mapsto mg$.

Example:
Construct a projective plane of order 4 via a difference set with multiplier 2.
Sol'n:
The difference set has params $(21, 5, 1)$
Let $G = \mathbb{Z}_{21}$. The orbits of $x \mapsto 2x$ are:

$\{0\}$, $\{1, 2, 4, 8, 16, 11\}$, $\{3, 6, 12\}$

$\{5, 10, 20, 19, 17, 13\}$,

$\{7, 14\}$, $\{9, 18, 15\}$

The only possibilities are $D = \{3, 6, 12, 7, 14\}$ or $D = \{9, 18, 15, 7, 14\}$ (since $|\{1,2,4,8,16,11\}| = |\{5,10,20,19,17,13\}| = 6 > 5$)
Check: Both choices of D work.
(If they didn't, it shows that there exists no difference set w/ multiplier 2) ~~wait~~

The Multiplier Theorem (Hall–Ryser)

Let D be a (v,k,λ)-difference set in an abelian group G, of order $n=k-\lambda$. If p is a prime such that $p>\lambda$ and $p \mid n$, then p is a multiplier.

~~Example~~:

(S_{10}, $p=2$ was chosen specifically in the previous example) ~~[illegible]~~ ~~theorem~~.

Example:

If $n \equiv 0 \pmod 6$, prove that there is no $(n^2+n+1, n+1, 1)$-difference set.

Sol'n

Suppose D is such a difference set. By the multiplier theorem, 2 and 3 are both multipliers. Since $\gcd(v,k) = \gcd(n^2+n+1, n+1) = 1$, we may assume $D = 2D = 3D$. But now, take any $x \in D$, $x \neq 0$. Since $D = 2D$, $2x \in D$ and since $D = 3D$, $3x \in D$. But now, $x = (3x-2x) = (2x-x)$ contradicts that $\lambda = 1$.