Solutions of exercise sheet 10

The content of the marked exercises **(*)** should be known for the exam.

1. **(*)** (Characterization of gcd and lcm in terms of principle ideals). Let A be a PID and take two non-zero elements $a, b \in A$. Show:

1. $aA + bA = dA$, where d is a *greatest common divisor* of (a, b) in the sense that
   a) $d|a$ and $d|b$, and
   b) for all $d' \in A$ s.t. $d'|a$ and $d'|b$, we have $d'|d$.
2. $aA \cap bA = mA$, where m is a *least common multiple* of (a, b) in the sense that
   a) $a|m$ and $b|m$, and
   b) for all $m' \in A$ s.t. $a|m'$ and $b|m'$, we have $m|m'$.
3. In the factorial ring $A = \mathbb{C}[X, Y]$ there are elements a and b which are irreducible, with $aA \neq bA$, but for which $aA + bA \neq A$.

Solution:

1. Being A a PID, there exists $d \in A$ such that $dA = aA + bA$. Then we have that $a, b \in dA$, which means that $d|a$ and $d|b$, proving property (a). Moreover, for $d' \in A$ a divisor of both a and b, we have $a, b \in d'A$, which implies that $dA = aA + bA \subseteq d'A$, so that in particular $d \in d'A$, meaning that $d'|d$, which proves (b).
2. Again A is a PID and there exists $m \in A$ such that $mA = aA \cap bA$. Then $m \in aA$ and $m \in bA$, so that $a|m$ and $b|m$, proving (a). For (b), suppose that m' is a multiple of both a and b. Then $m' \in aA \cap bA = mA$, so that $m|m'$, which proves (b).
3. Let $a = X$ and $b = Y$. Then a is irreducible, since for any factorization $X = fg$, we have that f and g are constant in Y and one of them has to be constant in X, so that f or g is a unit. Similarly, one can prove that b is irreducible. Since $X \notin Y \cdot A$ (by reasoning on the degree in Y), we have $aA \neq bA$. But $aA + bA$ is not a principal ideal (as we proved in Exercise sheet 8, Exercise 4), and in particular it differs from A.

2. Let A be a factorial ring.

1. Suppose that $a \in A \setminus A^\times$, $a \neq 0$, with $a = \prod_{i=1}^k r_i^{n_i}$ for some $k, n_i \in \mathbb{Z}_{>0}$ and some irreducible elements $r_i \in A$ such that $r_i A \neq r_j A$ for $i \neq j$. Prove that for every $b \in A$, we have that b divides a if and only if we can write

$$b = u \prod_{i=1}^{k} r_i^{m_i}, \text{ for some } u \in A^\times \text{ and } 0 \leq m_i \leq n_i \text{ for all } i.$$

2. Let A be a PID, and $a, b \in A$ elements of the form $a = \prod_{i=1}^k r_i^{n_i}$ and $b = \prod_{j=1}^l s_j^{m_j}$, where $r_i, s_j \in A$ are all irreducible elements, $k, l, m_i, n_j \in \mathbb{Z}_{>0}$, and $r_i A \neq r_{i'} A$ for $i \neq i'$ and $s_j A \neq s_{j'} A$ for $j \neq j'$. Prove that a gcd (defined as in Exercise 1) of a and b is

$$d = \prod_{h=1}^{f} q_h^{l_h},$$

where

- $\{q_1, \ldots, q_f\}$ is a finite subset of irreducible elements of A,
- $q_\alpha A \neq q_\beta A$ for $\alpha \neq \beta$,
- $\forall h \in \{1, \ldots, f\}$, there exist i, j such that $q_h A = r_i A = s_j A$ and $l_h = \min(m_i, n_j)$.

Solution:

1. The "if" part is easy: for b of the given form, we have that

$$a = \prod_{i=1}^{k} r_i^{n_i} = u\big(\prod_{i=1}^{k} r_i^{m_i}\big)u^{-1} \prod_{i=1}^{k} r_i^{n_i - m_i} = bu^{-1} \prod_{i=1}^{k} r_i^{n_i - m_i},$$

so that $b|a$.

