Isomorphism Classes of Almost Completely Decomposable Groups

Dissertation zur Erlangung des
naturwissenschaftlichen Doktorgrades
der Bayerischen Julius–Maximilians–Universität Würzburg

vorgelegt von

Michael Nahler

aus Würzburg

Würzburg 2001

Genie ist Fleiß.

— Joubert

Eingereicht am: 17. Mai 2001

bei der Fakultät für Mathematik und Informatik

1. Gutachter: Prof. Dr. O. Mutzbauer
2. Gutachter: Prof. Dr. H. Heineken

Tag der mündlichen Prüfung: 10. Juli 2001

Danksagung

Ich möchte mich an dieser Stelle bei Professor Mutzbauer für die intensive Betreuung herzlich bedanken. Vieles habe ich aus dem hervorragenden Buch [Mad00] von Professor Mader gelernt. Den größten Dank schulde ich meiner Familie; meiner lieben Mutter und meinem Vater. Die Familie ist immer das Rückgrat von Erfolg und Leistung.

Würzburg, Mai 2001

Michael Nahler

Abstract

In this thesis we investigate near–isomorphism classes and isomorphism classes of almost completely decomposable groups.

In Chapter 2 we introduce the concept of almost completely decomposable groups and sum up their most important facts. A local group is an almost completely decomposable group with a primary regulator quotient. A uniform group is a rigid local group with a homocyclic regulator quotient.

In Chapter 3 a weakening of isomorphism, called type–isomorphism, appears. It is shown that type–isomorphism agrees with Lady's near–isomorphism. By the Main Decomposition Theorem and the Primary Reduction Theorem we are allowed to restrict ourselves on clipped local groups, namely groups without a direct rank–one summand.

In Chapter 4 we collect facts of matrices over commutative rings with an identity element. Matrices over the local ring $\mathbb{Z}/p^e\mathbb{Z}$ play an important role.

In Chapter 5 we introduce representing matrices of finite essential extensions. Here a normal form for local groups is found by the Gauß algorithm. Uniform groups have representing matrices in Hermite normal form.

The classification problems for almost completely decomposable groups up to isomorphism and up to near–isomorphism can be rephrased as equivalence problems for the representing matrices. In Chapter 6 we derive a criterion for the representing matrices of local groups in Gauß normal form.

In Chapter 7 we formulate the matrix criterion for uniform groups. Two representing matrices in Hermite normal form describe isomorphic groups if and only if the rest blocks of the representing matrices are T–diagonally equivalent.

Starting from a fixed near–isomorphism class in Chapter 8 we investigate isomorphism classes of uniform groups. We count groups and isomorphism classes.

In Chapter 9 we specialize on uniform groups of rank $2r$ with a regulator quotient of rank r such that the rest block of the representing matrix is invertible and normed.

Contents

1. Notations

The notation in this thesis follows `Fuchs` [Fuc73] and `Mader` [Mad00]. All appearing groups are additive abelian groups. We investigate torsion–free groups of finite rank and drop the adjective "torsion–free". Finite groups will be explicitly mentioned. We only use the inclusion symbols $\subseteq$, $\supseteq$ and $\subsetneq$, $\supsetneq$. Maps are written on the left.
Let h be a natural number. The factor $\mathbb{Z}/h\mathbb{Z} =: \mathbb{Z}_h$ denotes the ring of residue classes of the rational integers mod h just as the additive cyclic group of order h.

2. Almost Completely Decomposable Groups

Definition 2.1. Suppose that X is a group. With *rank* we mean the dimension of the $\mathbb{Q}$–vector space $\mathbb{Q}X := \langle qx \,|\, q \in \mathbb{Q},\, x \in X\rangle = \{\sum_{i=1}^{n} q_i x_i \,|\, n \in \mathbb{N}, q_i \in \mathbb{Q}, x_i \in X\}$. Short $\operatorname{rk} X = \dim \mathbb{Q}X$. We call $\mathbb{Q}X$ the *divisible hull* of X.

Remark 2.2. We consider a torsion–free group X as a pair $X \subseteq \mathbb{Q}X$. *Rank–one* groups are groups isomorphic to rational groups, i. e. subgroups of $\mathbb{Q}$.

Definition 2.3. Let X be an arbitrary abelian group and n be a natural number. The subgroup

$$X[n] = \{x \in X \mid nx = 0\}$$

is called the *n–socle* of X.

The subgroup $S(X) = \bigoplus_{p\in\mathbb{P}} X[p]$ consists of all $x \in X$ such that $\operatorname{ord}(x)$ is a square–free integer and is said to be the *socle* of X.

Remark 2.4. The socle is 0 if and only if X is torsion–free. For a p–group X we have $S(X) = X[p]$.

One of the most important tools for characterizing groups is the knowledge of divisibilities of elements by primes p. Let us start with basic concepts.

Definition 2.5. Let X be a group, $x \in X$ and p be a prime.

The largest integer k for which $p^{-k}x$ is still in X is called the *p–height* $\operatorname{hgt}_p(x)$ of x; if no such maximal integer exists, i. e. $p^{-k}x \in X$ for all $k \in \mathbb{N}$, we set $\operatorname{hgt}_p(x) = \infty$.

The sequence of p–heights

$$\chi(x) = \big(\operatorname{hgt}_{p_1}(x), \dots, \operatorname{hgt}_{p_i}(x), \dots\big)$$

is said to be the *characteristic* of x, where p_i is standing for the i–th prime. We mean by $\chi_1 \le \chi_2$ that every component of χ_1 is less or equal than the corresponding one in χ_2. Define the pointwise operations

$$\begin{aligned} (k_1, \dots, k_i, \dots) \wedge (l_1, \dots, l_i, \dots) &= (\min(k_1, l_1), \dots, \min(k_i, l_i), \dots) \\ \text{and}\quad (k_1, \dots, k_i, \dots) \vee (l_1, \dots, l_i, \dots) &= (\max(k_1, l_1), \dots, \max(k_i, l_i), \dots) \end{aligned}$$

for any two characteristics.

The *type* $\operatorname{tp}(x)$ of x is the equivalence class of all characteristics χ which have exactly the same ∞–components as $\chi(x)$ and which differ for at most finitely many components with finite entries from $\chi(x)$. For two types τ_1, τ_2 we set $\tau_1 \leq \tau_2$ if there are characteristics χ_1 in τ_1 and χ_2 in τ_2 with $\chi_1 \leq \chi_2$. We define $\tau_1 \wedge \tau_2$ [or $\tau_1 \vee \tau_2$] to be the equivalence class of the characteristic $\chi_1 \wedge \chi_2$ [or $\chi_1 \vee \chi_2$], where χ_1 is a characteristic in τ_1 and χ_2 is a characteristic in τ_2.

A group Y in which all elements $\neq 0$ are of the same type τ is called *homogeneous*. For example there is only one type occurring in a rank–one group. So it makes sense to speak of the type $\operatorname{tp}(Y)$ of a rank–one group Y.

Definition 2.6. Let X be a group. A subgroup U of X is called *pure* if $pX \cap U = pU$ for every prime p. The group

$$U_*^X := \{x \in X \mid \exists_{n\in\mathbb{N}}\, nx \in U\} = X \cap \mathbb{Q}U$$

is the *purification* of U in X.

Remark 2.7. The subgroup U_*^X is the intersection of all pure subgroups of X that contain U. Thus U_*^X is the minimal pure subgroup including U.

Lemma 2.8. [Mad00, Lemma 2.1.7] *Let X be a group and U a subgroup of X. Then the following are equivalent:*

(1) *U is pure in X,*
(2) *X/U is torsion–free,*
(3) *$\forall_{n\in\mathbb{N}}\, nX \cap U = nU$,*
(4) *$U_*^X = U$.*

Lemma 2.9. [Mad00, Lemma 2.1.1] *Let X be a group of finite rank and h a positive integer. Then X/hX is a finite group. Moreover, for every prime p, $\dim(X/hX)[p] \leq \operatorname{rk} X$.*

Definition 2.10. Let A be a torsion–free group of finite rank and h a positive integer. Let

$$\operatorname{FEE}(A, h) = \{X \leq \mathbb{Q}A \mid A \leq X \leq h^{-1}A\}\,.$$

Remark 2.11. For $X \in \operatorname{FEE}(A, h)$ the index $[X : A]$ is finite by Lemma 2.9, and X is a "**f**inite **e**ssential **e**xtension" of A.

For X, $Y \in \operatorname{FEE}(A, h)$,

$$X = Y \qquad \text{if and only if} \qquad X/A = Y/A.$$

Definition 2.12. Let X be an arbitrary group. A subgroup U of X that is carried into itself by every endomorphism [automorphism] of X is said to be a *fully invariant* [*characteristic*] subgroup of X.

Notation 2.13. Let $\mathrm{T}(X)$ denote the set of all types of non–zero elements in the group X.

With every type τ we can associate fully invariant "type–subgroups" of a given group which are useful tools in the theory.

Definition 2.14. Let X be a group and τ a type in X. Define

$$X(\tau) := \{x \in X \mid \mathrm{tp}(x) \geq \tau\}, \quad X^*(\tau) := \langle x \in X \mid \mathrm{tp}(x) > \tau\rangle, \quad X^\sharp(\tau) := X^*(\tau)_*^X.$$

Remark 2.15. Since $\mathrm{tp}(\phi x) \geq \mathrm{tp}(x)$ for any endomorphism ϕ, all type–subgroups are fully invariant. For $m \in \mathbb{N}$, $x \in X$ and $y \in X(\tau)$ with $mx = y \in X(\tau)$ one calculates $\mathrm{tp}(x) = \mathrm{tp}(mx) = \mathrm{tp}(y) \geq \tau$. Hence $x \in X(\tau)$ and $X(\tau)$ is pure in X. Of course $X^\sharp(\tau)$ is pure, too. One sees $X^*(\tau) \subseteq X^\sharp(\tau) \subseteq X(\tau) \subseteq X$.

Definition 2.16. Let X be a group. The type τ is a *critical type* of X if

$$\frac{X(\tau)}{X^\sharp(\tau)} \neq 0\ .$$

Let $\mathrm{T_{cr}}(X)$ denote the set of all critical types of X. If $\mathrm{T_{cr}}(X)$ is an antichain, i. e. if the critical types of X are pairwise incomparable, then X is called *block–rigid*. If $\mathrm{rk}\, X(\tau)/X^\sharp(\tau) = 1$ for all critical types, then X is called *slim*. If X is block–rigid and slim, then X is a *rigid* group.

Definition 2.17. The group A is called *completely decomposable* if it is the direct sum of rank–one groups.

Let $A = \bigoplus_{\rho \in \mathrm{T_{cr}}(A)} A_\rho$ be a direct decomposition into τ–homogeneous completely decomposable summands A_τ. We call the A_τ the *τ–homogeneous components* of A and $A = \bigoplus_{\rho \in \mathrm{T_{cr}}(X)} A_\rho$ a *homogeneous decomposition* of A.

We now define formally a class of torsion–free groups which are the center of attention throughout this thesis and are natural generalizations of completely decomposable groups.

Definition 2.18. An *almost completely decomposable group* is a torsion–free group of finite rank which contains a completely decomposable subgroup of finite index.

Lemma 2.19. (Butler Decomposition) [Mad00, Lemma 4.1.2] *Let X be an almost completely decomposable group and τ a critical type of X. Then*

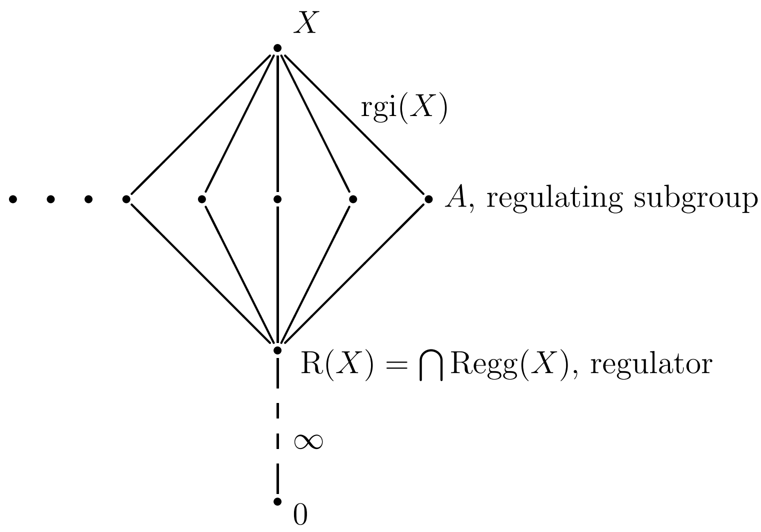
$$X(\tau) = A_\tau \oplus X^\sharp(\tau),$$

and the Butler complement A_τ *is τ–homogeneous completely decomposable and pure in X.*

Definition 2.20. Let X be an almost completely decomposable group, $\mathrm{T}_{\mathrm{cr}}(X)$ its critical typeset, and let $X(\tau) = A_\tau \oplus X^\sharp(\tau)$ be a Butler decomposition for each $\tau \in \mathrm{T}_{\mathrm{cr}}(X)$. The subgroup $A = \sum_{\rho \in \mathrm{T}_{\mathrm{cr}}(X)} A_\rho$ is called a *regulating subgroup* of X. The symbol $\mathrm{Regg}(X)$ denotes the family of all regulating subgroups of X.

The intersection of all regulating subgroups of X is the *regulator* $\mathrm{R}(X)$ of X. If there is only one regulating subgroup, the regulator is called *regulating regulator*.

Remark 2.21. Any two regulating subgroups of X are isomorphic. The number of regulating subgroups for X is finite.



Theorem 2.22. (Lady) [Mad00, Theorem 4.2.13] *Let X be an almost completely decomposable group and A a regulating subgroup of X. Then*

$$[X : A] =: \mathrm{rgi}(X)$$

is an invariant of X, the regulating index. *If B is a completely decomposable subgroup of finite index of X, then* $\mathrm{rgi}(X)$ *divides* $[X : B]$, *and* $[X : B] = \mathrm{rgi}(X)$ *if and only if B is regulating in X. The regulating subgroups are exactly the completely decomposable subgroups of X of minimal index* $\mathrm{rgi}(X)$.

Definition 2.23. Let X be an almost completely decomposable group and τ any type. The *Burkhardt invariants* β_τ^X of X are defined by

$$\beta_\tau^X = \exp \frac{X^\sharp(\tau)}{\mathrm{R}(X^\sharp(\tau))} .$$

Remark 2.24. It is $\beta_\tau^X = \exp \frac{X(\tau)}{\mathrm{R}(X(\tau))}$ for all types τ. If τ is maximal in $\mathrm{T}_{\mathrm{cr}}(X)$, then $\beta_\tau^X = 1$.

We now formulate the important description of the regulator due to Burkhardt [Mad00, Theorem 4.4.4].

Theorem 2.25. (Burkhardt Regulator Theorem) *Let X be any almost completely decomposable group and $A = \bigoplus_{\rho \in \mathrm{T}_{\mathrm{cr}}(X)} A_\rho$ any regulating subgroup of X. Then*

$$\mathrm{R}(X) = \bigoplus_{\rho \in \mathrm{T}_{\mathrm{cr}}(X)} \beta_\rho^X A_\rho \ .$$

Corollary 2.26. [Mad00, Corollary 4.4.5] *Let X be an almost completely decomposable group. Then*

$$\mathrm{R}(X) = \sum_{\rho \in \mathrm{T}_{\mathrm{cr}}(X)} \beta_\rho^X X(\rho) \ .$$

Remark 2.27. Let X be an almost completely decomposable group with regulator R. Then R is a fully invariant and completely decomposable subgroup of finite index in X. If h is the exponent of the regulator quotient X/R, then $R \subseteq X \subseteq h^{-1}R$.

Another important result of Burkhardt [Mad00, Theorem 4.4.6] characterizes the regulator among the completely decomposable subgroups of finite index.

Theorem 2.28. (Burkhardt Regulator Criterion) *Let U be a completely decomposable subgroup of finite index in the almost completely decomposable group X and let $\beta_\tau = \exp \frac{X^\sharp(\tau)}{U^\sharp(\tau)}$ for $\tau \in \mathrm{T}_{\mathrm{cr}}(X)$. Then $U = \mathrm{R}(X)$ if and only if there is a homogeneous decomposition*

$$U = \bigoplus_{\rho \in \mathrm{T}_{\mathrm{cr}}(X)} U_\rho$$

such that for each critical type τ,

$$U_\tau \subseteq \beta_\tau X(\tau) \subseteq U(\tau) \ .$$

The following application of Schlez [Sch98, Lemma 5.2] is a useful tool.

Lemma 2.29. *Let X be an almost completely decomposable group. Let $R = \bigoplus_{j=1}^n R_{\tau_j}$ be a rigid completely decomposable subgroup of finite index and X/R of exponent $m \in \mathbb{N}$. The following are equivalent:*

(1) $\mathrm{R}(X) = R$.
(2) $(R_{\tau_j})_*^X = R_{\tau_j}$ *for all* $j = 1, \dots, n$.
(3) $\frac{X}{R} \cap \frac{m^{-1}R_{\tau_j} + R}{R} = 0$ *for all* $j = 1, \dots, n$.

Proof. "(1)⇔(2)" One has $\tau_j = \mathrm{tp}(R_{\tau_j})$ for $j = 1, \dots, n$. By Burkhardt Regulator Criterion, the regulator of X is R if and only if $R_{\tau_j} \subseteq \beta_{\tau_j} X(\tau_j) \subseteq R(\tau_j)$ for all j, where $\beta_{\tau_j} = \exp[X^\sharp(\tau_j)/R^\sharp(\tau_j)]$. Since R is rigid, one obtains $\beta_{\tau_j} = 1$ and

$R(\tau_j) = R_{\tau_j}$ for all j. Hence $R_{\tau_j} \subseteq X(\tau_j) \subseteq R(\tau_j) = R_{\tau_j}$ with equality. Therefore $(R_{\tau_j})_*^X = [R(\tau_j)]_*^X = X(\tau_j)$ and so $(R_{\tau_j})_*^X = R_{\tau_j}$. Thus R is the regulator of X if and only if all R_{τ_j} are pure subgroups of X.
"(2)⇔(3)" By definition $(R_{\tau_j})_*^X = R_{\tau_j}$ if and only if $R_{\tau_j} \cap kX = kR_{\tau_j}$ for all $k \in \mathbb{N}$ and $j = 1, \dots, n$. Here $R_{\tau_j} \cap mX = mR_{\tau_j}$ implies the purity:

$$X/R_{\tau_j} \cong mX/mR_{\tau_j} = mX/(R_{\tau_j} \cap mX) \cong (mX + R_{\tau_j})/R_{\tau_j} \subseteq R/R_{\tau_j},$$

i. e. X/R_{τ_j} is torsion–free, since R/R_j is torsion-free, and therefore R_{τ_j} is pure in X. Hence the purity of R_{τ_j} is equivalent to $R_{\tau_j} \cap mX = mR_{\tau_j}$. Since all groups are torsion–free, this is equivalent to $m^{-1}R_{\tau_j} \cap X = R_{\tau_j}$, so $(m^{-1}R_{\tau_j} + R) \cap X = R$. Consideration modulo R implies the claim. □

Definition 2.30. An almost completely decomposable group X is called *p–local* for a prime p if $X/\mathrm{R}(X)$ is a (finite) p–group, where $\mathrm{R}(X)$ is the regulator of X. Groups with an arbitrary regulator quotient are called *global*.

Remark 2.31. A group X is p–local if and only if X has a regulating subgroup U such that X/U is a p–group, equivalently the regulating index $\mathrm{rgi}(X)$ is a power of p. Therefore X is called a *p–primary regulating quotient group*, too.

Definition 2.32. Let p be a prime and e, n, r natural numbers. Let $T = (\tau_1, \dots, \tau_n)$ be an ordered n–tuple of pairwise incomparable types with p–height $0 = \tau_j(p)$. Then $\mathcal{C}(T, p, e, r)$ denotes the class of almost completely decomposable groups X such that

(1) $T = \mathrm{T}_{\mathrm{cr}}(X)$ is the critical typeset of X,
(2) X is rigid, i. e. $X(\tau)$ has rank 1 for all $\tau \in T$,
(3) $\mathrm{rk}\, X = n$,
(4) the regulator quotient is homocyclic of exponent p^e, i. e. $X/\mathrm{R}(X) \cong (\mathbb{Z}_{p^e})^r = \underbrace{\mathbb{Z}_{p^e} \oplus \mathbb{Z}_{p^e} \oplus \cdots \oplus \mathbb{Z}_{p^e}}_{r}$ is a direct sum of r copies of $\mathbb{Z}_{p^e}$.

We call such groups X *uniform*.

Remark 2.33. Since such a uniform group X is rigid, one has $\mathrm{R}(X) = \bigoplus_{j=1}^n X(\tau_j)$.

Definition 2.34. Let p be a prime. A group D is said to be *p–divisible* if $pD = D$. If the group X has no non–trivial p–divisible subgroup, then X is called *p–reduced*.

Remark 2.35. Each uniform group $X \in \mathcal{C}(T, p, e, r)$ is p–local and p–reduced.

3. Near–Isomorphism

Definition 3.1. (Lady) Let X and Y be groups of finite rank. Then X and Y are called *nearly isomorphic*, in symbols $X \cong_{\mathrm{nr}} Y$, if for every positive integer n, there is a monomorphism $\phi_n : X \to Y$ such that $[Y : \phi_n X]$ is finite and $\gcd(n, [Y : \phi_n X]) = 1$.

Remark 3.2. Near–isomorphism is a weakening of isomorphism. Isomorphic groups are nearly isomorphic, too. Use the isomorphism for all monomorphisms ϕ_n of the definition.

Remark 3.3. Let R be a completely decomposable group and h a positive integer. The map

$$\overline{} : R \to \overline{R} = h^{-1}R/R, \; x \mapsto \overline{x} = h^{-1}x + R$$

denotes the natural epimorphism. Furthermore, $\overline{}$ will denote as well the induced homomorphism

$$\overline{} : \operatorname{Aut} R \to \operatorname{Aut} \overline{R}, \; \alpha \mapsto \overline{\alpha} \quad \text{via} \quad \overline{\alpha}(\overline{x}) := \overline{\alpha(x)}.$$

This definition is well–defined, since $\overline{x} = \overline{x'}$, i. e. $h^{-1}x + R = h^{-1}x' + R$, implies $x = x' + hr$ for a suitable $r \in R$. Then we get $\overline{\alpha}(\overline{x}) = \overline{\alpha(x)} = h^{-1}\alpha(x) + R = h^{-1}\alpha(x' + hr) + R = h^{-1}\alpha(x') + \underbrace{h^{-1}\alpha(hr)}_{\in R} + R = \overline{\alpha(x')} = \overline{\alpha}(\overline{x'})$ and the definition does not depend on the representative of $\overline{x} = \overline{x'}$. Let

$$\overline{\operatorname{Aut} R} = \{\overline{\alpha} \mid \alpha \in \operatorname{Aut} R\}$$

denote the *set of induced automorphisms* of $\overline{R}$.

Definition 3.4. Let R be a completely decomposable group and h a positive integer. Let

$$\mathrm{RFEE}(R, h) = \{X \le \mathbb{Q}R \mid R = \mathrm{R}(X) \text{ and } X \subseteq h^{-1}R\}.$$

The groups of $\mathrm{RFEE}(R, h)$ will be called *regulated extensions* of R *with h–bounded regulator quotient.*

Theorem 3.5. (Isomorphism Criterion) [Mad00, Theorem 8.1.13]
Let $X, Y \in \mathrm{RFEE}(R, h)$. Then $X \cong Y$ if and only if there is $\alpha \in \operatorname{Aut} R$ such that $\overline{\alpha}\,\overline{hX} = \overline{hY}$.

Remark 3.6. In this case we have $\overline{hX} = \{\overline{hx} \mid x \in X\} = \{x + R \mid x \in X\} = X/R$, since $\overline{hx} = x + R$, and $\overline{\alpha}(x + R) = \overline{\alpha}(\overline{hx}) = \overline{\alpha(hx)}$.

Definition 3.7. Let R be a completely decomposable group and h positive integer. A *type automorphism* ξ is an automorphism of $\overline{R}$ such that $\xi\,\overline{R(\tau)} = \overline{R(\tau)}$ for every critical type $\tau \in \mathrm{T}_{\mathrm{cr}}(R)$. The set of type automorphisms is a multiplicative group denoted by

$$\operatorname{TypAut} \overline{R} := \{\xi \in \operatorname{Aut} \overline{R} \mid \forall_{\tau \in \mathrm{T}_{\mathrm{cr}}(R)}\; \xi\,\overline{R(\tau)} = \overline{R(\tau)}\}.$$

Definition 3.8. Let $X, Y \in \mathrm{RFEE}(R, h)$. The groups X and Y are called *type–isomorphic in* $\overline{R} = h^{-1}R/R$ if there is $\xi \in \mathrm{TypAut}\,\overline{R}$ such that $\xi(\overline{hX}) = \overline{hY}$, and we write $X \cong_{\mathrm{tp}} Y$ in this case.

Remark 3.9. This equivalence relation on $\mathrm{RFEE}(R, h)$ is a weakening of isomorphism. Each induced automorphism $\overline{\alpha} \in \overline{\mathrm{Aut}\,R}$ satisfies $\overline{\alpha}\ \overline{R(\tau)} = \overline{\alpha\, R(\tau)} = \overline{R(\tau)}$. Hence $\overline{\mathrm{Aut}\,R} \subseteq \mathrm{TypAut}\,\overline{R}$ and the Isomorphism Criterion 3.5 shows that isomorphic groups X, $Y \in \mathrm{RFEE}(R, h)$ are type–isomorphic, too.

The equivalence of type–isomorphism and near–isomorphism is shown in [Mad00, Theorem 9.2.4]. The next theorem includes this fact and other characterizations of near–isomorphism.

Theorem 3.10. *Let X and Y be almost completely decomposable groups. Then the following are equivalent.*

(1) $X \cong_{\mathrm{nr}} Y$.
(2) *There exists a monomorphism $\phi : X \to Y$ such that $[Y : \phi X]$ is finite and relatively prime to* $\mathrm{rgi}(X)\,\mathrm{rgi}(Y)$.
(3) $X \oplus \mathrm{R}(X) \cong Y \oplus \mathrm{R}(X)$.
(4) $X \oplus A \cong Y \oplus A$ *for some completely decomposable group A.*
(5) $X/\mathrm{R}(X) \cong Y/\mathrm{R}(Y)$ *and there exists a monomorphism $\phi : X \to Y$ such that $[Y : \phi X]$ is finite and relatively prime to* $[X : \mathrm{R}(X)]$.
(6) $X \cong_{\mathrm{tp}} Y$.
(7) *There exists an integer n such that $X^n \cong Y^n$.*

The well known classification [Mut99] of almost completely decomposable groups up to near–isomorphism will be improved to a classification up to isomorphism within a near–isomorphism class. We reduce this problem up to clipped groups in Theorem 3.12 and p–primary constituents in Theorem 3.15.

Definition 3.11. An almost completely decomposable group X is called *clipped* if it does not have any rational direct summands.

Theorem 3.12. (Main Decomposition Theorem) [Mad00, Theorem 9.2.7] *Let X and Y be almost completely decomposable groups. Let $X = X_{\mathrm{cd}} \oplus X_{\mathrm{cl}}$ be a decomposition of X with completely decomposable summand X_{cd} and clipped summand X_{cl}. Then the following hold.*

(1) *X_{cd} is unique up to isomorphism and X_{cl} is unique up to near–isomorphism.*
(2) *If $Y = Y_{\mathrm{cd}} \oplus Y_{\mathrm{cl}}$ is such that Y_{cd} is completely decomposable and Y_{cl} is clipped, then $X \cong_{\mathrm{nr}} Y$ if and only if $X_{\mathrm{cd}} \cong Y_{\mathrm{cd}}$ and $X_{\mathrm{cl}} \cong_{\mathrm{nr}} Y_{\mathrm{cl}}$.*

Remark 3.13. Hence we only have to investigate clipped groups for near–isomorphism.

Definition 3.14. Let X be an almost completely decomposable group, A a completely decomposable subgroup, p a prime and h a positive integer such that $hX \subseteq A$. Recall that $\mathbb{Z}[p^{-1}] = \{\frac{m}{p^k} \,|\, m \in \mathbb{Z},\, k \in \mathbb{N}\}$. The subgroup

$$X_{\wr p} := \{x \in X \mid p^n x \in A \text{ for some } n\} = X \cap \mathbb{Z}[p^{-1}]A$$

is called *p–primary constituent* of X with respect to A.

Theorem 3.15. (Primary Reduction Theorem) [Mad00, Theorem 9.2.8]

(1) *Let X be an almost completely decomposable group, A a completely decomposable subgroup. Then $A = \mathrm{R}(X)$ if and only if $A = \mathrm{R}(X_{\wr p})$ for all primes p.*
(2) *If X and Y are almost completely decomposable groups, then $X \cong_{\mathrm{nr}} Y$ if and only if $X_{\wr p} \cong_{\mathrm{nr}} Y_{\wr p}$ for all primes p.*

Remark 3.16. The finite group X/A has a direct decomposition into primary components and we get

$$\frac{X_{\wr p}}{A} = p\text{–component of } \frac{X}{A}\ .$$

Set $A = \mathrm{R}(X)$. By Theorem 3.15, we only have to look at almost completely decomposable groups with a p–group being the regulator quotient to investigate the near–isomorphism class.

For easy reference we summarize the known properties shared by nearly isomorphic almost completely decomposable groups.

Theorem 3.17. [Mad00, Theorem 9.2.6] *Let X and Y be nearly isomorphic almost completely decomposable groups. Then the following hold.*

(1) $\mathrm{rk}(X) = \mathrm{rk}(Y)$ *and* $\mathrm{T_{cr}}(X) = \mathrm{T_{cr}}(Y)$.
(2) $\mathrm{rgi}(X) = \mathrm{rgi}(Y)$.
(3) $X \oplus \mathrm{R}(Y) \cong Y \oplus \mathrm{R}(Y)$.
(4) *For all* $\tau \in \mathrm{T_{cr}}(X) = \mathrm{T_{cr}}(Y)$, $\beta^X_\tau = \beta^Y_\tau$, $\mathrm{R}(X) \cong \mathrm{R}(Y)$, *and* $X/\mathrm{R}(X) \cong Y/\mathrm{R}(Y)$.
(5) *The isomorphism classes of regulating quotients of X and Y coincide.*
(6) *For all types τ whatsoever,* $X(\tau) \cong_{\mathrm{nr}} Y(\tau)$, $X^\sharp(\tau) \cong_{\mathrm{nr}} Y^\sharp(\tau)$.

