Abstract Algebra. Math 6310. Bertram/Utah 2022-23.

Abelian Groups (with * meaning "proofs to be supplied by the reader")

At the heart of it all are the integers, either in the form:

$$(\mathbb{Z}, +),$$

as the *infinite cyclic group* with identity 0, generated by either 1 or -1 or else

$$(\mathbb{Z}, +, \cdot),$$

as a *commutative ring* with multiplicative identity $1 \in \mathbb{Z}$.

Definition. An *abelian group* $(A, +)$ is a set A with an addition operation:

$$+ : A \times A \to A \text{ that is}$$

(i) Associative: $(a_1 + a_2) + a_3 = a_1 + (a_2 + a_3)$ for all triples $a_1, a_2, a_3 \in A$.

(ii) Equipped with a unique* additive identity element, labelled $0 \in A$.

(iii) Pairs each $a \in A$ with a unique* inverse $-a$ satisfying* $-(-a) = a$.

(iv) Commutative: $a_1 + a_2 = a_2 + a_1$ for all $a_1, a_2 \in A$.

Examples. $(\mathbb{Z}, +), (n\mathbb{Z}, +)$, the cyclic groups $(\mathbb{Z}/n\mathbb{Z}, + \bmod n), (\mathbb{Z}^n,$ vector addition$)$.

Non-Examples. $(\mathbb{Z} - \{0\}, \cdot)$ (iii), $(n \times n$ invertible matrices$, \cdot)$ (iv).

Definition. A *homomorphism* of abelian groups:

$$f : (A, +) \to (B, +)$$

is a set mapping from A to B such that:

(i) $f(a_1 + a_2) = f(a_1) + f(a_2)$ for all $a_1, a_2 \in A$ and

(ii) $f(0) = 0$, from which it follows* that $f(-a) = -f(a)$ for all $a \in A$.

Examples. (a) The inverse map* $- : A \to A$ is a homomorphism

(b) The map $n : A \to A$ defined* by $n(a) = a + \cdots + a$ (repeated n times).

(c) The composition* of homomorphisms is a homomorphism.

Note. When we are understood to be in the context of a homomorphism of abelian groups, we will denote such a homomorphism as $f : A \to B$.

Definition. (i) A subset $S \subset A$ of an abelian group $(A, +)$ is a *subgroup* $(S, +)$ if:

$$s_1 + s_2 \in S \text{ and } - s_i \in S \text{ for all } s_1, s_2 \in S$$

If $f : A \to B$ is a homomorphism, then

(ii) The *image* $f(A)$ is a subgroup* of B and

(iii) The *kernel* $f^{-1}(0)$ is a subgroup* of A.

Example. $n\mathbb{Z} \subset \mathbb{Z}$ the kernel subgroup of $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ and the image of $n : \mathbb{Z} \to \mathbb{Z}$.

Non-Example. The natural numbers $\mathbb{N} = \{0, 1, ...\} \subset \mathbb{Z}$ is only additively closed.

Definition. An *isomorphism* is a homomorphism with a (two-sided) inverse.

Definition. There are two products of a set of abelian groups $(A_\lambda, +_\lambda)$ for $\lambda \in \Lambda$, a totally ordered set.

(i) The *direct Cartesian product* $\prod_{\lambda \in \Lambda} A_\lambda$ with coordinatewise addition.

(ii) The *direct sum* $\oplus A_\lambda \subset \prod A_\lambda$ with only finitely many non-zero coordinates.

Examples. Let $\mathbb{Z}_n = \mathbb{Z}$ for $n \in \mathbb{N}$. The polynomial and formal power series groups:

$$(\mathbb{Z}[x], +) \quad \text{and} \quad (\mathbb{Z}[[x]], +)$$

are isomorphic to $\oplus \mathbb{Z}_n$ and $\prod \mathbb{Z}_n$, respectively.

Remark. When Λ is a set of n elements, then $\prod A_\lambda = \oplus A_\lambda$ is also written as:

$$A_{\lambda_1} \times \cdots \times A_{\lambda_n}$$

Fundamental Theorems*

Ab1. Every subgroup $S \subset (A, +)$ is the kernel of a surjective homomorphism:

$$f : A \to A/S$$

where A/S is the *quotient abelian group* of equivalence classes (aka cosets):

$$s + A = \{s + a \mid a \in A\}$$

with $(s + A) + (t + A) = (s + t) + A$.

Corollary. The image of any $f : A \to B$ is isomorphic to $A/\ker(f)$.

Definition. The *cokernel* of f is the group $B/\mathrm{im}(f)$.

Ab2. If $S, T \subset A$ are subgroups, then:

$$S \cap T \text{ and } S + T = \{s + t \mid s \in S, t \in T\}$$

are also subgroups of A, and

$$(S + T)/(S \cap T) \text{ is isomorphic to } (S + T)/S \times (S + T)/T$$

Corollary.(Chinese Remainder) If $n_1, ..., n_m$ are pairwise relatively prime, then:

$$\mathbb{Z}/n_1 \cdots n_m\mathbb{Z} \text{ is isomorphic to } \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m$$

Example. Find the explicit inverse map $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/105\mathbb{Z}$.

Non-Example. $\mathbb{Z}/4\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Ab3. (Classification) If $(A, +)$ is finitely generated, i.e. there is a surjective:

$$f : \mathbb{Z}^n \to A$$

then A is isomorphic to a product of cyclic groups:

$$\mathbb{Z}^r \times \prod \mathbb{Z}/d_i\mathbb{Z}$$

for unique integers $0 \le r \le n$ and $1 < d_1|d_2|....|d_m$ (i.e. each dividing the next).

Corollary. Every finite abelian group is a product of cyclic groups.

Conclusion. Subgroups of abelian groups are always kernels of a homomorphism, finitely generated abelian groups are classified, with an interesting pair of invariants (the *rank* r and the *torsion subgroup* $\prod \mathbb{Z}/d_i\mathbb{Z}$).

Abelian Groups in the Wild. The rational solutions of an equation:

$$y^2 = x^3 + Ax + B \text{ with } A, B \in \mathbb{Z} \text{ and } 4A^3 + 27B^2 \neq 0$$

defining an *elliptic curve* (together with a point 0 at infinity) have a commutative addition law, making them into a finitely generated group E (Mordell's Theorem).

The possible torsion subgroups of E are known (Mazur's Theorem), but there is much that is not known about the rank, e.g. can it be arbitrarily large?