Homework 3, Solutions

M. Gr. after [Gri07]

2012/11/10

1.5 Direct products

Exercise 1.5.1 (Product and coproduct, 直积与对偶直积)**.** Given two groups G and H.

a. Show that their direct product $G \times H$ together with the canonical projections $\pi_G \colon G \times H \to G$ and $\pi_H \colon G \times H \to H$ is a product (in the sense of category theory), i.e. for every pair of homomorphisms $\rho_G \colon K \to G$ and $\rho_H \colon K \to H$ there is a unique morphism $\tilde{\rho} \colon K \to G \times H$ such that $\pi_G \circ \tilde{\rho} = \rho_G$ and $\pi_H \circ \tilde{\rho} = \rho_H$.

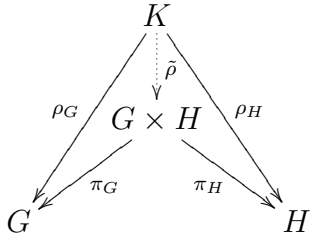
b. Show that $G \oplus H = G \times H$ together with the canonical embeddings $e_G \colon G \to G \oplus H$ and $e_H \colon H \to G \oplus H$ is a coproduct, i.e. for every pair of homomorphisms $\rho_G \colon G \to K$ and $\rho_H \colon H \to K$ with $\rho_G(g)\rho_H(h) = \rho_H(h)\rho_G(g)$ for all $g \in G$ and $h \in H$, there is a unique morphism $\tilde{\rho} \colon G \oplus H \to K$ such that $\rho_G = \tilde{\rho} \circ e_G$ and $\rho_H = \tilde{\rho} \circ e_H$.

c. Draw the mapping behavior of the morphisms in Parts a and b. You may use solid arrows for given morphisms and dashed arrows for morphisms implied during your proof.

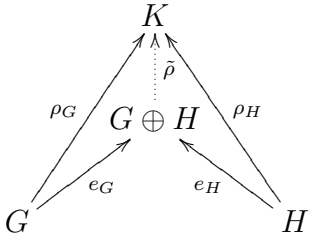
Solution.

c. Let us first visualize what we want to construct:

a. product



b. coproduct



a. Given the above diagram, it is clear how to define the map $\tilde{\rho}\colon K \to G \times H : k \mapsto (\rho_G(k), \rho_H(k))$. Since ρ_α for $\alpha \in \{G, H\}$ are group homomorphisms as well as the pairing, also $\tilde{\rho}$ is a group homomorphism. From the definition of π_α for $\alpha \in \{G, H\}$ it also follows that $\pi_\alpha \circ \tilde{\rho} = \rho_\alpha$. The uniqueness is now also clear, because the last equation also implies that $\tilde{\rho}(k) = (\rho_G(k), \rho_H(k))$.

b. Knowing that every element in $G \oplus H$ can be written in the form gh with $g \in G$ and $h \in H$, we define the map $\tilde{\rho}\colon G \oplus H \to K : (gh) \mapsto \rho_G(g)\rho_H(h)$. Since $e_G(G) \cap e_H(H) = \{\mathrm{id}\}$ we see that this is well-defined. Knowing that $\rho_H(h)\rho_G(g) = \rho_G(g)\rho_H(h)$ we also conclude that $\tilde{\rho}$ is a group homomorphism.[1] Finally, obviously $\tilde{\rho} \circ e_\alpha = \rho_\alpha$ for $\alpha \in \{G, H\}$, because $\rho_\alpha(\mathrm{id}) = \mathrm{id}_K$. Conversely $\tilde{\rho}$ is uniquely determined by the mapping behavior for the $e_G(G)$ and $e_H(H)$. But these are given by ρ_G and ρ_H respectively. This completes the proof. □

Exercise 1.5.2. Find all abelian groups (up to isomorphism) of order

a. 35,

b. 36,

c. 360.

