NOTES 3

Throughout A is PID.

1. Basic Definitions

The set of *non-zero* prime ideals of A will be denoted S. Thus

$$S = \{\mathfrak{p} \mid \mathfrak{p} \text{ is a prime ideal of } A \text{ and } \mathfrak{p} \neq 0\}.$$

- If $I = (a)$ is an ideal and M a module, then (as before), we write

$$\begin{aligned}\Gamma_I(M) &= 0 \underset{M}{:} I \\ &= \{x \in M \mid \text{there exists } n \geq 0 \text{ such that } a^n x = 0\} \\ &= \varinjlim_n \operatorname{Hom}_A(A/I^n,\, M)\end{aligned}$$

- If $x \in M$, the *annihilator of* x is the ideal

$$\operatorname{ann}(x) = \{a \in A \mid ax = 0\}.$$

  A *period of* x is a generator of $\operatorname{ann}(x)$. Note that periods are unique up to multiplication by a unit, and we often write "the" period of x instead of "a" period of x. Note that the period of x is non-zero if and only if $x \in M_{\text{tor}}$, and $x = 0$ if and only if its period is a unit.
- The *annihilator of* M is the ideal

$$\operatorname{ann}(M) = \bigcap_{x \in M} \operatorname{ann}(x).$$

  An *non-zero* element of $\operatorname{ann}(M)$ is called an *exponent* of M. Clearly M has an exponent only if M is a torsion module, i.e., only if $M = M_{\text{tor}}$. A sufficient condition for a torsion module M to have an exponent is that M is finitely generated. This is not necessary however. Indeed let M be an infinite direct sum of the $\mathbb{Z}$-module $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number, and regard this as a $\mathbb{Z}$-module. Then p is an exponent of M, even though M is not finitely generated.
- For a module M and for $\mathfrak{p} \in S$, define the $\mathfrak{p}$-*socle* of M to be the submodule $\operatorname{soc}_{\mathfrak{p}}(M) = \operatorname{Hom}_A(A/\mathfrak{p},\, M)$. If $\kappa(\mathfrak{p}) = A/\mathfrak{p}$, then $\operatorname{soc}_{\mathfrak{p}}(M)$ is a $\kappa(\mathfrak{p})$ vector space.
- For a module M and an element $x \in M$, the symbol (x) will denote the submodule of M generated by x. In other words

$$(x) = Ax.$$

  A module M is said to be *cyclic* if $M = (x)$ for some $x \in M$.

2. **Torsion modules over PIDs**

Recall that an A-module is called *torsion* if $M_{\text{tor}} = M$.

Date: September 1, 2015.

2.1. We begin with a general description of torsion A-modules. It can be regarded as a primary decomposition theorem, except we do not assume M is finitely generated.

Proposition 2.1.1. *Let M be a torsion module. Then*

$$M = \bigoplus_{\mathfrak{p} \in S} \Gamma_{\mathfrak{p}}(M). \tag{2.1.1.1}$$

More precisely, the submodule $\sum_{\mathfrak{p} \in S} \Gamma_{\mathfrak{p}}(M)$ of M is an internal direct sum of the constituent summands.

Remark: Since the decomposition (2.1.1.1) is an internal direct sum, it is a canonical decompostion.

Proof. Let $x \in M$ and let $\operatorname{ann}(x) = (a)$. Then $a = \pi^{r_1} \dots \pi_l^{r_l}$ where for $i = 1, \dots, l$, π_i are distinct prime elements and r_i positive integers. By the Chinese Remainder Theorem, $A/(a) \xrightarrow{\sim} \prod_{i=1}^{l} A/(\pi_i^{r_i})$. Let $e_i \in A/(a)$, $i = 1, \dots, l$ be the element corresponding to $(0, \dots, 0, 1, 0 \dots, 0) \in \prod_{i=1}^{l} A/(\pi_i^{r_i})$ where the 1 is in the i-th spot of the l-tuple. Then $\sum_{i=1}^{l} e_i = 1 \in A/(a)$. Since Ax is an $A/(a)$-module, we have $x = (e_1 + \dots + e_l)x = \sum_{i=1}^{l} e_i x$. Now $\pi^{r_i} e_i = 0$ by definition of e_i. Hence $e_i x \in \Gamma_{(\pi_i)}(M)$. Thus $x \in \sum_{\mathfrak{p} \in S} \Gamma_{\mathfrak{p}}(M)$. Hence $M = \sum_{\mathfrak{p} \in S} \Gamma_{\mathfrak{p}}(M)$.

