Reminder about groups

Definition 1. *A* **group** *is a set G together with a binary operation $\cdot : G \times G \to G$ on G satisfying the following properties:*

(i) **(associativity)** $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ *for all* $g, h, k \in G$;

(ii) **(existence of an identity)** *there is an* $e \in G$ *such that* $e \cdot g = g \cdot e = g$ *for all* $g \in G$ *[it is easy to see that this* e *is unique];*

(iii) **(existence of inverses)** *for every* $g \in G$ *there is an* $h \in G$ *such that* $g \cdot h = h \cdot g = e$.

If the group satisfies the additional *property* $g \cdot h = h \cdot g$ *for all* $g, h \in G$, *then the group is* **commutative** *or* **Abelian**.

We often (somewhat sloppily) say that G is a group rather than $(G, \cdot)$ is a group.
Note that we used the standard notation $g \cdot h$ (or simply gh) rather than $\cdot(g, h)$.
With the above multiplicative notation we often write 1 for the identity e, and g^{-1} for the inverse of g. With an additive notation $(G, +)$ (typically used for Abelian groups), we usually write 0 for the identity, and $-g$ for the inverse of g.

The most essential properties of groups: For any $a, b \in G$, the equations $ax = b$ and $xa = b$ have unique solutions. (The two solutions $x = a^{-1}b$ and $x = ba^{-1}$ may be different!)
Cancellation rules: $ac = bc$ implies $a = b$, and $ca = cb$ implies $a = b$.
Inverse of products: $(ab)^{-1} = b^{-1}a^{-1}$.

Some facts about finite groups

The number of elements in G is called the order of the group ($o(G) = |G|$). Given $g \in G$, the smallest $n \in \mathbb{N}$ such that $g^n = e$ is called the order of the element g (written as $o(g)$).
It is easy to see that if g has order n and $k \in \mathbb{N}$, then $o(g^k) = n/gcd(k, n)$.

Theorem 1 (Lagrange). *For any* $g \in G$, *the order* $o(g)$ *divides* $o(G)$. *Hence* $g^{o(G)} = e$. *In fact,*

$$\{n \in \mathbb{Z} : g^n = e\} = o(g)\mathbb{Z} := \{o(g)k : k \in \mathbb{Z}\}.$$

More generally, if H *is a subgroup of* G, *then* $o(H)|o(G)$ *(divides).*

Theorem 2 (Cauchy). *If* p *is prime and* $p|o(G)$, *then* G *has an element of order* p.

Theorem 3 (Sylow). *If* p *is prime and* $p^\alpha|o(G)$ $(\alpha \in \mathbb{N})$, *then* G *has a subgroup of order* p^α.

Definition 2. *Let* $G_1, \ldots, G_k$ *be subgroups of an Abelian group* G. *We say that* G *is the direct product of these subgroups if every element* $g \in G$ *can be written uniquely in the form* $g = g_1 g_2 \cdots g_k$ *with* $g_i \in G_i$.

Definition 3. G *is called* **cyclic** *if it is generated by one element, that is, if* $G = \{g^n : n \in \mathbb{Z}\}$ *for some* $g \in G$.

Theorem 4 (The Fundamental Theorem of Finite Abelian Groups). *Every finite (or finitely generated) Abelian group is a direct product of cyclic groups.*

Reminder about fields

Definition 4. *A* **field** *is a set F with two* **commutative** *binary operations $+$ and $\cdot$ (addition and multiplication) such that*

(i) F is a group under $+$

(ii) $F^* := F \setminus \{0\}$ is a group under $\cdot$

(iii) $\cdot$ **distributes** *over $+$, that is, $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.*

(Recall properties A1-A4, M1-M4 and D in Math 311.)
Note: (ii) implies $|F| \geq 2$ since a group (by virtue of the existence of identity) is non-empty.

We usually write 0 and 1 for the additive and the multiplicative identities (as we did in the definition), $-a$ for the additive inverse of a, and a^{-1} for the multiplicative inverse of a.

Standard examples: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
Example of a finite field: $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = GF(p)$ where p is prime: "integers modulo p."
(GF stands for Galois field after the creator of modern algebra, Evariste Galois 1811-32.)

Some facts about fields

The smallest subfield contained in a field F ("prime subfield of F") is either Z_p for some prime p (we say "F has characteristic p") or $\mathbb{Q}$ ("F has characteristic 0").

The order (number of elements) of any finite field is a prime-power, and for each prime-power p^α there is a unique (up to isomorphism) field $GF(p^\alpha)$ of that order.

The multiplicative group F^* of a finite field F is cyclic. In fact, a finite multiplicative subgroup of any field is cyclic.

$GF(p^\alpha)$ has characteristic p, and all non-zero elements in $GF(p^\alpha)$ have additive order p. Hence $GF(p^\alpha)$ is a vector space over $GF(p)$. (See HW below.)

Recommended homework: If in a non-trivial additive Abelian group G all non-zero elements happen to have the same order p, then p is prime (try directly w/o Cauchy's or Sylow's theorem). Furthermore, G is a vector space over $\mathbb{Z}_p$ with the natural scalar multiplication $kg = \underbrace{g + g + \ldots + g}_{k}$ for $k = 0, 1, \ldots, p-1$.

(Non-trivial means $o(G) > 1$.)