Remark 3.18. Since nearly isomorphic groups have isomorphic regulators we restrict ourselves for simplification to groups with a common regulator.

4. Matrix Theory

Definition 4.1. Let S be a commutative ring with 1, let r, n be natural numbers. Let S^* denote the set of units in S. Let the set of $(r \times n)$–matrices over S be denoted by $\mathbb{M}^{r\times n}(S)$. A matrix which is obtained by striking out rows and columns of a matrix A is called a *submatrix of* A. The maximal natural number k such that there is an invertible k–rowed submatrix of A is called *determinantal rank of* A. Write $\mathrm{rk}_{\det}(A) = k$. Note that a square matrix over S is invertible if and only if its determinant is a unit in S. Such matrices are also called *regular* or *nonsingular*. Let $\mathrm{GL}(n, S)$ denote the set of all invertible $(n \times n)$–matrices with coefficients in S, the ***g**eneral **l**inear group* of degree n over S. Abbreviate a diagonal matrix by

$$\mathrm{diag}(d_1, \dots , d_n) := \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} \in \mathbb{M}^{n\times n}(S).$$

If $r < n$ and $D = \mathrm{diag}(d_1, \dots , d_r, d_{r+1}, \dots , d_n)$, then define the submatrices $D_{\leqslant r} := \mathrm{diag}(d_1, \dots , d_r)$ and $D_{>r} := \mathrm{diag}(d_{r+1}, \dots , d_n)$.

Definition 4.2. Let S be a commutative ring with 1, let n be a natural number. Let U, $U_1, \dots , U_n$ be subgroups of $(S^*, \cdot\,)$. Write

$$\mathrm{DIAG}(n; U) := \{\mathrm{diag}(d_1, \dots , d_n) \mid \forall_{j=1,\dots,n}\ d_j \in U\}$$

for the set of all $(n \times n)$–diagonal matrices over U. This definition can be generalized by

$$\mathrm{DIAG}(U_1, \dots , U_n) := \{\mathrm{diag}(f_1, \dots , f_n) \mid \forall_{j=1,\dots,n}\ f_j \in U_j\}.$$

Lemma 4.3. *Let p be a prime and e, m, n, $r \in \mathbb{N}$ natural numbers. For $M \in \mathbb{M}^{m\times n}(\mathbb{Z}_{p^e})$ the following are equivalent.*

1. *The maximal number of p–independent rows is r.*
2. *The maximal number of p–independent columns is r.*
3. *The determinantal rank is r.*

Proof. Since $\mathrm{rk}_{\det}(M) = \mathrm{rk}_{\det}(M^{\mathrm{tr}})$ we only have to show that p–independence of the rows of an $(r \times n)$–submatrix A is equivalent to the fact that A has determinantal rank r. Note that a square matrix over $\mathbb{Z}_{p^e}$ has p–independent rows if and only if it describes an automorphism of a homocyclic group, i. e. if and only if it is invertible.
If the $(r \times n)$–matrix A has determinantal rank r, then it has an invertible square r–rowed submatrix, whose rows are p–independent. But then the rows of A are p–independent.
Conversely, if A has p–independent rows, then A is a submatrix of some square n–rowed matrix B whose n rows are p–independent, since a p–independent set is contained in a maximal p–independent set. Thus B is invertible and A contains an invertible r–rowed submatrix by Laplace's expansion of determinants. □

Definition 4.4. Let S be a commutative ring with 1, let r, n be natural numbers. The matrices M, $N \in \mathbb{M}^{r\times n}(S)$ are said to be *equivalent* if there are invertible matrices $U \in \mathrm{GL}(r, S)$ and $V \in \mathrm{GL}(n, S)$ such that

$$N = U\,M\,V\;.$$

Let $\mathcal{U} \subseteq \mathrm{GL}(r, S)$ and $\mathcal{V} \subseteq \mathrm{GL}(n, S)$ be not empty subsets. If $U \in \mathcal{U}$ and $V \in \mathcal{V}$ this is called *$\mathcal{U}|\mathcal{V}$–equivalence.* If V is specialized to be a diagonal matrix this is called *$g|d$–equivalence* (g = general, d = diagonal). If U is the identity matrix and V is a permutation matrix this is called *column permutation equivalence.* If U and V both are specialized to be diagonal matrices this is called *diagonal equivalence.*

Two square matrices M and N over S are called *similar* if there is an invertible matrix V with $N = V^{-1}M\,V$.

Lemma 4.5. *Let S be a commutative ring with 1, let r, n be natural numbers. If M, $N \in \mathbb{M}^{r\times n}(S)$ are $g|d$–equivalent, then for all $k = 1,\dots,n$ the matrices $M^{(k)}$, $N^{(k)}$ obtained from M, N by deleting the k–th column are $g|d$–equivalent, too.*

Proof. Assume that $N = U\cdot M\cdot \mathrm{diag}(d_1,\dots,d_n)$. Then $N^{(k)} = U\cdot M^{(k)}\cdot \mathrm{diag}(d_1,\dots,d_{k-1},d_{k+1},\dots,d_n)$, since it does not matter whether you delete firstly a column and multiply secondly the others by units d_j or you turn this around. ☐

Remark 4.6. Let $M \in \mathbb{M}^{r\times n}(S)$. Striking out the k–th column is represented by multiplying by the following $[n\times(n-1)]$–matrix from the right side:

$$S_k = \left(\begin{array}{ccc|c|cc} 1 & & & & & \\ 0 & \ddots & & & & \\ & \ddots & 1 & & & \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \hline & & & 1 & \ddots & \\ & & & & \ddots & 0 \\ & & & & & 1 \end{array}\right) \leftarrow k$$

$$\begin{aligned} \text{Hence}\qquad N^{(k)} &= N\cdot S_k = U\cdot M\cdot \mathrm{diag}(d_1,\dots,d_n)\cdot S_k \\ &= U\cdot \underbrace{M\cdot S_k}_{=M^{(k)}}\cdot \mathrm{diag}(d_1,\dots,d_{k-1},d_{k+1},\dots,d_n). \end{aligned}$$

Lemma 4.7. *Let p be a prime and e, n, $r \in \mathbb{N}$ natural numbers with $r \le n$. Let M, $N \in \mathbb{M}^{r\times n}(\mathbb{Z}_{p^e})$ be $g|d$–equivalent.*

Any submatrix obtained from M by striking out one column has p–independent rows if and only if this is true for N.

Proof. Let $M^{(k)}$ denote the $[r\times(n-1)]$–matrix over $\mathbb{Z}_{p^e}$ obtained from M by deleting the k–th column. By Lemma 4.5 the matrices $M^{(k)}$, $N^{(k)}$ are $g|d$–equivalent, too. Hence $\mathrm{rk}_{\det}(M^{(k)}) = \mathrm{rk}_{\det}(N^{(k)})$ and both submatrices $M^{(k)}$, $N^{(k)}$ have an identical number of p–independent rows. □

Example 4.8. Let

$$M := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad V := \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Let $M^{(1)} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ denote the matrix obtained from M by deleting the first column. We calculate

$$MV = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad (MV)^{(1)} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}.$$

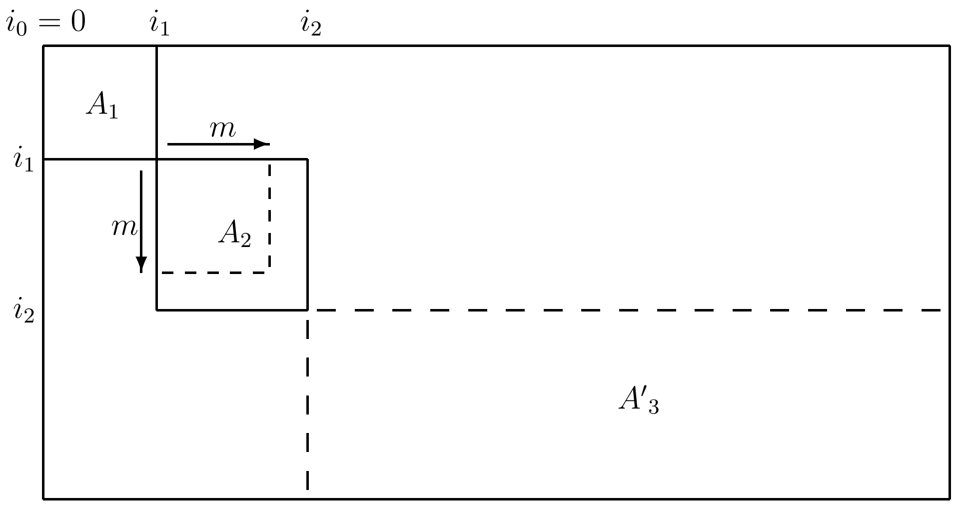
Although M and MV are equivalent, the submatrices $M^{(1)}$ and $(MV)^{(1)}$ have distinct determinantal rank. Hence equivalence in general does not preserve the striking out–property of Lemma 4.7. △

Definition 4.9. Let p be a prime and $e, n, r \in \mathbb{N}$ natural numbers. Let $A = (\alpha_{ij})$ be an $(r\times n)$–matrix over $\mathbb{Z}_{p^e} = \mathbb{Z}/p^e\mathbb{Z}$. Note that $\mathbb{Z}_{p^e}$ is a local ring and all ideals are principal. Let $p^\delta\mathbb{Z}_{p^e}$ be the ideal of $\mathbb{Z}_{p^e}$ generated by the set of all entries α_{ij} of A. The exponent δ is called the *stripping exponent of* A. The matrix A^{st} with entries in $\mathbb{Z}_{p^e}$ is called *stripped form of* A if $p^\delta A^{\mathrm{st}} = A$. The determinantal rank of A^{st} is called *lower determinantal rank of* A. Note that the entries of A^{st} are uniquely determined up to $p^{e-\delta}\mathbb{Z}_{p^e}\left[\cong(\mathbb{Z}_{p^\delta},+)\right]$.

Let $A \neq 0$. The tuple $(i_1,\dots,i_f)$ determines a block structure on the matrix A if $1 \le i_1 < \ldots < i_f = \min(r,n)$ as follows: Let $i_0 = 0$. The square $(i_l - i_{l-1})$–rowed submatrices $A_l = (\alpha_{ij})_{i_{l-1}<i,j\le i_l}$ of A, $1 \le l \le f$, are the *diagonal blocks of* A. Let $A'_l = (\alpha_{ij})_{i_{l-1}<i,j}$ denote the *rest block* of the diagonal block A_l. Let δ_l be the stripping exponent of A'_l and let $C'_l = (\gamma_{i,j})$ be the stripped form of A'_l. The matrix A is called *straight with block structure* $(i_1,\dots,i_f)$ and *stripping sequence* $(\delta_1,\dots,\delta_f)$, if

(1) $i_l - i_{l-1}$ is the lower determinantal rank of the rest block A'_l, $1 \le l \le f$.

(2) All main submatrices $(\gamma_{ij})_{i_{l-1}<i,j\le i_{l-1}+m}$ of all stripped diagonal blocks $\neq 0$ of A, separately, are invertible.



Remark 4.10. Note that $0 \le \delta_1 \le \delta_2 \le \ldots \le \delta_f \le e$ and that $\delta_l = e$ is equivalent to $A'_l = 0$, i. e. in particular, $A_l = 0$. Moreover, the properties of straight only relate to the maximal main square submatrix of a matrix.

Proposition 4.11. *Every $(r \times n)$–matrix with determinantal rank r is column permutation equivalent to a straight matrix.*

More precise, let r, $n \in \mathbb{N}$ be natural numbers with $r \le n$ and let $M \in \mathbb{M}^{r\times n}(\mathbb{Z}_{p^e})$ be a matrix with $\mathrm{rk}_{\det}(M) = r$. Then a permutation matrix P exists such that MP is straight.

Proof. Since M has determinantal rank r, there is an invertible $(r \times r)$–submatrix A which can moved to the left edge by a rearrangement of the columns. We restrict ourselves to A. We use an induction on the number r of rows. An invertible (1×1)–matrix is straight. Suppose that for every invertible $[(r-1) \times (r-1)]$–matrix B there is a permutation matrix Q such that BQ is straight. Now let $A = (\alpha_{ij})_{\substack{i=1,\ldots,r\\ j=1,\ldots,r}}$ be invertible over $\mathbb{Z}_{p^e}$. Let $A^{(r,k)} = (\alpha_{ij})_{\substack{i\neq r\\ j\neq k}}$ denote the $[(r-1)\times(r-1)]$–submatrix obtained from A by deleting the r–th row and the k–th column. There exists $k \in \{1, \ldots, r\}$ such that $A^{(r,k)}$ is invertible. Otherwise $\det A^{(r,k)}$ is a non–unit for all $k = 1, \ldots, r$. Note that the set of non–units is an ideal in the local ring $\mathbb{Z}_{p^e}$. By Laplace's expansion of determinants, $\det A = \sum_{k=1}^{r}(-1)^{r+k}\alpha_{rk} \det A^{(r,k)}$ is also a non–unit, contradiction. Hence $A^{(r,k)}$ is invertible. This invertible $[(r-1)\times(r-1)]$–submatrix can be moved to the left upper corner of A by a permutation of columns. Thus there is a permutation matrix P such that

$$A\,P = \left(\begin{array}{ccc|c} & & & * \\ & A^{(r,k)} & & \vdots \\ & & & * \\ \hline * & \cdots & * & * \end{array}\right).$$

By the induction hypothesis there is a permutation matrix Q such that $A^{(r,k)}Q$ is straight. Then

$$A\,P \left(\begin{array}{ccc|c} & & & 0 \\ & Q & & \vdots \\ & & & 0 \\ \hline 0 & \cdots & 0 & 1 \end{array} \right) = \left(\begin{array}{ccc|c} & & & * \\ & A^{(r,k)}Q & & \vdots \\ & & & * \\ \hline * & \cdots & * & * \end{array} \right)$$

is straight, since it is invertible and $A^{(r,k)}Q$ is straight. □

Definition 4.12. Let p be a prime and e, n, $r \in \mathbb{N}$ natural numbers. Let M be an $(r \times n)$–matrix over $\mathbb{Z}_{p^e}$ with determinantal rank r. Then there are invertible submatrices of size $r \times r$. The set of indices of the columns for such an invertible submatrix is called a *pivot set* of the matrix M.

Remark 4.13. A pivot set is not uniquely determined in general.

Definition 4.14. A straight matrix C is said to be *normed* if all the main submatrices of the stripped diagonal blocks $C_l \neq 0$ have determinant 1.

Two diagonally equivalent normed matrices with the same block structure $(i_1, \ldots, i_f)$ and the same stripping sequence $(\delta_1, \ldots, \delta_f)$ are called *modified diagonally similar* if the stripped forms of the diagonal blocks $A_l \neq 0$, $1 \leq l \leq f$, are diagonally similar modulo $p^{\delta_l}\mathbb{Z}_{p^e}$, respectively.

Remark 4.15. Note that modified diagonal similarity is defined for non–square matrices, too, and that for square matrices with determinant 1, modified diagonal similarity is exactly diagonal similarity.

Definition 4.16. Let p be a prime, $r \leq n$ natural numbers and $e = e_1 \geq \cdots \geq e_r \geq 1$ integers. A matrix $M \in \mathbb{M}^{r\times n}(\mathbb{Z}_{p^e})$ is said to be in *Gauß normal form* if

$$M = \Lambda\,(E \mid A)\,, \qquad \text{where} \qquad \Lambda = \operatorname{diag}(p^{e-e_1}, \ldots, p^{e-e_r})\,, \qquad \text{and}$$

$$E = \begin{pmatrix} 1 & m_{12} & \cdots & m_{1r} \\ 0 & 1 & \cdots & m_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

$m_{ij} \in \{k + p^e\mathbb{Z} \in \mathbb{Z}/p^e\mathbb{Z} \mid 0 \leq k < p^{e_i - e_j}\}$ for all $1 \leq i < j \leq r$.

Definition 4.17. Let r, n be positive integers with $r \leq n$. Let $M = (\alpha_{ij})_{i,j}$ be an $(r \times n)$–matrix over $\mathbb{Z}_{p^e}$. Then M is said to be in *Hermite normal form* if $\alpha_{ij} = \delta_{ij} = \begin{cases} 1 \text{ for } i = j, \\ 0 \text{ for } i \neq j, \end{cases}$ for all $1 \leq i, j \leq r$. In this way M decomposes into the $(r \times r)$–identity matrix I_r and $A = (\alpha_{ij})_{\substack{i=1,\dots,r \\ j=r+1,\dots,n}}$. We get

$$M = (I_r \mid A) = \left(\begin{array}{ccc|ccc} 1 & & & \alpha_{1,r+1} & \cdots & \alpha_{1,n} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & \alpha_{r,r+1} & \cdots & \alpha_{r,n} \end{array} \right).$$

Lemma 4.18. *If a square $(r \times r)$–matrix $C = (\gamma_{i,j})_{1 \le i,j \le r}$ over a local ring is invertible, then there exists a permutation $\sigma \in S_r$ such that $\gamma_{i,\sigma(i)}$ is a unit for all $i = 1, \dots, r$. In particular each row and each column has an entry which is a unit.*

Proof. Let S be a local ring, i. e. a commutative ring with 1 which has a unique maximal ideal I. Then $I = S \setminus S^*$ is the set of non–units. Let C be an $(r \times r)$–matrix over S.
Suppose that there is no permutation $\sigma \in S_r$ such that $\gamma_{i,\sigma(i)}$ is a unit for all $i = 1, \dots, r$. Since the set of non–units I is an ideal, for all permutations $\sigma \in S_r$ the product $\gamma_{1,\sigma(1)}\gamma_{2,\sigma(2)} \cdots \gamma_{r,\sigma(r)}$ is a non–unit, too. Hence

$$\det C = \sum_{\sigma \in S_r} \operatorname{sign}(\sigma)\gamma_{1,\sigma(1)}\gamma_{2,\sigma(2)} \cdots \gamma_{r,\sigma(r)}$$

is in the ideal I and is a non–unit. Then C is not invertible. □

Example 4.19. The condition of this Lemma is only necessary but not sufficient, e.g. $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ is not invertible.

An invertible matrix over a general commutative ring with 1 need not to have a unit in each row or column. For example

$$\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \in \mathbb{M}^{2\times 2}(\mathbb{Z})$$

has determinant 1 and is invertible. But no entry is a unit $\{\pm 1\}$ in $\mathbb{Z}$.

Definition 4.20. Let m, $r \in \mathbb{N}$ be natural numbers. The matrix $A \in \mathbb{M}^{r\times m}(\mathbb{Z}_{p^e})$ is called *primitive* if each row of A has an entry which is a unit in $\mathbb{Z}_{p^e}$, i. e. $\forall_i \; \exists_j \quad \alpha_{ij} \in \mathbb{Z}^*_{p^e}$.

Lemma 4.21. *Let $M = (I_r \mid A) \in \mathbb{M}^{r\times n}(\mathbb{Z}_{p^e})$ be a matrix in Hermite normal form. Then any submatrix obtained from M by striking out one column has p–independent rows if and only if the rest block A is primitive.*

Proof. Let $M^{(k)}$ denote the $[r \times (n-1)]$–matrix over $\mathbb{Z}_{p^e}$ obtained from M by deleting the k–th column.
"$\Rightarrow$" Assume for contradiction that there is no unit in the k–th row of A. Then the k–th row of $M^{(k)} = (I_r^{(k)} \mid A)$ contains no unit, too, and therefore the k–th row of $M^{(k)}$ is not p–independent by definition.
"$\Leftarrow$" Assume that each row of $A = (\alpha_{ij})_{\substack{i=1,\dots,r \\ j=r+1,\dots,n}}$ has an entry which is a unit

in $\mathbb{Z}_{p^e}$. For $k > r$ the matrix $M^{(k)} = (I_r \mid A^{(k)})$ has determinantal rank r and therefore p–independent rows. Let $k \in \{1, \dots, r\}$ be fixed and let α_{kj} be a unit in the k–th row of A by assumption. The matrix $M^{(k)} = (I_r^{(k)} \mid A)$ has p–independent rows, since it has the following invertible $(r \times r)$–submatrix

$$\begin{pmatrix} 1 & & & & & & \alpha_{1j} \\ 0 & \ddots & & & & & \vdots \\ & \ddots & 1 & & & & \vdots \\ & & 0 & 0 & & & \alpha_{kj} \\ & & & 1 & \ddots & & \vdots \\ & & & & \ddots & 0 & \vdots \\ & & & & & 1 & \alpha_{nj} \end{pmatrix} \leftarrow k$$

with determinant $(-1)^{k+j} \cdot \alpha_{kj}$, which is a unit in $\mathbb{Z}_{p^e}$. □

Definition 4.22. Let p be a prime and $e = e_1 \geq \cdots \geq e_r \geq 1$ natural numbers. Abbreviate $\varepsilon = (e_1, \dots, e_r)$. Let $\mathcal{P}(p;\varepsilon) \subseteq \mathrm{GL}(r, \mathbb{Z}_{p^e})$ denote the set of invertible $(r \times r)$–matrices $P = (\gamma_{ij})_{1 \leq i,j \leq r}$ with $\gamma_{ij} \in p^{e_j - e_i}\mathbb{Z}_{p^e}$ if $j \leq i$.

Let $\mathcal{Q}(p;\varepsilon) \subseteq \mathrm{GL}(r, \mathbb{Z}_{p^e})$ denote the set of invertible $(r \times r)$–matrices $Q = (\rho_{ij})_{1 \leq i,j \leq r}$ with $\rho_{ij} \in p^{e_i - e_j}\mathbb{Z}_{p^e}$ if $i \leq j$.

Proposition 4.23. *If $P \in \mathcal{P}(p;\varepsilon)$, then there exists $Q \in \mathcal{Q}(p;\varepsilon)$ such that*

$$P \cdot \mathrm{diag}(p^{e-e_1}, \dots, p^{e-e_r}) = \mathrm{diag}(p^{e-e_1}, \dots, p^{e-e_r}) \cdot Q\,. \tag{4.24}$$

If $Q \in \mathcal{Q}(p;\varepsilon)$, then there exists $P \in \mathcal{P}(p;\varepsilon)$ such that (4.24) holds.

Proof. Assume that $P = (\gamma_{ij})_{1 \leq i,j \leq r}$ is invertible with $\gamma_{ij} \in p^{e_j - e_i}\mathbb{Z}_{p^e}$ for all $j \leq i$. For $\gamma \in p^a\mathbb{Z}_{p^e}$, $a \in \mathbb{N}_0$, there is a $\rho \in \mathbb{Z}_{p^e}$ such that $p^a\rho = \gamma$ and ρ is well–defined modulo $p^{e-a}\mathbb{Z}_{p^e}$. We denote briefly $\rho = p^{-a}\gamma$. In this sense the matrix $Q = (\rho_{ij})_{1 \leq i,j \leq r}$ is well–defined by $\rho_{ij} := p^{e_i - e_j}\,\gamma_{ij}$. If $i \leq j$, then $\rho_{ij} \in p^{e_i - e_j}\mathbb{Z}_{p^e}$, since $\gamma_{ij} \in \mathbb{Z}_{p^e}$ in that case. We have the identity $\mathrm{diag}(p^{e-e_1}, \dots, p^{e-e_r}) \cdot Q = (p^{e-e_i}\,\rho_{ij})_{i,j} = (p^{e-e_i}\,p^{e_i-e_j}\,\gamma_{ij})_{i,j} = (\gamma_{ij}\,p^{e-e_j})_{i,j} = P \cdot \mathrm{diag}(p^{e-e_1}, \dots, p^{e-e_r})$ and equation (4.24) holds. We have to show that Q is invertible. We use Leibniz's determinantal formula to determine $\det Q$. For all permutations $\sigma \in S_r$ we calculate $\sum_{i=1}^r [e_i - e_{\sigma(i)}] = \sum_{i=1}^r e_i - \sum_{k \in \{1,\dots,r\}} e_k = 0$ and therefore $\prod_{i=1}^r p^{e_i - e_{\sigma(i)}} = p^{\sum_i e_i - e_{\sigma(i)}} = p^0 = 1$. We get

$$\begin{aligned} \det Q &= \det(\rho_{ij})_{i,j} = \det(p^{e_i - e_j}\gamma_{ij})_{i,j} = \\ &= \sum_{\sigma \in S_r} \left(\mathrm{sign}(\sigma) \prod_{i=1}^r p^{e_i - e_{\sigma(i)}} \gamma_{i,\sigma(i)} \right) = \\ &= \sum_{\sigma \in S_r} \left(\mathrm{sign}(\sigma) \prod_{i=1}^r \gamma_{i,\sigma(i)} \right) = \det(\gamma_{ij})_{i,j} = \det P\,, \end{aligned}$$

and $\det Q$ is a unit in $\mathbb{Z}_{p^e}$. Hence the inverse Q^{-1} exists.
The other way round is similar. □

Remark 4.25. Let S be a commutative ring with an identity element and let r, n be natural numbers with $r < n$. Note that $\mathrm{DIAG}(n; S^*) = \{\mathrm{diag}(d_1, \dots, d_n) \mid d_j \in S^*\} \cong (S^*)^n$ is an abelian subgroup of $\mathrm{GL}(n, S)$. The group $\mathrm{DIAG}(n; S^*)$ acts on $\mathbb{M}^{r\times(n-r)}(S)$ via diagonal equivalence:

$$\mathrm{DIAG}(n; S^*) \times \mathbb{M}^{r\times(n-r)}(S) \longrightarrow \mathbb{M}^{r\times(n-r)}(S), \quad (D, M) \longmapsto D_{\leqslant r}^{-1}\, M\, D_{>r}.$$

This is a group action, since $(I_n, M) \mapsto M$ and $(D{\cdot}D', M) \mapsto D'^{-1}_{\leqslant r}\cdot\big(D_{\leqslant r}^{-1}\, M\, D_{>r}\big)\cdot D'_{>r}$. Let $A \in \mathbb{M}^{r\times(n-r)}(S)$. The *stabilizer* of A in $\mathrm{DIAG}(n; S^*)$ is defined as

$$\mathrm{Stab}_{\mathrm{DIAG}(n;S^*)}(A) = \big\{D \in \mathrm{DIAG}(n; S^*) \mid D_{\leqslant r}^{-1}\, A\, D_{>r} = A\big\}\,. \tag{4.26}$$

The $\mathrm{DIAG}(n; S^*)$*–orbits* are known as diagonal equivalence classes in $\mathbb{M}^{r\times(n-r)}(S)$. The orbit of A is

$$\begin{aligned}\mathrm{Orb}(A) = \big\{D_{\leqslant r}^{-1}\, A\, D_{>r} \ \mid\ & D_{\leqslant r} = \mathrm{diag}(d_1, \dots, d_r),\\ & D_{>r} = \mathrm{diag}(d_{r+1}, \dots, d_n),\ \text{where } d_j \in S^*\big\}.\end{aligned}$$

Lemma 4.27. *Let S be a finite commutative ring with 1, let r, n be natural numbers with $r < n$. Let $A \in \mathbb{M}^{r\times(n-r)}(S)$.*

The number of matrices which are diagonally equivalent to A is

$$\big[\mathrm{DIAG}(n; S^*) : \mathrm{Stab}_{\mathrm{DIAG}(n;S^*)}(A)\big] = \frac{|S^*|^n}{|\,\mathrm{Stab}_{\mathrm{DIAG}(n;S^*)}(A)|}\,.$$

The diagonal equivalence class of A has at most $|S^*|^{n-1}$ matrices.

Proof. The stabilizer $\mathrm{Stab}_{\mathrm{DIAG}(n;S^*)}(A)$ of A relating to the diagonal equivalence of matrices is a subgroup of $\mathrm{DIAG}(n; S^*)$. The cardinality of the orbit of A is the index of the stabilizer of A in the group of all invertible diagonal matrices: $|\,\mathrm{Orb}(A)| = \big[\mathrm{DIAG}(n; S^*) : \mathrm{Stab}_{\mathrm{DIAG}(n;S^*)}(A)\big]$. In order to establish this consider the map

$$\mathrm{Orb}(A) \longrightarrow \frac{\mathrm{DIAG}(n; S^*)}{\mathrm{Stab}_{\mathrm{DIAG}}(A)}, \quad D_{\leqslant r}^{-1}\, A\, D_{>r} \longmapsto \left(\begin{array}{c|c} D_{\leqslant r} & \\ \hline & D_{>r}\end{array}\right)\cdot \mathrm{Stab}_{\mathrm{DIAG}}(A)\,.$$

From $D_{\leqslant r}^{-1}\, A\, D_{>r} = F_{\leqslant r}^{-1}\, A\, F_{>r} \Leftrightarrow \big(D_{\leqslant r}\, F_{\leqslant r}^{-1}\big)^{-1} A\, (D_{>r}\, F_{>r}^{-1}) = A \Leftrightarrow D\, F^{-1} \in \mathrm{Stab}_{\mathrm{DIAG}(n;S^*)}(A) \Leftrightarrow D \cdot \mathrm{Stab}_{\mathrm{DIAG}(n;S^*)}(A) = F \cdot \mathrm{Stab}_{\mathrm{DIAG}(n;S^*)}(A)$ we conclude that this is a well–defined and bijective map from the orbit $\mathrm{Orb}(A)$ to the set of left cosets of $\mathrm{Stab}_{\mathrm{DIAG}(n;S^*)}(A)$ in $\mathrm{DIAG}(n; S^*)$.

