Vrije Universiteit Brussel

FACULTEIT WETENSCHAPPEN EN
BIO-INGENIEURSWETENSCHAPPEN
DEPARTEMENT WISKUNDE

Vrije groepen van eenheden in gehele groepringen

Proefschrift ingediend met het oog op het behalen van de graad van Master in de Wiskunde

Shaun Bundervoet

Promotor : Prof. Dr. E. Jespers

2011 - 2012

Dankwoord

Het is zover. Nog een aanpassing hier en daar en dé masterproef is eindelijk af. Maandenlang heb ik naar dit moment toegewerkt. Het voorbije jaar heeft dan ook nieuwe werelden geopend voor mij. Ik heb de kans gekregen om met enkele fantastische mensen samen te werken, een ervaring waar ik veel uit geleerd heb. In mijn eentje was het dan ook nooit gelukt om deze masterproef te realiseren. Daarom wil ik de tijd nemen om enkele mensen te bedanken.
Eerst en vooral wil ik mijn promotor professor Eric Jespers bedanken; niet alleen voor de goede begeleiding en vrijheid die hij mij gaf maar vooral omdat hij altijd in mij is blijven geloven, zelfs wanneer ik hem daar geen reden toe gaf. Ook wil ik de algebraïsten bedanken waaronder professor Philippe Cara, Inneke Van Gelder, Ann Kiefer, Florian Eisele en Geoffrey Janssens. Zij stonden altijd paraat om te antwoorden op mijn vragen en hebben mij een grote dienst bewezen met hun commentaar op deze masterproef. *I would like to thank professor Jairo Gonçalves for his quick correspondence these last few months. Thank you for all your patience and insightful answers to my questions.* Ook kan ik de vakgroep Wiskunde niet vergeten die verantwoordelijk is voor de goede opleiding die ik de laatste jaren heb genoten hier aan de Vrije Universiteit Brussel.
Mijn familie en in het bijzonder mijn ouders ben ik zeer dankbaar voor de continue steun en het vertrouwen die zij mij de voorbije jaren hebben gegeven. Mijn grootste dankbaarheid gaat naar Dorien. Doorheen deze ganse periode is zij er altijd geweest voor mij. Zonder haar aan mijn zijde was dit alles betekenisloos.

Shaun Bundervoet
Oostende, Mei 2012

Samenvatting

Eén van de talrijke vragen waar wiskundigen zich hedendaags mee bezighouden is: gegeven twee matrices in een lineaire groep, wat zijn de relaties tussen deze twee matrices? Meer specifiek is men geïnteresseerd in het weten of de deelgroep voortgebracht door deze twee matrices vrij is, i.e. er zijn geen relaties. Beschouw bijvoorbeeld de volgende 2×2 matrices in $\mathrm{GL}_2(\mathbb{C})$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \quad \text{en} \quad \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}.$$

Indien deze twee matrices een vrije deelgroep voortbrengen van $\mathrm{GL}_2(\mathbb{C})$, dan wordt λ een vrij element genoemd van $\mathbb{C}$. Een klassiek resultaat [San47] toont dat λ vrij is als $|\lambda| \geq 2$. Echter als dit niet het geval is, dan is het antwoord in het algemeen niet gekend. Wel zijn er veel deelresultaten bekend. Zo werd bijvoorbeeld in [CJR58] aangetoond dat λ ook vrij is als het geen element is van de eenheidsschijven rond -1, 0 en 1. Anderzijds toonde Rimhak Ree aan dat $]-2, 2[$ en $]-i, i[$ elk bevat zijn in een open verzameling van het complexe vlak waarin de niet-vrije punten dicht verdeeld zijn. Verrassend genoeg is het dus blijkbaar niet eenvoudig om te weten of een gegeven complex getal λ vrij is, laat staan in het algemeen of de deelgroep voortgebracht door twee willekeurige matrices vrij is.

Het hoofddoel van deze masterproef is om de technieken geïntroduceerd door Gonçalves en Passman in hun artikel *"Linear groups and group rings"* [GP06] te bestuderen. Hierin verschaffen ze een methode om paren van vrije matrices te identificeren, meer bepaald als beide matrices *diagonaliseerbaar* zijn, *veralgemeende transvesties* zijn of een combinatie van de twee. Ook algemenere gevallen worden besproken. Hierbij maken ze gebruik van het Ping-pong Lemma door het veralgemenen van een eerder resultaat bekomen door Jacques Tits [Tit72]. De bekomen technieken zijn zo algemeen mogelijk geformuleerd voor lokaal compacte velden. Dit is de hoofdreden waarom deze masterproef begint met twee inleidende hoofdstukken over dit onderwerp. Het is de bedoeling om enerzijds een classificatie te geven van alle lokaal compacte velden en anderzijds om de lezer vertrouwd te maken met de rijke structuur aanwezig in deze velden, alsook om het nauw verband te belichten tussen de analytische en algebraïsche begrippen.