Next suppose $\mathfrak{p}_i \in S$, $i = 1, \dots, n$, are distinct prime ideals and $x_i \in \Gamma_{\mathfrak{p}_i}(M)$ are elements such that $x_1 + \dots + x_n = 0$. We have to show that $x_i = 0$ for each i. This will prove the proposition. Let N be a positive number such that $\pi_i^N x_i = 0$. Such an N clearly exists. Now π_1^N and $(\pi_2 \dots \pi_n)^N$ are clearly coprime. Let a and b be elements of A such that $a\pi_1^N + b(\pi_2 \dots \pi_n)^N = 1$. Then

$$\begin{aligned} x_1 &= (a\pi_1^N + b(\pi_2 \dots \pi_n)^N)x_1 \\ &= b(\pi_2 \dots \pi_n)^N x_1 \\ &= -b(\pi_2 \dots \pi_n)^N (x_2 + \dots + x_n) \\ &= 0. \end{aligned}$$

The same argument shows that $x_j = 0$ for every j. This completes the proof. □

2.2. Finitely generated $\mathfrak{p}$-torsion modules. For this subsection. Fix $\mathfrak{p} \in S$, say $\mathfrak{p} = (\pi)$. A module M is said to be $\mathfrak{p}$-torsion if $\Gamma_{\mathfrak{p}}(M) = M$. If M is $\mathfrak{p}$-torsion and $x \in M$, then the period of x must be of the form π^k for a suitable $k \geq 0$. In greater detail, we know that $\pi^n x = 0$ for some $n \geq 1$. If a is a period of x, then $a \mid \pi^n$, giving the result. In particular if $a \in A$ is such that $\pi \nmid a$, then the A-map $\mu_a \colon M \to M$ given by $x \mapsto ax$ is necessarily injective.

Fix a *finitely generated* $\mathfrak{p}$*-torsion* module M. Since M is finitely generated and torsion, $\operatorname{ann}(M) \neq 0$ and hence M has an exponent. Let $x \in M$ be an element such that the period of x is an exponent of M. Since M is finitely generated, such an x exists. To see this let $\operatorname{ann}(M) = (a)$. Then $a = u\pi^r$ for a suitable non-negative integer n and a unit u. Indeed, suppose $a = \pi^r b$ with $\pi \nmid b$. Then $0 = \mu_a = \mu_b \circ \mu_{\pi^r}$. However, as we pointed out, μ_b is an injective map, whence $\mu_{\pi^r} = 0$, and hence $\pi^r \in \operatorname{ann}(M)$. It follows that b is a unit, as claimed. Thus we may may set $a = \pi^r$. If $r = 0$, then $M = 0$ and clearly the period of $x = 0$ is an exponent of M. Otherwise, there exists $x \in M$ such that $\pi^{r-1}x \neq 0$, and clearly the period of such an x is π^r.

With M and x as above (i.e., M finitely generated and $\mathfrak{p}$-torsion, and $x \in M$ such that the period of x is an exponent of M), set

$$\overline{M} := M/(x).$$

Definition 2.2.1. If $\bar{y} \in \overline{M}$ and $y \in M$ is an element mapping to $\bar{y}$ under the canonical surjection $M \twoheadrightarrow \overline{M}$, then we say that y is a *representative* of $\bar{y}$ (or y *represents* $\bar{y}$). We say y is a *special representative* of $\bar{y}$ if the period of y equals the period of $\bar{y}$.