Since $D := \mathrm{diag}(d, \dots, d) = d \cdot I_n$, $d \in S^*$, has the property $D_{\leqslant r}^{-1}\, A\, D_{>r} = A$, i. e. $D \in \mathrm{Stab}_{\mathrm{DIAG}(n;S^*)}(A)$, we conclude $|S^*| \leq |\,\mathrm{Stab}_{\mathrm{DIAG}(n;S^*)}(A)|$. Hence

$$|\,\mathrm{Orb}(A)| = \frac{|S^*|^n}{|\,\mathrm{Stab}_{\mathrm{DIAG}(n;S^*)}(A)|} \leq \frac{|S^*|^n}{|S^*|} = |S^*|^{n-1}. \qquad \square$$

Example 4.28. Let $A = (1\ 1) \in \mathbb{M}^{1\times 2}(\mathbb{Z}_3)$ be a (1×2)–matrix with coefficients in the field $\mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z}$ with three elements. Here we have $n = 3$ and $r = 1$. By Lemma 4.27, there are at most $|\mathbb{Z}_3^*|^2 = 2^2 = 4$ matrices which are diagonally equivalent to A. Indeed there are exactly four diagonally equivalent matrices:

$$(1\ 1),\ (2\ 2) = (2)\cdot(1\ 1),\ (1\ 2) = (1\ 1)\cdot\begin{pmatrix}1 & \\ & 2\end{pmatrix},\ (2\ 1) = (1\ 1)\cdot\begin{pmatrix}2 & \\ & 1\end{pmatrix}.$$

Hence the upper bound of Lemma 4.27 is sharp. △

Remark 4.29. Let S be a commutative ring with 1 and let r, n be natural numbers with $r < n$. Assume that $U_1, \ldots, U_n$ are subgroups of $(S^*,\ \cdot\ )$. Note that $\mathrm{DIAG}(U_1, \ldots, U_n) = \{\mathrm{diag}(f_1, \ldots, f_n) \mid \forall_{j=1,\ldots,n}\ f_j \in U_j\} \cong \prod_{j=1}^n U_j$ is an abelian subgroup of $\mathrm{GL}(n, S)$. The group $\mathrm{DIAG}(U_1, \ldots, U_n)$ acts on $\mathbb{M}^{r\times(n-r)}(S)$ via diagonal equivalence:

(4.30)
$$\mathrm{DIAG}(U_1, \ldots, U_n) \times \mathbb{M}^{r\times(n-r)}(S) \longrightarrow \mathbb{M}^{r\times(n-r)}(S), \quad (F, M) \longmapsto F_{\leqslant r}^{-1}\, M\, F_{>r}\,.$$

This is a group action, since $(I_n, M) \mapsto M$ and $(F \cdot F', M) \mapsto F'^{-1}_{\leqslant r}\left(F_{\leqslant r}^{-1}\, M\, F_{>r}\right) F'_{>r}$. Let $A \in \mathbb{M}^{r\times(n-r)}(S)$. The *stabilizer* of A in $\mathrm{DIAG}(U_1, \ldots, U_n)$ is defined as

$$\mathrm{Stab}_{\mathrm{DIAG}(U_1,\ldots,U_n)}(A) = \left\{F \in \mathrm{DIAG}(U_1, \ldots, U_n) \mid F_{\leqslant r}^{-1}\, A\, F_{>r} = A\right\}.$$

The $\mathrm{DIAG}(U_1, \ldots, U_n)$*–orbits* are known as diagonal equivalence classes in $\mathbb{M}^{r\times(n-r)}(S)$. The orbit of A is

$$\mathrm{Orb}(A) = \Big\{F_{\leqslant r}^{-1}\, A\, F_{>r} \ \Big|\ F_{\leqslant r} = \mathrm{diag}(f_1, \ldots, f_r),\ F_{>r} = \mathrm{diag}(f_{r+1}, \ldots, f_n),\ \text{where } f_j \in U_j\Big\}.$$

Lemma 4.31. *Let S be a finite commutative ring with 1, let r, n be natural numbers with $r < n$. Assume that $U_1, \ldots, U_n$ are subgroups of $(S^*,\ \cdot\ )$. Let $A \in \mathbb{M}^{r\times(n-r)}(S)$.*

The number of matrices which are $\mathrm{DIAG}(U_1, \ldots, U_n)$–diagonally equivalent to A is

$$\left[\mathrm{DIAG}(U_1, \ldots, U_n) : \mathrm{Stab}_{\mathrm{DIAG}(U_1,\ldots,U_n)}(A)\right] = \frac{\prod_{j=1}^n |U_j|}{|\,\mathrm{Stab}_{\mathrm{DIAG}(U_1,\ldots,U_n)}(A)|}\,.$$

Proof. The stabilizer $\mathrm{Stab}_{\mathrm{DIAG}(U_1,\ldots,U_n)}(A)$ of A relating to the $\mathrm{DIAG}(U_1, \ldots, U_n)$–diagonal equivalence of matrices is a subgroup of $\mathrm{DIAG}(U_1, \ldots, U_n)$. The cardinality of the orbit of A is the index of the stabilizer of A in the group of all $\mathrm{DIAG}(U_1, \ldots, U_n)$ matrices: $|\,\mathrm{Orb}(A)| = \left[\mathrm{DIAG}(U_1, \ldots, U_n) : \mathrm{Stab}_{\mathrm{DIAG}(U_1,\ldots,U_n)}(A)\right]$. In order to establish this consider the map

$$\mathrm{Orb}(A) \longrightarrow \frac{\mathrm{DIAG}(U_1, \ldots, U_n)}{\mathrm{Stab}(A)}, \quad F_{\leqslant r}^{-1}\, A\, F_{>r} \longmapsto \left(\begin{array}{c|c} F_{\leqslant r} & \\ \hline & F_{>r}\end{array}\right)\cdot \mathrm{Stab}(A)\,.$$

From $D_{\leqslant r}^{-1}\, A\, D_{>r} = F_{\leqslant r}^{-1}\, A\, F_{>r} \Leftrightarrow \left(D_{\leqslant r}\, F_{\leqslant r}^{-1}\right)^{-1} A\, (D_{>r}\, F_{>r}^{-1}) = A \Leftrightarrow D\, F^{-1} \in \mathrm{Stab}_{\mathrm{DIAG}(U_1,\dots,U_n)}(A) \Leftrightarrow D \cdot \mathrm{Stab}_{\mathrm{DIAG}(U_1,\dots,U_n)}(A) = F \cdot \mathrm{Stab}_{\mathrm{DIAG}(U_1,\dots,U_n)}(A)$ we conclude that this is a well–defined and bijective map from the orbit $\mathrm{Orb}(A)$ to the set of left cosets of $\mathrm{Stab}_{\mathrm{DIAG}(U_1,\dots,U_n)}(A)$ in $\mathrm{DIAG}(U_1, \dots , U_n)$. □

Example 4.32. Let p be a prime and e a natural number. By [Mut99, p. 126–127] the number of normed invertible (2×2)–matrices over $\mathbb{Z}_{p^e} = \mathbb{Z}/p^e\mathbb{Z}$ is $\frac{p^{e+1}+p^e-2}{p-1}$.

We want to determine the cardinality of an arbitrary diagonal equivalence class. A 2–rowed matrix A is invertible and normed if and only if

$$A = \begin{pmatrix} 1 & \alpha \\ \beta & 1+\alpha\beta \end{pmatrix},$$

where $\alpha = \lambda p^m$, $\beta = \mu p^l$ and λ, μ are units, $0 \leq m,\, l \leq e$.

By Lemma 4.27 we have to calculate the cardinality of $\mathrm{Stab}_{\mathrm{DIAG}(4;\mathbb{Z}_{p^e}^*)}(A)$. By Definition 4.26 we have $D = \mathrm{diag}(d_1, d_2, d_3, d_4) \in \mathrm{Stab}_{\mathrm{DIAG}(4;\mathbb{Z}_{p^e}^*)}(A)$ if and only if

$$\begin{aligned} \begin{pmatrix} d_1^{-1} & \\ & d_2^{-1} \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ \beta & 1+\alpha\beta \end{pmatrix} \begin{pmatrix} d_3 & \\ & d_4 \end{pmatrix} &= \begin{pmatrix} d_1^{-1}d_3 & d_1^{-1}d_4\,\alpha \\ d_2^{-1}d_3\,\beta & d_2^{-1}d_4\,(1+\alpha\beta) \end{pmatrix} \\ &= \begin{pmatrix} 1 & \alpha \\ \beta & 1+\alpha\beta \end{pmatrix}. \end{aligned}$$

Comparison of the coefficients yields $d_3 = d_1 \wedge d_2\beta = d_3\beta = d_1\beta \wedge d_4\alpha = d_1\alpha \wedge d_4(1+\alpha\beta) = d_2(1+\alpha\beta)$. The last equation shows

$$d_4 + \underbrace{d_4\alpha\beta}_{=d_1\alpha\beta} = d_2 + \underbrace{d_2\alpha\beta}_{=d_1\alpha\beta}.$$

Thus $d_4 = d_2$ and the matrix equivalence is a similarity, in fact. The matrix equation is equivalent to the following linear equation system for the indeterminates $d_1, \dots , d_4$:

$$d_3 = d_1 \;\wedge\; d_4 = d_2 \;\wedge\; (d_2 - d_1)\cdot\alpha = 0 \;\wedge\; (d_2 - d_1)\cdot\beta = 0. \tag{4.33}$$

We have to count the possibilities of the solutions to determine $|\,\mathrm{Stab}_{\mathrm{DIAG}(4;\mathbb{Z}_{p^e}^*)}(A)|$.

1. case: $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then $|\,\mathrm{Stab}_{\mathrm{DIAG}(4;\mathbb{Z}_{p^e}^*)}(A)| = \varphi(p^e)^2$ and

$$|\,\mathrm{Orb}(A)| = \varphi(p^e)^2 = \left(p^{e-1}(p-1)\right)^2 .$$

2. case: $A \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then $|\,\mathrm{Stab}_{\mathrm{DIAG}(4;\mathbb{Z}_{p^e}^*)}(A)| = \varphi(p^e)\cdot p^{\min(l,m)}$ and

$$|\,\mathrm{Orb}(A)| = \varphi(p^e)^3 \cdot p^{-\min(l,m)} = p^{3e-3-\min(l,m)}\,(p-1)^3 .$$

Here $|\operatorname{Orb}(A)|$ is the number of (2×2)–matrices over $\mathbb{Z}_{p^e}$ which are diagonally equivalent to A. Recall that φ denotes the Euler φ–function.

For case 1 let $A = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, so $\alpha=\beta=0$. Then $\operatorname{Stab}_{\mathrm{DIAG}(4;\mathbb{Z}^*_{p^e})}(A) = \{\operatorname{diag}(d_1,d_2,d_1,d_2) \mid d_1,d_2\in\mathbb{Z}^*_{p^e}\} \cong \left(\mathbb{Z}^*_{p^e}\right)^2$. Hence there are

$$\frac{|\mathbb{Z}^*_{p^e}|^4}{|\mathbb{Z}^*_{p^e}|^2} = |\mathbb{Z}^*_{p^e}|^2 = \varphi(p^e)^2 = \left(p^{e-1}(p-1)\right)^2$$

matrices which are diagonally equivalent to I_2.

For case 2 let $A \neq \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. The linear equation system (4.33) holds. Without loss of generality suppose that $\alpha = p^m$ and $\beta = p^l$, where $0\le m,\, l\le e$, since we are able to divide the last two equations by units. By the assumption we have $k := \min(l,m) < e$. The ideal–structure of $\mathbb{Z}_{p^e}$ is

$$0 \subsetneq p^{e-1}\mathbb{Z}_{p^e} \subsetneq p^{e-2}\mathbb{Z}_{p^e} \subsetneq \ldots \subsetneq p\mathbb{Z}_{p^e} \subsetneq \mathbb{Z}_{p^e}\,.$$

The last two equations of (4.33) are equivalent to

$$(d_2-d_1)\,p^k = 0 \in p^e\,(\mathbb{Z}/p^e\mathbb{Z}) \quad\Longleftrightarrow\quad (d_2-d_1)\in p^{e-k}\,(\mathbb{Z}/p^e\mathbb{Z}) \cong \mathbb{Z}/p^k\mathbb{Z}\,.$$

Hence d_1 is an arbitrary unit in $\mathbb{Z}_{p^e}$ and $d_2 \in d_1 + p^{e-k}\mathbb{Z}_{p^e}$ is a unit, too. There are $|\mathbb{Z}/p^k\mathbb{Z}| = p^k$ possibilities for d_2. Hence we get $\operatorname{Stab}_{\mathrm{DIAG}(4;\mathbb{Z}^*_{p^e})}(A) = \{\operatorname{diag}(d_1,d_2,d_1,d_2) \mid d_1,\ d_2 \in \mathbb{Z}^*_{p^e} \text{ such that } d_2-d_1 \in p^{e-k}\mathbb{Z}_{p^e}\} = \{\operatorname{diag}(d_1,d_2,d_1,d_2) \mid d_1\in\mathbb{Z}^*_{p^e},\ d_2\in d_1+p^{e-k}\mathbb{Z}_{p^e}\}$ and $|\operatorname{Stab}_{\mathrm{DIAG}(4;\mathbb{Z}^*_{p^e})}(A)| = |\mathbb{Z}^*_{p^e}|\cdot p^k$. Therefore

$$|\operatorname{Orb}(A)| = \frac{|\mathbb{Z}^*_{p^e}|^4}{|\mathbb{Z}^*_{p^e}|\,p^k} = \varphi(p^e)^3\cdot p^{-k} = p^{3e-3-k}(p-1)^3. \qquad \triangle$$

5. Representing Matrices

Definition 5.1. Let R be a completely decomposable group of rank n and h an integer. Suppose that $T = (\tau_1, \dots, \tau_n)$ is an indexing of the critical typeset of R.

Then the tuple $\mathbf{x} = (x_1, \dots, x_n)$ of elements in R is called an *ordered decomposition basis* of R if

$$R = \bigoplus_{j=1}^{n} \langle x_j \rangle_*^R .$$

If in addition $\tau_j = \mathrm{tp}^R(x_j)$ for all $j = 1, \dots, n$, then $\mathbf{x}$ is called a *decomposition basis ordered by* T.

The ordered decomposition basis is an *ordered h–decomposition basis* of R if it meets the condition $\mathrm{hgt}_p^R(x_j) \in \{0, \infty\}$ for all $j = 1, \dots, n$ and all primes $p \mid h$. If R is p–reduced, then $\mathrm{hgt}_p^R(x_j) = 0$ for all j.

Definition 5.2. Let R be a completely decomposable group and h a natural number. Let $\mathbf{x} = (x_1, \dots, x_n)$ be an ordered h–decomposition basis of R. The map

$$^{-} : R \to \overline{R} = h^{-1}R/R,\ x \mapsto \overline{x} = h^{-1}x + R$$

denotes the natural epimorphism. The quotient group $h^{-1}R/R$ is a $\mathbb{Z}_h$–module and $h^{-1}R/R = \overline{R} = \bigoplus_{j=1}^{n} \mathbb{Z}_h \overline{x}_j$, where $\overline{x}_j = h^{-1}x_j + R$. Then $\overline{\mathbf{x}} := (\overline{x}_1, \dots, \overline{x}_n)$ is called an *ordered induced decomposition basis* of $h^{-1}R/R$. The basis $\overline{\mathbf{x}}$ is called *induced* by $\mathbf{x}$.

Remark 5.3. Let p be a prime. Then R is p–reduced if and only if no critical type τ_j is p–divisible: $\tau_j(p) \neq \infty$, i. e. $\mathrm{hgt}_p^R(x_j) \neq \infty$.

The $\mathbb{Z}_h$–module $\overline{R}$ need not be free. If R is p–reduced for every prime divisor p of h, then $\overline{R}$ is a free $\mathbb{Z}_h$–module and

$$h^{-1}R/R = \overline{R} = \bigoplus_{j=1}^{n} \mathbb{Z}_h \overline{x}_j \cong (\mathbb{Z}_h)^n ,$$

i. e. $\overline{\mathbf{x}}$ is a free basis with $\mathrm{ord}\,\overline{x}_j = h$ for all j.

Definition 5.4. Assume that h, n, $r \in \mathbb{N}$ are natural numbers. Let X be an almost completely decomposable group of rank n with completely decomposable subgroup R such that $R \subseteq X \subseteq h^{-1}R$. Suppose that $\overline{\mathbf{x}} = (\overline{x}_1, \dots, \overline{x}_n)$ is an ordered induced decomposition basis of $h^{-1}R/R$. Let $\overline{\mathbf{a}} = (\overline{a}_1, \dots, \overline{a}_r)$ be an ordered basis of $X/R \subseteq h^{-1}R/R$. Then the basis elements $\overline{a}_i$ may be written as linear combinations of the induced decomposition basis

$$\overline{a}_i = \sum_{j=1}^{n} \alpha_{ij} \overline{x}_j , \qquad \text{for} \qquad i = 1, \dots, r, \tag{5.5}$$

where $\alpha_{ij} \in \mathbb{Z}_h$. The $(r \times n)$–matrix

$$M = (\alpha_{ij})_{\substack{i=1,\dots,r \\ j=1,\dots,n}} \in \mathbb{M}^{r \times n}(\mathbb{Z}_h)$$

is called *representing matrix* of X over R relative to $\bar{\mathbf{a}}$ and $\bar{\mathbf{x}}$.

Remark 5.6. (1) In general $h^{-1}R/R$ need not be a free $\mathbb{Z}_h$–module and $\bar{\mathbf{x}}$ is not necessarily a free basis. Hence for given $\bar{\mathbf{a}}$ and $\bar{\mathbf{x}}$ the matrix M is not uniquely determined over $\mathbb{Z}_h$. Since $\bar{\mathbf{a}}$ is a minimal generating system, we infer from $\langle \overline{a}_1, \dots, \overline{a}_r \rangle = X/R \subseteq h^{-1}R/R = \langle \overline{x}_1, \dots, \overline{x}_n \rangle$ that $r \leq n$.

(2) Let $h^{-1}R/R \cong (\mathbb{Z}_h)^n$ be a free $\mathbb{Z}_h$–module. Then $\bar{\mathbf{x}}$ is a free basis. The basis elements $\overline{a}_i$ can be written uniquely as linear combinations of the induced decomposition basis. Note that $\sum_{j=1}^n \alpha_{ij}\overline{x}_j = \overline{a}_i = \sum_{j=1}^n \beta_{ij}\overline{x}_j$ is equivalent to $\sum_{j=1}^n (\alpha_{ij} - \beta_{ij})\overline{x}_j = 0$. Then we get $\alpha_{ij} = \beta_{ij}$ in $\mathbb{Z}_h$, since $\{\overline{x}_1, \dots, \overline{x}_n\}$ is a free $\mathbb{Z}_h$–basis. Hence there is exactly one representation (5.5). For given $\bar{\mathbf{a}}$ and $\bar{\mathbf{x}}$ the representing matrix M is therefore *uniquely* determined over $\mathbb{Z}_h$.

(3) We wish to investigate almost completely decomposable groups up to near–isomorphism and subsequently up to isomorphism. The Primary Reduction Theorem is a local–global relationship for almost completely decomposable groups. By this Theorem 3.15 we restrict ourselves to (rigid) ***p*–local** almost completely decomposable groups X, meaning that the regulator quotient $X/\operatorname{R}(X)$ is a p–group. Therefore choose the integer h as a p–power, say $h = p^e$. In this case a p–divisible critical type τ_j creates a p–divisible direct rank–one summand $\tau_j x_j$ of X. By the Main Decomposition Theorem 3.12 we only have to investigate clipped groups, i. e. groups without rational direct summands. The ranks $\operatorname{rk}(X_{\mathrm{cd},\tau_j})$ taken for all critical types $\tau_j \in \operatorname{T_{cr}}(X)$ form a complete independent system of invariants for the maximal completely decomposable direct summand X_{cd}.
We therefore assume that the groups under consideration are ***p*–reduced**, meaning that there are no non–trivial p–divisible subgroups. In this situation a p^e–basis $\mathbf{x} = (x_1, \dots, x_n)$ is the same as a p–basis and it means that $\operatorname{hgt}_p^R(x_j) = 0$, or equivalently $\tau_j(p) = 0$.

(4) Let R be a p–reduced completely decomposable group of rank n. Then $p^{-e}R/R$ is a homocyclic group of rank n and of exponent p^e. Hence $p^{-e}R/R \cong (\mathbb{Z}_{p^e})^n$ can be regarded as a free $\mathbb{Z}_{p^e}$–module. An ordered induced decomposition basis $\bar{\mathbf{x}} = (\overline{x}_1, \dots, \overline{x}_n)$ is a free basis. Let X be a p–local group with subgroup $R \subseteq X \subseteq p^{-e}R$. Let $\bar{\mathbf{a}}$ be a basis of X/R. By 5.6(2) the representing matrix M of X/R relative to $\bar{\mathbf{a}}$ and $\bar{\mathbf{x}}$ is uniquely determined over $\mathbb{Z}_{p^e}$.

For fixed bases the representing matrices of reduced p–local groups are uniquely determined.

(5) If X is a uniform group with regulator $R \subseteq X \subseteq p^{-e}R$, then $X/R \cong (\mathbb{Z}_{p^e})^r$ and therefore $\bar{\mathbf{a}}$ and $\bar{\mathbf{x}}$ are both free $\mathbb{Z}_{p^e}$–bases.

Representing Matrices of p–local Groups

The next result is a generalization of [Mut99, Lemma 4.1].

Lemma 5.7. *Let p be a prime and n, $r \in \mathbb{N}$ natural numbers with $r \leq n$. Let R be completely decomposable p–reduced group of rank n with p–decomposition* *basis* $(x_1, \dots, x_n)$. *Let* $e = e_1 \geq \cdots \geq e_r \geq 1$ *be natural numbers. Let* $M = (\alpha_{i,j})_{\substack{i=1,\dots,r\\ j=1,\dots,n}} \in \mathbb{M}^{r\times n}(\mathbb{Z}/p^e\mathbb{Z})$ *be a matrix such that*

$$M = \operatorname{diag}(p^{e-e_1}, \dots, p^{e-e_r}) \cdot B$$

for some $B \in \mathbb{M}^{r\times n}(\mathbb{Z}/p^e\mathbb{Z})$. *Let* $a_i = \sum_{j=1}^n \alpha'_{i,j} x_j$, $1 \leq i \leq r$, *where* $\alpha'_{i,j} \in \mathbb{Z}$ *such that* $\alpha'_{i,j} + p^e\mathbb{Z} = \alpha_{i,j}$ *for all* i, j. *Let*

$$X = R + \sum_{i=1}^r \mathbb{Z}p^{-e}a_i \subseteq \mathbb{Q}R\,.$$

Then

$$X/R \cong \bigoplus_{i=1}^r (\mathbb{Z}/p^{e_i}\mathbb{Z})$$

if and only if the matrix B *over* $\mathbb{Z}/p^e\mathbb{Z}$ *has determinantal rank* r.

Proof. Let $\overline{} : R \to \overline{R} = p^{-e}R/R$, $x \mapsto \overline{x} = p^{-e}x + R$ denote the natural epimorphism. Then $\overline{\mathbf{x}} = (\overline{x}_1, \dots, \overline{x}_n)$ is an induced decomposition basis of $p^{-e}R/R \cong (\mathbb{Z}/p^e\mathbb{Z})^n$. We have $p^{-e}a_i + R = \overline{a}_i = \sum_{j=1}^n \alpha_{i,j}\,\overline{x}_j$ and $\{\overline{a}_i \mid 1 \leq i \leq r\}$ is a generating system of X/R. Hence $X/R \cong \bigoplus_{i=1}^r (\mathbb{Z}/p^{e_i}\mathbb{Z})$ if and only if the set $\{\overline{a}_i \mid 1 \leq i \leq r\}$ is a p–basis of X/R or equivalently a maximal p–independent system of X/R with $\operatorname{ord}\overline{a}_i = p^{e_i}$, cf. [Fuc73, 32.2]. Write $B = (\beta_{i,j})_{\substack{i=1,\dots,r\\ j=1,\dots,n}}$ and define $\overline{y}_i := \sum_{j=1}^n \beta_{i,j}\,\overline{x}_j$ for $1 \leq i \leq r$. Hence $\langle \overline{y}_i \mid 1 \leq i \leq r\rangle \cong \bigoplus_{i=1}^r (\mathbb{Z}/p^e\mathbb{Z})$ if and only if $\{\overline{y}_i \mid 1 \leq i \leq r\}$ is a p–independent system with $\operatorname{ord}\overline{y}_i = p^e$ or equivalently B has p–independent rows. Since $(\alpha_{i,j}) = (p^{e-e_i}\beta_{i,j})_{i,j}$, we compute $\overline{a}_i = \sum_{j=1}^n \alpha_{i,j}\,\overline{x}_j = p^{e-e_i}\ \sum_{j=1}^n \beta_{i,j}\,\overline{x}_j = p^{e-e_i}\,\overline{y}_i$.

"$\Leftarrow$" Suppose that $\operatorname{rk}_{\det} B = r$. Then the rows of $B = (\beta_{i,j})$ are p–independent and B is primitive by Lemma 4.18. Hence $\operatorname{ord}\overline{y}_i = p^e$ for all i and $\{\overline{y}_i \mid 1 \leq i \leq r\}$ is a p–independent system. Therefore

$$\langle \overline{a}_i \mid 1 \leq i \leq r\rangle \subseteq \langle \overline{y}_i \mid 1 \leq i \leq r\rangle = \bigoplus_{i=1}^r \langle \overline{y}_i\rangle \cong \bigoplus_{i=1}^r (\mathbb{Z}/p^e\mathbb{Z})\ .$$

From $\overline{a}_i = p^{e-e_i}\,\overline{y}_i$ we conclude $\operatorname{ord}\overline{a}_i = p^{e_i}$ and $\overline{a}_i \in \langle \overline{y}_i\rangle$. Hence

$$X/R = \langle \overline{a}_i \mid 1 \leq i \leq r\rangle = \bigoplus_{i=1}^r \langle \overline{a}_i\rangle \cong \bigoplus_{i=1}^r (\mathbb{Z}/p^{e_i}\mathbb{Z})\ .$$

"$\Rightarrow$" Suppose that $X/R = \langle \overline{a}_i \mid 1 \leq i \leq r\rangle = \bigoplus_{i=1}^r \langle \overline{a}_i\rangle \cong \bigoplus_{i=1}^r (\mathbb{Z}/p^{e_i}\mathbb{Z})$. We use p–elementary row operations of the Gauß–algorithm to transform B into an upper triangular matrix. Any permutation of columns means a renumbering of the basis $(\overline{x}_1, \dots, \overline{x}_n)$. Adding a multiple of the j–th row to the i–th row means to replace $\overline{a}_i$ by $\overline{a}_i + h\overline{a}_j$. For $i > j$ we have $\operatorname{ord}(\overline{a}_i + h\overline{a}_j) = p^{e_i}$ if and only if $h \in p^{e_j - e_i} \cdot \mathbb{Z}_{p^e}$. These row operations preserve the p–rank of the rows and also the determinantal rank. This algorithm creates a new basis $\overline{\mathbf{a}}' = (\overline{a}'_1, \dots, \overline{a}'_r)$ with the same property $\langle \overline{a}'_i\rangle \cong \mathbb{Z}/p^{e_i}\mathbb{Z}$.

(1) An entry of the first row of B is a unit in $\mathbb{Z}_{p^e}$. Otherwise all entries $\beta_{1,j}$ for $1 \leq j \leq n$ are in $p\,\mathbb{Z}_{p^e}$ and then

$$p^{e_1-1} \cdot \overline{a}_1 = p^{e_1-1} \left(p^{e-e_1} \sum_{j=1}^{n} \beta_{1,j}\, \overline{x}_j \right) = \sum_{j=1}^{n} \underbrace{p^{e-1}\beta_{1,j}}_{=0}\, \overline{x}_j = 0$$

contradicts $\operatorname{ord} \overline{a}_1 = p^{e_1}$. We rearrange the columns of B such that $\beta_{1,1}$ is this unit. For all $i > 1$ we do the following procedure: We subtract the $\left(p^{e_1-e_i} \cdot \frac{\beta_{i,1}}{\beta_{1,1}}\right)$–multiple of the first row from the i–th row. Then the new coefficient at the place $(i,1)$ in the matrix M is $p^{e-e_i}\,\beta_{i,1} - \left(p^{e_1-e_i} \cdot \frac{\beta_{i,1}}{\beta_{1,1}}\right) \cdot p^{e-e_1}\,\beta_{1,1} = 0$. Hence we get the new form

$$B_{(1)} = \left(\begin{array}{c|cccccc} \beta_{1,1} & * & \cdots & * & * & \cdots & * \\ \hline 0 & \beta_{2,2} & \cdots & \beta_{2,r} & \vdots & & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \beta_{r,2} & \cdots & \beta_{r,r} & * & \cdots & * \end{array} \right).$$

(2) An entry of the second row of $B_{(1)}$ is a unit in $\mathbb{Z}_{p^e}$. We rearrange the columns $2, \ldots, n$ of $B_{(1)}$ such that $\beta_{2,2}$ is this unit. The Gauß–algorithm eliminates the coefficients $\beta_{3,2}, \ldots, \beta_{r,2}$.

(i) We rerun this procedure in step (i) for the i–th column.

Then we get recursively

$$B_{(r-1)} = \begin{pmatrix} \beta_{1,1} & * & \cdots & * & * & \cdots & * \\ 0 & \beta_{2,2} & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \beta_{r,r} & * & \cdots & * \end{pmatrix}.$$

The diagonal elements $\beta_{1,1}, \beta_{2,2}, \ldots, \beta_{r,r}$ are units in $\mathbb{Z}_{p^e}$. Therefore B has determinantal rank r. ☐

Lemma 5.8. *Let p be a prime and e, n, $r \in \mathbb{N}$ natural numbers with $r \leq n$. Let R be completely decomposable p–reduced group of rank n with p–decomposition basis $\mathbf{x} = (x_1, \ldots, x_n)$. Let $\overline{\mathbf{x}} = (\overline{x}_1, \ldots, \overline{x}_n)$ be the ordered induced decomposition basis of $p^{-e}R/R$. Let $e = e_1 \geq \cdots \geq e_r \geq 1$ be natural numbers. Let $B \in \mathbb{M}^{r\times n}(\mathbb{Z}_{p^e})$ be a matrix of maximal determinantal rank $\operatorname{rk}_{\det}(B) = r$. Let*

$$M = \operatorname{diag}(p^{e-e_1}, \ldots, p^{e-e_r}) \cdot B$$

be an $(r \times n)$–matrix over $\mathbb{Z}_{p^e}$.

Then there exists exactly one almost completely decomposable group X with $R \subseteq X \subseteq p^{-e}R$ and an ordered basis $\overline{\mathbf{a}}$ of $X/R \cong \bigoplus_{i=1}^{r} (\mathbb{Z}/p^{e_i}\mathbb{Z})$ such that M is the representing matrix of X/R relative to $\overline{\mathbf{a}}$ and $\overline{\mathbf{x}}$.

Proof. Write $M = (\alpha_{ij})_{\substack{i=1,\ldots,r \\ j=1,\ldots,n}} \in \mathbb{M}^{r\times n}(\mathbb{Z}_{p^e})$.

For existence let $(\alpha^*_{ij})_{i,j} \in \mathbb{M}^{r\times n}(\mathbb{Z})$ with $\alpha^*_{ij} + p^e\mathbb{Z} = \alpha_{ij}$ for all i, j. Set $a_i = \sum_{j=1}^n \alpha^*_{ij} x_j$ and $\overline{a}_i = \sum_{j=1}^n \alpha_{ij}\overline{x}_j$ for $i = 1, \dots, r$. Define

$$X := \langle R, p^{-e}a_1, \dots, p^{-e}a_r\rangle.$$

Then $X/R = \langle \overline{a}_i \mid i = 1, \dots, r\rangle$. Now $\mathrm{rk}_{\det}(B) = r$ implies $X/R = \bigoplus_{i=1}^r \langle \overline{a}_i\rangle \cong \bigoplus_{i=1}^r (\mathbb{Z}/p^{e_i}\mathbb{Z})$ by Lemma 5.7. In particular $\overline{\mathbf{a}} := (\overline{a}_1, \dots, \overline{a}_r)$ is a basis of X/R and M is the representing matrix of X/R relative to $\overline{\mathbf{a}}$ and $\overline{\mathbf{x}}$.