1: In het eerste hoofdstuk beginnen wij met het veralgemenen van de *klassieke modulus* $|.|_\infty$ op de complexe getallen $\mathbb{C}$ naar een *absolute waarde* op een veld F. Dit zijn functies van F naar $\mathbb{R}^+$ met dezelfde elementaire eigenschappen. Een voorbeeld hiervan is de *triviale* absolute waarde, die het nulelement van F op 0 stuurt en alle andere elementen op 1. Dit is tevens de enige mogelijke absolute waarde die definieerbaar is op een eindig veld. Vermits elk oneindig veld F het rationaal veld $\mathbb{Q}$ bevat, is het logisch om eerst te proberen alle mogelijke absolute velden op $\mathbb{Q}$ te beschrijven. Hierbij onderscheiden wij twee types absolute waarden, namelijk de *archimedische* en de *niet-archimedische*. Het zal blijken dat elke archimedische absolute waarde *topologisch equivalent* is met de klassieke $|.|_\infty$, terwijl elke niet-triviale, niet-archimedische topologisch equivalent zal zijn met een zogenaamde *p-adische* absolute waarde $|.|_p$, waar p een priem getal is. Deze bevindingen zullen voornamelijk interessant zijn bij de studie van *completies*. In het bijzonder zal de completie van $\mathbb{Q}$ ten opzichte van $|.|_p$ gelijk zijn aan de p-adische getallen $\mathbf{Q}_p$. Daartegenover staat het resultaat van Ostrowski die aantoont

dat de enige velden die compleet zijn ten opzichte van een archimedische absolute waarde de reële getallen $\mathbb{R}$ en de complexe getallen $\mathbb{C}$ zijn. Dit zijn tevens ook de enige *lokaal compacte* velden waarop een archimedische absolute waarde gedefinieerd is.

2: Hoofdstuk twee begint met een alternatieve beschrijving van een *geordende abelse groep* G. Deze beschrijving zal vooral nuttig zijn om het concept van een niet-archimedische absolute waarde op een veld F te veralgemenen naar dat van een *valuatie*. Dit zijn functies van F naar $G \cup \{0\}$ met de standaard eigenschappen. Men kan dit doen omdat een dergelijke absolute waarde geen gebruik maakt van de optelling in $\mathbb{R}^+$, maar enkel van de vermenigvuldiging en de orde. Ook wordt het equivalente concept van een *valuatiering* geïntroduceerd . Dit zal nodig zijn voor de studie van *lokale velden*, welke in essentie de velden zijn met een niet-archimedische absolute waarde $|.|$ zodat de *geïnduceerde topologie* lokaal compact is. Samen met de resultaten uit hoofdstuk 1 geeft dit ons een volledige beschrijving van alle lokaal compacte velden.

3: In dit derde hoofdstuk beginnen wij met het bespreken van [GP06]. Wij zijn dus op zoek naar criteria die garanderen dat de deelgroep voortgebracht door twee matrices/operatoren S en T, in een lineaire groep $\mathrm{GL}_k(F)$, vrij is van graad 2. Zoals eerder vermeld zal hiervoor gebruik gemaakt worden van het Ping-pong Lemma. Dit zegt dat $\langle S, T\rangle$ natuurlijk isomorf is met $\langle S\rangle * \langle T\rangle$ als er twee niet lege deelverzamelingen $P_1 \neq P_2$ van F^k bestaan zodat $SP_1 \subseteq P_2$ en $TP_2 \subseteq P_1$. Het probleem is dus min of meer gereduceerd tot het vinden van deze "aantrekkende" en "afstotende" verzamelingen P_1 en P_2.
Beschouw daarom eerst het probleem vanuit het standpunt van een veralgemeende transvectie $S = 1 + a\sigma \in \mathrm{GL}_k(F)$, waar $a \in F_0$ en σ een niet nulle operator is met $\sigma^2 = 0$. Merk alvast op dat $S^n = 1 + na\sigma$. Als nu $|na|$ groot is dan kan men vermoeden dat het deel $na\sigma$ de operator S^n zal domineren. Specifiek willen wij aantonen dat voor elke vector x, die "dicht" bij een goed gekozen deelruimte X van F^k ligt, de beeldvector $S^n(x)$ "dicht" bij $I = \sigma(F^k)$ zal liggen, indien n groot genoeg is. De enige voorwaarde op X zal zijn dat $X \cap K = \{0\}$, waar $K = \ker\sigma$ een hypervlak is. Om deze notie van "dichtbij" wiskundig correct uit te drukken zal gebruik moeten worden gemaakt van de *projectieve metriek*. Het is in de definitie van deze metriek dat zal worden verondersteld dat F lokaal compact is. Als nu $\overline{X}$ de open bol rond X is in deze projectieve metriek, dan wordt bewezen dat, onder de juiste omstandigheden, $S^n(\overline{X}) \subseteq \overline{I}$.
Anderzijds als $T = 1 + b\tau \in \mathrm{GL}_k(F)$ een tweede veralgemeende transvestie is met $J = \tau(F^k)$ en $L = \ker\tau$, dan kan men opnieuw een deelruimte Y vinden, deze keer gescheiden van L, zodat $T^m(\overline{Y}) = \overline{J}$, voor m groot genoeg.
Gezien de keuzes van X en Y; als nu $J \cap K = \{0\}$ en $I \cap L = \{0\}$ dan impliceert het voorgaande dat $S^n(\overline{J}) \subseteq \overline{I} = P_2$ en $T^m(\overline{I}) \subseteq \overline{J} = P_1$ voor n en m groot genoeg. Zo bekomt men opnieuw een voldoende voorwaarde opdat $\langle S^n, T^m\rangle = \langle S^n\rangle * \langle T^m\rangle$. Tevens is deze relatief eenvoudig om na te gaan. Een gelijkaardige methode zal gebruikt worden om hetzelfde resultaat te bekomen voor diagonaliseerbare operatoren en zelfs voor een combinatie van beide.