Lemma 2.2.2. *Let $\bar{y} \in \overline{M}$. Then there exists a special representative of $\bar{y}$ in M.*

Proof. First pick any representative y of $\bar{y}$. Let π^r be the period of x. Suppose π^n is the period of $\bar{y}$. Then $\pi^{n-1}y \neq 0$ (for $\pi^{n-1}\bar{y} \neq 0$). Moreover $\pi^n y \in (x)$, say $\pi^n y = bx$, $b \in A$. We may write $b = c\pi^s$ where $\pi \nmid c$. Then $\pi^n y = c\pi^s x$. If $s \geq r$, then $\pi^n y = 0$ and hence π^n is a period of y, i.e., y is a special representative of $\bar{y}$. Otherwise, $s < r$ and $\pi^{n+r-s}y = 0$, and in fact π^{n+r-s} is a period of y. It follows that $n + r - s \leq r$ since r is an exponent of M. Hence $s - n \geq 0$. Now $y - c\pi^{s-n}x$ represents $\bar{y}$ and clearly $\pi^n(y - c\pi^{s-n}x) = 0$. Hence $y - c\pi^{s-n}x$ is a special representative of $\bar{y}$. □

Definition 2.2.3. We shall say elements $y_1, \ldots, y_n$ in M are *independent* if the y_i are non-zero and $\sum_{i=1}^n (y_i) = \bigoplus_{i=1}^n (y_i)$. Equivalently, $y_1, \ldots, y_n$ are independent if $y_i \neq 0$ for $i = 1, \ldots, n$ and any relation of the form $\sum_{i=1}^n a_i y_i = 0$ with $a_i \in A$ implies that $a_i y_i = 0$ for $i = 1, \ldots, n$.

Note that independence does not mean imply linear independence.

Lemma 2.2.4. *If $\bar{y}_1, \ldots, \bar{y}_n \in \overline{M}$ are independent and $y_1, \ldots, y_n \in M$ are elements such that each y_i $(i = 1, \ldots, n)$ is a special representative of $\bar{y}_i$, then $x, y_1, \ldots, y_n$ are independent.*

Proof. Suppose $ax + a_1 y_1 + \cdots + a_n y_n = 0$ for a, a_i in A. Then $\sum_{i=1}^n a_i \bar{y}_i = 0$. Since the $\bar{y}_i$ are independent, this means $a_i \bar{y}_i = 0$. But the period of y_i is the period of $\bar{y}_i$ for each i, and hence $a_i y_i = 0$. In greater detail, suppose π^{r_i} is the common period of y_i and $\bar{y}_i$. Then $a_i \bar{y}_i = 0$ implies that $\pi^{r_i} \mid a_i$. It follows that $a_i y_i = 0$. This means $ax = 0$. Hence $x, y_1, \ldots, y_n$ are independent. □

Lemma 2.2.5. *Let $k = A/\mathfrak{p}$. Then* $\dim_k \operatorname{soc}_{\mathfrak{p}}(\overline{M}) < \dim_k \operatorname{soc}_{\mathfrak{p}}(M)$.

Proof. Now for any $\mathfrak{p}$-torsion module N, elements $x_1, \ldots, x_l \in \operatorname{soc}_{\mathfrak{p}}(N)$ are independent if and only if the are linearly independent over k. Indeed an direct sum decomposition $\sum_{i=1}^l (x_i) = \bigoplus_{i=1}^l (x_i)$ remains valid whether thought of over A or over k. Let $\bar{y}_1, \ldots, \bar{y}_n \in \operatorname{soc}_{\mathfrak{p}}(\overline{M})$ be a k-basis for $\operatorname{soc}_{\mathfrak{p}}(\overline{M})$. Since they are independent, by Lemma 2.2.4 $x, y_1, \ldots, y_n$ are independent in M, where the y_i are special representatives of the $\bar{y}_i$. Since the period of $\bar{y}_i$ is π for every i, it follows that the period of y_i is π for every i. Hence $y_i \in \operatorname{soc}_{\mathfrak{p}}(M)$ for every M. Now if π^r is the period of x, then $\pi^{r-1}x \in \operatorname{soc}_{\mathfrak{p}}(M)$. Moreover, $\pi^{r-1}x, y_1, \ldots, y_n$ are independent. Therefore they are linearly independent over k in $\operatorname{soc}_{\mathfrak{p}}(M)$. The lemma follows. □

Remark 2.2.6. It is easy to see that if M is cyclic then $M \cong A/\mathfrak{p}^s$ for some $s \geq 1$. Indeed, suppose $M = (x)$. Then $\operatorname{ann}(x) = (\pi^s)$ for some $s \geq 1$.