Conversely, assume that $b|a$, and write $a = bc$ for some $c \in A$. As A is a UFD, b and c both have a decomposition into irreducible elements, $b = \prod_{h \in H} s_h$ and $c = \prod_{j \in J} q_j$. Multiplying those two decompositions together we obtain a decomposition into irreducibles for a. Then, again because A is a UFD, there is a bijection of indexes $\gamma : H \sqcup J \to \bigcup_{i=1}^{r} \bigsqcup_{\alpha=1}^{n_i} \{i\}$ such that each s_h or q_j is equivalent to the corresponding r_i (that is, they are equal up to multiplying by a unit). In particular, we have that for each $h \in H$ there exists $u_h \in A^\times$ such that $s_h = u_h r_{\gamma(h)}$, and as γ is a bijection, for each $i \in I$ we have that $0 \leq m_i := |\{h \in H : i = \gamma(h)\}| \leq n_i$. So we can conclude that

$$b = \prod_{h \in H} s_h = \prod_{h \in H} u_h r_{\gamma(h)} = u \prod_{i=1}^{k} r_i^{m_i},$$

where $u = \prod_{h \in H} u_h$.

See next page!

2. Now let $a = \prod_{i=1}^k r_i^{n_i}$ and $b = \prod_{j=1}^l s_j^{m_j}$, and let d be a greatest common divisor of them. Then $d|a$ and $d|b$, so that applying previous point twice, we can write, for some $u, v \in A^\times$ and some integers $0 \le \lambda_i \le n_i$ and $0 \le \mu_j \le m_j$,

$$u \prod_{i=1}^k r_i^{\lambda_i} = d = v \prod_{j=1}^l s_j^{\mu_j}.$$

Then, as A is a UFD, and using the hypothesis that the r_i's (resp., the s_j's) are pairwise non-equivalent, we get a bijection

$$\vartheta : I' := \{i : \lambda_i \neq 0\} \to J' := \{j : \mu_j \neq 0\},$$

such that $s_{\vartheta(i)} = w_i r_i$ and $\mu_{\vartheta(i)} = \lambda_i$ for all $i \in I'$, where $w_i \in A^\times$. Notice that $\lambda_i = \mu_{\vartheta(i)} \le n_i, m_{\vartheta(i)}$ for each $i \in I'$, but that if such an inequality is strict for both n_i and $m_\vartheta(i)$, then by multiplying $r_i \cdot d$ would still divide both a and b, contradicting maximality of d (as $r_i d \nmid d$, since $r_i \notin A^\times$). Hence $\lambda_i = \mu_{\vartheta(i)} = \min(n_i, m_{\vartheta(i)})$. The statement is proven by "renaming" some indexes and elements:
Take $f := |I'|$, $H = \{1, \ldots, f\}$ fix a bijection $\xi : H \to I'$. Then define, for all $h \in H$, $q_t = r_{\xi(h)}$. Those are clearly irreducible pairwise non-equivalent elements of A. The last of the three conditions is finally satisfied by taking $i = \xi(h)$ and $j = \vartheta(\xi(h))$ for each $h \in H$.

3. (*) (Another formulation of the classification of finitely generated torsion modules) Let A be a PID and $M \neq 0$ a finitely generated torsion module. Show that there exists $k \ge 1$ and elements $a_1 | a_2 | \cdots | a_k \in A$ such that $a_i \neq 0$, $a_i \notin A^\times$ for all i and

$$M \cong A/a_1 A \oplus \cdots \oplus A/a_k A.$$

[*Hint:* Use the classification you have seen in class and the Chinese Remainder Theorem]

Solution:

By classification for finitely generated torsion modules over a PID, we have that there exist finitely many (pairwise non-equivalent) irreducible elements $p_1, \ldots, p_m \in A$ such that $M \cong \bigoplus_{i=1}^m M(p_i)$ (taking only the irreducible elements p such that $M(p) \neq 0$, which can be proven to be finitely many), and for each i there exist a positive integer s_i and positive integers $\nu_{i,1} \le \cdots \le \nu_{i,s_i}$ such that

$$M(p_i) \cong \bigoplus_{j=1}^{s_i} A/p_i^{\nu_{i,j}} A.$$

Let now $k = \max_i(s_i)$. We add some zeroes in the beginning of the sequences of exponents $(\nu_{i,1}, \ldots, \nu_{i,s_i})$ in order to make them all of length k. More precisely, we define, for $1 \le i \le m$ and $1 \le j \le k$,

$$v_{ij} = \begin{cases} 0 & \text{if } j \le k - s_i \\ \nu_{i,j-(k-s_i)} & \text{if } j > k - s_i \end{cases}$$