Als toepassing van deze technieken geven Gonçalves en Passman voorbeelden van vrije eenheden in gehele groepsringen. Hiervoor beschouwen ze twee belangrijke constructies van eenheden, namelijk de *Bass cyclische eenheden* en de *bicyclische eenheden*. Door middel van complexe representaties worden deze eerste afgebeeld op diagonaliseerbare operatoren en de laatste op veralgemeende transvecties. Merk op dat het voldoende is voor twee eenheden in een groepring $\mathbb{Z}[G]$ om een vrije groep van rang 2 voort te brengen dat hetzelfde geldt voor de homomorfe beelden van deze eenheden. Dit verschuift het probleem van groepringen naar lineaire groepen, wat behandeld werd in hoofdstuk 3. Wij merken op dat in het besproken artikel er vooral gefocust wordt op het vinden van vrije Bass cyclische eenheden daar dit nog nooit eerder werd gedaan, in tegenstelling tot bicyclische eenheden.

4: Merk op dat wij, bij de studie van veralgemeende transvecties, hadden dat $\dim I = 1 = \dim J$, waar $\overline{I} = P_2$ en $\overline{J} = P_1$. Bij het vaststellen van een voldoende voorwaarde opdat twee diagonaliseerbare operatoren een vrij paar zouden vormen, zal ook impliciet vereist worden dat bepaald dimensies van deelruimten gelijk zijn. Zoals gezegd, zijn het precies deze operatoren die beschouwd worden bij het zoeken naar toepassingen met Bass cyclische eenheden in gehele groepringen. Om de vereiste dimensies onder controle te krijgen zal het nodig zijn om enkele technische lemma's te bewijzen. Dit zal dan ook de hoofdtaak zijn van hoofdstuk 4. Specifiek als $\varepsilon = e^{2\pi/d}$ dan willen wij weten voor welke $a \in \mathbb{Z}_d$ de waarden $\left|(\varepsilon^{ak}-1)/(\varepsilon^a-1)\right|^m$ maximaal, respectievelijk minimaal, zijn. Deze waarden komen overeen met absolute waarden van projecties van Bass cyclische eenheden. Ook willen wij nagaan voor welke $a, b \in \mathbb{Z}_d$

$$\left|\frac{\varepsilon^{ak}-1}{\varepsilon^a-1}\right|^m = \left|\frac{\varepsilon^{bk}-1}{\varepsilon^b-1}\right|^m.$$

5: In het laatste hoofdstuk wordt het hoofdresultaat bewezen, welke zegt dat *voor elke niet-abelse groep G, waarvan de orde relatief priem is met 6, de gehele groepring $\mathbb{Z}[G]$ tenminste één koppel vrije Bass cyclische eenheden (u, v) bevat.* Deze stelling wordt bewezen door middel van inductie op de orde $o(G)$ van G. Als nu H een echte niet-abelse deelgroep is van G, dan is de orde $o(H)$ nog steeds relatief priem met 6 en bovendien is $o(H) < o(G)$. Door de inductiehypothese mogen wij dan veronderstellen dat $\mathbb{Z}[H]$ twee Bass cyclische eenheden u en v bevat zodat $\langle u, v\rangle$ natuurlijk isomorf is met $\langle u\rangle * \langle v\rangle$. Duidelijk zijn u en v ook Bass cyclische eenheden van $\mathbb{Z}[G]$ en de groep voortgebracht door deze twee is nog steeds vrij van rang 2. Dit reduceert het probleem tot niet-abelse groepen G zodat elke echte deelgroep abels is. Door een gelijkaardige redenering te gebruiken zullen wij ook mogen veronderstellen dat elk echt epimorf beeld van G abels is. Daarom start hoofdstuk 5 met een classificatie van deze "minimaal" niet-abelse groepen. Uiteindelijk wordt het probleem zo gereduceerd tot drie gevallen. Het grote voordeel van deze drie types groepen is dat de irreduciebele complexe representaties makkelijk te beschrijven zijn. Zo wordt het nagaan van de criteria uit hoofdstuk 3 veel eenvoudiger.