Solution.

a. $35 = 5 \cdot 7$ therefore there is only one group $C_{35} \cong C_7 \times C_5$;

b. $36 = 6^2 = 2^2 \cdot 3^2 = 4 \cdot 9 = 2 \cdot 2 \cdot 9 = 2 \cdot 2 \cdot 3 \cdot 3 = 4 \cdot 3 \cdot 3$ thus there are 4 non-isomorphic groups: $C_{36} \cong C_4 \times C_9$, $C_2 \times C_2 \times C_9$, $C_6 \times C_6 \cong (C_2 \times C_3)^2$, $C_4 \times (C_3)^2$;

c. $360 = 6^2 \cdot 2 \cdot 5 = 2^3 \cdot 3^2 \cdot 5 = 8 \cdot 9 \cdot 5 = 2 \cdot 4 \cdot 9 \cdot 5 = 2 \cdot 2 \cdot 2 \cdot 9 \cdot 5 = 8 \cdot 3 \cdot 3 \cdot 5 = 2 \cdot 4 \cdot 3 \cdot 3 \cdot 5 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$ corresponding to the 6 non-isomorphic groups $C_{360} \cong C_8 \times C_9 \times C_5$, $C_2 \times C_4 \times C_9 \times C_5$, $(C_2)^3 \times C_9 \times C_5$, $C_8 \times (C_3)^2 \times C_5$, $C_2 \times C_4 \times (C_3)^2 \times C_5$, $(C_2)^3 \times (C_3)^2 \times C_5$. □

[1] If this relation is not given, you should rather map from $G * H$ and obtain the free coproduct.

Exercise 1.5.3. Define Euler's ϕ-function as $\phi\colon \mathbb{N}_+ \to \mathbb{N}_+$ such that $\phi(n)$ is the cardinality of $\{k \in [1,n] : \gcd(k,n) = 1\}$, i.e. the numbers that are relatively prime to n. Show the following formula for ϕ:

$$\phi(n) = n \prod_{p|n} (1 - \tfrac{1}{p})$$

where $p \in \mathbb{P}$ runs over all prime divisors of n.

You can proceed as follows:

a. Show that the group C_p has exactly $p-1$ generators, i.e. there are $p-1$ numbers between 1 and p (inclusive) that are relatively prime to p;

b. Show that the group C_{p^n} has exactly $p^n - p^{n-1}$ elements of order p^n, i.e. $\phi(p^n) = p^n(1 - \frac{1}{p})$;

c. Show that the group C_{mn} where $\gcd(m,n) = 1$ has the generators $(C_m)^* \times (C_n)^*$ where $(C_m)^*$ are the generators of C_m. Conclude that $\phi(mn) = \phi(m)\phi(n)$ and thus the formula for ϕ.

Solution.

a. In C_p where $p \in \mathbb{P}$ is a prime, every element except the identity has order p and thus $\phi(p) = |C_p^*| = p - 1 = p(1 - \frac{1}{p})$.

b. Conversely C_{p^n} has exactly p^{n-1} elements that are divisible by p. All the others are relatively prime and thus $\phi(p^n) = |C_{p^n}^*| = p^n - p^{n-1} = p^n(1 - \frac{1}{p})$.

c. For $\gcd(m,n) = 1$ we have $C_{mn} \cong C_m \times C_n$. But the units of C_m are $|C_m^*| = \phi(m)$ and thus together $C_{mn}^* = C_m^* \times C_n^* \subset C_m \times C_n$ with $\phi(mn) = |C_{mn}^*| = |C_m^*|\,|C_n^*| = \phi(m)\phi(n)$. Therefore for $n = p_1^{n_1} \dots p_k^{n_k}$ we have

$$\phi(n) = \prod_{p_i|n} \phi(p_i^{n_i}) = \prod_{p_i|n} p_i^{n_i}(1 - \tfrac{1}{p_i}) = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \quad \square$$

Exercise 1.5.4. A group G is called **indecomposable** iff for every direct sum $G \cong A \oplus B$ either $A = 1$ or $B = 1$.

a. Prove that D_5 is indecomposable;

b. prove that D_4 is indecomposable;

c. prove that C_{p^n} is indecomposable when p is a prime and $n \in \mathbb{N}$.