Then clearly we have that $v_{i,j} \leq v_{i,j+1}$, for each i and j for which the two sides are defined, so that $p_i^{v_{i,j}} | p_i^{v_{i,j+1}}$. Moreover, as $p_i^0 = 1$ for each i and $A/1A = 0$, we have that

$$M(p_i) \cong \bigoplus_{j=1}^{s_i} A/p_i^{\nu_{i,j}} A \cong \bigoplus_{j=1}^{k} A/p_i^{v_{i,j}} A.$$

Next, define $a_j = \prod_{i=1}^m p_i^{v_{i,j}}$ for $1 \leq j \leq k$ and notice that $a_j | a_{j+1}$ for $1 \leq j \leq k-1$, with $a_j \neq 0$ for each j as it is a product of irreducible elements. Furthermore, $a_1 \notin A^\times$ (so that non of the a_j is a unit being divisible by a_1), since by maximality of k we have that $v_{i1} \neq 0$ for some i, for which then $p_i | a_1$. The a_j satisfy the desired divisibility property, and we are done if we prove the required isomorphism. We have

$$M \cong \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{k} A/p_i^{v_{i,j}} A \cong \bigoplus_{j=1}^{k} \bigoplus_{i=1}^{m} A/p_i^{v_{i,j}} A \cong \bigoplus_{j=1}^{k} A/a_j A,$$

where the last isomorphism is obtained by applying Chinese Remainder Theorem, which can be done since the p_i are pairwise non-equivalent, so that the $p_i^{v_{i,j}}$ are pairwise coprime.

4. Let G be a finite abelian group generated by two elements.

1. Show that
$$G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_1 d_2 \mathbb{Z},$$
where $d_1, d_2 \geq 1$ are integers.
2. For every prime p, determine $G(p)$.

Solution:

1. Let $G = \langle a, b \rangle$, $\alpha = \mathrm{ord}_G(a)$ and $\beta = \mathrm{ord}_G(b)$. By the classification theorem for modules over a PID (which can be applied since $\mathbb{Z}$ is a PID), we have that $G \cong \bigoplus G(p)$, as G is torsion, where the sum ranges on positive prime numbers, and $G(p) = 0$ for almost all p. Then for each prime p we have a canonical projection $\pi_p : G \to G(p)$, and $G(p)$ is generated by $\pi_p(a)$ and $\pi_p(b)$. Still by the classification theorem for finitely generated modules, we can then write, for each p,
$$G(p) = \mathbb{Z}/p^{u_p}\mathbb{Z} \oplus \mathbb{Z}/p^{v_p}\mathbb{Z},$$
with $u_p \leq v_p$, and $v_p \neq 0$ for only finitely many primes p. Then using the same argument of the previous exercise (with $M = G$, $R = \mathbb{Z}$ and $k = 2$), we obtain that $G \cong \mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/a_2\mathbb{Z}$, with $a_1 | a_2$ (those two numbers are equal, respectively, to the products $\prod_p p^{u_p}$ and $\prod_p p^{v_p}$). Choosing $d_1 = a_1$ and $d_2 = a_2/a_1$ we obtain
$$G = \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_1 d_2 \mathbb{Z},$$
as desired.

See next page!

2. By construction, for each prime p we have that $G(p) = \mathbb{Z}/p^{u_p}\mathbb{Z} \oplus \mathbb{Z}/p^{v_p}\mathbb{Z}$, where u_p and v_p are the exponents with which p appears in the factorization into primes of the numbers d_1 and d_1d_2, respectively. In particular, $G(p) = 0$ if and only if $p \nmid d_1$ and $p \nmid d_2$. Moreover, $G(p)$ is cyclic of order p^k if and only if $p \nmid d_1$ and $p^k || d_2$ (i.e., $p^k | d_2$ but $p^{k+1} \nmid d_2$). The only other possibility is that $p|d_1$ and $p|d_2$. in which case $G(p)$ is not cyclic.