Vrije Universiteit Brussel

FACULTY OF SCIENCE AND
BIO-ENGINEERING SCIENCES
DEPARTMENT OF MATHEMATICS

Free groups of units in integral group rings

Graduation thesis submitted in partial fulfillment of the requirements for the degree of Master in Mathematics

Shaun Bundervoet

Promotor : Prof. Dr. E. Jespers

2011 - 2012

Contents

Introduction

The theory of group rings has a somewhat peculiar history. Group rings initially appeared in an article [Cay54] of Arthur Cayley in the mid nineteenth century, the same article in which he gave the first definition of an abstract group. Given a finite group $G = \{g_0, \dots g_n\}$ he considered elements of the form

$$\alpha = x_0 g_0 + x_1 g_1 \dots + x_n g_n,$$

where the x_i's with $0 \leq i \leq n$ where either real or complex numbers. The addition is defined component-wise while the multiplication is extended distributively from the group operations on G. This is precisely the definition of a group ring $R[G]$, in the case where $R = \mathbb{R}$ or $\mathbb{C}$. Unfortunately their importance was not recognized at the time and group rings would remain unstudied for half a century. It was an, until then, unknown Estonian named Theodor Molien who reintroduced group rings when he wrote his PhD-thesis [Mol92] at the end of the nineteen century. The subject only really gained its momentum in the late twenties when Emmy Noether [Noe29] made the connection between group representation theory and the structure theory of algebra, using group rings. Ultimately group rings gained their interest as a separate subject in the sixties after Irving Kaplansky included some questions concerning group rings in his lists of open problems. From that point on group rings $R[G]$, where G is a potentially infinite group, attracted a lot of attention, which is why the first book entirely devoted to group rings [Pas71] by Donald S. Passman is mainly concerned with this subject. A more elaborate history on the origin of group rings can be found in [PMS02, Chapter 3].

A group ring $R[G]$ is in essence the most natural way to link a ring to the group G. Moreover they provide a class of rings in which calculations are relatively easy. Now one can ask in what way the ring-theoretical properties of $R[G]$ are influenced by those of R and also by the group-theoretical properties of G, and vice-versa. For instance if $R[G]$ is isomorphic to $R[H]$ does this imply that $G \cong H$? It is easily seen that this will not always be the case in general. Namely, if G and H are both abelian groups of the same order then $\mathbb{C}[G] \cong \mathbb{C}[H]$. This could be due to the fact that $\mathbb{C}$ adds too much structure to the group ring. Thus one can wonder if adding the minimal possible structure to the group G in the construction of $R[G]$ will result in a positive answer. Specifically if $\mathbb{Z}[G] \cong \mathbb{Z}[H]$ does this imply that G is isomorphic to H. This is commonly known as the isomorphism problem for integral group rings. Higman [Hig40], was the first to ask this question and immediately settled the abelian group case. Also for other classes the question has been proven to be positive, for example when G is finite nilpotent, see [RS87]. This result was the first real indication that the isomorphism problem might actually be true and even more that a proof might even be obtainable. However, much to the surprise of everybody in the mathematical world, Hertweck [Her01] gave a counterexample to the isomorphism problem in 2001.

One other problem imposed by Sudarshan Sehgal in [Seh93] is to find presentations of the units group $\mathcal{U}(\mathbb{Z}[G])$ where G is a finite group. As in this case $\mathcal{U}(\mathbb{Z}[G])$ is finitely generated, one thus wonders which are the generating units and what are the relations between these units. A closely related problem is knowing whether or not $\mathcal{U}(\mathbb{Z}[G])$ contains units without any relation between them. The first result was obtained simultaneously by Sehgal [Seh78]

and by Hartley and Pickel [HP80]. They showed if G is finite group then $\mathcal{U}(\mathbb{Z}[G])$ contains a free subgroup if and only if G is neither abelian nor a Hamiltonian 2-group. Unfortunately the proof is not constructive and the need still exists to find concrete free pairs of units in $\mathbb{Z}[G]$. To this end Marciniak and Sehgal [MS97] showed that if u is a non-trivial bicyclic unit in $\mathbb{Z}[G]$ then u and u^* generate a non-abelian free subgroup of the unit group $\mathcal{U}(\mathbb{Z}[G])$. This solved the problem for non-abelian non Hamiltonian groups. The Hamiltonian case was settled by Ferraz [Fer03] by the use of Bass units.