To show the uniqueness let X' be another group with $R \subseteq X' \subseteq p^{-e}R$ and basis $\overline{\mathbf{a}}' = (\overline{a}'_1, \dots, \overline{a}'_r)$ of X'/R such that M is the representing matrix of X'/R relative to $\overline{\mathbf{a}}'$ and $\overline{\mathbf{x}}$. By definition we have $\overline{a}'_i = \sum_{j=1}^n \alpha_{ij}\overline{x}_j$ for $i = 1, \dots, r$. There are $\alpha^{**}_{ij} \in \mathbb{Z}$ with $\alpha^{**}_{ij} + p^e\mathbb{Z} = \alpha_{ij}$ for all i, j which yield $a'_i = \sum_{j=1}^n \alpha^{**}_{ij} x_j$ such that $\overline{\mathbf{a}}'$ is induced by $\mathbf{a}' = (a'_1, \dots, a'_r)$. Then

$$X' = \langle R, p^{-e}a'_1, \dots, p^{-e}a'_r\rangle.$$

For all $i = 1, \dots, r$ we have $p^{-e}a'_i - p^{-e}a_i = \sum_{j=1}^r p^{-e}(\alpha^{**}_{ij} - \alpha^*_{ij})x_j \in R$, since $\alpha^{**}_{ij} \equiv \alpha^*_{ij} \mod p^e$. So $X' = \langle R, p^{-e}a_1, \dots, p^{-e}a_r\rangle = X$. □

The next theorem is an improvement of [MMN01, Theorem 3.7].

Theorem 5.9. *Let p be a prime and e, n, r natural numbers. Let X be a p–reduced almost completely decomposable group of rank n with completely decomposable subgroup R such that*

$$X/R \cong (\mathbb{Z}/p^{e_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{e_r}\mathbb{Z}), \qquad \text{with} \qquad e = e_1 \geq \cdots \geq e_r \geq 1.$$

Then there is an ordered induced decomposition basis $\overline{\mathbf{x}} = (\overline{x}_1, \dots, \overline{x}_n)$ of $p^{-e}R/R$ and an ordered basis $\overline{\mathbf{a}} = (\overline{a}_1, \dots, \overline{a}_r)$ of X/R with $\langle \overline{a}_i\rangle \cong \mathbb{Z}/p^{e_i}\mathbb{Z}$ such that the representing matrix of X/R relative to $\overline{\mathbf{x}}$ and $\overline{\mathbf{a}}$ is in Gauß normal form

$$M = \Lambda\,(E \mid A)\,, \qquad \text{where} \qquad \Lambda = \mathrm{diag}(p^{e-e_1}, \dots, p^{e-e_r})\,, \qquad \text{and}$$

$$E = \begin{pmatrix} 1 & m_{1,2} & \dots & m_{1,r-1} & m_{1,r} \\ 0 & 1 & \dots & m_{2,r-1} & m_{2,r} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & m_{r-1,r} \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \tag{5.10}$$

$m_{i,j} \in \{k + p^e\mathbb{Z} \in \mathbb{Z}/p^e\mathbb{Z} \mid 0 \leq k < p^{e_i - e_j}\}$ for all $1 \leq i < j \leq r$. If especially $e_i = e_j$, then $m_{i,j} = 0$. In particular, when $e = e_1 = \cdots = e_r$, there are bases $\overline{\mathbf{x}}$ and $\overline{\mathbf{a}}$ such that X/R has a representing matrix in Hermite normal form *$M = (I_r \mid A)$, where I_r is the $(r \times r)$–identity matrix.*

Proof. Let $\overline{\mathbf{a}} = (\overline{a}_1, \dots, \overline{a}_r)$ be a basis of X/R such that $\langle \overline{a}_i\rangle \cong \mathbb{Z}/p^{e_i}\mathbb{Z}$. Let $M = (\alpha_{i,j})_{\substack{i=1,\dots,r\\ j=1,\dots,n}} \in \mathbb{M}^{r\times n}(\mathbb{Z}_{p^e})$ be the representing matrix of X/R relative to $\overline{\mathbf{a}}$ and $\overline{\mathbf{x}}$. We use p–elementary row operations of the Gauß–algorithm to transform M into the Gauß normal form (5.10). Any permutation of columns means a renumbering of the basis $(\overline{x}_1, \dots, \overline{x}_n)$. Multiplying the i–th row by a unit λ means to exchange $\overline{a}_i$ by $\lambda\,\overline{a}_i$. Adding a multiple of the j–th row to the i–th row means to replace

$\overline{a}_i$ by $\overline{a}_i + h\overline{a}_j$. If $i < j$, then $\mathrm{ord}(\overline{a}_i + h\overline{a}_j) = p^{e_i}$ in general. For $i > j$ we have $\mathrm{ord}(\overline{a}_i + h\overline{a}_j) = p^{e_i}$ if and only if $h \in p^{e_j - e_i} \cdot \mathbb{Z}_{p^e}$. Clearly $\langle \overline{a}_1, \dots, \overline{a}_i, \dots, \overline{a}_r \rangle = \langle \overline{a}_1, \dots, \overline{a}_i + h\overline{a}_j, \dots, \overline{a}_r \rangle$. The row operations create a new basis $\overline{\mathbf{a}}' = (\overline{a}'_1, \dots, \overline{a}'_r)$ with the same property $\langle \overline{a}'_i \rangle \cong \mathbb{Z}/p^{e_i}\mathbb{Z}$. The group X/R does not change.

Since $\mathrm{ord}(\overline{a}_i) = p^{e_i}$, we conclude $0 = p^{e_i}\,\overline{a}_i = p^{e_i} \sum_{j=1}^n \alpha_{i,j}\overline{x}_j = \sum_{j=1}^n (p^{e_i}\alpha_{i,j})\,\overline{x}_j$ by definition. Therefore $p^{e_i}\alpha_{i,j} = 0$ in $\mathbb{Z}_{p^e}$, so $\alpha_{i,j} \in p^{e-e_i} \cdot \mathbb{Z}_{p^e}$ for all j. By extracting the highest p–power divisors from the rows, we can write

$$M = \Lambda\, B, \qquad \text{where} \qquad \Lambda = \mathrm{diag}(p^{e-e_1}, \dots, p^{e-e_r})\ .$$

Since $\overline{\mathbf{a}}$ is a basis of X/R, the matrix B has determinantal rank r by Lemma 5.7. Hence B has an invertible $(r \times r)$–submatrix E. By renumbering of the basis $(\overline{x}_1, \dots, \overline{x}_n)$ we move E to the left side such that $B = (E \mid A)$. Since E is invertible, we can permute the columns to a straight matrix, cf. Proposition 4.11. By [Mut99, Proposition 2.1] we can multiply the rows by units such that we may assume that $E = (m_{i,j})_{\substack{i=1,\dots,r\\ j=1,\dots,r}}$ is normed. Now we transform (ΛE) into an upper triangular matrix.

(1) It is $m_{1,1} = 1$. For all $i > 1$ we perform the following procedure: We subtract the $(p^{e_1-e_i} \cdot m_{i,1})$–multiple of the first row from the i–th row. Then the new coefficient at the place $(i,1)$ in the matrix (ΛE) is $p^{e-e_i}m_{i,1} - (p^{e_1-e_i}m_{i,1}) \cdot p^{e-e_1}\underbrace{m_{1,1}}_{=1} = p^{e-e_i}(m_{i,1} - m_{i,1}) = 0$. Since these p–elementary row operations do not change the determinant, the new matrix E is normed again.

(2) Now $m_{2,2} = 1$, since E is normed and $m_{2,1} = 0$. The Gauß–algorithm eliminates the coefficients $m_{3,2}, \dots, m_{r,2}$.

(i) We rerun this procedure in step (i) for the i–th column.

Then $E = \begin{pmatrix} 1 & & m_{i,j} \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ is an upper triangular matrix.

Each element $m \in \mathbb{Z}_{p^e}$ from the ring of residue classes of the rational integers mod p^e has a unique integral representative $m^* \in \{0, 1, \dots, p^e - 1\}$ such that $m = m^* + p^e\mathbb{Z}$. Let $0 \le l < e$ be an integer. We can use division by p^l to obtain integers $m' \in \{0, 1, \dots, p^l - 1\}$ and $m'' \in \{0, 1, \dots, p^{e-l} - 1\}$ such that

$$m^* = m' + m'' \cdot p^l.$$

Now we shorten the p–adic expansion of the coefficients $m_{i,j}$ in E. For all $i < j$ we do the following procedure: Let $l = e_i - e_j \ge 0$. We subtract the $(m''_{i,j})$–multiple of the j–th row from the i–th row. Then the representative of the new coefficient at the place (i,j) in the matrix (DE) is

$$p^{e-e_i}m^*_{i,j} - m''_{i,j} \cdot p^{e-e_j}\underbrace{m^*_{j,j}}_{=1} = p^{e-e_i}(m'_{i,j} + m''_{i,j} \cdot p^{e_i-e_j}) - p^{e-e_j}m''_{i,j} = p^{e-e_i}m'_{i,j}\ ,$$

where $0 \le m'_{i,j} \le p^{e_i - e_j} - 1$. This is the cut off expansion of the new representative. Let this procedure run through the columns 2 to r. In that way an entry changes only once a time. □

Remark 5.11. Each element of the representing matrix $M = \operatorname{diag}(p^{e-e_1}, \dots, p^{e-e_r}) \cdot B$ has the form

$$p^{e-e_i}\, m_{i,j} \in \mathbb{Z}_{p^e} \ ,$$

where $m_{i,j}$ is unique modulo $p^{e_i}\,\mathbb{Z}_{p^e}$.

Example 5.12. Let p be a prime and τ_1, τ_2, τ_3 pairwise incomparable types with p–height $0 = \tau_j(p)$. Then $R := \tau_1 x_1 \oplus \tau_2 x_2 \oplus \tau_3 x_3$ is a p–reduced rigid completely decomposable group. Let

$$X = R + \mathbb{Z}\frac{1}{p^2}(x_1 + x_2 \qquad) + \mathbb{Z}\frac{1}{p^2}(\qquad px_2 + px_3)$$

be an almost completely decomposable group. One calculates $X/R \cong (\mathbb{Z}/p^2\mathbb{Z}) \oplus (\mathbb{Z}/p\mathbb{Z})$ and therefore $\exp \frac{X}{R} = p^2$. We use Lemma 2.29 to identify the regulator with $R = \mathrm{R}(X)$. By the Modular Law we get

$$X \cap (p^{-2}\tau_j x_j + R) = (X \cap p^{-2}\tau_j x_j) + R = \tau_j x_j + R = R \ \Rightarrow\ \frac{X}{R} \cap \frac{p^{-2}\tau_j x_j + R}{R} = 0$$

for all $j \in \{1, 2, 3\}$. Abbreviate $a_1 := x_1 + x_2$ and $a_2 := px_2 + px_3$. Let $\overline{} : R \to \overline{R} = p^{-2}R/R$, $x \mapsto \overline{x} = p^{-2}x + R$ denote the natural epimorphism. Then $\overline{\mathbf{a}} = (\overline{a}_1, \overline{a}_2)$ is a basis of X/R and $\overline{\mathbf{x}} = (\overline{x}_1, \overline{x}_2, \overline{x}_3)$ is a basis of $\overline{R} = p^{-2}R/R \cong (\mathbb{Z}/p^2\mathbb{Z})^3$. The representing matrix of X/R relative to $\overline{\mathbf{a}}$ and $\overline{\mathbf{x}}$ is in Gauß normal form (5.10):

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & p & p \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \underbrace{\left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 1 & 1 \end{array}\right)}_{=B} .$$

Each submatrix obtained from the right factor B by deleting one column has p–independent rows. Note that the rest block $\binom{0}{1}$ is not primitive. Hence the statement $R = \mathrm{R}(X)$ is not equivalent to a primitive rest block. This equivalence holds for uniform groups, cf. Lemma 5.13. △

Lemma 5.13. *Let p be a prime and e, n, $r \in \mathbb{N}$ natural numbers with $r < n$. Let X be a p–reduced rigid almost completely decomposable group of rank n with a completely decomposable subgroup R such that $X/R \cong \bigoplus_{i=1}^{r} (\mathbb{Z}/p^{e_i}\mathbb{Z})$, where $e = e_1 \ge \cdots \ge e_r \ge 1$. Let $\overline{\mathbf{x}}$ be an ordered basis of $p^{-e}R/R$ and $\overline{\mathbf{a}} = (\overline{a}_1, \dots, \overline{a}_r)$ an ordered basis of X/R with $\langle \overline{a}_i \rangle \cong \mathbb{Z}/p^{e_i}\mathbb{Z}$. Let $B \in \mathbb{M}^{r \times n}(\mathbb{Z}_{p^e})$ be some matrix such that*

$$M = \operatorname{diag}(p^{e-e_1}, \dots, p^{e-e_r}) \cdot B$$

is the representing matrix of X/R relative to $\overline{\mathbf{a}}$ and $\overline{\mathbf{x}}$.

Then $R = \mathrm{R}(X)$ is the regulator of X if and only if any submatrix obtained from B by deleting one column has determinantal rank r.

If in addition $e = e_1 = \cdots = e_r$ and $M = (I_r \mid A)$ is in Hermite normal form, then R is the regulator of X if and only if A is primitive.

Proof. Write $R = \bigoplus_{j=1}^n R_{\tau_j} = \bigoplus_{j=1}^n \langle x_j \rangle_*^R$, where $\mathbf{x} = (x_1, \dots, x_n)$ is an ordered p–decomposition basis with $\mathrm{tp}(x_j) = \tau_j \in \mathrm{T}_{\mathrm{cr}}(R)$. Let $\overline{} : R \to \overline{R} = p^{-e}R/R$, $x \mapsto \overline{x} = p^{-e}x + R$ denote the natural epimorphism. Recall that $\frac{X}{R} = \bigoplus_{i=1}^r \mathbb{Z}_{p^e}\overline{a}_i$ and $\bigoplus_{j=1}^n \frac{p^{-e}R_{\tau_j}+R}{R} = \frac{p^{-e}R}{R} = \overline{R} = \bigoplus_{j=1}^n \overline{R}_{\tau_j} = \bigoplus_{j=1}^n \mathbb{Z}_{p^e}\overline{x}_j$. Write $B = (\beta_{ij})_{\substack{i=1,\dots,r\\ j=1,\dots,n}}$ and $(\alpha_{ij})_{i,j} = M = \mathrm{diag}(p^{e-e_1}, \dots, p^{e-e_r}) \cdot B = (p^{e-e_i}\beta_{ij})_{i,j}$. Let $B^{(k)}$ denote the $[r \times (n-1)]$–matrix over $\mathbb{Z}_{p^e}$ obtained from B by deleting the k–th column. This matrix $B^{(k)}$ has p–independent rows if and only if $\mathrm{rk}_{\det} B^{(k)} = r$. By the regulator criterion 2.29, we have to show:

$$
\begin{aligned}
&\frac{X}{R} \cap \frac{p^{-e}R_{\tau_k}+R}{R} = 0 \text{ for all } k = 1, \dots, n \quad \Big[\overset{2.29}{\Longleftrightarrow} R = \mathrm{R}(X) \Big] \\
\Longleftrightarrow \quad & B^{(k)} \text{ has } p\text{–independent rows for all } k = 1, \dots, n\, .
\end{aligned}
$$

“$\Leftarrow$” Assume that $k \in \{1, \dots, n\}$ and $B^{(k)}$ has p–independent rows. Let $\sum_{i=1}^r m_i\overline{a}_i \in \frac{X}{R} \cap \frac{p^{-e}R_{\tau_k}+R}{R} \subseteq \frac{p^{-e}R_{\tau_k}+R}{R} = \mathbb{Z}_{p^e}\overline{x}_k$ be an arbitrary element of the intersection. Then

$$
\sum_{i=1}^r m_i\overline{a}_i = \sum_{i=1}^r m_i\Big(\sum_{j=1}^n \alpha_{ij}\overline{x}_j\Big) = \sum_{j=1}^n \Big(\sum_{i=1}^r m_i\alpha_{ij}\Big)\overline{x}_j \in \mathbb{Z}_{p^e}\overline{x}_k\, .
$$

Since the sum $\overline{R} = \bigoplus_{j=1}^n \mathbb{Z}_{p^e}\overline{x}_j$ is direct, we conclude $\sum_{i=1}^r m_i\alpha_{ij} = \sum_{i=1}^r (m_ip^{e-e_i})\,\beta_{ij} = 0$ in $\mathbb{Z}_{p^e}$ for all $j \neq k$. Hence

$$
(m_1p^{e-e_1}, \dots, m_rp^{e-e_r}) \cdot B^{(k)} = (\underbrace{0, \dots, 0}_{n-1 \text{ times}})\, .
$$

So $(m_1p^{e-e_1}, \dots, m_rp^{e-e_r}) = (0, \dots, 0)$ as the rows of $B^{(k)}$ are p–independent. Thus $\sum_{i=1}^r m_i\overline{a}_i = \sum_{i=1}^r m_i\big(\sum_{j=1}^n \alpha_{ij}\overline{x}_j\big) = \sum_{j=1}^n \sum_{i=1}^r \underbrace{m_ip^{e-e_i}}_{=0}\beta_{ij}\overline{x}_j = 0$ and therefore $\frac{X}{R} \cap \frac{p^{-e}R_{\tau_k}+R}{R} = 0$. Since this is true for all $k = 1, \dots, n$, $\mathrm{R}(X) = R$ follows.

“$\Rightarrow$” Assume that $k \in \{1, \dots, n\}$ and $\frac{X}{R} \cap \frac{p^{-e}R_{\tau_k}+R}{R} = 0$. Then $\frac{X}{R}[p] \cap \frac{p^{-1}R_{\tau_k}+R}{R} = 0$. Notice that $\frac{X}{R}[p] = \frac{p^{-1}R \cap X}{R} = \langle p^{e_i-1}\overline{a}_i \mid 1 \le i \le r \rangle$ is the p–socle of $\frac{X}{R}$ and $\frac{p^{-1}R_{\tau_k}+R}{R} = \langle p^{e-1}\overline{x}_k \rangle$ is the p–socle of $\overline{R}_{\tau_k} = \frac{p^{-e}R_{\tau_k}+R}{R}$. Let $m_1, \dots, m_r \in \mathbb{Z}_{p^e}$ such that $(m_1,\dots,m_r)\cdot B^{(k)} \in p\,(\mathbb{Z}_{p^e})^{n-1}$. Then

$$\begin{aligned}
\frac{X}{R}[p] \ni \sum_{i=1}^{r} m_i p^{e_i-1}\overline{a}_i &= \sum_{i=1}^{r} m_i p^{e_i-1}\Big(\sum_{j=1}^{n} \underbrace{\alpha_{ij}}_{=p^{e-e_i}\beta_{ij}} \overline{x}_j\Big) \\
&= \sum_{j=1}^{n} p^{e-1}\Big(\underbrace{\sum_{i=1}^{r} m_i\beta_{ij}}_{\in p\mathbb{Z}_{p^e} \text{ for } j\neq k}\Big)\overline{x}_j \\
&= p^{e-1}\Big(\sum_{i=1}^{r} m_i\beta_{ik}\Big)\overline{x}_k \in \langle p^{e-1}\overline{x}_k\rangle = \frac{p^{-e}R_{\tau_k}+R}{R}[p]\,.
\end{aligned}$$

Therefore $p^{e-1}\big(\sum_{i=1}^r m_i\beta_{ik}\big)\overline{x}_k \in \frac{X}{R}[p] \cap \frac{p^{-e}R_{\tau_k}+R}{R}[p] = 0$, so $(m_1,\dots,m_r)\cdot(\beta_{1k},\dots,\beta_{rk})^{\mathrm{tr}} = \sum_{i=1}^r m_i\beta_{ik} \in p\mathbb{Z}_{p^e}$, since $\operatorname{ord}\overline{x}_k = p^e$. Hence

$$(m_1,\dots,m_r)\cdot B \in p\,(\mathbb{Z}_{p^e})^n\,,$$

and therefore $(m_1,\dots,m_r) \in (p\mathbb{Z}_{p^e})^n$, since B has p–independent rows by Lemma 5.7. We have shown

$$(m_1,\dots,m_r)\cdot B^{(k)} \in p\,(\mathbb{Z}_{p^e})^{n-1} \implies (m_1,\dots,m_r) \in (p\mathbb{Z}_{p^e})^r\,.$$

For $1 \le l \le e$ we get recursively the implication

$$(n_1,\dots,n_r)\cdot B^{(k)} \in p^l\,(\mathbb{Z}_{p^e})^{n-1} \implies (n_1,\dots,n_r) \in \big(p^l\mathbb{Z}_{p^e}\big)^r\,.$$

This shows, by definition [Fuc73, 32.], the p–independence of the rows of $B^{(k)}$ in $\big[(\mathbb{Z}_{p^e})^{n-1}, +\big]$ for all $k = 1,\dots,n$.

For the second statement use Lemma 4.21. □

Lemma 5.14. *Let p be a prime and e, n, r natural numbers. Let X be a rigid p–reduced almost completely decomposable group of rank n with regulator R such that*

$$X/R \cong (\mathbb{Z}/p^{e_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{e_r}\mathbb{Z}), \qquad \textit{where} \qquad e = e_1 \ge \cdots \ge e_r \ge 1.$$

Let $\overline{\mathbf{x}}$ be an ordered induced basis of $p^{-e}R/R$ and $\overline{\mathbf{a}} = (\overline{a}_1,\dots,\overline{a}_r)$ an ordered basis of X/R with $\langle\overline{a}_i\rangle \cong \mathbb{Z}/p^{e_i}\mathbb{Z}$. Let $B \in \mathbb{M}^{r\times n}(\mathbb{Z}_{p^e})$ be some matrix such that

$$M = \operatorname{diag}(p^{e-e_1},\dots,p^{e-e_r})\cdot B$$

is the representing matrix of X/R relative to $\overline{\mathbf{a}}$ and $\overline{\mathbf{x}}$.

Then a pivot set of B does not depend on the bases $\overline{\mathbf{a}}$ and $\overline{\mathbf{x}}$. In particular, pivot sets are invariants of X.

Proof. From a basis $\overline{\mathbf{a}} = (\overline{a}_1,\dots,\overline{a}_r)$ one gets another basis $\overline{\mathbf{a}}'$ by a sequence of p–elementary row operations of the Gauß–algorithm to M. Clearly, p–elementary row operations do not change the p–independence of the r pivot columns. Thus pivot sets do not depend on a basis $\overline{\mathbf{a}}$ of X/R.

Write $M = (\alpha_{ij})_{i,j}$ and $B = (\beta_{ij})_{i,j}$. Then $\alpha_{ij} = p^{e-e_i}\beta_{ij}$ for all i, j. Let $\overline{} : R \to \overline{R} = p^{-e}R/R,\ x \mapsto \overline{x} = p^{-e}x + R$ denote the natural epimorphism and let $\mathbf{x} = (x_1, \dots, x_n)$ be a p–basis of R such that $\overline{\mathbf{x}} = (\overline{x}_1, \dots, \overline{x}_n)$ is induced by $\mathbf{x}$. Since R is p–reduced and rigid, one obtains every other ordered p–decomposition basis $\mathbf{y} = (y_1, \dots, y_n)$ of R by multiplying $\mathbf{x} = (x_1, \dots, x_n)$ by rational numbers $q_j \in \mathbb{Q}_p \setminus p\mathbb{Q}_p$ whose numerators and denominators are relatively prime to p, i. e. $y_j = q_j x_j$. Let

$$\sim \; : \; \mathbb{Q}_p \to \mathbb{Z}_{p^e}, \; \frac{a}{b} \mapsto (b + p^e\mathbb{Z})^{-1}(a + p^e\mathbb{Z}),$$

where $a, b \in \mathbb{Z}$ with $p \nmid b$, be a ring homomorphism which supplies $\overline{y}_j = \overline{q_j x_j} = \widetilde{q}_j \overline{x}_j$. Here $q_j \in \mathbb{Q}_p \setminus p\mathbb{Q}_p$ yields $\widetilde{q}_j \in \mathbb{Z}_{p^e} \setminus p\mathbb{Z}_{p^e} = \mathbb{Z}^*_{p^e}$. Then $\overline{\mathbf{y}} = (\overline{y}_1, \dots, \overline{y}_n) = (\widetilde{q}_1\overline{x}_1, \dots, \widetilde{q}_n\overline{x}_n)$ is the new ordered induced decomposition basis of $p^{-e}R/R$. Therefore $\overline{a}_i = \sum_{j=1}^n \alpha_{ij}\overline{x}_j = \sum_{j=1}^n \alpha_{ij}\widetilde{q}_j^{-1}\overline{y}_j$ for $i = 1, \dots, r$ and $M' = (\alpha_{ij}\widetilde{q}_j^{-1})_{i,j} = (p^{e-e_i}\beta_{ij}\widetilde{q}_j^{-1})_{i,j} = \operatorname{diag}(p^{e-e_1}, \dots, p^{e-e_r}) \cdot B \cdot \operatorname{diag}(\widetilde{q}_1^{-1}, \dots, \widetilde{q}_n^{-1})$ is the new representing matrix of X/R relative to $\overline{\mathbf{a}}$ and $\overline{\mathbf{y}}$. Since $\widetilde{q}_j^{-1} \in \mathbb{Z}^*_{p^e}$ is a unit, the r pivot columns of $B \cdot \operatorname{diag}(\widetilde{q}_1^{-1}, \dots, \widetilde{q}_n^{-1})$ are again p–independent. □

Definition 5.15. Let p be a prime and e, n, $r \in \mathbb{N}$ natural numbers with $r < n$. Let X be a p–reduced almost completely decomposable group of rank n with regulator R such that $X/R \cong \bigoplus_{i=1}^r (\mathbb{Z}/p^{e_i}\mathbb{Z})$, where $e = e_1 \geq \cdots \geq e_r \geq 1$. Let $\mathbf{x} = (x_1, \dots, x_n)$ be a decomposition basis of R ordered by the critical typeset $T = (\tau_1, \dots, \tau_n)$, i. e. $\operatorname{tp}^R(x_j) = \tau_j$. Let $\overline{\mathbf{x}}$ be the induced basis of $\overline{R} = p^{-e}R/R$ and $\overline{\mathbf{a}} = (\overline{a}_1, \dots, \overline{a}_r)$ an ordered basis of X/R with $\langle \overline{a}_i \rangle \cong \mathbb{Z}/p^{e_i}\mathbb{Z}$. Let $B = (\beta_{ij})_{\substack{i=1,\dots,r \\ j=1,\dots,n}}$ be some matrix over $\mathbb{Z}_{p^e}$ such that

$$M = \operatorname{diag}(p^{e-e_1}, \dots, p^{e-e_r}) \cdot B$$

is the representing matrix of X/R relative to $\overline{\mathbf{a}}$ and $\overline{\mathbf{x}}$.

Then the subset $\{\tau_{j_1}, \dots, \tau_{j_r}\}$ of T corresponding to some pivot set $\{j_1, \dots, j_r\} \subseteq \{1, \dots, n\}$ of the columns of B is called a *pivot set* of X.

The n–tuple $T = (\tau_1, \dots, \tau_r, \tau_{r+1}, \dots, \tau_n)$ is said to be an *admissible indexing* of the critical typeset of X if there is a basis $\overline{\mathbf{a}}'$ of X/R such that $B = (E \mid A)$ is the Gauß normal form (5.10), where

$$E = \begin{pmatrix} 1 & m_{12} & \cdots & m_{1r} \\ 0 & 1 & \cdots & m_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathbb{M}^{r \times r}(\mathbb{Z}_{p^e}) \; .$$

6. Matrix [Near–]Isomorphism Criterion for p–local Groups

Remark 6.1. Let p be a prime. In this chapter we want to describe the concept of near–isomorphism of p–local groups in a new way. We develop a method to investigate two given p–local groups up to near–isomorphism and isomorphism.

Let X and Y be p–local groups with a common regulator $\mathrm{R}(X) = \mathrm{R}(Y) = R$. Thus $X, Y \subseteq p^{-e}R$. Let $\overline{} : R \to \overline{R} = p^{-e}R/R,\ x \mapsto \overline{x} = p^{-e}x + R$ denote the natural epimorphism. Furthermore, $\overline{}$ will denote as well the induced homomorphism $\overline{} : \operatorname{Aut} R \to \operatorname{Aut} \overline{R}$, $\alpha \mapsto \overline{\alpha}$ via $\overline{\alpha}(\overline{x}) := \overline{\alpha(x)}$. Recall that

$$\operatorname{TypAut} \overline{R} = \{\xi \in \operatorname{Aut} \overline{R} \mid \forall_{\tau \in \mathrm{T_{cr}}(R)}\ \xi\overline{R(\tau)} = \overline{R(\tau)}\}$$

is the set of type automorphisms of $\overline{R}$ and

$$\overline{\operatorname{Aut} R} = \{\overline{\alpha} \mid \alpha \in \operatorname{Aut} R\}$$

is the set of induced automorphisms of $\overline{R}$.

(1) The groups X and Y are nearly isomorphic if and only if there exists $\xi \in \operatorname{TypAut} \overline{R}$ such that $\xi \frac{X}{R} = \frac{Y}{R}$.

(2) The groups X and Y are isomorphic if and only if there exists $\zeta \in \overline{\operatorname{Aut} R}$ such that $\zeta \frac{X}{R} = \frac{Y}{R}$.

Definition 6.2. Let m be a natural number and τ any type. Define

$$\mathbb{Z}_m^*(\tau) := \langle -1 + m\mathbb{Z},\ q + m\mathbb{Z} \in \mathbb{Z}_m^* \mid q \text{ prime number},\ \tau(q) = \infty \rangle_{\text{mult.}}.$$

Denote its order by $\varphi(\tau; m) := |\mathbb{Z}_m^*(\tau)|$.

Remark 6.3. (a) The group $\mathbb{Z}_m^*(\tau)$ is a subgroup of the multiplicative group $\mathbb{Z}_m^* = \{n + m\mathbb{Z} \in \mathbb{Z}_m \mid \gcd(n, m) = 1\}$ of units in $\mathbb{Z}_m$. Hence $\varphi(\tau; m)$ divides $\varphi(m) := |\mathbb{Z}_m^*| = |\{n \in \mathbb{Z} \mid 1 \le n < m,\ \gcd(n, m) = 1\}|$, by Lagrange. Recall that the *Euler φ–function* $\varphi : \mathbb{N} \to \mathbb{N}$ is multiplicative.

