difference set*

CWoo[†]

2013-03-21 22:18:35

Definition. Let A be a finite abelian group of order n. A subset D of A is said to be a *difference set* (in A) if there is a positive integer m such that every non-zero element of A can be expressed as the difference of elements of D in exactly m ways.

If D has d elements, then we have the equation

$$m(n-1)=d(d-1).$$

In the equation, we are counting the number of pairs of distinct elements of D. On the left hand side, we are counting it by noting that there are $m(n-1)$ pairs of elements of D such that their difference is non-zero. On the right hand side, we first count the number of elements in D^2, which is d^2, then subtracted by d, since there are d pairs of $(x,y)\in D^2$ such that $x=y$.

A difference set with parameters n,m,d defined above is also called a (n,d,m)-difference set. A difference set is said to be *non-trivial* if $1<d<n-1$. A difference set is said to be *planar* if $m=1$.

Difference sets versus square designs. Recall that a square design is a τ-(ν,κ,λ)-design where $\tau=2$ and the number ν of points is the same as the number b of blocks. In a general design, b is related to the other numbers by the equation

$$b\binom{\kappa}{\tau}=\lambda\binom{\nu}{\tau}.$$

So in a square design, the equation reduces to $b\kappa(\kappa-1)=\lambda\nu(\nu-1)$, or

$$\lambda(\nu-1)=\kappa(\kappa-1),$$

which is identical to the equation above for the difference set. A square design with parameters λ,ν,κ is called a square (ν,κ,λ)-design.

One can show that a subset D of an abelian group A is an (n,d,m)-difference set iff it is a square (n,d,m)-design where A is the set of points and $\{D+a\mid a\in A\}$ is the set of blocks.

*⟨*DifferenceSet*⟩ created: ⟨*2013-03-21*⟩ by: ⟨*CWoo*⟩ version: ⟨*39077*⟩ Privacy setting: ⟨*1*⟩ ⟨*Definition*⟩ ⟨*05B10*⟩