Since the constructions of Marciniak, Sehgal and Ferraz, the hunt is on to find more concrete free pairs of units in integral group rings $\mathbb{Z}[G]$ for any group G. This will be the central topic of this graduation thesis where we overgo the joint work of Gonçalves and Passman in their article *"Linear groups and group rings"* [GP06] from 2006. The techniques they introduced do not only allow for finding free pairs of Bass cyclic units and bicyclic units but also free pairs formed by a bicyclic unit and a Bass cyclic unit. They accomplished this by generalizing a result of Tits [Tit72], used to prove that finitely generated linear groups are either solvable-by-finite or contain a non-abelian free subgroup. The main result relating to group rings which was proven is the following.

Main result. *Let G be a finite non-abelian group whose order is relatively prime to 6, then there exist two elements g and h in G of prime power order and two Bass cyclic units $u_{k,t}(g)$ and $u_{r,s}(h)$ such that $\langle u_{k,t}(g), u_{r,s}(h)\rangle$ is a non-abelian free subgroup of the unit group of the integral group ring $\mathbb{Z}[G]$.*

Now $\mathbb{Z}[G] \subseteq \mathbb{C}[G]$, which is why complex representations are used to prove this theorem. Suitable irreducible representations $\mathfrak{X} : G \to \mathrm{GL}_n(\mathbb{C})$ are described which are then linearly extended to representations of $\mathbb{C}[G]$. It is enough for two units in $\mathcal{U}(\mathbb{Z}[G])$ to form a free pair if the same holds for their image in $\mathrm{GL}_n(\mathbb{C})$. This reduces the problem to finding free pairs of operators in linear groups. This will be facilitated through the use of the Ping-pong lemma which is commonly attributed to Felix Klein. More specifically the Bass cyclic units will be mapped to diagonalizable operators under the complex representation $\mathfrak{X}$. Using these same techniques a secondary result is also given.

Secondary result. *Let G be a finite non-abelian group whose order is relatively prime to 6, then $\mathbb{Z}[G]$ contains a bicyclic unit β and a Bass cyclic unit u such that β^t and u generate a non-abelian free group of the unit group $\mathcal{U}(\mathbb{Z}[G])$, for any sufficiently large integer t.*

We only give a description of the proof which is due to Gonçalves and del Río [GP06]. Again complex representation theory is used as a means to prove this result. Here the bicyclic units will be mapped to generalized transvections. A more thorough description of what is to be expected will be given at the beginning of each chapter.

Chapter 1

Absolute values on a field

The field of complex numbers $\mathbb{C}$ and its subfields naturally possess a function called the *absolute value* or modulus $|.|_\infty$ which is defined as $\sqrt{z\overline{z}}$ for every complex number z. First if we consider $\mathbb{C}$ as a 2-dimensional $\mathbb{R}$-vector space then this function from $\mathbb{C}$ to $\mathbb{R}$ is not only a norm, it is more since it also admits the property that $|z||z'| = |zz'|$ for all complex numbers z and z'. On the other hand every field, including $\mathbb{C}$, can be seen as a 1-dimensional vector space over itself. In this case every norm is automatically an *absolute value*. In this sense the concept of an *absolute value* on a field is not really original but it has its benefits to observe this structure more closely. One of the origins for this field of study can be found in number theory with Hensel's description of p-adic numbers in 1897. When Kürschák developed the theory of *real valued valuations* or *absolute values* in 1912 he showed that Hensel's p-adic numbers could be seen as the completion of $\mathbb{Q}$ relative to a p-adic *absolute value*. This already shows that this theory forms a solid link between subjects like number theory, algebra and analysis. Other advantages are it permits the study of algebraic functions, also it leads to the introduction of analytical concepts in the study of arithmetic questions.

Our purpose will be to provide an introduction to the theory, this to give the reader an idea of the richness in the underlying structures we will be using. Continuing this reasoning we will try to categorize all the fields that are *locally compact* relative to an *absolute value*. This could help to generalize ideas used in later chapters where we will mainly assume our field to be equal to the complex numbers. The chronology of this chapter is mostly based on Chapter 9 from Nathan Jacobson's Basic Algebra II [Jac89]. The main differences with the book will be found in the approach used to add more intuition to the subject, this due to the difference in goals between the book and this master thesis.

1.1 Topological equivalence of two absolute values

We start off by extending the classical absolute value $|.|_\infty$ on the field of complex numbers $\mathbb{C}$ to arbitrary fields by generalizing its basic properties.