(b) Let p be a prime and e a natural number. Observe that $\mathbb{Z}_{p^e}^*(\tau) \subseteq \mathbb{Z}_{p^e}^*$ and $\mathbb{Z}_{p^e}^*$ is cyclic of order $\varphi(p^e) = p^{e-1}(p-1)$. Therefore, each subgroup $\mathbb{Z}_{p^e}^*(\tau)$ is also cyclic and its order divides $p^{e-1}(p-1)$.

(c) Let p be a prime, e a natural number and τ a type with $\tau(p) \neq \infty$. If A is a τ–homogeneous group, then $\mathbb{Z}_{p^e}^*(\tau) = \langle -1 + p^e\mathbb{Z},\ q + p^e\mathbb{Z} \mid q \text{ prime},\ qA = A\rangle_{\text{mult.}}$. By assumption all primes q with $\tau(q) = \infty$ are relatively prime to p^e. Since A is a homogeneous group of type τ, we have $\tau(q) = \infty$ for a prime q if and only if $qA = A$.

(d) In the particular case that $\tau \in T$ is a critical type of the p–reduced completely decomposable group $R = \bigoplus_{\rho \in T} R_\rho$ we obtain

$$\mathbb{Z}_{p^e}^*(\tau) = \langle -1 + p^e\mathbb{Z},\ q + p^e\mathbb{Z} \mid q \text{ prime number},\ qR_\tau = R_\tau\rangle_{\text{mult.}}.$$

Lemma 6.4. *Let R be a rigid and p–reduced completely decomposable group with decomposition basis $\mathbf{x} = (x_1, \dots, x_n)$, which is ordered by the critical typeset $T = (\tau_1, \dots, \tau_n)$. Then $\overline{\mathbf{x}} = (\overline{x}_1, \dots, \overline{x}_n)$ is an ordered induced decomposition basis of $\overline{R} = p^{-e}R/R$. Let $\xi, \zeta \in \operatorname{Aut} \overline{R}$.*

(1) *Then $\xi \in \operatorname{TypAut} \overline{R}$ is a type automorphism of $\overline{R}$ if and only if there exist $d_j \in \mathbb{Z}^*_{p^e}$ such that*
$$\xi \overline{x}_j = d_j \overline{x}_j$$
for $j = 1, \dots, n$.

(2) *Then $\zeta \in \overline{\operatorname{Aut} R}$ is an induced automorphism of $\overline{R}$ if and only if there exist $f_j \in \mathbb{Z}^*_{p^e}(\tau_j)$ such that*
$$\zeta \overline{x}_j = f_j \overline{x}_j$$
for $j = 1, \dots, n$.

Proof. (1) The arrangement of the basis $\mathbf{x}$ by T means $\tau_j = \operatorname{tp}^R(x_j)$. Since R is rigid, $R(\tau) = R_\tau$ has rank 1 for all $\tau \in T$. We have $R = \bigoplus_{j=1}^n \langle x_j \rangle_*^R = \bigoplus_{j=1}^n R(\tau_j)$ and $p^{-e}R/R = \overline{R} = \bigoplus_{j=1}^n \overline{R(\tau)} = \bigoplus_{j=1}^n \mathbb{Z}_{p^e} \overline{x}_j$. A type automorphism ξ is completely determined by the images of the basis $\overline{\mathbf{x}}$. It follows that $\xi \overline{x}_j \in \xi \overline{R(\tau_j)} = \overline{R(\tau_j)} = \mathbb{Z}_{p^e} \overline{x}_j$, since R is rigid. Thus $\xi \overline{x}_j = d_j \overline{x}_j$, where $d_j \in \mathbb{Z}_{p^e}$. Since $\xi \in \operatorname{Aut} \overline{R}$ is an automorphism, we have $\xi^{-1} \in \operatorname{Aut} \overline{R}$ such that $\overline{x}_j = \xi^{-1}\xi \overline{x}_j = \xi^{-1} d_j \overline{x}_j = d_j \xi^{-1} \overline{x}_j = d_j d'_j \overline{x}_j$. Therefore, there are $d_j \in \mathbb{Z}^*_{p^e}$ such that $\xi \overline{x}_j = d_j \overline{x}_j$ for $j = 1, \dots, n$.
On the other hand $\xi \overline{x}_j := d_j \overline{x}_j$ — where $d_j \in \mathbb{Z}^*_{p^e}$ for $j = 1, \dots, n$ — defines a type automorphism ξ of $\overline{R}$.

(2) This is a special case of [KM84, Theorem 1.3]. We provide evidence in another way. Since $\overline{\operatorname{Aut} R} \subseteq \operatorname{TypAut} \overline{R}$ we can use part (1) of this Lemma. If $\zeta \in \overline{\operatorname{Aut} R}$ is induced by an automorphism ζ^* of R, then $\zeta = \overline{\zeta^*}$ and there are $f_j \in \mathbb{Z}^*_{p^e}$ such that $\zeta \overline{x}_j = f_j \overline{x}_j$. There is a $f_j^* \in \mathbb{Z}$ such that $\zeta^* R_{\tau_j} = f_j^* R_{\tau_j} = R_{\tau_j}$, since R is rigid. Then $f_j = f_j^* + p^e\mathbb{Z} \in \langle -1 + p^e\mathbb{Z},\ q + p^e\mathbb{Z} \mid q \text{ prime number},\ qR_{\tau_j} = R_{\tau_j} \rangle$. Therefore there are $f_j \in \mathbb{Z}^*_{p^e}(\tau_j)$ such that $\zeta \overline{x}_j = f_j \overline{x}_j$ for $j = 1, \dots, n$.
On the other hand $\zeta \overline{x}_j := f_j \overline{x}_j$ — where $f_j \in \mathbb{Z}^*_{p^e}(\tau_j)$ for $j = 1, \dots, n$ — defines an induced automorphism ζ of $\overline{R}$. □

Definition 6.5. Let p be a prime and e, n natural numbers. Let R be a rigid and p–reduced completely decomposable group of rank n. Suppose that $T = (\tau_1, \dots, \tau_n)$ is an indexing of the critical typeset. Let $\overline{} : R \to \overline{R} = p^{-e}R/R$, $x \mapsto \overline{x} = p^{-e}x + R$ denote the canonical epimorphism. Let $\mathbf{x} = (x_1, \dots, x_n)$ be a decomposition basis of R ordered by T and $\overline{\mathbf{x}} = (\overline{x}_1, \dots, \overline{x}_n)$ the ordered induced decomposition basis of $\overline{R}$.

(1) Let $\xi \in \operatorname{TypAut} \overline{R}$ such that $\xi \overline{x}_j = d_j \overline{x}_j$ with $d_j \in \mathbb{Z}^*_{p^e}$ for $j = 1, \dots, n$. The invertible diagonal matrix
$$D := \operatorname{diag}(d_1, \dots, d_n) \in \mathbb{M}^{n \times n}(\mathbb{Z}_{p^e})$$
is called *representing matrix* of the type automorphism ξ relative to $\overline{\mathbf{x}}$.

(2) Let $\zeta \in \overline{\operatorname{Aut} R}$ such that $\zeta\overline{x}_j = f_j\overline{x}_j$ with $f_j \in \mathbb{Z}^*_{p^e}(\tau_j)$ for $j = 1, \dots, n$. The invertible diagonal matrix

$$F := \operatorname{diag}(f_1, \dots, f_n) \in \mathbb{M}^{n\times n}(\mathbb{Z}_{p^e})$$

is called *representing matrix* of the induced automorphism ζ relative to $\overline{\mathbf{x}}$.

Remark 6.6. Let p be a prime and $e = e_1 \geq \cdots \geq e_r \geq 1$ natural numbers. Let $M = \bigoplus_{i=1}^r \langle \overline{a}_i \rangle$ be a finite $(\mathbb{Z}/p^e\mathbb{Z})$–module, where $\langle \overline{a}_i \rangle \cong p^{e-e_i}(\mathbb{Z}/p^e\mathbb{Z}) \cong \mathbb{Z}/p^{e_i}\mathbb{Z}$. Let $\Gamma : M \to M$ be a module endomorphism and $\gamma_{ij} \in \mathbb{Z}_{p^e}$, $1 \leq i, j \leq r$, such that $\Gamma(\overline{a}_i) = \sum_{j=1}^r \gamma_{ij}\overline{a}_j$ for all i.

Then $\gamma_{ij} \in p^{e_j - e_i}\mathbb{Z}_{p^e}$ for all $j \leq i$ and Γ is an automorphism of M if and only if $P = (\gamma_{ij})_{1\leq i,j\leq r}$ is invertible.

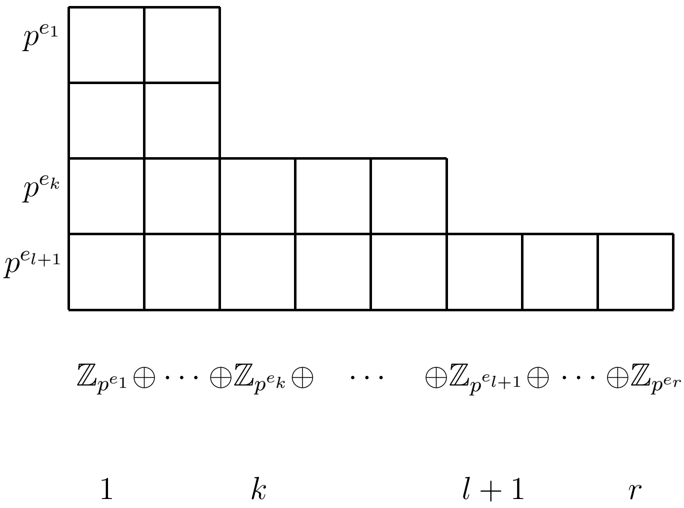
Proof. From $\operatorname{Ann} \overline{a}_i = p^{e_i}\,\mathbb{Z}_{p^e}$ we conclude $0 = \Gamma(0) = \Gamma(p^{e_i}\,\overline{a}_i) = p^{e_i}\,\Gamma(\overline{a}_i) = \sum_{j=1}^r p^{e_i}\gamma_{ij}\overline{a}_j$. This implies $p^{e_i}\gamma_{ij} \in \operatorname{Ann} \overline{a}_j = p^{e_j}\mathbb{Z}_{p^e}$ for the j–th summand, since the sum is direct. Therefore $\gamma_{ij} \in p^{e_j - e_i}\mathbb{Z}_{p^e}$ if $e_j \geq e_i$ or equivalently $j \leq i$.
The equivalence is clear. □

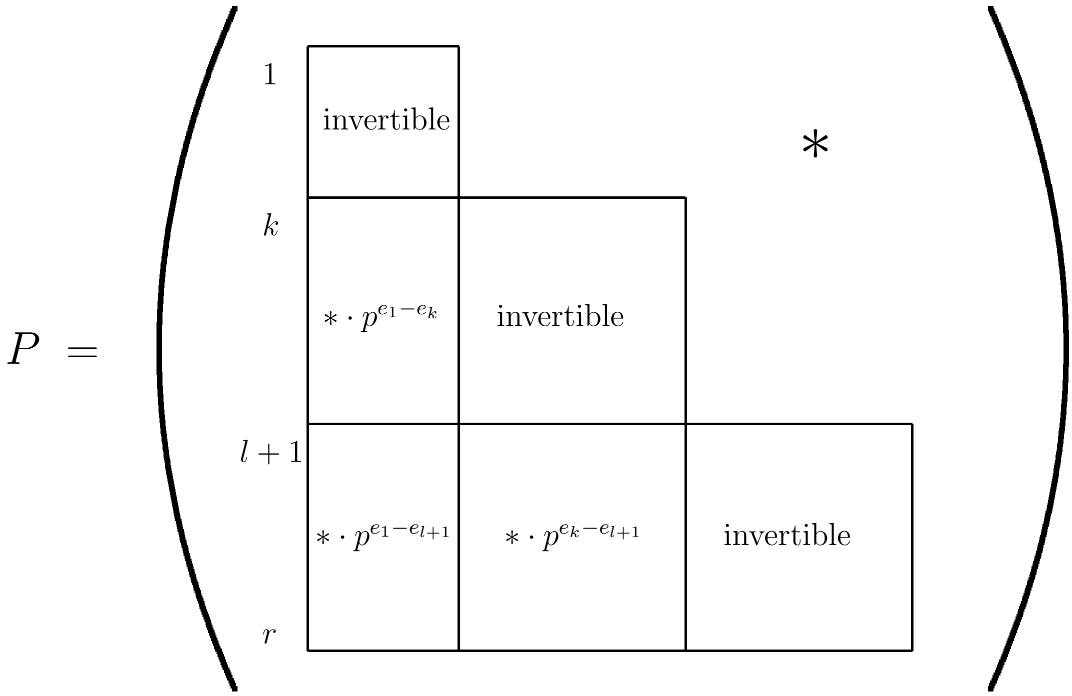
Definition 6.7. Let p be a prime and $e = e_1 \geq \cdots \geq e_r \geq 1$ natural numbers. Let $M = \bigoplus_{i=1}^r \langle \overline{a}_i \rangle$ be a $(\mathbb{Z}/p^e\mathbb{Z})$–module, where $\langle \overline{a}_i \rangle \cong p^{e-e_i}(\mathbb{Z}/p^e\mathbb{Z})$. Let $\Gamma : M \to M$ be an automorphism and $\gamma_{ij} \in \mathbb{Z}_{p^e}$, $1 \leq i, j \leq r$, such that $\Gamma(\overline{a}_i) = \sum_{j=1}^r \gamma_{ij}\overline{a}_j$ for all i. The regular matrix

$$P = (\gamma_{ij})_{1\leq i,j\leq r}$$

is called *representing matrix* of the automorphism Γ relative to $\overline{\mathbf{a}} := \{\overline{a}_1, \dots, \overline{a}_r\}$.

Remark 6.8. The representing matrix P of the automorphism $\Gamma : \bigoplus_{i=1}^{r} \mathbb{Z}_{p^{e_i}} \to \bigoplus_{i=1}^{r} \mathbb{Z}_{p^{e_i}}$ has the following form:





This matrix $P = (\gamma_{ij})_{1 \leq i,j \leq r}$ is invertible with $\gamma_{ij} \in p^{e_j - e_i}\mathbb{Z}_{p^e}$ if $j \leq i$. If $e_{k-1} > e_k = \ldots = e_l > e_{l+1}$, then the diagonal block $(\gamma_{ij})_{k \leq i,j \leq l}$ is invertible. Notice that the coefficient γ_{ij} is only unique modulo $p^{e_j}\mathbb{Z}_{p^e}$: Since $\operatorname{Ann} \overline{a}_j = p^{e_j}\mathbb{Z}_{p^e}$, we recognize that $\Gamma(\overline{a}_i) = \sum_{k \neq j} \gamma_{ik}\overline{a}_k + \gamma_{ij}\overline{a}_j = \sum_{k \neq j} \gamma_{ik}\overline{a}_k + (\gamma_{ij} + m \cdot p^{e_j})\overline{a}_j$ for all $m \in \mathbb{Z}_{p^e}$.

Definition 6.9. Let p be a prime and r, n natural numbers. Let $e = e_1 \geq \cdots \geq e_r \geq 1$ be integers and $\varepsilon = (e_1, \ldots, e_r)$. The matrices A, $B \in \mathbb{M}^{r \times n}(\mathbb{Z}_{p^e})$ are called *ε–congruent* if

$$\operatorname{diag}(p^{e-e_1}, \ldots, p^{e-e_r}) \cdot A = \operatorname{diag}(p^{e-e_1}, \ldots, p^{e-e_r}) \cdot B,$$

and we write $A \equiv_\varepsilon B$ in that case.

Remark 6.10. This ε–congruence "$\equiv_\varepsilon$" is an equivalence relation on $\mathbb{M}^{r \times n}(\mathbb{Z}_{p^e})$.

Theorem 6.11. *Let p be a prime and $r < n$ natural numbers. Let $e = e_1 \geq \cdots \geq e_r \geq 1$ be integers and $\varepsilon = (e_1, \ldots, e_r)$. Let X and Y be p–reduced rigid groups of rank n with a common regulator R such that $X/R \cong \bigoplus_{i=1}^r (\mathbb{Z}/p^{e_i}\mathbb{Z}) \cong Y/R$. Let $\overline{\mathbf{x}} = (\overline{x}_1, \ldots, \overline{x}_n)$ be an induced decomposition basis of $\overline{R} = p^{-e}R/R$ ordered by the indexing $T = (\tau_1, \ldots, \tau_n)$ of the critical typeset. Let $\overline{\mathbf{a}} = (\overline{a}_1, \ldots, \overline{a}_r)$ be a basis of X/R and $\overline{\mathbf{b}} = (\overline{b}_1, \ldots, \overline{b}_r)$ be a basis of Y/R with $\langle \overline{a}_i \rangle \cong \mathbb{Z}/p^{e_i}\mathbb{Z} \cong \langle \overline{b}_i \rangle$. Set $\Lambda = \operatorname{diag}(p^{e-e_1}, \ldots, p^{e-e_r})$. Let A and B be some $(r \times n)$–matrices over $\mathbb{Z}_{p^e}$ such that $M = \Lambda A$ is the representing matrix of X/R relative to $\overline{\mathbf{x}}$ and $\overline{\mathbf{a}}$, and $N = \Lambda B$ is the representing matrix of Y/R relative to $\overline{\mathbf{x}}$ and $\overline{\mathbf{b}}$.*

(1) *The groups X and Y are nearly isomorphic, $X \cong_{\mathrm{nr}} Y$, if and only if there exist an invertible matrix $P = (\gamma_{ij})_{1 \leq i,j \leq r}$ with $\gamma_{ij} \in p^{e_j - e_i}\mathbb{Z}_{p^e}$ for all $j \leq i$ and an invertible diagonal matrix D such that*

$$P\,M\,D \;=\; N\,.$$

Equivalently there is an invertible matrix $Q = (\rho_{ij})_{1 \leq i,j \leq r}$ with $\rho_{ij} \in p^{e_i - e_j}\mathbb{Z}_{p^e}$ for all $i \leq j$ such that $QAD \equiv_\varepsilon B$.

(2) *The groups X and Y are isomorphic, $X \cong Y$, if and only if there exist an invertible matrix $P = (\gamma_{ij})_{1 \leq i,j \leq r}$ with $\gamma_{ij} \in p^{e_j - e_i}\mathbb{Z}_{p^e}$ for all $j \leq i$ and a matrix $F = \operatorname{diag}(f_1, \ldots, f_n)$ with $f_j \in \mathbb{Z}_{p^e}^*(\tau_j)$ such that*

$$P\,M\,F \;=\; N\,.$$

Equivalently there is an invertible matrix $Q = (\rho_{ij})_{1 \leq i,j \leq r}$ with $\rho_{ij} \in p^{e_i - e_j}\mathbb{Z}_{p^e}$ for all $i \leq j$ such that $QAF \equiv_\varepsilon B$.

Proof. Write $M = (\mu_{ij})_{\substack{i=1,\ldots,r \\ j=1,\ldots,n}}$. Recall the abbreviations $P \in \mathcal{P}(p;\varepsilon)$ and $Q \in \mathcal{Q}(p;\varepsilon)$ of Definition 4.22.

(1) "$\Leftarrow$" Assume firstly that $X \cong_{\mathrm{nr}} Y$. Then there exists $\xi \in \operatorname{TypAut} \overline{R}$ with $\xi \frac{X}{R} = \frac{Y}{R}$ and there are units $d_1, \ldots, d_n \in \mathbb{Z}_{p^e}^*$ such that $\xi \overline{x}_j = d_j \overline{x}_j$ for $j = 1, \ldots, n$. Let $D = \operatorname{diag}(d_1, \ldots, d_n)$ be the representing matrix of the type automorphism ξ relative to $\overline{\mathbf{x}}$. We infer from $\langle \xi\overline{a}_1, \ldots, \xi\overline{a}_r \rangle = \xi(\langle \overline{a}_1, \ldots, \overline{a}_r \rangle) = \xi\frac{X}{R} = \frac{Y}{R} \cong \bigoplus_{i=1}^r (\mathbb{Z}/p^{e_i}\mathbb{Z})$ and $\langle \xi\overline{a}_i \rangle = \xi \langle \overline{a}_i \rangle \cong \mathbb{Z}/p^{e_i}\mathbb{Z}$ that $(\xi\overline{a}_1, \ldots, \xi\overline{a}_r) =: \overline{\mathbf{b}}'$ defines a new ordered basis of Y/R. There is an automorphism $\Gamma : \frac{Y}{R} \to \frac{Y}{R}$ which maps the new basis elements $\xi\overline{a}_i =: \overline{b}_i'$ to the old ones $\overline{b}_i$. Let $P = (\gamma_{ij})_{1 \leq i,j \leq r}$ be the representing matrix of the automorphism Γ relative to $\overline{\mathbf{b}}'$. Then $P \in \mathcal{P}(p;\varepsilon)$, by Remark 6.6, and $\overline{b}_i = \Gamma(\overline{b}_i') = \sum_{j=1}^r \gamma_{ij}\overline{b}_j'$.

One computes $\overline{b}_i' = \xi\overline{a}_i = \xi \sum_{j=1}^n \mu_{ij}\overline{x}_j = \sum_{j=1}^n \mu_{ij}\xi\overline{x}_j = \sum_{j=1}^n \mu_{ij}d_j\overline{x}_j$ and $N' := (\mu_{ij}d_j)_{\substack{i=1,\dots,r\\ j=1,\dots,n}} = MD = \Lambda AD$ is the representing matrix of Y/R relative to $\overline{\mathbf{b}}'$ and $\overline{\mathbf{x}}$. By Proposition 4.23 there is a matrix $Q \in \mathcal{Q}(p;\varepsilon)$ such that $P\Lambda = \Lambda Q$. Since Γ maps $\overline{b}_i'$ to $\overline{b}_i$, we conclude for the representing matrix N of Y/R relative to $\overline{\mathbf{b}}$ that

$$\Lambda B = N = PN' = PMD = P\Lambda AD = \Lambda QAD\,,$$

so $B \equiv_\varepsilon QAD$.

"$\Rightarrow$" Conversely let $\Lambda QAD = \Lambda B$, where $Q \in \mathcal{Q}(p;\varepsilon)$ and $D = \operatorname{diag}(d_1,\dots,d_n)$, $d_j \in \mathbb{Z}_{p^e}^*$. Then $\xi\overline{x}_j := d_j\overline{x}_j$ for $j = 1,\dots,n$ defines a type automorphism ξ of $\overline{R}$, by Lemma 6.4(1). There is a matrix $P \in \mathcal{P}(p;\varepsilon)$ with the property $\Lambda Q = P\Lambda$. With the definition $N' := MD$ we get $N = \Lambda B = \Lambda QAD = P\Lambda AD = PMD = PN'$. Set $\overline{b}_i' := \sum_{j=1}^n \mu_{ij}d_j\overline{x}_j = \sum_{j=1}^n \mu_{ij}\xi\overline{x}_j = \xi \sum_{j=1}^n \mu_{ij}\overline{x}_j = \xi\overline{a}_i$ for all i. Note that P is the representing matrix of an automorphism $\Gamma : \frac{Y}{R} \to \frac{Y}{R}$ with $\Gamma(\overline{b}_i') = \overline{b}_i$. Therefore $\overline{\mathbf{b}}' := (\overline{b}_1',\dots,\overline{b}_r')$ is an ordered basis of Y/R with $\operatorname{ord}\overline{b}_i' = \operatorname{ord}\overline{a}_i = p^{e_i}$. Now N' is the representing matrix of Y/R relative to $\overline{\mathbf{b}}'$ and $\overline{\mathbf{x}}$. We have $\frac{Y}{R} = \langle\overline{b}_1',\dots,\overline{b}_r'\rangle = \langle\xi\overline{a}_1,\dots,\xi\overline{a}_r\rangle = \xi(\langle\overline{a}_1,\dots,\overline{a}_r\rangle) = \xi\frac{X}{R}$. Therefore $X \cong_{\mathrm{nr}} Y$.

(2) By the Isomorphism Criterion 3.5, we have $X \cong Y$ if and only if there is an induced automorphism $\zeta \in \overline{\operatorname{Aut} R} \subseteq \operatorname{Aut}\overline{R}$ such that $\zeta\frac{X}{R} = \frac{Y}{R}$. An automorphism ζ is induced exactly if there is a matrix $F = \operatorname{diag}(f_1,\dots,f_n)$ with $f_j \in \mathbb{Z}_{p^e}^*(\tau_j)$ and $\zeta\overline{x}_j = f_j\overline{x}_j$, cf. Lemma 6.4(2). Use F instead of D in part (1) of this proof. All conclusions are the same. □

The following result is a generalization of [DO93, Theorem 2.10].

Theorem 6.12. *Pivot sets are near–isomorphism invariants for reduced p–local rigid groups. Moreover, admissible indexings of the critical typeset are near–isomorphism invariants.*

Proof. Let the group X be given by a representing matrix $\Lambda\,(E \mid A)$, where Λ is a diagonal matrix with p–power entries. Let the critical typeset have a fixed admissible ordering such that

$$E = \begin{pmatrix} 1 & m_{12} & \cdots & m_{1r} \\ 0 & 1 & \cdots & m_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

is of the form (5.10). Let Y be nearly isomorphic to X. Let $\Lambda\,(E' \mid B)$ be the representing matrix of Y relative to the same ordering of the critical typeset. Near–isomorphism means $\mathcal{P}|$ diag–equivalence of the representing matrices. By comparison of the left $(r \times r)$–blocks, there is a representing matrix P of an automorphism of $Y/\operatorname{R}(Y)$ and an invertible diagonal matrix $D_{\leqslant r}$ such that

$P\,E' = E\,D_{\leqslant r}$. Then

$$D_{\leqslant r}^{-1}\,P\,E' = D_{\leqslant r}^{-1}\,E\,D_{\leqslant r} = \begin{pmatrix} 1 & & d_i^{-1}m_{ij}d_j \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

is the upper triangular form (5.10), too. Thus the indexing of the columns is also admissible for Y. □

We investigate p–local groups with a simultaneous admissible indexing of the critical typeset:

Theorem 6.13. (Matrix [Near–]Isomorphism Criterion for p–local Groups)
Let $r < n$ be natural numbers and $e = e_1 \geq \cdots \geq e_r \geq 1$ integers. Let X and Y be p–reduced rigid groups of rank n with a common regulator R such that

$$X/R \cong \bigoplus_{i=1}^{r} (\mathbb{Z}/p^{e_i}\mathbb{Z}) \cong Y/R\,.$$

Let $\overline{\mathbf{x}} = (\overline{x}_1, \ldots, \overline{x}_n)$ be an induced decomposition basis of $\overline{R} = p^{-e}R/R$ ordered by a simultaneous admissible indexing $T = (\tau_1, \ldots, \tau_n)$ of the critical typeset for X and Y. Let $\overline{\mathbf{a}} = (\overline{a}_1, \ldots, \overline{a}_r)$ be a basis of X/R and $\overline{\mathbf{b}} = (\overline{b}_1, \ldots, \overline{b}_r)$ a basis of Y/R with $\langle \overline{a}_i \rangle \cong \mathbb{Z}/p^{e_i}\mathbb{Z} \cong \langle \overline{b}_i \rangle$. Set $\Lambda = \operatorname{diag}(p^{e-e_1}, \ldots, p^{e-e_r})$. Let the representing matrix $M = \Lambda\,(A_{\leqslant r} \mid A_{>r})$ of X/R and the representing matrix $N = \Lambda\,(B_{\leqslant r} \mid B_{>r})$ of Y/R be in the Gauß normal form, where

$$A_{\leqslant r} = \begin{pmatrix} 1 & m_{12} & \cdots & m_{1r} \\ 0 & 1 & \cdots & m_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \quad \text{and} \quad B_{\leqslant r} = \begin{pmatrix} 1 & n_{12} & \cdots & n_{1r} \\ 0 & 1 & \cdots & n_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

(1) *The groups X and Y are nearly isomorphic, $X \cong_{\text{nr}} Y$, if and only if there is a matrix $D = \operatorname{diag}(d_1, \ldots, d_n)$ with $d_j \in \mathbb{Z}_{p^e}^*$ and an upper triangular matrix*

$$P = \begin{pmatrix} d_1^{-1} & & * \\ & \ddots & \\ 0 & & d_r^{-1} \end{pmatrix}$$

such that

$$N = P\,M\,D\,.$$

(2) *The groups X and Y are isomorphic, $X \cong Y$, if and only if there there is a matrix $F = \operatorname{diag}(f_1, \ldots, f_n)$ with $f_j \in \mathbb{Z}_{p^e}^*(\tau_j)$ and an upper triangular matrix*

$$P = \begin{pmatrix} f_1^{-1} & & * \\ & \ddots & \\ 0 & & f_r^{-1} \end{pmatrix}$$

such that

$$N = P\,M\,F\,.$$

Proof. (1) "$\Leftarrow$" Invertible matrices D and P with $N = PMD$ show $X \cong_{\mathrm{nr}} Y$, by Theorem 6.11(1).

"$\Rightarrow$" Assume that $X \cong_{\mathrm{nr}} Y$. By Theorem 6.11(1), there exists an invertible matrix $D = \mathrm{diag}(d_1, \ldots, d_n)$ and a representing matrix P of an automorphism $\Gamma \in \mathrm{Aut}\,\frac{X}{R}$ such that $PMD = N$. We compare the left $(r \times r)$–blocks of this matrix equation:

$$P\,\Lambda \underbrace{\begin{pmatrix} 1 & & m_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix}}_{=A_{\leqslant r}} D_{\leqslant r} = \Lambda \underbrace{\begin{pmatrix} 1 & & n_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix}}_{=B_{\leqslant r}} . \tag{6.14}$$

All appearing matrices are invertible except Λ. Then $P\,\Lambda = \Lambda B_{\leqslant r}\, D_{\leqslant r}^{-1}\, A_{\leqslant r}^{-1}$ is an upper triangular matrix. Hence we can choose $P = (\gamma_{ij})_{1 \le i,j \le r}$ to be an upper triangular matrix, too. Note that the entry γ_{ij} is unique modulo $p^{e_j}\mathbb{Z}_{p^e}$. The coefficient (i, i) of the matrix equation (6.14) is $\gamma_{ii} \cdot p^{e-e_i} \cdot 1 \cdot d_i = p^{e-e_i} \cdot 1$. Hence we can assume $\gamma_{ii} = d_i^{-1}$ for $P = (\gamma_{ij})_{i,j}$.

