

PS8

Sasha Redden

November 11, 2025

1. Let F be an abelian group and $S \subset F$ be a subset. We say that F is **free abelian** on the set S , if for any abelian group A and any function $\tau : S \rightarrow A$, there exists a unique group homomorphism $\varphi : F \rightarrow A$ such that $\varphi(s) = \tau(s)$ for all $s \in S$. [Just like the definition of free group, except that we restrict to maps to abelian groups.]
 - (a) Prove that $\mathbb{Z}^2$ is free abelian on the set $\{(1, 0), (0, 1)\}$.
 - (b) Let S be an infinite countable set (such as $S = \mathbb{N}$). Find a free abelian group on S .
 - (c) Let F be a free group (not free abelian) on a set S . Let F' be its commutator subgroup, as in the previous problem set. Prove that F/F' is free abelian on the image of S in F/F' .
 - (d) If we choose $A = \mathbb{Z}$ and define $\tau : \{(1, 0), (0, 1)\} \rightarrow \mathbb{Z}$ by $\tau((1, 0)) = 1$ and $\tau((0, 1)) = 0$, then there exists unique homomorphism $\varphi : \mathbb{Z}^2 \rightarrow \mathbb{Z}$ define as follows: $\varphi(a, b) = a$. With this construction we have $\varphi((1, 0)) = 1 = \tau((1, 0))$ and $\varphi((0, 1)) = 0 = \tau((0, 1))$. This is a homomorphism because

$$\varphi((a, b) + (c, d)) = \varphi((a + c, b + d)) = a + c = \varphi((a, b)) + \varphi((c, d)).$$

To demonstrate uniqueness, suppose there exists another homomorphism $\varphi' : \mathbb{Z}^2 \rightarrow \mathbb{Z}$ such that $\varphi' \neq \varphi$, then $\varphi'((1, 0) + (0, 1)) = \varphi'((1, 1)) = 1 = \varphi'((1, 0)) + \varphi'((0, 1))$ so $\varphi'((1, 0))$ must be 0 and $\varphi'((0, 1))$ must be 1, but then $\tau((1, 0)) = 1 \neq 0 = \varphi'((1, 0))$ and furthermore $\tau((0, 1)) \neq \varphi'((0, 1))$.

- (b) Consider a set F of tuples of length $|S|$ where only finitely many entries are non-zero integers, with point-wise addition as group operation. Let $x = (x_{s_1}, x_{s_2}, \dots)$ for all $s_i \in S$ and have $e_{s_i} = (0, \dots, 1, \dots, 0)$ where the 1 is in the i -th entry, and $\gamma : S \rightarrow F$ such that $\gamma(s) = e_s$ (to associate every $s \in S$ with an element in F . For any abelian group A define $\varphi : F \rightarrow A$ by $\varphi(x) = \sum_{s_i \in S} x_{s_i} \tau(s_i)$, where τ is any function. This sum is finite because there are only finitely many non zero x_{s_i} .

Homomorphism: For $x_1, x_2 \in F$ we have

$$\varphi(x_1 + x_2) = \sum_{s_i \in S} (x_{1_{s_i}} + x_{2_{s_i}}) \tau(s_i) = \sum_{s_i \in S} x_{1_{s_i}} \tau(s_i) + \sum_{s_i \in S} x_{2_{s_i}} \tau(s_i) = \varphi(x_1) + \varphi(x_2)$$

and $\varphi(e_s) = \tau(s) \forall s \in S$ and we have $\varphi \circ \gamma = \tau$.

Uniqueness: Suppose ϕ is another homomorphism where $\phi(e_s) = \tau(s)$.

$$\phi(x) = \sum_{s_i \in S} x_{s_i} \phi(e_{s_i}) = \sum_{s_i \in S} x_{s_i} \tau(s_i) = \varphi(x)$$