Definition 1.1.1 (Absolute value)**.** *Let F be a field, and $|.| : F \to \mathbb{R}^+ : a \mapsto |a|$ a map such that for all $a, b \in F$*

(1) $|a| = 0$ *if and only if* $a = 0$.

(2) $|ab| = |a||b|$.

(3) $|a + b| \leq |a| + |b|$.

In this case we say that $|.|$ is an absolute value on F. The third requirement will be referred to as the triangle inequality.

Remark 1.1.2 (Weak triangle inequality)**.** *As a consequence of the second property we can weaken the request of a triangle inequality to*

(4) $|c+1| \leq |c|+1$.

for every $c \in F$*. Since* $|b| \geq 0$*, (4) implies the inequality* $|a/b+1||b| \leq (|a/b|+1)|b|$ *which by (2) implies (3). Clearly this states that both requirements are equivalent.*

First let us note that any field F can be equipped with at least one absolute value called the trivial absolute value and which is defined as

$$|.|_0 : F \to \mathbb{R}^+ : a \mapsto \begin{cases} 0 & \text{if} \quad a = 0, \\ 1 & \text{if} \quad a \neq 0. \end{cases}$$

Unfortunately this observation is completely redundant as it does not introduce any new structure to the field. What will be interesting is the fact that for some fields this will be the only absolute value which can be defined on them. This presents a possible incompatibility between the field structure and that of an absolute value which will be caused by certain finiteness issues. Before we go into the subjects let us first give an important example which is the class of absolute values on $\mathbb{Q}$ called the p-adic absolute values.

Example 1.1.3. Let p be an arbitrary but fixed prime in $\mathbb{Z}$. Every $a \in \mathbb{Q}_0 = \mathbb{Q} \setminus \{0\}$ can uniquely be written as $a = (b/c)p^k$ with $b, c \in \mathbb{N}_0, k \in \mathbb{Z}$ and $\gcd(b,p) = 1 = \gcd(c,p)$. As said k is uniquely determined by a which allows us to define

$$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\} : a \mapsto \begin{cases} k & \text{if} \quad a = (b/c)p^k, \\ \infty & \text{if} \quad a = 0. \end{cases}$$

Note that

(i) $v_p(a) = \infty$ if and only if $a = 0$.

(ii) $v_p(ab) = v_p(a) + v_p(b)$.

(iii) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$.

Next take $\gamma \in]0,1[$. We now define a *p-adic function* $|.|_p$ on $\mathbb{Q}$ as follows

$$|.|_p : \mathbb{Q} \to \mathbb{R}^+ : a \to \gamma^{v_p(a)},$$

where we take $\gamma^\infty = 0$. Clearly the mapping $|.| = |.|_p$ is an absolute value on $\mathbb{Q}$ for which holds

$$|a+b| \leq \max\{|a|, |b|\}. \tag{1.1}$$

Absolute values that attain this stronger property are called *non-archimedean*, otherwise we say the absolute value is *archimedean*. These terms were first introduced by Ostrowski in 1917. Nowadays the term "ultrametric" is also widely used instead of non-archimedean. △

In many textbooks "the" p-adic absolute value is the function $|.|_p$ on $\mathbb{Q}$ where γ is chosen to be equal to $1/p$, others simply set $\gamma = e^{-1}$ whatever the prime p may be. Also note that if we allow γ to be equal to 1 in the definition of a p-adic absolute value then in this case the trivial absolute value is also a p-adic absolute value. Let us now isolate some fundamental properties.

Properties 1.1.4. *For every absolute value $|.|$ on a field F the following basic properties hold for every $a, b \in F$:*

(i) $1| = 1$,

(ii) $|a| = 1$ *if there exists an* $n \in N$ *such that* $a^n = 1$,

(iii) $|a| = |-a|$,

(iv) $|a^{-1}| = |a|^{-1}$ *if* $a \neq 0$ *and*

(v) $||a| - |b||_\infty \leq |a - b|$.

Proof. We will only prove the second property *(ii)*. Suppose F contains an element a of finite order with $|a| \neq 1$. Since in this case a^{-1} also has finite order we may assume that $1 < |a|$. Then $|a^2| = |a|^2 > |a|$ and we obtain an ascending chain

$$1 < |a| < |a^2| < |a^3| < \ldots < |a^n| < \ldots.$$

Clearly this chain can never stabilize and thus $|a^n| \neq 1$ for every nonzero positive integer. This implies a cannot have finite order which is a contradiction to our assumption. □

Remark 1.1.5. *Notice that by the second property a field F with absolute value $|.|$ cannot contain an element a of finite order with $|a| \neq 1$. This implies that the only absolute value that can be defined on a finite field is the trivial absolute value. Also if F is equipped with a non trivial absolute value we can always find an ascending chain as in the previous proof which shows that in this case F cannot be bounded.*

As mentioned in the introduction of this chapter every field F can be viewed as a 1-dimensional vector space over itself. By this fact the absolute value of F becomes a norm.