(2) Use a representing matrix $F = \mathrm{diag}(f_1, \ldots, d_n)$, $f_j \in \mathbb{Z}^*_{p^e}(\tau_j)$, of an induced automorphism $\zeta \in \overline{\mathrm{Aut}\,R}$ instead of D in part (1) of this proof. All conclusions are the same. Then the representing matrix $P = (\gamma_{ij})_{1 \le i,j \le r}$ of the relevant automorphism of X/R is also an upper triangular matrix with diagonal elements $\gamma_{ii} = f_i^{-1}$. If $i < j$, then $\gamma_{ij} \in \mathbb{Z}_{p^e}$ is arbitrary, by Remark 6.6. □

Remark 6.15. If X and Y are uniform groups with representing matrices in *Hermite normal form*, then $X \cong_{\mathrm{nr}} Y$ if and only if the representing matrices are diagonally equivalent, cf. Theorem 7.5(1).

In general diagonal equivalence of the representing matrices in *Gauß normal form* is not necessary for the near–isomorphism of p–local groups:

Example 6.16. Let $p \neq 2$ be a prime and τ_1, τ_2, τ_3 pairwise incomparable types with p–height $0 = \tau_j(p)$. Then $R := \tau_1 x_1 \oplus \tau_2 x_2 \oplus \tau_3 x_3$ is a p–reduced rigid completely decomposable group. Let

$$\begin{aligned} X &= R + \mathbb{Z}\frac{1}{p^2}(x_1 + x_2 - x_3) + \mathbb{Z}\frac{1}{p^2}(\qquad px_2 + px_3) \in p^{-2}R, \\ Y &= R + \mathbb{Z}\frac{1}{p^2}\,(x_1 + x_2 - (1+2p)x_3) + \mathbb{Z}\frac{1}{p^2}(\qquad px_2 + px_3) \quad \text{and} \\ Z &= R + \mathbb{Z}\frac{1}{p^2}\,(x_1 + (p-1)x_2 - (p+1)x_3) + \mathbb{Z}\frac{1}{p^2}(\qquad px_2 + px_3) \end{aligned}$$

be almost completely decomposable groups. One calculates $(\mathbb{Z}/p^2\mathbb{Z}) \oplus (\mathbb{Z}/p\mathbb{Z}) \cong X/R \cong Y/R \cong Z/R \subseteq p^{-2}R/R \cong (\mathbb{Z}/p^2\mathbb{Z})^3$. The representing matrices are in

Gauß normal form:

$$\begin{aligned} X \;\leftrightarrow\; A &= \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \left(\begin{array}{cc|c} 1 & 1 & -1 \\ 0 & 1 & 1 \end{array}\right) \in \mathbb{M}^{2\times 3}(\mathbb{Z}/p^2\mathbb{Z}) \,, \\ Y \;\leftrightarrow\; B &= \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \left(\begin{array}{cc|c} 1 & 1 & (-1-2p) \\ 0 & 1 & 1 \end{array}\right) \qquad \text{and} \\ Z \;\leftrightarrow\; C &= \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \left(\begin{array}{cc|c} 1 & (p-1) & (p+1) \\ 0 & 1 & 1 \end{array}\right) \,. \end{aligned}$$

By Lemma 5.13, the regulator of X, Y and Z is R. Here

$$P_1 = \begin{pmatrix} (1+p) & -1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad P_2 = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$

are the representing matrices of automorphisms of X/R. Clearly, $D = \mathrm{diag}(1-p,\,1,\,1)$ is the representing matrix of a type–automorphism of $p^{-2}R/R$, and $F = \mathrm{diag}(-1,\,1,\,1)$ is the representing matrix of an induced automorphism of $p^{-2}R/R$. Then we have the identities:

$$P_1\,A\,D = B \qquad \text{and} \qquad P_2\,A\,F = C\,.$$

Hence $X \cong_{\mathrm{nr}} Y$, but we cannot choose P_1 to be a diagonal matrix. These groups X and Y are mentioned in [DO93, p. 148], too. Here the near–isomorphism is proved in a more group theoretic sense. The second matrix equation shows $X \cong Z$ although the left (2×2)–blocks of the relevant matrices are not equal. △

7. Matrix [Near–]Isomorphism Criterion for Uniform Groups

Lemma 7.1. *Let p be a prime and $e,\ n,\ r \in \mathbb{N}$ natural numbers with $r \leq n$. Let $R = \bigoplus_{j=1}^{n} R_{\tau_j}$ be a p–reduced rigid completely decomposable group of rank n with an indexing $T = (\tau_1, \dots, \tau_n)$ of the critical typeset. Suppose that $\mathbf{x} = (x_1, \dots, x_n)$ is a p–decomposition basis of R ordered by T and $\overline{\mathbf{x}} = (\overline{x}_1, \dots, \overline{x}_n)$ is the induced decomposition basis of $\overline{R} = p^{-e}R/R$. Let $M,\ N \in \mathbb{M}^{r\times n}(\mathbb{Z}_{p^e})$ be diagonally equivalent matrices of determinantal rank r. Let $X,\ Y$ be almost completely decomposable groups with the common subgroup R such that $X/R \cong (\mathbb{Z}_{p^e})^r \cong Y/R$. Let $\overline{\mathbf{a}},\ \overline{\mathbf{b}}$ be ordered bases of $X/R,\ Y/R$ such that $M,\ N$ are the representing matrices of $X/R,\ Y/R$ relative to $\overline{\mathbf{x}}$ and $\overline{\mathbf{a}},\ \overline{\mathbf{b}}$.*

Then $R = \mathrm{R}(X)$ is the regulator of X if and only if $R = \mathrm{R}(Y)$ is the regulator of Y.

Proof. Let $M^{(k)}$ denote the $[r \times (n-1)]$–matrix over $\mathbb{Z}_{p^e}$ obtained from M by canceling the k–th column. By Lemma 5.13, the regulator of X is R if and only if $M^{(k)}$ has determinantal rank r for all $k = 1, \dots, n$. Since $\mathrm{rk}_{\det}(M^{(k)}) \overset{4.7}{=} \mathrm{rk}_{\det}(N^{(k)})$, this is equivalent to $R = \mathrm{R}(Y)$. ☐

Isomorphism of Uniform Groups

Example 7.2. Let $\tau_1 = \mathbb{Z}[2^{-1}] = \{\frac{n}{2^k} \mid n \in \mathbb{Z},\ k \in \mathbb{N}_0\}$ and $\tau_2 = \mathbb{Z}[13^{-1}]$. Then $R := \tau_1 x_1 \oplus \tau_2 x_2$ is 17–reduced. Consider the almost completely decomposable groups

$$X = R + \mathbb{Z}\frac{1}{17}(x_1 + x_2), \qquad Y = R + \mathbb{Z}\frac{1}{17}(x_1 + 3x_2).$$

Then X and Y are indecomposable with common regulator $\mathrm{R}(X) = \mathrm{R}(Y) = R$ and regulator quotient $X/R \cong Y/R \cong \mathbb{Z}/17\mathbb{Z}$. Here $X, Y \in \mathcal{C}((\tau_1, \tau_2), 17, 1, 1)$ and the map $^{-} : R \to 17^{-1}R/R,\ x \mapsto 17^{-1}x + R$ denotes the natural epimorphism. Then $\overline{\mathbf{x}} = (\overline{x}_1, \overline{x}_2)$ is an ordered induced–decomposition basis of $17^{-1}R/R$. Here $M = (1 \mid 1)$, $N = (1 \mid 3)$ are the corresponding representing matrices in Hermite normal form of X, Y, respectively. The rest blocks are diagonally equivalent: $1 \cdot (1) \cdot 3 = (3)$. Hence $X \cong_{\mathrm{nr}} Y$ by [Mad00, Lemma 12.5.6].

Look at $\overline{17X} = X/R = \left\{\frac{k}{17}(x_1 + x_2) + R \mid k \in \{0, 1, \dots, 16\}\right\}$ and $\overline{17Y} = Y/R = \left\{\frac{l}{17}(x_1 + 3x_2) + R \mid l \in \{0, 1, \dots, 16\}\right\}$. We use the Isomorphism Criterion 3.5 to show that $X \ncong Y$.

$$\begin{aligned}\operatorname{Aut} R &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \,\middle|\, a \text{ unit in } \mathbb{Z}[2^{-1}],\ b \text{ unit in } \mathbb{Z}[13^{-1}] \right\} \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \,\middle|\, \exists_{s,t\in\mathbb{Z}}\ a = \pm 2^s, b = \pm 13^t \right\}.\end{aligned}$$

Hence, for all $\alpha \in \operatorname{Aut} R$ exist $e_1, e_2 \in \{1, -1\}$ and $s, t \in \mathbb{Z}$ such that $\alpha(x_1+x_2) = e_1 2^s x_1 + e_2 13^t x_2$ or equivalently

$$\overline{\alpha}\left(\frac{X}{R}\right) = \left\{ \frac{\alpha(k(x_1+x_2))}{17} + R \;\middle|\; k \in \{0,1,\dots,16\} \right\}$$
$$= \left\{ \frac{k(e_1 2^s x_1 + e_2 13^t x_2)}{17} + R \;\middle|\; k \in \{0,1,\dots,16\} \right\}.$$

Because of the linear independence of $\{x_1, x_2\} \subseteq \mathbb{Q}R$ there are no $k \in \{0, 1, \dots, 16\}$, $e_1, e_2 \in \{1, -1\}$, $s, t \in \mathbb{Z}$ such that

$$x_1 + 3x_2 = k(e_1 2^s x_1 + e_2 13^t x_2).$$

Then for all admissible k, e_1, e_2, s, t we have

$$\overline{\alpha}\left(\frac{X}{R}\right) \ni \frac{k(e_1 2^s x_1 + e_2 13^t x_2)}{17} + R \neq \frac{x_1 + 3x_2}{17} + R \in \frac{Y}{R}.$$

That's why $X \ncong Y$. △

Definition 7.3. Let p be a prime and e, n, $r \in \mathbb{N}$ natural numbers with $r < n$. Let $T = (\tau_1, \dots, \tau_n)$ be an ordered n–tuple of types. We call

$$\begin{aligned} \operatorname{DIAG}(T; \mathbb{Z}^*_{p^e}) &:= \operatorname{DIAG}(\mathbb{Z}^*_{p^e}(\tau_1), \dots, \mathbb{Z}^*_{p^e}(\tau_n)) \\ &= \{\operatorname{diag}(f_1, \dots, f_n) \mid \forall_{j=1,\dots,n}\; f_j \in \mathbb{Z}^*_{p^e}(\tau_j)\} \end{aligned}$$

the set of T–*diagonal matrices* over $\mathbb{Z}_{p^e}$.

Let A and B be $[r \times (n-r)]$–matrices over $\mathbb{Z}_{p^e}$. Then A and B are called T–*diagonally equivalent* if there is a T–diagonal matrix $F \in \operatorname{DIAG}(T; \mathbb{Z}^*_{p^e})$ such that

$$B = F^{-1}_{\leqslant r}\, A\, F_{>r}\,.$$

Remark 7.4. This matrix equation is equivalent to

$$B = \begin{pmatrix} f_1^{-1} & & \\ & \ddots & \\ & & f_r^{-1} \end{pmatrix} \cdot A \cdot \begin{pmatrix} f_{r+1} & & \\ & \ddots & \\ & & f_n \end{pmatrix}, \quad \text{where } f_j \in \mathbb{Z}^*_{p^e}(\tau_j);$$

$\iff$ if $A = (\alpha_{ij})_{\substack{i=1,\dots,r \\ j=r+1,\dots,n}}$ and $B = (\beta_{ij})_{\substack{i=1,\dots,r \\ j=r+1,\dots,n}}$, then there are $f_j \in \mathbb{Z}^*_{p^e}(\tau_j)$, $1 \le j \le n$, such that

$$\beta_{ij} = f_i^{-1} \alpha_{ij} f_j$$

in $\mathbb{Z}_{p^e}$ for $i = 1, \dots, r$ and $j = r+1, \dots, n$;

$\iff$ A and B are $\operatorname{DIAG}(\mathbb{Z}^*_{p^e}(\tau_1), \dots, \mathbb{Z}^*_{p^e}(\tau_n))$–diagonally equivalent;

$\iff$ $B \in \operatorname{Orb}(A) = \{F^{-1}_{\leqslant r} A F_{>r} \mid F = \operatorname{diag}(f_1, \dots, f_n),\ f_j \in \mathbb{Z}^*_{p^e}(\tau_j)\}$ relative to the group action 4.30.

Theorem 7.5. (Matrix [Near–]Isomorphism Criterion for Uniform Groups)
Let $X, Y \in \mathcal{C}(T,p,e,r)$ be uniform groups with a common regulator R. Let $\overline{\mathbf{x}} = (\overline{x}_1,\dots,\overline{x}_n)$ be an induced decomposition basis of $\overline{R} = p^{-e}R/R$ ordered by a simultaneous admissible indexing $T = (\tau_1,\dots,\tau_n)$ of the critical typeset for X and Y. Let $M = (I_r \,|\, A)$ and $N = (I_r \,|\, B)$ be the representing matrices of X/R and Y/R relative to $\overline{\mathbf{x}}$ in Hermite normal form, where A and B are $[r \times (n-r)]$–matrices over $\mathbb{Z}_{p^e}$.

(1) *The groups X and Y are nearly isomorphic, $X \cong_{\mathrm{nr}} Y$, if and only if A and B are diagonally equivalent.*

(2) *The groups X and Y are isomorphic, $X \cong Y$, if and only if A and B are T–diagonally equivalent.*

Proof. Write $A = (\alpha_{ij})_{\substack{i=1,\dots,r\\ j=r+1,\dots,n}}$ and $B = (\beta_{ij})_{\substack{i=1,\dots,r\\ j=r+1,\dots,n}}$.

(2) "$\Leftarrow$" Assume that the second statement holds: There are $f_k \in \mathbb{Z}^*_{p^e}(\tau_k)$, $1 \le k \le n$, such that

$$\beta_{ij} = f_i^{-1}\alpha_{ij} f_j$$

in $\mathbb{Z}_{p^e}$ for $i = 1,\dots,r$ and $j = r+1,\dots,n$. The units $f_1,\dots,f_n$ determine an induced automorphism ζ of $\overline{R}$ relative to $\overline{\mathbf{x}}$ via $\zeta\overline{x}_j := f_j\overline{x}_j$. The representing matrix $F = \mathrm{diag}(f_1,\dots,f_n)$ of this induced automorphism decomposes into $F_{\leqslant r} := \mathrm{diag}(f_1,\dots,f_r)$ and $F_{>r} := \mathrm{diag}(f_{r+1},\dots,f_n)$. Then $(\beta_{ij}) = (f_i^{-1}\alpha_{ij}f_j)_{\substack{i=1,\dots,r\\ j=r+1,\dots,n}}$ means $B = F_{\leqslant r}^{-1}AF_{>r}$, since $F_{\leqslant r}^{-1} = \mathrm{diag}(f_1^{-1},\dots,f_r^{-1})$. Hence we get

$$\begin{aligned} N &= (I_r \mid B) = (F_{\leqslant r}^{-1}F_{\leqslant r} \mid F_{\leqslant r}^{-1}AF_{>r}) = F_{\leqslant r}^{-1}\,(I_r \mid A)\left(\begin{array}{c|c} F_{\leqslant r} & \\ \hline & F_{>r}\end{array}\right) \\ &= F_{\leqslant r}^{-1}\,M\,F. \end{aligned}$$

Application of Lemma 6.11(2) yields $X \cong Y$.

"$\Rightarrow$" Now let X and Y be isomorphic. Lemma 6.11(2) yields a regular matrix $P \in \mathbb{M}^{r\times r}(\mathbb{Z}_{p^e})$ and a regular diagonal matrix $F = \mathrm{diag}(f_1,\dots,f_n)$, where $f_j \in \mathbb{Z}^*_{p^e}(\tau_j)$, such that $N = PMF$. Again F decomposes into $F = \left(\begin{array}{c|c} F_{\leqslant r} & \\ \hline & F_{>r}\end{array}\right)$. Thus we calculate

$$(I_r \,|\, B) = N = P\,M\,F = P\,(I_r \mid A)\left(\begin{array}{c|c} F_{\leqslant r} & \\ \hline & F_{>r}\end{array}\right) = (PF_{\leqslant r} \mid PAF_{>r})\,.$$

By comparison of the first $[r \times r]$–block we conclude $P = F_{\leqslant r}^{-1}$. The second $[r \times (n-r)]$–block shows that

$$B = F_{\leqslant r}^{-1}\,A\,F_{>r}\,.$$

(1) This result is written down in [Mad00, Lemma 12.5.6.1]. As R is rigid, a type–automorphism ξ is represented by an invertible diagonal matrix $D \in \mathbb{M}^{n\times n}(\mathbb{Z}_{p^e})$,

cf. Lemma 6.4(1). Use $D = \left(\begin{array}{c|c} D_{\leqslant r} & \\ \hline & D_{>r} \end{array}\right)$ instead of F in the part above. All conclusions are the same. □

Example 7.6. Look at Example 7.2 again. $M = (1 \mid 1)$ and $N = (1 \mid 3)$ are the representing matrices of X and Y. Here $\tau_1 = \mathbb{Z}[2^{-1}]$, $\tau_2 = \mathbb{Z}[13^{-1}]$ and we compute $\mathbb{Z}^*_{17}(\tau_1) = \langle -1 + 17\mathbb{Z},\, 2 + 17\mathbb{Z}\rangle_{\text{mult.}} = \{\pm 1 + 17\mathbb{Z},\, \pm 2 + 17\mathbb{Z},\, \pm 4 + 17\mathbb{Z},\, \pm 8 + 17\mathbb{Z}\} \cong \mathbb{Z}_8$, since $2^4 = 16 \equiv -1 \pmod{17}$, and $\mathbb{Z}^*_{17}(\tau_2) = \langle -1 + 17\mathbb{Z},\, 13 + 17\mathbb{Z}\rangle_{\text{mult.}} = \{\pm 1 + 17\mathbb{Z},\, \pm 13 + 17\mathbb{Z}\} \cong \mathbb{Z}_4$, since $13^2 = 169 \equiv -1 \pmod{17}$. We get $\mathbb{Z}^*_{17}(\tau_2) \subsetneq \mathbb{Z}^*_{17}(\tau_1) \subsetneq \mathbb{Z}^*_{17}$, where $\mathbb{Z}^*_{17}$ is cyclic of order $16 = 2^4$.

From Theorem 7.5 we obtain $X \cong Y \Leftrightarrow \exists_{\overline{f}_1 \in \mathbb{Z}^*_{17}(\tau_1),\, \overline{f}_2 \in \mathbb{Z}^*_{17}(\tau_2)} \overline{1} = \overline{f}_1\, \overline{3}\, \overline{f}_2$ in $\mathbb{Z}_{17} \Leftrightarrow \exists_{\overline{f}_k \in \mathbb{Z}^*_{17}(\tau_k)} \overline{f}_1\, \overline{f}_2 = \overline{3^{-1}}$ in $\mathbb{Z}_{17}$. But $\mathbb{Z}^*_{17} = \langle 3 + 17\mathbb{Z}\rangle_{\text{mult.}}$, hence $3 + 17\mathbb{Z} \notin \mathbb{Z}^*_{17}(\tau_1)$. There are no $\overline{f}_1 \in \mathbb{Z}^*_{17}(\tau_1)$, $\overline{f}_2 \in \mathbb{Z}^*_{17}(\tau_2)$ such that $\overline{f}_1\, \overline{f}_2 = \overline{3^{-1}}$ in $\mathbb{Z}_{17}$. Hence $X \ncong Y$ again. △

8. Isomorphism Classes of Uniform Groups

Remark 8.1. Starting from a fixed near–isomorphism class in $\mathcal{C}(T, p, e, r)$ we are looking for a criterion to decide if any groups X, Y with a common regulator R within this class are isomorphic. Let $\mathbf{x} = (x_1, \dots, x_n)$ be a decomposition basis of R ordered by the critical typeset $T = (\tau_1, \dots, \tau_n)$, i. e. $\mathrm{tp}^R(x_j) = \tau_j$. The map $\overline{} : R \to p^{-e}R/R,\ x \mapsto p^{-e}x + R$ denotes the canonical epimorphism. Then $\overline{\mathbf{x}} = (\overline{x}_1, \dots, \overline{x}_n)$ is the ordered induced decomposition basis of $\overline{R} = p^{-e}R/R$. Suppose that T is an admissible ordering, with corresponding block structure and stripping sequence, of the critical typeset for all groups in this near–isomorphism class. This assumption is no loss of generality as admissible orderings are near–isomorphism invariants. There is a modified diagonal similarity class of normed $[r \times (n-r)]$–matrices over $\mathbb{Z}_{p^e}$ belonging to this near–isomorphism class [Mut99, Theorem 4.3]. Let $C = (\gamma_{ij})_{\substack{i=1,\dots,r \\ j=r+1,\dots,n}} \in \mathbb{M}^{r\times(n-r)}(\mathbb{Z}_{p^e})$ be out of this class. By Lemma 5.13, the rest block C is primitive. Using Lemma 5.8, we see that there exists exactly one uniform group Z with regulator $R \subseteq Z \subseteq p^{-e}R$ and an ordered basis $\overline{\mathbf{c}}$ of Z/R such that $Q = (I_r \mid C)$ is the representing matrix of Z/R relative to $\overline{\mathbf{c}}$ and $\overline{\mathbf{x}}$.

Lemma 8.2. *Let R be a rigid and p–reduced completely decomposable group of rank n. Let $C \in \mathbb{M}^{r\times(n-r)}(\mathbb{Z}_{p^e})$ be a normed and primitive matrix. Let $X \in \mathcal{C}(T, p, e, r)$ be a uniform group with regulator R. Let $\overline{\mathbf{x}} = (\overline{x}_1, \dots, \overline{x}_n)$ be an induced decomposition basis of $\overline{R} = p^{-e}R/R$ with fixed admissible ordering of T.*

The group X is from the near–isomorphism class relative to C if and only if there is a basis $\overline{\mathbf{a}} = (\overline{a}_1, \dots, \overline{a}_r)$ of X/R such that the representing matrix M of X over R relative to $\overline{\mathbf{a}}$ and $\overline{\mathbf{x}}$ is in the form

$$M = (I_r \mid A) = (I_r \mid D_{\leqslant r}^{-1} C D_{>r})$$

where $D_{\leqslant r} := \mathrm{diag}(d_1, \dots, d_r)$ and $D_{>r} := \mathrm{diag}(d_{r+1}, \dots, d_n)$, $d_j \in \mathbb{Z}_{p^e}^*$.

Proof. Let Z be the unique group with regulator $R \subseteq Z \subseteq p^{-e}R$ and ordered basis $\overline{\mathbf{c}}$ of Z/R such that $Q = (I_r \mid C)$ is the representing matrix of Z/R relative to $\overline{\mathbf{c}}$ and $\overline{\mathbf{x}}$, where $C = (\gamma_{ij})_{\substack{i=1,\dots,r \\ j=r+1,\dots,n}}$. Using Theorem 7.5, $X \cong_{\mathrm{nr}} Z$ if and only if the matrix rest blocks are diagonally equivalent. Write $A = D_{\leqslant r}^{-1} C D_{>r}$, where $D_{\leqslant r} := \mathrm{diag}(d_1, \dots, d_r)$ and $D_{>r} := \mathrm{diag}(d_{r+1}, \dots, d_n)$, $d_j \in \mathbb{Z}_{p^e}^*$. □

Remark 8.3. (1) In particular there is a one–to–one correspondence between groups within the near–isomorphism class and sets of diagonal matrices over $\mathbb{Z}_{p^e}$: For each group X in the near–isomorphism class there is an invertible diagonal matrix D. On the other hand it is true that each matrix $D = \mathrm{diag}(d_1, \dots, d_n)$, $d_j \in \mathbb{Z}_{p^e}^*$, leads to a unique group of the near–isomorphism class. But several distinct matrices $D \neq D'$ can form the same matrix $D_{\leqslant r}^{-1} C D_{>r} = D'^{-1}_{\leqslant r} C D'_{>r}$ corresponding to exactly one group. For example let $C = (1)$. Each matrix $D =$

$\begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}^*_{p^e}$, leads to the same matrix $D^{-1}_{\leqslant 1} C D_{>1} = (d^{-1})\,(1)\,(d) = \;(1) = C$ and the unique group Z of Remark 8.1.

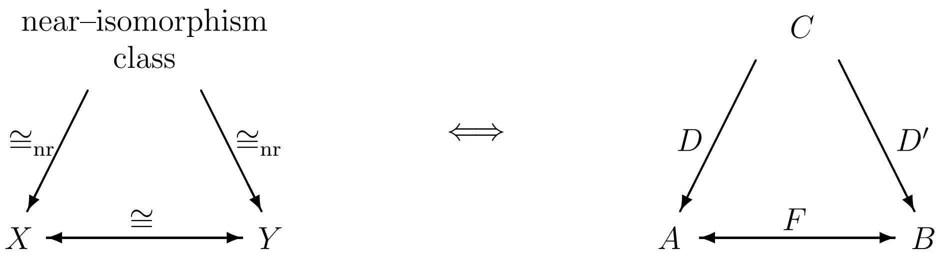
(2) For each diagonal matrix D over $\mathbb{Z}^*_{p^e}$ the representing matrix $(I_r \mid A) = (I_r \mid D^{-1}_{\leqslant r}\; C\; D_{>r}) = D^{-1}_{\leqslant r}\; (I_r \mid C) \left(\begin{array}{c|c} D_{\leqslant r} & \\ \hline & D_{>r} \end{array}\right)$ is diagonally equivalent to $(I_r \mid C)$. Since $(I_r \mid C)$ is in Hermite straight form, A is straight and has the same block structure and the same stripping sequence as C, by [Mut99, Corollary 3.2].

Lemma 8.4. *Let R be a rigid and p–reduced completely decomposable group of rank n. Let $C = (\gamma_{ij})_{\substack{i=1,\dots,r\\ j=r+1,\dots,n}}$ be a normed and primitive matrix over $\mathbb{Z}_{p^e}$. Let $D = \operatorname{diag}(d_1,\dots,d_n)$ and $D' = \operatorname{diag}(d'_1,\dots,d'_n)$ be invertible diagonal matrices. Let $X, Y \in \mathcal{C}(T,p,e,r)$ be groups of the near–isomorphism class relative to C with representing matrices $M = (I_r \mid A) = (I_r \mid D^{-1}_{\leqslant r} C D_{>r})$, $N = (I_r \mid B) = (I_r \mid\; D'^{-1}_{\leqslant r} C D'_{>r})$ relative to a given induced decomposition basis $\overline{\mathbf{x}}$ of $\overline{R} = p^{-e}R/R$ ordered by $T = (\tau_1,\dots,\tau_n)$.*

Then $X \cong Y$ if and only if there are $f_j \in \mathbb{Z}^*_{p^e}(\tau_j)$, $1 \le j \le n$, such that $\gamma_{ij} = d'_i\, f_i^{-1}\, d_i^{-1}\, \gamma_{ij}\, d_j\, f_j\, d'^{-1}_j$ in $\mathbb{Z}_{p^e}$ for all $i = 1,\dots,r$, $j = r+1,\dots,n$.

Proof. The assumption $A = D^{-1}_{\leqslant r} C D_{>r}$ means $(\alpha_{ij}) = (d_i^{-1}\gamma_{ij}d_j)_{\substack{i=1,\dots,r\\ j=r+1,\dots,n}}$ and $B = D'^{-1}_{\leqslant r} C D'_{>r}$ means $(\beta_{ij}) = (d'^{-1}_i \gamma_{ij} d'_j)_{\substack{i=1,\dots,r\\ j=r+1,\dots,n}}$. By Theorem 7.5, $X \cong Y$ if and only if there are $f_j \in \mathbb{Z}^*_{p^e}(\tau_j)$, $1 \le j \le n$, such that $d'^{-1}_i \gamma_{ij} d'_j = \beta_{ij} \overset{7.5}{=} f_i^{-1}\alpha_{ij} f_j = f_i^{-1} d_i^{-1} \gamma_{ij} d_j f_j$ in $\mathbb{Z}_{p^e}$ for $i = 1,\dots,r$ and $j = r+1,\dots,n$. This is equivalent to the claim. ☐

Remark 8.5. The following diagram illustrates the situation of Lemma 8.2 and 8.4:



$$\begin{aligned} X \cong Y \;&\Leftrightarrow\; D'^{-1}_{\leqslant r}\, C\, D'_{>r} \;=\; B \;=\; F^{-1}_{\leqslant r}\, A\, F_{>r} \;=\; F^{-1}_{\leqslant r}\, D^{-1}_{\leqslant r}\, C\, D_{>r}\, F_{>r} \\ &\Leftrightarrow\; C \;=\; D'_{\leqslant r}\, F^{-1}_{\leqslant r}\, D^{-1}_{\leqslant r}\, C\, D_{>r}\, F_{>r}\, D'^{-1}_{>r} \\ &\Leftrightarrow\; \gamma_{ij} = d'_i\, f_i^{-1}\, d_i^{-1}\, \gamma_{ij}\, d_j\, f_j\, d'^{-1}_j \text{ in } \mathbb{Z}_{p^e} \text{ for all } i = 1,\dots,r, \\ &\qquad j = r+1,\dots,n, \text{where } d_k, d'_k \in \mathbb{Z}^*_{p^e} \text{ and } f_k \in \mathbb{Z}^*_{p^e}(\tau_k). \end{aligned}$$

Theorem 8.6. *Let p be a prime and e, n, $r \in \mathbb{N}$ natural numbers with $r < n$. Let R be a rigid and p–reduced completely decomposable group of rank n. Suppose that $C = (\gamma_{ij}) \in \mathbb{M}^{r\times(n-r)}(\mathbb{Z}_{p^e})$ is a normed and primitive matrix. Let* $\mathrm{Stab}_{\mathrm{DIAG}(n;\mathbb{Z}^*_{p^e})}(C) = \{D = \mathrm{diag}(d_1, \dots , d_n) \mid d_j \in \mathbb{Z}^*_{p^e},\ D^{-1}_{\leqslant r}\, C\, D_{>r} = C\}$.
The number of groups X contained in the near–isomorphism class relative to C and with regulator $R \subseteq X \subseteq p^{-e}R$ is

$$\frac{\left(p^{e-1}(p-1)\right)^n}{|\,\mathrm{Stab}_{\mathrm{DIAG}(n;\mathbb{Z}^*_{p^e})}(C)|}\,.$$

There are at most $\varphi(p^e)^{n-1} = \left(p^{e-1}(p-1)\right)^{n-1}$ groups within the near–isomorphism class relative to C.