- (c) F is free on S , so if we take A to be any abelian group and any $\tau : S \rightarrow A$ then there exists a unique homomorphism $\phi : F \rightarrow A$ where $\phi(s) = \tau(s) \forall s \in S$. Let $\varphi : F \rightarrow F/F'$ be the usual map, then $\varphi(S) \subset F/F'$. Let $\tau' : \varphi(S) \rightarrow A$ be a function, then we have $\tau' \circ \varphi : S \rightarrow A$ and then there exists a unique homomorphism $\phi : F \rightarrow A$ such that $\phi'(s) = \tau' \circ \varphi(s) \forall s \in S$. For $xyx^{-1}y^{-1} \in F'$, $\phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi^{-1}(x)\phi^{-1}(y) = e$ because A is abelian, so $F' \subset \text{Ker}(\phi)$. Define $\gamma : F/F' \rightarrow A$ where $\gamma(xF') = \phi(x) \in A$. This is well defined because $F' \subset \text{Ker}(\phi)$ so for $xF' = yF' \in F/F'$ we have $y^{-1}x \in F' \implies y^{-1}x \in \text{Ker}(\phi)$ so $\phi(y^{-1}x) = e \implies \phi(x) = \phi(y)$. Homomorphism because for $xF', yF' \in F/F'$, $\gamma(xF' \cdot yF') = \gamma(xyF') = \phi(xy) = \phi(x)\phi(y) = \gamma(xF')\gamma(yF')$
2. Let S be a set and let $F(S)$ be the free group on S (defined as the set of reduced words in S). Let $R \subset F(S)$ be a subset of reduced words. Let $N(R)$ be the smallest normal subgroup of $F(S)$ containing R . We define $\langle S|R \rangle$ to be the quotient $F(S)/N(R)$.
- (a) Formulate and prove a universal property satisfied by the group $\langle S|R \rangle$. [If G is a group and $\tau : S \rightarrow G$ is a function such that $\dots$, then there exists a unique group homomorphism $\varphi : \langle S|R \rangle \rightarrow G$ such that $\dots$]
- (b) Prove that $\langle r, s|r^n, s^2, sr sr \rangle$ is the dihedral group D_n .
3. The **characteristic** of a ring R is the smallest positive integer n such that the sum of n ones is equal to 0, i.e. $1 + \dots + 1 = 0$ (where there are n ones). If no such n exists, then we say that R has characteristic 0.
- (a) Suppose that R has characteristic n for some $n \in \mathbb{N}$. Prove that there is an injective ring homomorphism $\varphi : \mathbb{Z}/n \rightarrow R$ such that $\varphi(1) = 1$.
- (b) Suppose that R has characteristic 0. Prove that there is an injective ring homomorphism $\varphi : \mathbb{Z} \rightarrow R$ such that $\varphi(1) = 1$.
- (c) Suppose that F is a field and is has characteristic n for some $n \in \mathbb{N}$. Prove that n is a prime.
- (a) Let $\varphi(n) = 1 + \dots + 1 = n \cdot (1)$. Then we have $\varphi(0) = \varphi(n) = 1 + \dots + 1 = n \cdot (1) = 0$, $\varphi(1) = 1$, $\varphi(a+b) = a \cdot (1) + b \cdot (1) = \varphi(a) + \varphi(b)$, and $\varphi(a \cdot b) = a \cdot (1) \cdot b \cdot (1) = \varphi(a)\varphi(b)$. For injectivity suppose $\exists n, m \in \mathbb{Z}/n : n \neq m$ we have that $\varphi(n) = n \cdot (1) \neq m \cdot (1) = \varphi(m)$.
- (b) Again, let $\varphi(n) = 1 + \dots + 1 = n \cdot (1)$. Then we have $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(a+b) = a \cdot (1) + b \cdot (1) = \varphi(a) + \varphi(b)$, and $\varphi(a \cdot b) = a \cdot (1) \cdot b \cdot (1) = \varphi(a)\varphi(b)$. For injectivity suppose $\exists n, m \in \mathbb{Z}/n : n \neq m$ we have that $\varphi(n) = n \cdot (1) \neq m \cdot (1) = \varphi(m)$.
- (c) Suppose n composite, then $n = ab$ so $0 = (1 + \dots + 1)(1 + \dots + 1) = (a \cdot 1)(b \cdot 1)$ where there are a and b ones respectively, then $(a \cdot 1)$ or $(b \cdot 1)$ equal zero, but then the characteristic is not n .

4. Let R be a ring. A **nilpotent** in R is an element $a \in R$ such that $a^m = 0$ for some m .

- (a) For which $n \in \mathbb{N}$ does $\mathbb{Z}/n$ contain non-zero nilpotents?
- (b) Let $p = ax + b \in R[x]$. Prove that p is a unit in $R[x]$ if and only if b is a unit in R and a is nilpotent in R .
- (c) Let R be a ring. Prove that the set $\text{nil}(R) = \{a \in R : a \text{ is nilpotent}\}$ is an ideal. [It is called the **nilradical** of R .]
- (a) $n = p^k m$ for some $k \geq 2, m \in \mathbb{N}$ and p prime.
- (b) Suppose p is a unit in $R[x]$, then there exists a $q \in R[x]$ such that $p \cdot q = (ax + b) \cdot q = ax \cdot q + b \cdot q = 1$, we cannot have $q = 0$, but we must have $ax \cdot q = 0$ (because it will never be constant), and thus $b \cdot q = 1$, so b is a unit and a is a zero divisor. We can show a nilpotent

If we have a prime ideal P of R , then we have a ring homomorphism $\varphi : R \rightarrow R/P$, then realize $ax + b$ in R/P with $\varphi(a) = a'$ and $\varphi(b) = b'$ then $a'x + b' \in R/P[x]$ must be a unit in because of the homomorphism properties, but R/P is an integral domain, but the only units in R/P are non-zero constants so $a' = 0$ in R/P and then $a \in P$. Since P is arbitrary, a is in every prime ideal so a is nilpotent because it is in the intersection of all prime ideals.

Suppose b is a unit and a is nilpotent in R such that $a^m = 0$. Let $d = a^{m-1}$ and $c = dq$ for some q such that $bc = 1$. Then $c(ax + b) = q \cdot (a^{m-1})ax + cb = 1$.

- (c) For $a, b \in \text{nil}(R)$ let $a^m = 0, b^n = 0$ for some $m, n \in \mathbb{N}$.

$$(a + b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k} = 0$$

This is true because when $k \leq m$ we have $m + n - k \geq n$ so $b^{m+n-k} = 0$, and when $k > m$ we have $a^k = 0$, so $(a + b) \in \text{nil}(R)$. For $a \in \text{nil}(R), b \in R$ let $a^m = 0$ for some $m \in \mathbb{N}$ then $(ab)^m = a^m b^m = 0$ so $ab \in \text{nil}(R)$.