Proposition 2.2.7. *M is isomorphic to a direct sum of cyclic modules.*

Proof. This is proved by induction on $d(M) = \dim_k \operatorname{soc}_{\mathfrak{p}}(M)$. The statement is clearly true if $d(M) = 0$, for in that case $M = 0$. If $d_M = 1$, then $d(\overline{M}) = 0$, whence $\overline{M} = 0$. This means $M = (x)$. Now suppose $d(M) > 1$ and the statement of the proposition is true for all finitely generated $\mathfrak{p}$-torsion modules N with $d(N) < d(M)$. Then by Lemma 2.2.5 and our induction hypothesis, $\overline{M} = \bigoplus_{i=1}^{l}(\bar{y}_i)$. If $y_1, \ldots, y_n$ are representatives of $\bar{y}_1, \ldots, \bar{y}_n$ respectively, then clearly $x, y_1, \ldots, y_n$ generate M. If further $y_1, \ldots, y_n$ are special representatives then Lemma 2.2.4 gives us that $M = (x) \oplus \bigoplus_{i=1}^{l}(y_i)$ and we are done. □

Proposition 2.2.8. *Suppose $L = \bigoplus_{i=1}^{s}(A/\mathfrak{p}^i)^{l_i}$ and $N = \bigoplus_{i=1}^{t}(A/\mathfrak{p}^i)^{n_i}$ are isomorphic. Then $s = t$ and and $l_i = n_i$ for $i = 1, \ldots, s$.*

Proof. For any finitely generated $\mathfrak{p}$-torsion module T, let us define $e(T)$ to be the non-negative integer such that $(\pi^{e(T)}) = \operatorname{ann}(T)$. If T and T' are isomorphic, clearly $e(T) = e(T')$.

Now $e(L) = s$ and $e(N) = t$. Since $L \cong N$ therefore $s = t$. We prove the proposition by induction on $e(L)(= e(N))$.

Clearly $\operatorname{soc}_{\mathfrak{p}}(L) \cong \operatorname{soc}_{\mathfrak{p}}(N)$. But $\operatorname{soc}_{\mathfrak{p}}(L) = k^{l_1}$ and $\operatorname{soc}_{\mathfrak{p}}(N) = k^{n_1}$. Thus $l_1 = n_1$. Now, $\pi L \xrightarrow{\sim} \bigoplus_{i=2}^{s}(A/\mathfrak{p}^{i-1})^{m_i}$ and $\pi N \xrightarrow{\sim} \bigoplus_{i=2}^{s}(A/\mathfrak{p}^{i-1})^{n_i}$. Moreover $\pi L \cong \pi N$ and $e(\pi L) = e(\pi N) = s - 1$. Our induction hypothesis therefore applies, and we have $l_i = n_i$ for $i = 2, \ldots, s$. □

We are now ready to state the main theorem of this section

Theorem 2.2.9. *Let M be as in this subsection, i.e., M is finitely generated and $\mathfrak{p}$-torsion. Let $M \neq 0$. Then*

$$M \cong \bigoplus_{i=1}^{r} A/\mathfrak{p}^{\nu_i}$$

with $1 \leq \nu_1 \leq \nu_2 \leq \cdots \leq \nu_r$. The sequence of integers $\nu_1 \leq \cdots \leq \nu_r$ is unique.

Proof. This follows immediately from Proposition 2.2.7 and Proposition 2.2.9. □

2.3. Structure theorem for finitely generated torsion modules. In this subsection M is a finitely generated torsion module. Recall that according to Proposition 2.1.1 we have a canonical decomposition $M = \bigoplus_{\mathfrak{p} \in S} \Gamma_{\mathfrak{p}}(M)$. This decomposition does not need the hypothesis that M is finitely generated. However, since M is finitely generated, each $\Gamma_{\mathfrak{p}}(M)$ is finitely generated, and clearly $\Gamma_{\mathfrak{p}}(M)$ is $\mathfrak{p}$-torsion. Let $\operatorname{Supp}(M) = \{\mathfrak{p} \in S \mid \Gamma_{\mathfrak{p}}(M) \neq 0$. Since M is finitely generated $\operatorname{Supp}(M)$ is a finite set, say $\operatorname{Supp}(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. In fact, if $\operatorname{ann}(M) = (a)$, then $\operatorname{Supp}(M) = \{\mathfrak{p} \in S \mid a \in \mathfrak{p}\}$, and this is a finite set, namely the set $\{(\pi_1), \ldots, (\pi_n)\}$ where π_i are the distinct primes occuring in the factorization $a = u\pi^{r_1} \ldots \pi^{r_n}$ with u a unit and $r_1, \ldots r_n$ positive integers. Theorem 2.2.9 applies to $\Gamma_{\mathfrak{p}}(M)$ and we have a sequence of positive integers, depending only on M and $\mathfrak{p}$, $\nu_1(\mathfrak{p}) \leq \cdots \leq \nu_{r(\mathfrak{p})}$ such that $\Gamma_{\mathfrak{p}}(M) \cong \bigoplus_{i=1}^{r(\mathfrak{p})} A/\mathfrak{p}^{\nu_i(\mathfrak{p})}$.