Proof. By Lemma 8.2 the group X is of the near–isomorphism class relative to C if and only if there is a basis $\bar{\mathbf{a}}$ of X/R such that $M = (I_r \mid D^{-1}_{\leqslant r} C D_{>r})$ is the representing matrix of X/R, where $D_{\leqslant r} = \mathrm{diag}(d_1, \dots , d_r)$ and $D_{>r} = \mathrm{diag}(d_{r+1}, \dots , d_n)$, $d_j \in \mathbb{Z}^*_{p^e}$. We have $|\mathbb{Z}^*_{p^e}| = \varphi(p^e) = p^{e-1}(p-1)$. By Lemma 4.27 there are $\frac{\left(p^{e-1}(p-1)\right)^n}{|\mathrm{Stab}_{\mathrm{DIAG}(n;\mathbb{Z}^*_{p^e})}(C)|}$ matrices which are diagonally equivalent to C. Every of these diagonal equivalent matrices belongs to a group X of the near–isomorphism class as Lemma 5.8 shows. By Lemma 7.1 the regulator of X is R. The upper bound for the number of near–isomorphic groups is shown in Lemma 4.27, too. □

Theorem 8.7. *Let p be a prime and e, n, $r \in \mathbb{N}$ natural numbers with $r < n$. Let $R = \bigoplus_{j=1}^{n} R_{\tau_j}$ be a rigid and p–reduced completely decomposable group of rank n. Let $B \in \mathbb{M}^{r\times(n-r)}(\mathbb{Z}_{p^e})$ be a normed and primitive matrix and let* $\mathrm{Stab}_{\cong}(B) = \{F = \mathrm{diag}(f_1, \dots , f_n) \mid f_j \in \mathbb{Z}^*_{p^e}(\tau_j),\ F^{-1}_{\leqslant r}\, B\, F_{>r} = B\}$.
The number of groups X contained in the isomorphism class relative to B and with regulator $R \subseteq X \subseteq p^{-e}R$ is

$$\frac{\prod_{j=1}^{n} |\mathbb{Z}^*_{p^e}(\tau_j)|}{|\,\mathrm{Stab}_{\cong}(B)|}\,.$$

Proof. Let $T = (\tau_1, \dots , \tau_n)$ be an indexing of the critical typeset. By Lemma 7.5 the group X belongs to the isomorphism class relative to B if and only if there is a basis $\bar{\mathbf{a}}$ of X/R such that $M = (I_r \mid F^{-1}_{\leqslant r} B F_{>r})$ is the representing matrix of X/R, where $F_{\leqslant r} = \mathrm{diag}(f_1, \dots , f_r)$ and $F_{>r} = \mathrm{diag}(f_{r+1}, \dots , f_n)$, $f_j \in \mathbb{Z}^*_{p^e}(\tau_j)$. Then we have $F \in \mathrm{DIAG}(\mathbb{Z}^*_{p^e}(\tau_1), \dots , \mathbb{Z}^*_{p^e}(\tau_n)) = \mathrm{DIAG}(T; \mathbb{Z}^*_{p^e})$. By Lemma 4.31 there are

$$\frac{|\,\mathrm{DIAG}(T; \mathbb{Z}^*_{p^e})|}{|\,\mathrm{Stab}_{\cong}(B)|}$$

matrices which are T–diagonally equivalent to B. Each of these diagonally equivalent matrices belongs to a group X of the isomorphism class as Lemma 5.8 shows. By Lemma 7.1 the regulator of X is R. □

Theorem 8.8. *Let p be a prime and $e,\ n,\ r\ \in\ \mathbb{N}$ natural numbers with $r < n$. Let $R = \oplus_{j=1}^{n} R_{\tau_j}$ be a rigid and p–reduced completely decomposable group of rank n with an indexing $T = (\tau_1, \dots, \tau_n)$ of its critical typeset. Let $C \in \mathbb{M}^{r\times(n-r)}(\mathbb{Z}_{p^e})$ be a normed and primitive matrix. Let $\mathrm{Stab}_{\cong_{\mathrm{nr}}}(C) = \big\{D = \mathrm{diag}(d_1, \dots, d_n) \mid d_j \in \mathbb{Z}_{p^e}^*,\ D_{\leqslant r}^{-1}\, C\, D_{>r} = C\big\}$ and $\mathrm{Stab}_{\cong}(C) = \big\{F = \mathrm{diag}(f_1, \dots, f_n) \mid f_j \in \mathbb{Z}_{p^e}^*(\tau_j),\ F_{\leqslant r}^{-1}\, C\, F_{>r} = C\big\}$.*

Each near–isomorphism class is the union of isomorphism classes all of equal length. The number of distinct isomorphism classes contained in the near–isomorphism class of C and with regulator R is

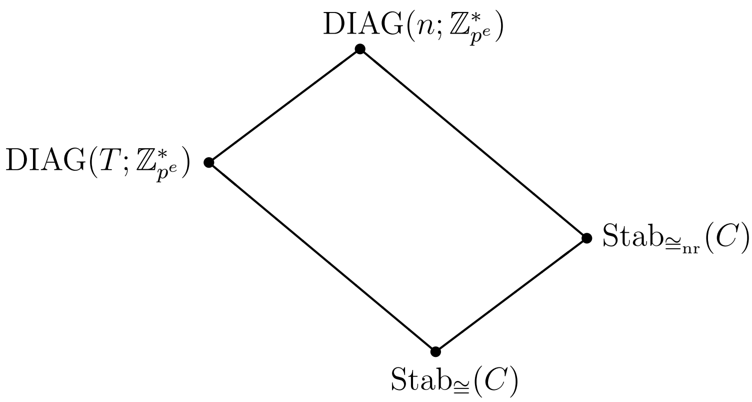
$$\frac{\left(p^{e-1}(p-1)\right)^n}{\prod_{j=1}^{n} |\mathbb{Z}_{p^e}^*(\tau_j)| \cdot [\mathrm{Stab}_{\cong_{\mathrm{nr}}}(C) : \mathrm{Stab}_{\cong}(C)]} = \frac{\left(p^{e-1}(p-1)\right)^n}{|\,\mathrm{DIAG}(T; \mathbb{Z}_{p^e}^*) \cdot \mathrm{Stab}_{\cong_{\mathrm{nr}}}(C)|}\,.$$

Proof. Here $\mathrm{DIAG}(n; \mathbb{Z}_{p^e}^*)$ acts on $\mathbb{M}^{r\times(n-r)}$ via diagonal equivalence. The stabilizer of A under this action is $\mathrm{Stab}_{\cong_{\mathrm{nr}}}(A)$ and the orbit of A is $\mathrm{Orb}_{\cong_{\mathrm{nr}}}(A) = \{D_{\leqslant r}^{-1} A D_{>r} \mid D \in \mathrm{DIAG}(n; \mathbb{Z}_{p^e}^*)\}$.
In addition $\mathrm{DIAG}(T; \mathbb{Z}_{p^e}^*) = \mathrm{DIAG}(\mathbb{Z}_{p^e}^*(\tau_1), \dots, \mathbb{Z}_{p^e}^*(\tau_n))$ acts on $\mathbb{M}^{r\times(n-r)}$ via diagonal equivalence, too. The stabilizer of A under this action is $\mathrm{Stab}_{\cong}(A)$ and the orbit of A is $\mathrm{Orb}_{\cong}(A) = \{F_{\leqslant r}^{-1} A F_{>r} \mid F \in \mathrm{DIAG}(T; \mathbb{Z}_{p^e}^*)\}$.
Firstly, we show that the isomorphism classes of near–isomorphic groups have equal length. For that let C' be diagonally equivalent to C, i. e. $C' = D_{\leqslant r}^{-1}\, C\, D_{>r}$, where $D \in \mathrm{DIAG}(n; \mathbb{Z}_{p^e}^*)$. Then

$$\begin{aligned} &F \in \mathrm{Stab}_{\cong}(C) \iff F_{\leqslant r}^{-1}\, C\, F_{>r} = C \iff D_{\leqslant r}^{-1}\, (F_{\leqslant r}^{-1} C F_{>r})\, D_{>r} = D_{\leqslant r}^{-1}\, C\, D_{>r} \\ &\iff F_{\leqslant r}^{-1}\, \underbrace{(D_{\leqslant r}^{-1} C D_{>r})}_{C'}\, F_{>r} = \underbrace{D_{\leqslant r}^{-1}\, C\, D_{>r}}_{C'} \iff F \in \mathrm{Stab}_{\cong}(C'). \end{aligned}$$

Hence $\mathrm{Stab}_{\cong}(C) = \mathrm{Stab}_{\cong}(C')$ and therefore $|\,\mathrm{Orb}_{\cong}(C)| = |\,\mathrm{Orb}_{\cong}(C')|$.
Now we use Theorem 8.6 and Theorem 8.7 to compute

$$\begin{aligned} |\{\mathrm{Orb}_{\cong}(A) \mid A \in \mathrm{Orb}_{\cong_{\mathrm{nr}}}(C)\}| &= \frac{|\,\mathrm{Orb}_{\cong_{\mathrm{nr}}}(C)|}{|\,\mathrm{Orb}_{\cong}(C)|} \\ &= \frac{\left[\mathrm{DIAG}(n; \mathbb{Z}_{p^e}^*) : \mathrm{Stab}_{\cong_{\mathrm{nr}}}(C)\right]}{\left[\mathrm{DIAG}(T; \mathbb{Z}_{p^e}^*) : \mathrm{Stab}_{\cong}(C)\right]} \\ &= \frac{|\,\mathrm{DIAG}(n; \mathbb{Z}_{p^e}^*)|}{|\,\mathrm{DIAG}(T; \mathbb{Z}_{p^e}^*)| \cdot [\mathrm{Stab}_{\cong_{\mathrm{nr}}}(C) : \mathrm{Stab}_{\cong}(C)]} \\ &= \frac{\left(p^{e-1}(p-1)\right)^n}{\prod_{j=1}^{n} |\mathbb{Z}_{p^e}^*(\tau_j)| \cdot [\mathrm{Stab}_{\cong_{\mathrm{nr}}}(C) : \mathrm{Stab}_{\cong}(C)]}\,. \end{aligned}$$

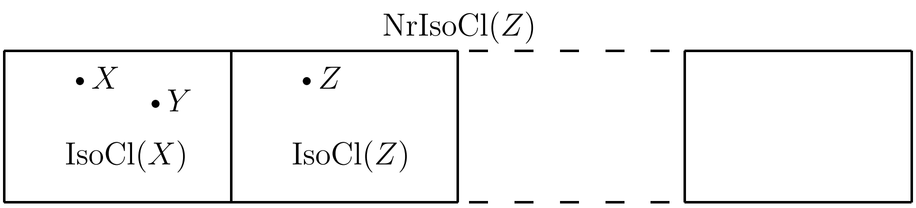


We have $\mathrm{DIAG}(T;\mathbb{Z}_{p^e}^*) \cap \mathrm{Stab}_{\cong_{\mathrm{nr}}}(C) = \mathrm{Stab}_{\cong}(C)$. Therefore the denominator simplifies:

$$\begin{aligned} |\,\mathrm{DIAG}(T;\mathbb{Z}_{p^e}^*)| \cdot [\mathrm{Stab}_{\cong_{\mathrm{nr}}}(C) : \mathrm{Stab}_{\cong}(C)] &= \frac{|\,\mathrm{DIAG}(T;\mathbb{Z}_{p^e}^*)| \cdot |\,\mathrm{Stab}_{\cong_{\mathrm{nr}}}(C)|}{|\,\mathrm{Stab}_{\cong}(C)|} \\ &= |\,\mathrm{DIAG}(T;\mathbb{Z}_{p^e}^*) \cdot \mathrm{Stab}_{\cong_{\mathrm{nr}}}(C)| \end{aligned}$$

and the claim follows. □

Remark 8.9. According to Theorem 8.8 each near–isomorphism class decomposes into isomorphism classes all of the same cardinality:



This is a general result in [Mad00, Theorem 8.2.5].

Corollary 8.10. *There are at most*

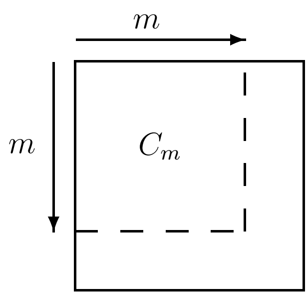
$$\prod_{j=1}^{n} \left[\mathbb{Z}_{p^e}^* \;:\; \mathbb{Z}_{p^e}^*(\tau_j)\right] = \frac{(p^{e-1}(p-1))^n}{\prod_{j=1}^{n} |\mathbb{Z}_{p^e}^*(\tau_j)|}$$

pairwise non–isomorphic groups within the near–isomorphism class of the normed and primitive matrix $C \in \mathbb{M}^{r\times(n-r)}(\mathbb{Z}_{p^e})$.

Proof. Since $[\mathrm{Stab}_{\cong_{\mathrm{nr}}}(C) : \mathrm{Stab}_{\cong}(C)] \geq 1$, Theorem 8.8 shows the claim. □

9. Uniform Groups of Even Rank with Normed Representing Matrices

Remark 9.1. Let us investigate uniform groups of even rank $n = 2r$. A fixed near–isomorphism class of groups is represented by a modified diagonal similarity class of normed $(r \times r)$–matrices. These are the rest blocks of the representing matrices. Let $C = (\gamma_{ij})_{\substack{i=1,\dots,r \\ j=r+1,\dots,2r}} \in \mathbb{M}^{r\times r}(\mathbb{Z}_{p^e})$ be a representative. Additionally suppose for simplification that the normed matrix C is invertible. Then C is primitive by Lemma 4.18. All main submatrices $C_m = (\gamma_{ij})_{\substack{i=1,\dots,m \\ j=r+1,\dots,r+m}}$ for $1 \leq m \leq r$ have determinant 1 by Definition 4.14.



If $X \cong Y$, then we can prove the following necessary condition.

Lemma 9.2. *Let R be a rigid and p–reduced completely decomposable group of rank $2r$. Let C be a normed and invertible $(r \times r)$–matrix over $\mathbb{Z}_{p^e}$. Let $D = \operatorname{diag}(d_1, \dots, d_{2r})$ and $D' = \operatorname{diag}(d'_1, \dots, d'_{2r})$ be invertible matrices. Let $X, Y \in \mathcal{C}(T, p, e, r)$ be groups of the near–isomorphism class relative to C with representing matrices $M = (I_r \mid D^{-1}_{\leqslant r} C D_{>r})$, $N = (I_r \mid D'^{-1}_{\leqslant r} C D'_{>r})$ relative to a given induced decomposition basis $\overline{\mathbf{x}}$ of $\overline{R} = p^{-e}R/R$ which is ordered by the admissible critical typeset $T = (\tau_1, \dots, \tau_{2r})$.*

If $X \cong Y$, then there are $f_j \in \mathbb{Z}^*_{p^e}(\tau_j)$, $1 \leq j \leq 2r$, such that $d'_m\, f_m^{-1}\, d_m^{-1}\, d_{r+m}\, f_{r+m}\, d'^{-1}_{r+m} = 1$ in $\mathbb{Z}_{p^e}$ for all $m = 1, \dots, r$.

Proof. Since $C = (\gamma_{ij})_{\substack{1\leq i\leq r \\ r+1\leq j\leq 2r}}$ is normed and invertible, all main submatrices $C_m = (\gamma_{ij})_{\substack{1\leq i\leq m \\ r+1\leq j\leq r+m}}$ for $m = 1, \dots, r$ have determinant 1. We proceed by induction on m. The assumptions of Lemma 8.4 hold. Hence $1 = \det C_1 \overset{8.4}{=} d'_1\, f_1^{-1}\, d_1^{-1}\, d_{r+1}\, f_{r+1}\, d'^{-1}_{r+1}$. Suppose that the claim has been established for all integers $< m$. Now Lemma 8.4 implies

$$\begin{aligned}
1 &= \det(C_m) = \det(\gamma_{ij})_{\substack{1\le i\le m\\ r+1\le j\le r+m}} \overset{8.4}{=} \det(d'_i\, f_i^{-1}\, d_i^{-1}\, \gamma_{ij}\, d_j\, f_j\, d'^{-1}_j)_{\substack{1\le i\le m\\ r+1\le j\le r+m}}\\
&= \det\Big(\operatorname{diag}(d'_1,\dots,d'_m)\cdot\operatorname{diag}(f_1^{-1},\dots,f_m^{-1})\cdot\operatorname{diag}(d_1^{-1},\dots,d_m^{-1})\cdot C_m\,\cdot\\
&\qquad\cdot\operatorname{diag}(d_{r+1},\dots,d_{r+m})\cdot\operatorname{diag}(f_{r+1},\dots,f_{r+m})\cdot\operatorname{diag}(d'^{-1}_{r+1},\dots,d'^{-1}_{r+m})\Big)\\
&= d'_1\cdots d'_m\cdot f_1^{-1}\cdots f_m^{-1}\cdot d_1^{-1}\cdots d_m^{-1}\cdot 1\,\cdot\\
&\quad\cdot d_{r+1}\cdots d_{r+m}\cdot f_{r+1}\cdots f_{r+m}\cdot d'^{-1}_{r+1}\cdots d'^{-1}_{r+m}\\
&= \left(\prod_{k=1}^{m-1}\underbrace{d'_k\, f_k^{-1}\, d_k^{-1}\, d_{r+k}\, f_{r+k}\, d'^{-1}_{r+k}}_{=1}\right)\cdot d'_m\, f_m^{-1}\, d_m^{-1}\, d_{r+m}\, f_{r+m}\, d'^{-1}_{r+m}\\
&= d'_m\, f_m^{-1}\, d_m^{-1}\, d_{r+m}\, f_{r+m}\, d'^{-1}_{r+m}\,,
\end{aligned}$$

by the induction hypothesis. □

Lemma 9.3. *Let m be a natural number and τ_1, τ_2 any types, i. e. rational groups including $\mathbb{Z}$. Then $\mathbb{Z}^*_m(\tau_1)\cdot\mathbb{Z}^*_m(\tau_2) = \mathbb{Z}^*_m(\tau_1\vee\tau_2)$.*

Proof. The lattice operation of types $\tau_1\vee\tau_2=\tau$ means $\tau(q)=\max\{\tau_1(q),\,\tau_2(q)\}$ for all primes q. Hence $\mathbb{Z}^*_m(\tau_1)\cdot\mathbb{Z}^*_m(\tau_2) = \langle\mathbb{Z}^*_m(\tau_1),\,\mathbb{Z}^*_m(\tau_2)\rangle_{\text{mult.}} \overset{6.2}{=}$
$\langle -1+m\mathbb{Z},\, q+m\mathbb{Z} \mid q \text{ prime},\ \tau_1(q)=\infty \text{ or } \tau_2(q)=\infty\rangle_{\text{mult.}} =$
$\langle -1+m\mathbb{Z},\, q+m\mathbb{Z} \mid q \text{ prime},\ (\tau_1\vee\tau_2)(q)=\infty\rangle_{\text{mult.}} \overset{6.2}{=} \mathbb{Z}^*_m(\tau_1\vee\tau_2)$. □

Remark 9.4. Let m be a natural number and τ_1, τ_2 any types i. e. rational groups including $\mathbb{Z}$. Then $\mathbb{Z}^*_m(\tau_1\wedge\tau_2)\subseteq\mathbb{Z}^*_m(\tau_1)\cap\mathbb{Z}^*_m(\tau_2)$. This can be a proper inclusion.

Proof. The lattice operation of types $\tau_1\wedge\tau_2=\tau$ means $\tau(q)=\min\{\tau_1(q),\,\tau_2(q)\}$ for all primes q. Hence each generator $q+m\mathbb{Z}$ of $\mathbb{Z}^*_m(\tau_1\wedge\tau_2)$ satisfies $\min\{\tau_1(q),\,\tau_2(q)\}=\infty$. Therefore we have $\tau_1(q)=\infty=\tau_2(q)$ and $q+m\mathbb{Z}\in\mathbb{Z}^*_m(\tau_1)$, $q+m\mathbb{Z}\in\mathbb{Z}^*_m(\tau_2)$. This shows the inclusion.
For the inequality choose $m=17$, $\tau_1=\mathbb{Z}[3^{-1}]$ and $\tau_2=\mathbb{Z}[5^{-1}]$. Then we calculate $\tau_1\wedge\tau_2=\operatorname{tp}(\mathbb{Z})$, $\mathbb{Z}^*_{17}(\tau_1\wedge\tau_2)=\langle -1+17\mathbb{Z}\rangle_{\text{mult.}}=\{\pm1+17\mathbb{Z}\}$ $[\cong(\mathbb{Z}_2,+)]$ and $\mathbb{Z}^*_{17}(\tau_1)=\mathbb{Z}^*_{17}=\mathbb{Z}^*_{17}(\tau_2)$ $[\cong(\mathbb{Z}_{16},+)]$, since $\operatorname{ord}(3+17\mathbb{Z})=16=\operatorname{ord}(5+17\mathbb{Z})$. Thus the inclusion is proper. □

Remark 9.5. Let p be a prime and e,n natural numbers. Let R be a rigid and p–reduced completely decomposable group of rank n. Suppose that $T=(\tau_1,\dots,\tau_n)$ is an indexing of the critical typeset of R, such that $R=\bigoplus_{j=1}^n R_{\tau_j}$ is a homogeneous decomposition of R.

If $\tau_i,\,\tau_j\in T$, then

$$\begin{aligned}
\mathbb{Z}^*_{p^e}(\tau_i\vee\tau_j) &\overset{9.3}{=} \big\langle\mathbb{Z}^*_{p^e}(\tau_i),\,\mathbb{Z}^*_{p^e}(\tau_j)\big\rangle_{\text{mult.}}\\
&\overset{6.3}{=} \big\langle -1+p^e\mathbb{Z},\, q+p^e\mathbb{Z} \mid q \text{ prime},\ qR_{\tau_i}=R_{\tau_i} \text{ or } qR_{\tau_j}=R_{\tau_j}\big\rangle_{\text{mult.}}.
\end{aligned}$$

Lemma 9.6. *Let R be a rigid and p–reduced completely decomposable group of rank $n = 2r$. Let C be a normed and invertible $(r\times r)$–matrix over $\mathbb{Z}_{p^e}$. Let $X, Y \in \mathcal{C}(T, p, e, r)$ be groups of the near–isomorphism class relative to C with corresponding $(r \times r)$–diagonal matrices $D_{\leqslant r} = \operatorname{diag}(d_1, \dots , d_r)$, $D_{>r} = \operatorname{diag}(d_{r+1}, \dots , d_{2r})$ with respect to X and $D'_{\leqslant r} = \operatorname{diag}(d'_1, \dots , d'_r)$, $D'_{>r} = \operatorname{diag}(d'_{r+1}, \dots , d'_{2r})$ with respect to Y.*

If $X \cong Y$, then $\frac{d'_m}{d'_{r+m}} \in \frac{d_m}{d_{r+m}} \cdot \mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})$ for all $m = 1, \dots , r$.

Proof. The assumptions of Lemma 9.2 hold. Thus there are $f_j \in \mathbb{Z}^*_{p^e}(\tau_j)$ such that $d'_m\, f_m^{-1}\, d_m^{-1}\, d_{r+m}\, f_{r+m}\, {d'}^{-1}_{r+m} = 1$ in $\mathbb{Z}_{p^e}$ or equivalently $\frac{d'_m}{d'_{r+m}} = \frac{d_m}{d_{r+m}} \cdot \frac{f_m}{f_{r+m}} \in \frac{d_m}{d_{r+m}} \cdot \mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})$ for all $m = 1, \dots , r$. □

Remark 9.7. We give a counter–example for the way back in 9.12. The condition of Lemma 9.6 is a relation for the diagonal elements of the rest blocks. If C is particularly the identity matrix, then the condition is also sufficient, cf. Corollary 9.16.

Theorem 9.8. *There are at least*

$$\prod_{m=1}^{r} \left[\mathbb{Z}^*_{p^e} \;:\; \mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})\right] = \frac{\left(p^{e-1}(p-1)\right)^r}{\prod_{m=1}^{r} |\mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})|}$$

pairwise non–isomorphic groups contained in the near–isomorphism class relative to a normed and invertible $(r \times r)$–matrix.

Proof. Assume that $C = (\gamma_{ij})_{\substack{i=1,\dots,r\\ j=r+1,\dots,2r}} \in \mathbb{M}^{r\times r}(\mathbb{Z}_{p^e})$ is normed and invertible. Let R be a rigid and p–reduced completely decomposable group of rank $2r$. Suppose that $T = (\tau_1, \dots , \tau_r, \tau_{r+1}, \dots \tau_{2r})$ is the admissible indexing of the critical typeset for the fixed near–isomorphism class in $\mathcal{C}(T, p, e, r)$ relative to C. Let $\overline{\mathbf{x}} = (\overline{x}_1, \dots , \overline{x}_n)$ be an induced decomposition basis of $\overline{R} = p^{-e}R/R$ which is ordered by T. We are looking for pairwise non–isomorphic groups within this near–isomorphism class.

Construction: For $m = 1, \dots , r$ abbreviate $k(m) := \left[\mathbb{Z}^*_{p^e} : \mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})\right] = \left|\frac{\mathbb{Z}^*_{p^e}}{\mathbb{Z}^*_{p^e}(\tau_m\vee\tau_{r+m})}\right| = \frac{p^{e-1}(p-1)}{|\mathbb{Z}^*_{p^e}(\tau_m\vee\tau_{r+m})|} \geq 1$. Thus for all $m = 1, \dots , r$ there are $k(m)$ left cosets of $\mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})$:

$s(m, 1)\cdot\mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m}),\ s(m, 2)\cdot\mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m}), \dots ,\ s(m, k(m))\cdot\mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})$.

Define $d_1 = \ldots = d_r = \overline{1} = 1 + p^e\mathbb{Z}$ and choose $d^{-1}_{r+m} \in \{s(m, 1), \dots , s(m, k(m))\}$ for $m = 1, \dots , r$. Hence there are $\prod_{m=1}^{r} k(m) = \prod_{m=1}^{r} \left[\mathbb{Z}^*_{p^e} : \mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})\right]$ distinct diagonal matrices $D = \operatorname{diag}(d_1, \dots , d_{2r}) = \operatorname{diag}(\underbrace{1, \dots , 1}_{r \text{ times}}, d_{r+1}, \dots , d_{2r})$ over $\mathbb{Z}^*_{p^e}$.

By Lemma 8.2 each diagonal matrix D of the construction leads to a uniform group $X \in \mathcal{C}(T, p, e, r)$ of the near–isomorphism class relative to C with regulator

$R \subseteq X \subseteq p^{-e}R$ and a basis $\bar{\mathbf{a}}$ of X/R such that $M = (I_r \mid CD_{>r})$ is the representing matrix of X/R relative to $\bar{\mathbf{a}}$ and $\bar{\mathbf{x}}$. Now let $D = \operatorname{diag}(1, \dots, 1, d_{r+1}, \dots, d_{2r})$ and $D' = \operatorname{diag}(1, \dots, 1, d'_{r+1}, \dots, d'_{2r})$ different diagonal matrices, which have been constructed as above, with corresponding groups X and Y of the near–isomorphism class. Since $D \neq D'$ over $\mathbb{Z}_{p^e}$, there is an integer $m \in \{1, \dots, r\}$ with the property $d_{r+m} \neq d'_{r+m}$ in $\mathbb{Z}_{p^e}$ or equivalently $d_{r+m}^{-1} \neq d'^{-1}_{r+m}$. Therefore $d_{r+m}^{-1} \cdot \mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})$ and $d'^{-1}_{r+m} \cdot \mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})$ are distinct, too, since the diagonal elements are representatives of distinct cosets of $\mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})$ by construction. Hence $d'^{-1}_{r+m} \notin d^{-1}_{r+m} \cdot \mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})$, since distinct left cosets are disjunct. Lemma 9.6 shows $X \not\cong Y$. □

Remark 9.9. Now we have got a lower and an upper bound for the number of isomorphism classes within a given near–isomorphism class from groups of even rank $n = 2r$.

$$\frac{(p^{e-1}(p-1))^r}{\prod_{m=1}^r |\mathbb{Z}^*_{p^e}(\tau_m \vee \tau_{r+m})|} \overset{9.8}{\leq} |\{\operatorname{IsoCl}(X) \mid X \in \operatorname{NrIsoCl}(Z)\}| \overset{8.10}{\leq} \frac{(p^{e-1}(p-1))^n}{\prod_{j=1}^n |\mathbb{Z}^*_{p^e}(\tau_j)|}.$$

Example 9.10. Let $\tau_1 = \mathbb{Z}[3^{-1}] = \{\frac{n}{3^k} \mid n \in \mathbb{Z},\ k \in \mathbb{N}_0\}$ and $\tau_2 = \mathbb{Z}[5^{-1}]$. Then $R := \tau_1 x_1 \oplus \tau_2 x_2$ is 17–reduced.
Consider the almost completely decomposable group

$$Z = R + \mathbb{Z}\frac{1}{17}(x_1 + x_2)$$

with corresponding representing matrix $M = (1 \mid 1)$.
We compute $3^8 \equiv -1 \pmod{17}$ and $5^8 \equiv -1 \pmod{17}$. Then we obtain $\mathbb{Z}^*_{17}(\tau_1) = \mathbb{Z}^*_{17}(\tau_2) = \mathbb{Z}^*_{17} \cong \mathbb{Z}_{16}$, since $\operatorname{ord}(3 + 17\mathbb{Z}) = 16 = \operatorname{ord}(5 + 17\mathbb{Z})$. Hence $\mathbb{Z}^*_{17}(\tau_1 \vee \tau_2) = \mathbb{Z}^*_{17}$ and therefore the formulas of 9.8 and 8.10 simplify:

$$\frac{16^1}{\prod_{m=1}^1 |\mathbb{Z}^*_{17}(\tau_m \vee \tau_{1+m})|} = 1 \quad \text{and} \quad \frac{16^2}{\prod_{j=1}^2 |\mathbb{Z}^*_{17}(\tau_j)|} = \frac{16^2}{16^2} = 1.$$

This means that the lower and upper bounds of 9.8 and 8.10 are sharp. All groups in the near–isomorphism class of Z are isomorphic.