Remark 1.1.6. *Recall that for any set X the definition of a topology $\mathcal{T}$ as being a set of subsets of X such that this set contains the empty set and X. This set is also defined as being closed for taking finite intersections and countable unions. The usual examples are the trivial topology $\mathcal{T} = \{\emptyset, X\}$ which is the coarsest topology on X and the discrete topology $\mathcal{T} = \mathcal{P}(X)$ which is the finest topology on X. If we now take F a field with an absolute value $|.|$ on F then with every $x \in F$ we can associate a class of subsets of F called the spherical neighborhoods of x. For each $r > 0$ such a subset is defined as follows,*

$$B_r(x) = \{a \in F \mid |x - a| < r\}.$$

The family $(B_r(x))_{x \in X, r \in \mathbb{R}_0}$ of all these subsets forms a basis for the neighborhood system of a topology. We call this the topology induced by $|.|$, or just induced topology and denote it by $\mathcal{T}_{|.|}$. Also,

$$\mathcal{T}_{|.|} = \{A \subseteq X \mid \forall x \in A \; \exists r > 0 : B_r(x) \subseteq A\}.$$

We note that this topology is the coarsest topology on F such that the absolute value $|.|$ is continuous and is compatible with the ring structure of F in the following sense

(i) the addition $+ : F \times F \to F$ is a continuous map and

(ii) the multiplication $. : F \times F \to F$ is a continuous map,

where $F \times F$ is equipped with the product topology.

Counterintuitive to what we know from norms, two distinct absolute values need not induce the same topology. This is of course due to the fact that this rule only applies to normed vector spaces build on the same field with identical absolute value. It is thus interesting to understand which conditions will cause two absolute values to induce the same topology.

Proposition 1.1.7. *Let F be a field and $|.|_1$ and $|.|_2$ be non trivial absolute values on F then the following are equivalent,*

(a) $|.|_1$ and $|.|_2$ induce the same topology $\mathcal{T}$ on F.

(b) For all $a \in F : |a|_1 < 1$ implies $|a|_2 < 1$.

(c) There exists an $s > 0$ such that $|.|_1^s = |.|_2$.

We denote $|.|_1 \sim |.|_2$ if and only if one, and thus all, of the above properties is satisfied, and this relation is an equivalence relation on the set of absolute values on F.

Proof. First suppose that (a) holds. This implies that if a sequence $(a_i)_{i\in\mathbb{N}}$ converges in F with respect to $|.|_1$ then the same holds for this sequence with respect to $|.|_2$ and vice versa. Now let $a \in F$ such that $|a|_1 < 1$ then,

$$|a^n|_1 = |a|_1^n \to 0$$

Therefore

$$|a|_2^n = |a^n|_2 \to 0$$

and thus $|a|_2 < 1$, so that (b) holds.

For the second part of the proof say that $|a|_1 < 1$ implies $|a|_2 < 1$ for all $a \in F$. By using the basic properties we find that $|a|_1 < |b|_1$ implies $|a|_2 < |b|_2$ and hence $|1|_1 = 1 < |a|_1$ implies $1 < |a|_2$. Because we assumed the absolute values to be non trivial there exists an $a_0 \in F$ such that $|a_0|_1 > 1$ and thus $|a_0|_2 > 1$. Now take $a \in F$ with $|a|_1 > 1$ and also $|a|_2 > 1$. Let

$$t = \log|a|_1 / \log|a_0|_1.$$

Clearly $t > 0$ and $|a|_1 = |a_0|_1^t$. Obviously there also exists a $t' > 0$ defined by

$$t' = \log|a|_2 / \log|a_0|_2,$$

so that $|a|_2 = |a_0|_2^{t'}$. We now claim that $t = t'$. To prove this, suppose the contrary. Then $t' \neq t$ so that there exists a $q = m/n \in \mathbb{Q}_0^+$ (with $m, n \in \mathbb{N}_0^+$ and $\gcd(m, n) = 1$) and

first case:	$t < q < t'$	which implies	$\|a\|_2 > \|a_0\|_2^q$	and
second case:	$t' < q < t$	which implies	$\|a\|_2 < \|a_0\|_2^q$.	

The contradiction of these cases will become clear if we can prove

first case:	for every q such that $t < q$	this implies	$\|a\|_2 < \|a_0\|_2^q$	and
second case:	for every q such that $0 < q < t$	this implies	$\|a\|_2 > \|a_0\|_2^q$.	