Solution.

a. Obviously the center of D_5 is trivial. The subgroups generated by one element are $\langle \sigma\tau^k \rangle$ all different for $0 \leq k \leq 4$ and $\langle \tau \rangle$. If you take two generators which are not already in one of the previous groups, then you obtain the whole D_5. The trivial subgroups 1 and D_5 are normal. By inspecton the only other normal subgroup is $\langle \tau \rangle$. Therefore D_5 is indecomposable.

b. The center of D_4 is $\operatorname{cent} D_4 = \langle \tau^2 \rangle$. Analogously to the previous part, the subgroups generated by one element are $\langle \sigma\tau^k \rangle$ all different for $0 \leq k \leq 4$ and $\langle \tau \rangle$. The subgroups generated by two elements are $\langle \sigma, \tau^2 \rangle$ or D_4. Beside the trivial subgroups 1 and D_5, the only other normal subgroups are $\operatorname{cent} D_5$, $\langle \tau \rangle$, and $\langle \sigma, \tau^2 \rangle$. But $\operatorname{cent} D_4 \subset \langle \tau \rangle, \langle \sigma, \tau^2 \rangle$, so $A \cap B = \{\mathrm{id}\}$ implies $A = 1$ or $B = 1$ and thus D_4 is not a direct product.

c. We have shown earlier that all subgroups of C_{p^n} are cyclic. Since C_{p^n} is cyclic itself, this implies that they are all normal subgroups. But on the other hand $\langle g \rangle$ for g of order p^K contains all elements of order p^k for $0 \leq k \leq K$. Thus the subgroups are linearly ordered and there are no two non-trivially intersecting ones.

□

1.6 Krull–Schmidt theorem

Exercise 1.6.1. Compute the Krull–Schmidt decomposition of the $D_n = \langle \sigma, \tau : \sigma^2 = \mathrm{id} = \tau^n, \sigma\tau\sigma = \tau^{-1} \rangle$.

Solution. We have seen so far $D_1 = C_2$, $D_2 = C_2 \times C_2$, and $D_3 = S_3 = A_3 \rtimes C_2$ with $A_3 = C_3$ which is therefore indecomposable, D_4 and D_5 are also indecomposable. We thus conjecture D_n is indecomposable for $n \geq 3$.

. . . □

Exercise 1.6.2. Compute the Krull–Schmidt decomposition of $\mathrm{GL}_2(\mathbb{F}_p)$ the automorphism group of the vector space $\mathbb{F}_p^2$ where $\mathbb{F}_p$ is the field with $p \in \mathbb{P}$ elements and p a prime.
Hint: If the general case is too hard, you may start with $p = 3$.

Solution. Examples are

2

$$\mathrm{GL}_2(\mathbb{F}_2) = \left\{ \mathbb{1}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

a group with 6 elements which is not cyclic. So $\mathrm{GL}_2(\mathbb{F}_2) \cong D_3$ which is indecomposable.

3

$$\mathrm{GL}_2(\mathbb{F}_3) = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm 1 & 0 \\ \pm 1 & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm 1 & \pm 1 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm 1 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}, \begin{pmatrix} \pm 1 & \pm 1 \\ \pm 1 & \pm 1 \end{pmatrix} \right\}$$

It has order $2 \cdot 4 + 4 \cdot 8 + 8 = 48 = 2^4 \cdot 3$ We know that it is not abelian (because for $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ we see $AB \neq BA$). Moreover it has an element B of order 8 ($B^2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $B^3 = \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}$, $B^4 = -\mathbb{1}$, $B^6 = -B^2$, $B^8 = (B^4)^2 = \mathbb{1}$).

p (the general case)

$$\mathrm{GL}_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda' \end{pmatrix}, \begin{pmatrix} 0 & \lambda \\ \lambda' & 0 \end{pmatrix}, \begin{pmatrix} 0 & \lambda \\ \lambda' & \mu \end{pmatrix}, \begin{pmatrix} \lambda & 0 \\ \mu & \lambda' \end{pmatrix}, \begin{pmatrix} \lambda & \mu \\ 0 & \lambda' \end{pmatrix}, \begin{pmatrix} \mu & \lambda \\ \lambda' & 0 \end{pmatrix}, \begin{pmatrix} \lambda & \mu \\ \mu' & \lambda' \end{pmatrix} : \lambda, \lambda', \mu, \mu' \in \mathbb{F}_p^*, \mu' \neq \lambda\lambda'/\mu \right\}$$

of order $2(p-1)^2 + 4(p-1)^3 + (p-2)(p-1)^3 = (p-1)^2(p+1)p$.

□