Example 9.11. In Example 7.2 the representing matrix $M = (1 \mid 1)$ of $X = R + \mathbb{Z}\frac{1}{17}(x_1 + x_2)$ is in Hermite *normed* form. Here $\tau_1 = \mathbb{Z}[2^{-1}] = \{\frac{n}{2^k} \mid n \in \mathbb{Z},\ k \in \mathbb{N}_0\}$, $\tau_2 = \mathbb{Z}[13^{-1}]$ and $R := \tau_1 x_1 \oplus \tau_2 x_2$ is 17–reduced. From $\mathbb{Z}^*_{17}(\tau_2) \subsetneq \mathbb{Z}^*_{17}(\tau_1) \subsetneq \mathbb{Z}^*_{17} = \mathbb{Z}_{17} \setminus \{0 + 17\mathbb{Z}\}$, by Example 7.6, we conclude $\mathbb{Z}^*_{17}(\tau_1 \vee \tau_2) = \mathbb{Z}^*_{17}(\tau_1) = \{\pm1 + 17\mathbb{Z},\ \pm2 + 17\mathbb{Z},\ \pm4 + 17\mathbb{Z},\ \pm8 + 17\mathbb{Z}\}$. Theorem 9.8 proves that there are at least

$$[\mathbb{Z}^*_{17} : \mathbb{Z}^*_{17}(\tau_1 \vee \tau_2)] = \frac{16}{8} = 2$$

isomorphism classes within the near–isomorphism class of X. We use Lemma 8.2 to determine all groups X' near–isomorphic to X with regulator $R \subseteq X' \subseteq \frac{1}{17}R$:

$$X' \cong_{\text{nr}} X \overset{8.2}{\iff} X' = R + \mathbb{Z}\tfrac{1}{17}(x_1 + \lambda x_2), \text{ where } \lambda \in \{\pm1,\ \pm2,\ \pm3,\ \dots,\ \pm8\}.$$

Recall that $X \not\cong Y = R + \mathbb{Z}\frac{1}{17}(x_1 + 3x_2)$. Theorem 7.5 shows that there are exactly two isomorphism classes of groups:
$X' \cong X \overset{7.5}{\iff} X' = R + \mathbb{Z}\frac{1}{17}(x_1 + \mu x_2)$, where $\mu = f_1^{-1}f_2 \in \{\pm 1, \pm 2, \pm 4, \pm 8\}$, and
$Y' \cong Y \overset{7.5}{\iff} Y' = R + \mathbb{Z}\frac{1}{17}(x_1 + \nu x_2)$, where $\nu = f_1^{-1}f_2 \in \{\pm 3, \pm 6, \pm 5, \pm 7\}$.
Hence $\{X' \mid X' \cong X,\, \mathrm{R}(X') = R\}$ and $\{Y' \mid Y' \cong Y,\, \mathrm{R}(Y') = R\}$ are the only two isomorphism classes. △

Example 9.12. Let $\tau_1 = \mathbb{Z}[3^{-1}]$, $\tau_2 = \mathbb{Z}[13^{-1}]$, $\tau_3 = \mathbb{Z}[47^{-1}]$, $\tau_4 = \mathbb{Z}[5^{-1}]$ then $R := \tau_1 x_1 \oplus \tau_2 x_2 \oplus \tau_3 x_3 \oplus \tau_4 x_4$ is rigid and 17–reduced. Here $\overline{\mathbf{x}} = (\overline{x}_1, \overline{x}_2, \overline{x}_3, \overline{x}_4)$ is an induced 17–decomposition basis of $\overline{R} = \frac{1}{17}R/R$, which is ordered by $T = (\tau_1, \tau_2, \tau_3, \tau_4)$. We compute $3^8 \equiv -1 \pmod{17}$ and $5^8 \equiv -1 \pmod{17}$. Similarly as in Example 7.6 we obtain
$\mathbb{Z}_{17}^*(\tau_1) = \langle -1 + 17\mathbb{Z},\, 3 + 17\mathbb{Z}\rangle_{\text{mult.}} = \mathbb{Z}_{17}^*$, since $\mathrm{ord}(3 + 17\mathbb{Z}) = 16$,
$\mathbb{Z}_{17}^*(\tau_2) = \mathbb{Z}_{17}^*(\tau_3) = \{\pm 1 + 17\mathbb{Z}, \pm 4 + 17\mathbb{Z}\}_{\text{mult.}} \cong \mathbb{Z}_4$, since $13 \equiv 47 \equiv -4 \pmod{17}$ and $4^2 = 16 \equiv -1 \pmod{17}$,
$\mathbb{Z}_{17}^*(\tau_4) = \langle -1 + 17\mathbb{Z},\, 5 + 17\mathbb{Z}\rangle_{\text{mult.}} = \mathbb{Z}_{17}^*$, since $\mathrm{ord}(5 + 17\mathbb{Z}) = 16$.
Hence $\mathbb{Z}_{17}^* = \mathbb{Z}_{17}^*(\tau_1) \subseteq \mathbb{Z}_{17}^*(\tau_1 \vee \tau_3) \subseteq \mathbb{Z}_{17}^*$ and $\mathbb{Z}_{17}^* = \mathbb{Z}_{17}^*(\tau_4) \subseteq \mathbb{Z}_{17}^*(\tau_2 \vee \tau_4) \subseteq \mathbb{Z}_{17}^*$ both with equality.

Consider the following uniform groups with corresponding representing matrices relative to $\overline{\mathbf{x}}$:

$$Z = R + \mathbb{Z}\frac{1}{17}(x_1 \quad + x_3 + x_4) + \mathbb{Z}\frac{1}{17}(\quad x_2 + x_3 + 2x_4)$$

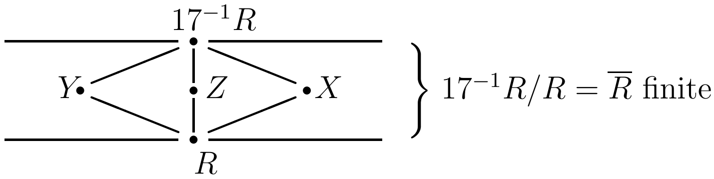
$$\leftrightarrow\ Q = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & \mathbf{1} & 2 \end{array}\right) = (I_2 \mid C),$$

$$X = R + \mathbb{Z}\frac{1}{17}(x_1 \quad + 2x_3 + x_4) + \mathbb{Z}\frac{1}{17}(\quad x_2 + 2x_3 + 2x_4)$$

$$\leftrightarrow\ M = \left(\begin{array}{cc|cc} 1 & 0 & 2 & 1 \\ 0 & 1 & \mathbf{2} & 2 \end{array}\right) = (I_2 \mid A),$$

$$Y = R + \mathbb{Z}\frac{1}{17}(x_1 \quad + x_3 + x_4) + \mathbb{Z}\frac{1}{17}(\quad x_2 + x_3 + x_4)$$

$$\leftrightarrow\ N = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{array}\right) = (I_2 \mid B).$$



Theorem 9.8 yields that there is at least $\prod_{m=1}^{2} [\mathbb{Z}_{17}^* : \mathbb{Z}_{17}^*(\tau_m \vee \tau_{2+m})] = 1 \cdot 1 = 1$ isomorphism class of groups with regulator R near–isomorphic to Z.

Clearly $Y \not\cong_{\mathrm{nr}} Z$, since $\mathrm{rk}_{17} B = 1 \neq 2 = \mathrm{rk}_{17} C$ and the matrices B, C are not (diagonally) equivalent.

Since $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) C \left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right) = A$, Lemma 8.2 shows $X \cong_{\mathrm{nr}} Z$. We apply Theorem 7.5 to the coefficient $(2,3)$ of C and A to decide that $X \not\cong Z$: There are no f_2, $f_3 \in \{\overline{\pm 1}, \overline{\pm 4}\} = \mathbb{Z}^*_{17}(\tau_2) = \mathbb{Z}^*_{17}(\tau_3)$ such that $\overline{\mathbf{2}} = \alpha_{23} = f_2^{-1} \underbrace{\gamma_{23}}_{=\overline{1}} f_3 = f_2^{-1} f_3 \in \{\overline{\pm 1}, \overline{\pm 4}\}$ in $\mathbb{Z}_{17}$. Hence there are more than one isomorphism class within the near–isomorphism class relative to C.

This is a counter–example for the way back of Lemma 9.6, too. Here it is $r = 2$, $D = \mathrm{diag}(1,1,2,1)$ and $D' = I_4$. The group Z agrees with Y of Lemma 9.6. We have $\frac{d_1}{d_3} \cdot \mathbb{Z}^*_{17}(\tau_1 \vee \tau_3) = \mathbb{Z}^*_{17}$ and $\frac{d_2}{d_4} \cdot \mathbb{Z}^*_{17}(\tau_2 \vee \tau_4) = \mathbb{Z}^*_{17}$. The statement $\frac{d'_m}{d'_{2+m}} \in \frac{d_m}{d_{2+m}} \cdot \mathbb{Z}^*_{17}(\tau_m \vee \tau_{2+m})$ for $m = 1, 2$ is not sufficient for isomorphism, since $X \not\cong Z$.

How many pairwise non–isomorphic groups are in the near–isomorphism class of Z? By Example 4.32 there are $\mathrm{Orb}_{\cong_{\mathrm{nr}}}(C) = 16^3 = 2^{12} = 4096$ matrices diagonally equivalent to C such that each matrix belongs to precisely one group which is near–isomorphic to Z. For $f_j \in \mathbb{Z}^*_{17}(\tau_j)$, where $j = 1, \ldots, 4$, we have to solve

$$\begin{pmatrix} f_1^{-1} & \\ & f_2^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} f_3 & \\ & f_4 \end{pmatrix} = \begin{pmatrix} f_1^{-1} f_3 & f_1^{-1} f_4 \\ f_2^{-1} f_3 & 2 f_2^{-1} f_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

This is equivalent to the linear equation system $f_1 = f_2 = f_3 = f_4 \in \cap_{j=1}^4 \mathbb{Z}^*_{17}(\tau_j) = \mathbb{Z}^*_{17}(\tau_2) \cong \mathbb{Z}_4$. Hence, by Theorem 8.7, the number of groups within the isomorphism class of Z is

$$\frac{\prod_{j=1}^4 |\mathbb{Z}^*_{17}(\tau_j)|}{|\mathbb{Z}^*_{17}(\tau_2)|} = \frac{16 \cdot 4 \cdot 4 \cdot 16}{4} = 2^{10} = 1024.$$

The number of distinct isomorphism classes contained in the near–isomorphism class of Z is

$$\frac{4096}{1024} = 4.$$

We determine the number of isomorphism classes of uniform groups $G \in \mathcal{C}(T, 17, 1, 2)$ with regulator $R \subseteq G \subseteq 17^{-1} R$ such that the representing matrix of $G/R \cong \mathbb{Z}_{17} \oplus \mathbb{Z}_{17}$ relative to $\overline{\mathbf{x}} = (\overline{x}_1, \overline{x}_2, \overline{x}_3, \overline{x}_4)$ is in Hermite normed form. Write

$$G = R + \mathbb{Z}\frac{1}{17}(x_1 \quad + \gamma_{13} x_3 + \gamma_{14} x_4) + \mathbb{Z}\frac{1}{17}(\quad x_2 + \gamma_{23} x_3 + \gamma_{24} x_4)$$

$$\leftrightarrow \left(\begin{array}{cc|cc} 1 & 0 & \gamma_{13} & \gamma_{14} \\ 0 & 1 & \gamma_{23} & \gamma_{24} \end{array}\right) = (I_2 \mid C).$$

Again $\mathrm{Orb}_{\cong_{\mathrm{nr}}}(C) = \{\mathrm{diag}(d_1, d_2)^{-1} C \,\mathrm{diag}(d_3, d_4) \mid d_j \in \mathbb{Z}^*_{17}\}$ agrees with the class of uniform groups nearly isomorphic to G. Similarly $\mathrm{Orb}_{\cong}(C) = \{\mathrm{diag}(f_1, f_2)^{-1} C \,\mathrm{diag}(f_3, f_4) \mid f_j \in \mathbb{Z}^*_{17}(\tau_j)\}$ agrees with the isomorphism class of G. Then $\frac{|\operatorname{Orb}_{\cong_{nr}}(C)|}{|\operatorname{Orb}_{\cong}(C)|}$ is the number of isomorphism classes of uniform groups within the near–isomorphism class of G.

By [Mut99, p. 133] there are $17 + 4 = 21$ normal forms of (2×2)–matrices over $\mathbb{Z}_{17}$ and therefore precisely 21 near–isomorphism classes of those groups in $\mathcal{C}(T, 17, 1, 2)$ of rank 4. Let $\eta \in \{0, 1, \dots, 16\}$.

NrIsoCl C	$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & \eta \\ 1 & 1+\eta \end{pmatrix}$
$\lvert\operatorname{Stab}_{\cong_{nr}}(C)\rvert$	2^8	2^8	2^4	2^4	2^4
$\lvert\operatorname{Orb}_{\cong_{nr}}(C)\rvert$	2^8	2^8	2^{12}	2^{12}	2^{12}
$\lvert\operatorname{Stab}_{\cong}(C)\rvert$	2^6	2^4	2^2	2^2	2^2
$\lvert\operatorname{Orb}_{\cong}(C)\rvert$	2^6	2^8	2^{10}	2^{10}	2^{10}
lower bound 9.8	–	1	–	1	1
upper bound 8.10	2^4	2^4	2^4	2^4	2^4
$\lvert\{\text{IsoCl}\}\rvert = \frac{\lvert\operatorname{Orb}_{\cong_{nr}}(C)\rvert}{\lvert\operatorname{Orb}_{\cong}(C)\rvert}$	2^2	1	2^2	2^2	2^2

$\triangle$

Remark 9.13. Example 9.10 shows that the lower bound of Theorem 9.8 and the upper bound of Corollary 8.10 cannot be improved with the same general assumptions. Example 9.12 shows that the precise number of isomorphism classes depends on C, namely the near–isomorphism class.

Applications to Groups of Small Rank

Remark 9.14. The situation simplifies if the normed and invertible matrix C is particularly the identity matrix. Then all groups taken under consideration have a finest direct decomposition into indecomposable rank two summands.

Corollary 9.15. *Let e be a natural number and p a prime. Let $\delta, \delta' \in \mathbb{Z} \setminus p\mathbb{Z}$ be integers. Then $d := \delta + p^e\mathbb{Z}$ and $d' := \delta' + p^e\mathbb{Z}$ are units of $\mathbb{Z}_{p^e}$. Let $T = (\tau_1, \tau_2)$ be a pair of incomparable types with $\tau_i(p) = 0$. Then $R = \tau_1 x_1 \oplus \tau_2 x_2$ is a rigid and p–reduced rank two group. Let $X = R + \mathbb{Z}\frac{1}{p^e}(x_1 + \delta x_2)$ and $Y = R + \mathbb{Z}\frac{1}{p^e}(x_1 + \delta' x_2)$ be groups.*

(1) *Then X and Y are nearly isomorphic uniform groups of $\mathcal{C}(T, p, e, r)$ with the common regulator R such that $R \subseteq X, Y \subseteq p^{-e}R$.*

(2) *The groups X and Y are isomorphic, $X \cong Y$, if and only if*

$$d' \in d \cdot \mathbb{Z}^*_{p^e}(\tau_1 \vee \tau_2) .$$

(3) *The total number of pairwise non–isomorphic groups contained in the near–isomorphism class of X is*

$$\frac{p^{e-1}(p-1)}{|\mathbb{Z}^*_{p^e}(\tau_1 \vee \tau_2)|} = \frac{\varphi(p^e) \cdot |\mathbb{Z}^*_{p^e}(\tau_1) \cap \mathbb{Z}^*_{p^e}(\tau_2)|}{|\mathbb{Z}^*_{p^e}(\tau_1)| \cdot |\mathbb{Z}^*_{p^e}(\tau_2)|} .$$

Proof. (1) The rest blocks (d) and (d') of the representing matrices are diagonally equivalent. It follows that X and Y are nearly isomorphic. By BURKHARDT REGULATOR CRITERION, the regulator of X and Y is R. We compute $X/R \cong \mathbb{Z}_{p^e} \cong Y/R$. Hence both groups are uniform.
(2) If X and Y are isomorphic, then $d' \in d \cdot \mathbb{Z}_{p^e}^*(\tau_1 \vee \tau_2)$, by Lemma 9.6.
For the converse we assume that there exist $f_1 \cdot f_2 \in \mathbb{Z}_{p^e}^*(\tau_1) \cdot \mathbb{Z}_{p^e}^*(\tau_2) = \mathbb{Z}_{p^e}^*(\tau_1 \vee \tau_2)$ such that $d' = d \cdot f_1 \cdot f_2$. The representing matrix rest blocks (d) and (d') are T–diagonally equivalent. Hence $X \cong Y$ by Theorem 7.5.
(3) The groups X and Y are isomorphic if and only if the elements d and d' of the rest blocks are in the same coset of $\mathbb{Z}_{p^e}^*(\tau_1 \vee \tau_2)$. Hence there are $\left[\mathbb{Z}_{p^e}^* : \mathbb{Z}_{p^e}^*(\tau_1 \vee \tau_2)\right] = \frac{p^{e-1}(p-1)}{|\mathbb{Z}_{p^e}^*(\tau_1 \vee \tau_2)|}$ matrices $D' = (d')$ which fail this condition. The cardinality of the complex product $\mathbb{Z}_{p^e}^*(\tau_1 \vee \tau_2) = \mathbb{Z}_{p^e}^*(\tau_1) \cdot \mathbb{Z}_{p^e}^*(\tau_2)$ is

$$|\mathbb{Z}_{p^e}^*(\tau_1) \cdot \mathbb{Z}_{p^e}^*(\tau_2)| = \frac{|\mathbb{Z}_{p^e}^*(\tau_1)| \cdot |\mathbb{Z}_{p^e}^*(\tau_2)|}{|\mathbb{Z}_{p^e}^*(\tau_1) \cap \mathbb{Z}_{p^e}^*(\tau_2)|} . \qquad \square$$

Corollary 9.16. *Let R be a rigid and p–reduced completely decomposable group of rank $n = 2r$ with an indexing $T = (\tau_1, \dots, \tau_n)$ of its critical typeset. Suppose that $\overline{\mathbf{x}} = (\overline{x}_1, \dots, \overline{x}_n)$ is an induced decomposition basis of $\overline{R} = p^{-e}R/R$. Let X and Y be groups with the common regulator R such that $R \subseteq X, Y \subseteq p^{-e}R$. Let $\overline{\mathbf{a}}$ and $\overline{\mathbf{b}}$ be bases of X/R and Y/R, respectively. Let*

$$M = \left(\begin{array}{ccc|ccc} 1 & & & d_1 & & \\ & \ddots & & & \ddots & \\ & & 1 & & & d_r \end{array}\right) \quad \text{and} \quad N = \left(\begin{array}{ccc|ccc} 1 & & & d'_1 & & \\ & \ddots & & & \ddots & \\ & & 1 & & & d'_r \end{array}\right),$$

where d_k, $d'_k \in \mathbb{Z}_{p^e}^*$, be the representing matrices of X and Y relative to $\overline{\mathbf{a}}$ and $\overline{\mathbf{b}}$.

(1) *Then X and Y are nearly isomorphic uniform groups of $\mathcal{C}(T, p, e, r)$.*

(2) *Both groups have a finest direct decomposition $X = \bigoplus_{m=1}^r X_m$ and $Y = \bigoplus_{m=1}^r Y_m$ into indecomposable rank two summands, i. e.* $\operatorname{rk} X_m = 2 = \operatorname{rk} Y_m$.

(3) *The groups X and Y are isomorphic, $X \cong Y$, if and only if*

$$d'_m \in d_m \cdot \mathbb{Z}_{p^e}^*(\tau_m \vee \tau_{r+m})$$

for all $m = 1, \dots, r$.

(4) *The total number of pairwise non–isomorphic groups contained in the near–isomorphism class of X is*

$$\prod_{m=1}^{r} \left[\mathbb{Z}_{p^e}^* : \mathbb{Z}_{p^e}^*(\tau_m \vee \tau_{r+m})\right] = \frac{(p^{e-1}(p-1))^r}{\prod_{m=1}^r |\mathbb{Z}_{p^e}^*(\tau_m \vee \tau_{r+m})|} .$$

Proof. The matrix rest blocks may be abbreviated by $D = \operatorname{diag}(d_1, \dots, d_r)$ and $D' = \operatorname{diag}(d'_1, \dots, d'_r)$. The r–rowed identity matrix I_r is a normed and invertible matrix. Define $c_i = x_i + x_{r+i}$ and $\overline{c}_i = \overline{x}_i + \overline{x}_{r+i}$ for $i = 1, \dots, r$. Then

$Z = \langle R, p^{-e}c_1, \dots, p^{-e}c_r \rangle$ is a uniform group with regulator $R \subseteq Z \subseteq p^{-e}R$. The ordered tuple $\overline{\mathbf{c}} = (\overline{c}_1, \dots, \overline{c}_r)$ is a basis of X/R such that $Q = (I_r \mid I_r)$ is the representing matrix of Z/R relative to $\overline{\mathbf{c}}$ and $\overline{\mathbf{x}}$.
(1) The rest blocks D and D' of M and N are diagonally equivalent to I_r. It follows that X and Y are nearly isomorphic to Z. Hence both groups are uniform, too.
(2) Define $X_m = \langle x_m, x_{r+m} \rangle_*^R + \mathbb{Z}p^{-e}(x_m + x_{r+m})$ for $m = 1, \dots, r$. Then we have $\operatorname{rk} X_m = 2$ and $X = \bigoplus_{m=1}^r X_m$.
(3) The groups X and Y are isomorphic if and only if the submatrices D and D' are T–diagonally equivalent. Thus there are $f_j \in \mathbb{Z}_{p^e}^*(\tau_j)$ such that $\operatorname{diag}(d'_1, \dots, d'_r) = \operatorname{diag}(f_1^{-1}, \dots, f_r^{-1}) \cdot \operatorname{diag}(d_1, \dots, d_r) \cdot \operatorname{diag}(f_{r+1}, \dots, f_n) = \operatorname{diag}(f_1^{-1} d_1 f_{r+1}, \dots, f_r^{-1} d_r f_n)$. This is equivalent to $d'_m = d_m f_m^{-1} f_{m+r} \in d_m \cdot \mathbb{Z}_{p^e}^*(\tau_m)\, \mathbb{Z}_{p^e}^*(\tau_{m+r})$ for all $m = 1, \dots, r$.
(4) The groups X and Y are isomorphic if and only if the diagonal elements d_m and d'_m of the rest blocks D and D' are in the same coset of $\mathbb{Z}_{p^e}^*(\tau_m \vee \tau_{r+m})$. Hence there are $\prod_{m=1}^r \left[\mathbb{Z}_{p^e}^* : \mathbb{Z}_{p^e}^*(\tau_m \vee \tau_{r+m})\right]$ matrices $D' = \operatorname{diag}(d'_1, \dots, d'_r)$ which fail this condition. $\square$

Corollary 9.17. *Let p be a prime and e a natural number. Let $R = \tau_1 x_1 \oplus \dots \oplus \tau_4 x_4$ be a rigid and p–reduced completely decomposable group with critical typeset $T = (\tau_1, \dots, \tau_4)$. Let $X \in \mathcal{C}(T, p, e, 2)$ be an almost completely decomposable group with regulator R such that $X/R = (\mathbb{Z}_{p^e})^2$. Let $\overline{\mathbf{x}} = (\overline{x}_1, \dots, \overline{x}_n)$ be the induced decomposition basis of $\overline{R} = p^{-e}R/R$ and $\overline{\mathbf{a}}$ be an ordered basis of X/R. Let the representing matrix M of X/R relative to $\overline{\mathbf{x}}$ and $\overline{\mathbf{a}}$ be in Hermite normed form with invertible rest block*

$$M = (I_2 \mid A) = \left(\begin{array}{cc|cc} 1 & & 1 & \alpha \\ & 1 & \beta & 1 + \alpha\beta \end{array}\right),$$

where $\alpha = \lambda p^m$, $\beta = \mu p^l$ for some units λ, μ and some integers $0 \le m, l \le e$. Let $\operatorname{Stab}_{\cong}(A) = \left\{F = \operatorname{diag}(f_1, \dots, f_4) \mid f_j \in \mathbb{Z}_{p^e}^*(\tau_j),\ F_{\leqslant 2}^{-1} A\, F_{>2} = A\right\}$ denote the stabilizer of A relative to the T–diagonal equivalence.
Let $A \neq \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then

$$\begin{aligned}\operatorname{Stab}_{\cong}(A) = \{\operatorname{diag}(f_1, f_2, f_1, f_2) \ \mid\ & f_1 \in \mathbb{Z}_{p^e}^*(\tau_1) \cap \mathbb{Z}_{p^e}^*(\tau_3),\ f_2 \in \mathbb{Z}_{p^e}^*(\tau_2) \cap \mathbb{Z}_{p^e}^*(\tau_4), \\ & \textit{such that } f_2 - f_1 \in p^{e - \min(m,l)} \cdot \mathbb{Z}_{p^e}\}.\end{aligned}$$

The number of distinct isomorphism classes contained in the near–isomorphism class of X is

$$N = \frac{\varphi(p^e)^3\, p^{-\min(m,l)} \cdot |\operatorname{Stab}_{\cong}(A)|}{\prod_{j=1}^4 \left|\mathbb{Z}_{p^e}^*(\tau_j)\right|}.$$

If α or β is a unit in $\mathbb{Z}_{p^e}$, then

$$N = \frac{\left(p^{e-1}(p-1)\right)^3 \cdot \left|\bigcap_{j=1}^4 \mathbb{Z}_{p^e}^*(\tau_j)\right|}{\prod_{j=1}^4 \left|\mathbb{Z}_{p^e}^*(\tau_j)\right|}.$$

Proof. Let $\mathrm{Stab}_{\cong_{\mathrm{nr}}}(A) = \{D = \mathrm{diag}(d_1, \dots, d_4) \mid d_j \in \mathbb{Z}^*_{p^e},\ D^{-1}_{\leqslant 2} A\, D_{>2} = A\}$ denote the stabilizer of A relative to arbitrary diagonal equivalence. Let $\mathrm{Orb}_{\cong_{\mathrm{nr}}}(A) = \{D^{-1}_{\leqslant 2} A D_{>2} \mid D \in \mathrm{DIAG}(4; \mathbb{Z}^*_{p^e})\}$ denote the diagonal equivalence class of A. Let $\mathrm{Orb}_{\cong}(A) = \{F^{-1}_{\leqslant 2} A F_{>2} \mid F \in \mathrm{DIAG}(T; \mathbb{Z}^*_{p^e})\}$ denote the T–diagonal equivalence class of A. Recall from Example 4.32 that $\mathrm{Stab}_{\cong_{\mathrm{nr}}}(A) = \{D = \mathrm{diag}(d_1, d_2, d_1, d_2) \mid d_1, d_2 \in \mathbb{Z}^*_{p^e}$ such that $d_2 - d_1 \in p^{e-\min(m,l)}\, \mathbb{Z}_{p^e}\}$ and $|\,\mathrm{Orb}_{\cong_{\mathrm{nr}}}(A)| = \varphi(p^e)^3\, p^{-\min(m,l)} = p^{3e-3-\min(l,m)}\,(p-1)^3$. We compute $\mathrm{Stab}_{\cong}(A) = \mathrm{DIAG}(T; \mathbb{Z}^*_{p^e}) \cap \mathrm{Stab}_{\cong_{\mathrm{nr}}}(A) = \{\mathrm{diag}(f_1, f_2, f_3, f_4) \mid f_j \in \mathbb{Z}^*_{p^e},\ f_1 = f_3,\ f_2 = f_4$ such that $f_2 - f_1 \in p^{e-\min(m,l)} \mathbb{Z}_{p^e}\}$ and we get the claim. Clearly we have $|\,\mathrm{Orb}_{\cong}(A)| = [\mathrm{DIAG}(T; \mathbb{Z}^*_{p^e}) : \mathrm{Stab}_{\cong}(A)] = \frac{\prod_{j=1}^4 |\mathbb{Z}^*_{p^e}(\tau_j)|}{\mathrm{Stab}_{\cong}(A)}$. By Theorem 8.8 the number of isomorphism classes within the near–isomorphism class of X is

$$N = \frac{|\,\mathrm{Orb}_{\cong_{\mathrm{nr}}}(A)|}{|\,\mathrm{Orb}_{\cong}(A)|} = \frac{\varphi(p^e)^3\, p^{-\min(m,l)} \cdot |\,\mathrm{Stab}_{\cong}(A)|}{\prod_{j=1}^4 |\mathbb{Z}^*_{p^e}(\tau_j)|}\,.$$

If α or β is a unit in $\mathbb{Z}_{p^e}$, then $\min(m, l) = 0$ and we compute $\mathrm{Stab}_{\cong}(A) = \{\mathrm{diag}(f, f, f, f) \mid f \in \bigcap_{j=1}^4 \mathbb{Z}^*_{p^e}(\tau_j)\}$. Then the statement follows. □

10. Resulting Problems

(1) The critical typeset of a local group can have several admissible orderings. In general not all orderings are equally good. Is there a distinguished ordering?

(2) There is a complete system of near–isomorphism invariants for uniform groups, cf. [DO93] and [Mut99]. Does there exist a complete system of near–isomorphism invariants for block–rigid groups with a primary homocyclic regulator quotient and for rigid local groups?

(3) Is there a complete system of isomorphism invariants for rigid local groups?

(4) Does there exist a complete system of isomorphism invariants for groups with isomorphic primary constituents?

References

[DO93] M. Dugas and E. Oxford. Near isomorphism invariants for a class of almost completely decomposable groups. In *Abelian Groups, Proceedings of the 1991 Curaçao Conference*, pages 129–150. Marcel Dekker, Inc., 1993.

[Fuc73] L. Fuchs. *Infinite Abelian Groups, Vol. I, II.* Academic Press, 1970 and 1973.

[KM84] K.-J. Krapf and O. Mutzbauer, Classification of almost completely decomposable groups, in *Abelian Groups and Modules, Proceedings of the Udine Conference* 1984, volume 287 of *CISM Courses and Lecture Notes*, pages 151–161. Springer Verlag, 1984.

[Mad00] A. Mader. *Almost Completely Decomposable Groups*, volume 13 of *Algebra, Logic and Applications Series.* Gordon and Breach Science Publishers, 2000.

[MMN01] A. Mader, O. Mutzbauer, and L. Nongxa. Representing matrices of almost completely decomposable groups. In *J. Appl. Alg.*, 2001.

[Mut99] O. Mutzbauer. Normal forms of matrices with applications to almost completely decomposable groups. In *Abelian Groups, Trends in Mathematics and Modules*, pages 121–134, 1999.

[Nah98] M. Nahler. Near–isomorphism invariants of almost completely decomposable groups. Diplomarbeit (Würzburg 1998).

[Sch98] M. Schlez. Anzahl von Isomorphieklassen fast vollständig zerlegbarer Gruppen. Diplomarbeit (Würzburg 1998).

Index

Michael Nahler
Rudolf–Clausius–Strasse 63 a
D-97080 Würzburg
GERMANY

E-mail address: nahler@mathematik.uni-wuerzburg.de