

§ 11 Direct products, finitely generated commutative groups

$X_1, X_2, \dots, X_n$ sets $\leadsto$ direct product (Cartesian pr.)
is the collection of ordered n -tuples

$$(a_1, \dots, a_n) \quad a_i \in X_i$$

Notation $X_1 \times \dots \times X_n$ or $\prod_{i=1}^n X_i$; X^n if $X = X_1 = \dots = X_n$

Rem. (when $X = X_1 = \dots = X_n$) we care about the order of terms a_i , so $(x, y) \neq (y, x)$ unless $x = y$

- sometimes the superscript notation means different things: S^n n -dim. sphere

Example $\mathbb{R}^n = \{(t_1, \dots, t_n) \mid t_i \in \mathbb{R}\}$

Thm / Def (11.2) $G_1, \dots, G_n$: groups (in multiplicative notation)
 $\leadsto$ the set $\prod_{i=1}^n G_i$ becomes a group with:

- binary op. $(a_1, \dots, a_n)(b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n)$
- identity elem. $(e, \dots, e)$
- inverse $(a_1, \dots, a_n)^{-1} = (a_1^{-1}, \dots, a_n^{-1})$

call this the direct product group

Ex. $\mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_6$

corresp. $\mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$, $a \mapsto (a, a)$ for integers a

$\mathbb{Z}_2 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_6$, $(b, c) \mapsto -(3b + 2c)$ for intr. b, c

so $1 \in \mathbb{Z}_6$ corr. to $(1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$; in additive notation

$$2(1, 1) = (1, 1) + (1, 1) = (2, 2) = (0, 2)$$

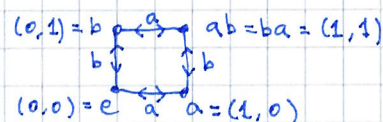
$$3(1, 1) = 2(1, 1) + (1, 1) = (0, 2) + (1, 1) = (1, 3) = (1, 0)$$

$$4(1, 1) = 3(1, 1) + (1, 1) = (0, 1), \quad 5(1, 1) = (1, 2)$$

$$6(1, 1) = (0, 0) \text{ as expected from } 6 \cdot 1 = 0 \text{ in } \mathbb{Z}_6$$

Ex. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a comm. grp. with 4-elements and any nontriv. elem. $g \in \mathbb{Z}_2 \times \mathbb{Z}_2$ satisfies $g^2 = e$

(the Klein 4-group)



Th'm (11.5) m, n : pos. integers

$\leadsto \mathbb{Z}_m \times \mathbb{Z}_n$ is isom. to $\mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$

Proof

Step 0 : the least common multiple $\text{lcm}(m, n)$

satisfies $\text{lcm}(m, n) = mn \iff \gcd(m, n) = 1$

Step 1 $\gcd(m, n) = 1 \Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$

claim : we get an isom $\phi : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ by

$$\phi(k) = (k, k)$$

Step 1-1 ϕ is compat. with binary ops

Step 1-2 ϕ is one-to-one: $\phi(j) = \phi(k)$ only if $j = k$

by Step 1-1 $\phi(j) = \phi(k)$ would imply $\phi(0) = \phi(k-j)$

$\leadsto$ want $(k-j, k-j) = (0, 0)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$ only if $k-j = 0$
 $\uparrow$ in $\mathbb{Z}_{mn}$ $\uparrow$
 $k-j = am$ and $k-j = bn$ $k-m = cmn$

this holds by $\gcd(m, n) = 1$

Step 1-3 ϕ is onto : $\forall i, j \exists k (i, j) = (k, k)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$

$\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ have the same number of elements $(m \cdot n)$

by Step 1-2 ϕ is one-to-one, so there are $m \cdot n$ - many elems. of the form $(k, k) = \phi(k)$

Step 2 $\gcd(m, n) \neq 1 \Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n \not\simeq \mathbb{Z}_{mn}$

proof by contradiction ; if $\phi : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ is an

isom. then $k \cdot \phi(1) = \phi(k)$ equals $e = (0, 0)$ iff $k = cmn$

$l = \text{lcm}(m, n) (< mn \text{ by } \gcd(m, n) \neq 1)$ satisfies

$$l(i, j) = (li, lj) = (0, 0) \text{ in } \mathbb{Z}_m \times \mathbb{Z}_n$$

for any $(i, j) \in \mathbb{Z}_m \times \mathbb{Z}_n$ $\square$

Cor (11.6) $\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k} \simeq \mathbb{Z}_{m_1 \dots m_k}$ iff. $\gcd(m_i, m_j) = 1$
for $i \neq j$

Fact (Thm 11.12) G : comm. group with a finite generating subset $S \subset G$

Then $\exists$ prime numbers $p_1, \dots, p_n$
pos. integers $e_1, \dots, e_n > 0$
non. neg. integer $r \geq 0$

$$\text{s.t. } G \cong \mathbb{Z}_{p_1^{e_1}} \times \dots \times \mathbb{Z}_{p_n^{e_n}} \times \mathbb{Z}^r$$

Rem. there can be repeat of the same primes in p_i
e.g. $\mathbb{Z}_2 \times \mathbb{Z}_2$

What do we need to prove this?