We state this as a theorem

Theorem 2.3.1. (Structure theorem for modules over a PID, Version-I) *Let $M \neq 0$ be a finitely generated torsion module over A. Then* $\operatorname{Supp} M$ *is a finite set $\{\mathfrak{p}_1, :, \mathfrak{p}_n\}$, and the canonical decomposition* (2.1.1) *reduces to a canonical finite* *decomposition* $M = \bigoplus_{i=1}^{n} \Gamma_{\mathfrak{p}_i}(M)$. *Let* $\mathfrak{p} \in \operatorname{Supp}(M)$. *Then*

$$(*)_{\mathfrak{p}} \qquad \Gamma_{\mathfrak{p}}(M) \cong \bigoplus_{i=1}^{r(\mathfrak{p})} A/\mathfrak{p}^{\nu_i(\mathfrak{p})}$$

with $1 \le \nu_1(\mathfrak{p}) \le \cdots \le \nu_{r(\mathfrak{p})}(\mathfrak{p})$. *The sequence of integers* $(\nu_1(\mathfrak{p}), \ldots, \nu_{r(\mathfrak{p})}(\mathfrak{p}))$ *is the only one which satisfies the properties that a decomposition for* $\Gamma_{\mathfrak{p}}(M)$ *of the form* $(*)_{\mathfrak{p}}$ *exists and the condition* $1 \le \nu_1(\mathfrak{p}) \le \cdots \le \nu_{r(\mathfrak{p})}(\mathfrak{p})$ *holds.*

Remark 2.3.2. Note that $\operatorname{ann}(M) = \mathfrak{p}_1^{\nu_{r(\mathfrak{p}_1)}(\mathfrak{p}_1)} \ldots \mathfrak{p}_n^{\nu_{r(\mathfrak{p}_n)}(\mathfrak{p}_n)}$.

Theorem 2.3.3. (Structure theorem for modules over a PID, Version-II) *Let* $M \neq 0$ *be a finitely generated torsion module over* A. *Then*

$$M \cong A/(q_1) \oplus \cdots \oplus A/(q_l)$$

where $q_1, \ldots, q_l$ *are non-zero elements of* A *such that* $q_1 \mid \cdots \mid q_l$. *The sequence of ideals* $(q_1), \ldots, (q_r)$ *is uniquely determined by the above conditions.*

Remark: This is often referred to as the *Elementary Divisor Theorem* and the essentially unique sequence $(q_1, \ldots, q_l$ are called elementary divisors.

Proof. Consider the decomposition $(*)_{\mathfrak{p}}$ in Theorem 2.3.1 for $\mathfrak{p} \in \operatorname{Supp}(M)$. Then We have for such a $\mathfrak{p}$ an integer $r(\mathfrak{p})$. Let $l = \max_{\mathfrak{p} \in \operatorname{Supp}(M)} r(\mathfrak{p})$. Now suppose $\operatorname{Supp}(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. For each $i \in \{1, \ldots, s\}$ by adding 0's in front of the sequence $\nu_1(\mathfrak{p}_i) \le \cdots \le \nu_{r(\mathfrak{p}_i)}(\mathfrak{p}_i)$ we have a sequence $0 \le \nu_{i1} \le \nu i2 \le \nu_{il}$, with $\nu_{il} = \nu_{r(\mathfrak{p}_i)}$. The sequence $(\nu_{i1}, \ldots, \nu_{il})$ essentially the same as $(\nu_1(\mathfrak{p}_i), \ldots, \nu_{r(\mathfrak{p}_i)}(\mathfrak{p}_i))$ except for a few 0's in front to ensure that the length of the sequence is l and $\nu_{il} = \nu_{r(\mathfrak{p}_i)}$. The data can be arranged as follows:

