

Algebra I: Solutions to selected homework problems

HW1:

4. (a) Let m and n be relatively prime integers. Prove that

$$(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \simeq (\mathbb{Z}/mn\mathbb{Z})^*.$$

Solution: Let us prove the following more general result. Under the same assumptions on n and m , the rings $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/mn\mathbb{Z}$ are isomorphic. Then the statement of the problem will follow from the fact that isomorphic rings have isomorphic groups of invertible elements.

Construct a map $\pi : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/mn\mathbb{Z}$ as follows.

$$\pi : a \mapsto (a \pmod{n}, a \pmod{m}).$$

Then π is well-defined, i.e. does not depend on the choice of a representative a in the congruence class modulo mn . Indeed, if $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$. Clearly, π takes sums to sums and products to products, i.e. it is a *ring homomorphism*. Let us prove that π is bijective.

Since $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/mn\mathbb{Z}$ have the same number of elements, it is enough to prove that π is injective. Suppose that $\pi(a) = \pi(b)$. This means $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$. Hence, $a - b$ is divisible both by m and n . This implies that $a - b$ is a multiple of mn . Indeed, we can write $a - b = km$ for some integer k . Then km is divisible by n . Since m and n are relatively prime, k is a multiple of n .

Note: The last statement may look self-evident, but in fact, Euclidean algorithm is necessary to prove it. This statement fails in rings without Euclidean algorithm.

The proof is as follows. By Euclidean algorithm there exist such integers s and t that $sm + tn = 1$. Multiply this identity by k . Then $smk + tnk = k$. The left hand side is divisible by n . Hence, k is divisible by n .

Here is a counterexample for non-euclidean rings. Take the ring $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$, and take $m = k = 2$, $n = 1 + \sqrt{5}$. Then $mk = 4 = (1 + \sqrt{5})(-1 + \sqrt{5})$, but both m and k are relatively prime with n .

5. For each pair of the groups below, find out if they are isomorphic. Justify your answer.

(b) (\mathbb{Q}^*, \times) and $(\mathbb{Q}, +)$;

(c) (\mathbb{R}^+, \times) and $(\mathbb{R}, +)$.

Solution: (b) The groups (\mathbb{Q}^*, \times) and $(\mathbb{Q}, +)$ are not isomorphic because the first group has the element -1 of order 2, and the second one does not (if $2q = 0$ for some $q \in \mathbb{Q}$, then $q = 0$).

(c) The groups (\mathbb{R}^+, \times) and $(\mathbb{R}, +)$ are isomorphic. The isomorphism is given by the exponential function: $x \mapsto e^x$.

HW 2:

4. For each pair of positive integers m and n find all homomorphisms from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$.

Solution: Since $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group any homomorphism π is uniquely defined by its value $\pi(1)$ on the generator $1 \in \mathbb{Z}/n\mathbb{Z}$. Let us find all possible values for $\pi(1)$. Since π is a homomorphism we have

$$\pi(\underbrace{1 + \dots + 1}_{n \text{ times}}) = \underbrace{\pi(1) + \dots + \pi(1)}_{n \text{ times}} = n\pi(1).$$

Since $n \equiv 0 \pmod{n}$, the homomorphism π is well-defined only if $n\pi(1) \equiv 0 \pmod{m}$. Let d be the greatest common divisor of m and n . Then $\pi(1)$ should be a multiple of m/d . So there are d different homomorphisms which send 1 to one of the following elements $0, m/d, 2m/d, \dots, (d-1)m/d$.

In particular, if n and m are relatively prime there are no nontrivial homomorphisms from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$.

HW 4:

Bonus (d*) Let p and q be different prime numbers. Classify all groups of order pq .

Solution: Let G be a group of order pq . Suppose that $p < q$. By Sylow's theorems G has n_q subgroups of order q where $n_q \equiv 1 \pmod{q}$ and n_q divides pq . It follows that n_q is relatively prime with q , hence n_q divides p . The only divisors of p are 1 and p , but $p-1$ is not a multiple of q since $q > p$. Thus $n_q = 1$, and the Sylow q -subgroup S_q of G is normal. The same arguments show that a Sylow p -subgroup S_p is also normal if $q-1$ is not a multiple of p . In this case, G has two cyclic normal subgroups $S_p \simeq \mathbb{Z}/p\mathbb{Z}$ and $S_q \simeq \mathbb{Z}/q\mathbb{Z}$ of relatively prime orders. Hence $S_p \cap S_q = \{e\}$, $S_p S_q = G$ and G is isomorphic to a direct product $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. This direct product is a cyclic group of order pq by the solution to Problem 4(a) from Homework 1.

Suppose now that $q-1$ is a multiple of p . Then S_q is still a normal subgroup of G , $S_p \cap S_q = \{e\}$, $S_p S_q = G$ and $S_p \subset G$ acts on S_q by conjugations. Hence, G is a semidirect product of $S_q \simeq \mathbb{Z}/q\mathbb{Z}$ and $S_p \simeq \mathbb{Z}/p\mathbb{Z}$. Each semi-direct product is uniquely defined by the corresponding homomorphism from $\mathbb{Z}/p\mathbb{Z}$ to $\text{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. By the previous problem there are exactly p such homomorphisms. Each of them maps $1 \in \mathbb{Z}/p\mathbb{Z}$ to $\pi^{i(q-1)/p}$, where π is a generator of $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$ and $i = 0, 1, \dots, p-1$. The corresponding semidirect product G_i can be described by generators and relations as follows. Let x be a generator of S_q and y be a generator of S_p . Then $G_i = \langle x, y : x^q = y^p = 1, yxy^{-1} = \pi^{i(q-1)/p}(x) \rangle$. In particular, if $i = 0$, then G_0 is Abelian, and, hence, cyclic of order pq . If $i \neq 0$, then G_i is isomorphic to G_1 . Indeed, the map $G_1 \rightarrow G_i$ that sends x to x and y to y^i is an isomorphism.

HW 6:

2. Prove that any subgroup of a finitely generated free Abelian group is a finitely generated free Abelian group.

Solution: Let G be a free Abelian group of rank n , and let H be a subgroup of G . By definition, there are n elements $e_1, \dots, e_n \in G$ such that any element $g \in G$ has a unique representation $g = a_1e_1 + \dots + a_n e_n$ for some integers a_1, \dots, a_n . We now choose an element $h \in H$ such that the coefficient a_1 in the decomposition $h = a_1e_1 + \dots + a_n e_n$ has the smallest nonzero absolute value.

Consider a free Abelian subgroup $K = \langle e_2, \dots, e_n \rangle \subset G$. Prove that $H = \langle h \rangle \oplus (K \cap H)$. It is clear that $\langle h \rangle \cap K = \{0\}$. Show that any $h' \in H$ lies in $\langle h \rangle + K$. Let $h' = b_1e_1 + \dots + b_n e_n$ be the decomposition of h' . Then a_1 divides b_1 . Indeed, we can divide b_1 by a_1 with residue: $b_1 = sa_1 + r$, and get that

$$h' - sh = re_1 + (b_2 - sa_2)e_2 + \dots + (b_n - sa_n)e_n,$$

where $0 \leq r < |a_1|$. Since $|a_1|$ is minimal nonzero, we have that $r = 0$. Hence, $h' - sh \in K$.

It remains to prove that the subgroup $K \cap H \subset K$ is free. The rank of K is less than the rank of G so we can use induction on n .