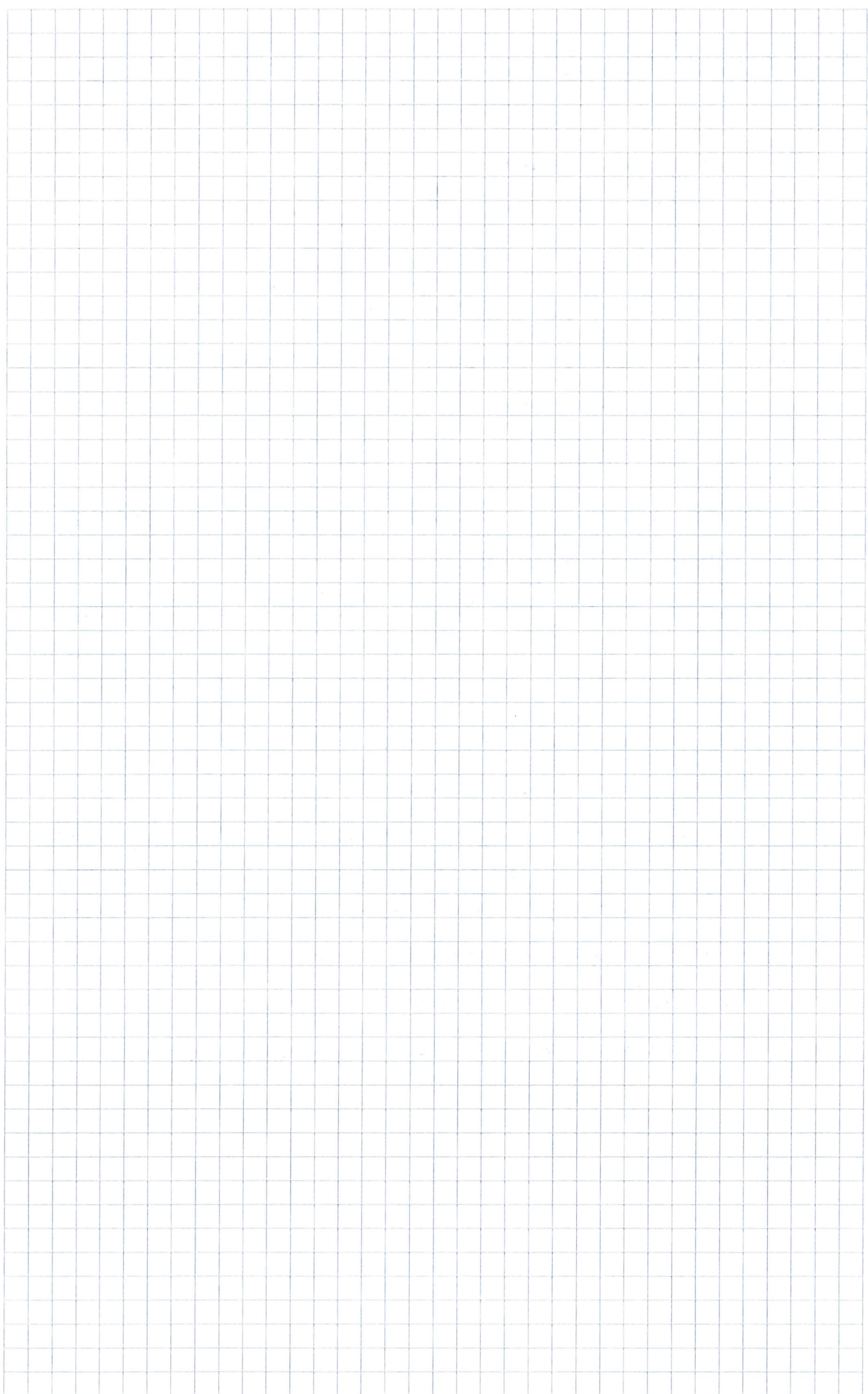
- corresp. between commutative groups and modules over the ring $\mathbb{Z}$
- structure theory for rings like $\mathbb{Z}$ (principal ideal domains)
- structure theory for modules over such rings

Groups covered by this th'm

- finite comm. grps (then $r=0$)
 - in particular $\mathbb{Z}_p^\times = \{n \in \mathbb{Z}_p \mid n \neq 0\}$ with multiplic. as binary op.
 p : prime num.
- (we will get $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$ by the field theory)

Commutative groups not covered by this th'm

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with addition
- $\mathbb{T} = \{z \in \mathbb{C} \mid |z|=1\}$ with multiplication



()

()

()

()