$$(2.3.4) \qquad \begin{array}{c}
\mathfrak{p}_1 \longleftrightarrow \nu_{11} \le \nu_{12} \le \cdots \le \nu_{1l} \\
\mathfrak{p}_2 \longleftrightarrow \nu_{21} \le \nu_{22} \le \cdots \le \nu_{2l} \\
\vdots \qquad\qquad \vdots \\
\mathfrak{p}_s \longleftrightarrow \nu_{s1} \le \nu_{s2} \le \cdots \le \nu_{sl}
\end{array}$$

Let $\mathfrak{p}_i = (\pi_i)$. Define

$$q_j = \pi_1^{\nu_{1j}} \pi_2^{\nu_{2j}} \ldots \pi_s^{\nu_{sj}}, \qquad j = 1, \ldots, l.$$

Then $q_1 \mid q_2 \mid \cdots \mid q_l$ and clearly (via the Chinese Remainder Theorem)

$$M \cong A/(q_1) \oplus \cdots \oplus A/(q_l)$$

holds. This proves the existence of a decomposition of M via elementary divisors.

The uniqueness assertion regarding the (q_i) in the elementary divisor decomposition of M is proved by observing that arrays such as (2.3.4) are essentially unique. In greater detail, suppose

$$\begin{array}{c}
\mathfrak{p}_1 \longleftrightarrow \mu_{11} \le \mu_{12} \le \cdots \le \mu_{1d} \\
\mathfrak{p}_2 \longleftrightarrow \mu_{21} \le \mu_{22} \le \cdots \le \mu_{2d} \\
\vdots \qquad\qquad \vdots \\
\mathfrak{p}_s \longleftrightarrow \mu_{s1} \le \nu_{s2} \le \cdots \le \mu_{sd}
\end{array}$$

is another array of non-negative numbers associated to the $\mathfrak{p}_i$ such that μ_{i1} is positive for at least one i (i.e., at least one integer in the first column is positive). Suppose $M \cong \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{d} A/\mathfrak{p}_i^{\mu_{ij}}$. Then by Theorem 2.3.1, $d = l$ and $\mu_{ij} = \nu_{ij}$ for $i = 1, \ldots, s$ and $j = 1, \ldots, l$.

Given a direct sum decomposition $M \cong A/(a_1) \oplus \cdots \oplus A/(a_d)$ with $a_1 \mid a_2 \mid \cdots \mid a_d$ ($a_i \geq 1$), we produce such an array. Note that the minimal ideal occurring in the elementary divisor decomposition, namely (a_d), is $\operatorname{ann}(M)$. Thus this ideal is intrinsic to M. It follows from Remark 2.3.2 that the prime ideals containing (a_d) are precisely $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, and the prime divisors of a_d are precisely $\pi_1, \ldots, \pi_s$ for $\operatorname{Supp}(M) = \{(\pi_i) \mid i = 1, \ldots, s\}$. Moreover, since $a_j \mid a_d$ for all $1 \leq j \leq d$, therefore the prime divisors of a_j are a subset of $\{\pi_1, \ldots, \pi_s\}$ and hence for each j we have non-negative integers $\mu_{1j}, \ldots, \mu_{sj}$ such that $a_j = u\pi_1^{\mu_{1j}} \ldots \pi_s^{\mu_{sj}}$. Moreover, since $a_j \mid a_{j+1}$, for a fixed i, the sequence $(\mu_{i1}, \mu_{i2}, \ldots, \mu_{id})$ is non-decreasing. Since (a_1) is a non-trivial ideal, at least one μ_{i1} is positive. Finally clearly, $M \cong \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{d} A/\mathfrak{p}_i^{\mu_{ij}}$. Thus $d = l$, $\mu_{ij} = \nu_{ij}$ for all $i \in \{1, \ldots, s\}$ and all $j \in \{1, \ldots, d\}$, whence $(a_i) = (q_i)$ for $i = 1, \ldots, d$. $\square$