5. Let G be a finite abelian group and H be a subgroup of G. Prove: there exists a subgroup $H' \leq G$ such that $H' \cong G/H$. [*Hint:* Abelian groups are $\mathbb{Z}$-modules]

Solution:

By the classification theorem for modules over a PID (which can be applied since $\mathbb{Z}$ is a PID), we have that there exists finitely many (eventually zero) positive prime numbers $p_1, \ldots, p_m$ such that $G = \bigoplus_{i=1}^m G(p_i)$ and $G(p_i) \neq 0$. Now we claim that for any subgroup $H \leq G$ we have $H(p_i) \leq G(p_i)$. This will allow us to restrict our attention to p-groups, as a direct sum of quotients over coprime subgroups can be seen as a quotient by the Chinese Remainder Theorem.

To prove the claim, it is enough to check that if A_1, A_2 and C are abelian groups with $C = A_1 \oplus A_2$, with $a_1 = |A_1|$ and $a_2 = |A_2|$ coprime numbers, then for every subgroup $D \leq C$ we have $D = p_1(D) \oplus p_2(D)$, where the maps $p_i : C \to A_i$ are the canonical projection. Indeed, we have by definition of direct sum the inclusion "$\subseteq$". Moreover, we have $D = \alpha_1\alpha_2$ for some uniquely determined $\alpha_i | a_i$ (as a_1 and a_2 are coprime). Also, $p_i(D) \leq A_i$, so that by Lagrange's Theorem $|p_i(D)|$ divides a_i, but it also divides $|D|$ (easily seen via the map p_i), so that $|p_i(D)|$ has to divide α_i, and $|p_1(D) \oplus p_2(D)| = |p_1(D)| \cdot |p_2(D)| \leq \alpha_1\alpha_2 = |D|$, which together with the previous inclusion gives equality.

Hence without loss of generality we can assume that $G = G(p)$ for some prime number p, that is, G is an abelian p-group. Then $H \leq G$ is also an abelian p-group, and so is $K := G/H$. Then the classification of finitely generated torsion module allows us to write down G and K as finite direct sums of cyclic groups of order equal to a prime power, and we know that the number of direct summands in this decomposition is equal to the minimal number of generators of the group. Since generators of G are mapped via the quotient map $p : G \to K$ to generators of K, we have some integers $1 \leq k$, $1 \leq v_1 \leq \cdots \leq v_k$ and $0 \leq w_1 \leq \cdots \leq w_k$ such that

$$G \cong \bigoplus_{i=1}^{k} \mathbb{Z}/p^{v_i}\mathbb{Z} \text{ and } K \cong \bigoplus_{i=1}^{k} \mathbb{Z}/p^{w_i}\mathbb{Z}.$$

To conclude, it is enough to prove that $w_i \leq v_i$ for every $i = 1, \ldots, k$, because then we can embed $\mathbb{Z}/p^{w_i}\mathbb{Z} \cong p^{v_i - w_i}\mathbb{Z}/p^{v_i}\mathbb{Z} \subseteq \mathbb{Z}/p^{v_i}\mathbb{Z}$ for each i. Suppose by contradiction that this does not hold, with $w_j > v_j$ for some maximal j, so that $v_j < w_j \leq w_{j+1} \leq v_{j+1}$.

Please turn over!

Then

$$p^{v_j}G \cong \bigoplus_{i=j+1}^{k} \mathbb{Z}/p^{v_i - v_j}\mathbb{Z} \text{ and } p^{v_j}K \cong \bigoplus_{i=j}^{k} \mathbb{Z}/p^{w_i - v_j}\mathbb{Z},$$

so that the minimal number of generators of $p^{v_j}G$ is strictly smaller than $k - j$, while the minimal number of generators of $p^{v_j}K$ is precisely $k - j$. But $p^{v_j}K = p^{v_j}(G/H) = (p^{v_j}GH)/H = (p^{v_j}G)/(p^{v_j}G \cap H)$ by Exercise 2 from Exercise sheet 4, so that $p^{v_j}K$ is a quotient of $p^{v_j}G$, contradiction (as generators of the latter are mapped by the quotient map to generators of the former).