So first suppose $t < q$. Then $|a|_1 < |a_0|_1^{m/n}$ and $|a^n|_1 < |a_0^m|_1$. It follows that $|a^n|_2 < |a_0^m|_2$ and $|a|_2 < |a_0|_2^{m/n}$. Similarly for $m/n = q < t$ we find $|a|_2 > |a_0|_2^{m/n}$. Hence $t = t'$ and

$$t = \frac{\log|a|_1}{\log|a_0|_1} = \frac{\log|a|_2}{\log|a_0|_2},$$

or also

$$s = \frac{\log|a|_1}{\log|a|_2} = \frac{\log|a_0|_1}{\log|a_0|_2}.$$

We clearly get $|a|_1^s = |a|_2$ for all a so that $|a|_1 > 1$. If $|a|_1 < 1$ we note that $|a^{-1}|_1^s = |a^{-1}|_2$ and again comes the conclusion $|a|_1^s = |a|_2$.

For the final part of the proof suppose that (c) is true for some $s > 0$. Take $a \in F$ arbitrary and consider the ϵ-neighborhood with $\epsilon > 0$ around a for the $|.|_1$ norm. We have

$$\begin{aligned} B_{\epsilon,1}(a) &= \{x \in F \mid |x-a|_1 < \epsilon\} \\ &= \{x \in F \mid |x-a|_2^{s^{-1}} < \epsilon\} \\ &= \{x \in F \mid |x-a|_2 < \epsilon^s\} \\ &= B_{\epsilon^s,2}(a). \end{aligned}$$

Now take $G \subseteq F$ open for the topology $\mathcal{T}_{|.|_1}$ on F. Then for every $a \in G$ there exists an ϵ-ball such that

$$B_{\epsilon,1}(a) \subseteq G.$$

But this implies by our previous remark that for every a

$$B_{\epsilon^s,2}(a) \subseteq G.$$

This shows that G is also open for the topology $\mathcal{T}_{|.|_2}$ so that $\mathcal{T}_{|.|_1} \subseteq \mathcal{T}_{|.|_2}$. The proof of the other inclusion is completely similar to the previous. The resulting equivalency now follows from the three implications. □

Clearly from this, two p-adic absolute values $|.|_p$ and $|.|_p'$ with different basis numbers γ and γ' define the same topology on $\mathbb{Q}$ as they are equivalent for $s = \log\gamma'/\log\gamma$. This implies that every choice of $0 < \gamma < 1$ is valid for defining "the" p-adic absolute value on $\mathbb{Q}$. It is also obvious that the trivial absolute value is not equivalent with any other absolute value and this is why γ is taken strictly smaller than 1. Furthermore the trivial absolute value is the only one on the field F which induces the discrete topology.

Remember from Example 1.1.3 that an absolute value is either non-archimedean if the strong property (1.1) holds or archimedean if this is not the case. We will now prove that whether or not an absolute value is archimedean can be reduced to a property of the prime ring $1\mathbb{Z}$ of F.

Theorem 1.1.8. *An absolute value $|.|$ on a field F is non-archimedean if and only if $|n1| \leq 1$ for all $n \in \mathbb{Z}$.*

Proof. First take $|.|$ to be non-archimedean, then

$$\begin{aligned} |n1| &= |1+1+\ldots 1|, \qquad \text{(n-terms)} \\ &\leq \max|1| = |1| = 1. \end{aligned}$$

Conversely, suppose $|n1| \leq 1$ for all $n \in \mathbb{Z}$ and let $a, b \in F$. Then for any positive interger n it holds that

$$\begin{aligned} |a+b|^n &= \left|\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k\right| \\ &\leq \sum_{k=0}^{n} \left|\binom{n}{k}\right| \left|a^{n-k}\right| \left|b^k\right| \\ &\leq \sum_{k=0}^{n} \left|a^{n-k}\right| \left|b^k\right| \\ &\leq (n+1)\max\{|a|^n, |b|^n\}. \end{aligned}$$

It follows that

$$|a+b| \leq (n+1)^{1/n}\max\{|a|,|b|\} \to \max\{|a|,|b|\} \quad \text{when } n \to \infty.$$

For the latter we have used that $\lim_{n\to\infty}(n+1)^{1/n} = 1$. This proves the claim of this theorem. □

Notice that an absolute value $|.|$ induces a preorder $\preccurlyeq$ on the field F by setting $a \preccurlyeq b$ if and only if $|a| \leq |b|$ for every $a, b \in F$. Both the reflexive and transitive properties are fulfilled but the antisymmetric property can not be guaranteed. Take for example $\mathbb{C}$ with the classical absolute value. Now in a preordered group $(G, <)$ an element x is called infinitesimal with respect to the element y if

$$\forall n \in \mathbb{N}_0 : nx < y,$$

where nx stands for the sum of n terms x. If no such elements x and y exist then G is called archimedean. Clearly this is equivalent with the known archimedean property that for every x and y in G

$$\exists n \in \mathbb{N}_0 : x < ny.$$

From the previous theorem, an absolute valued field F is non-archimedean if and only if 1 is infinitesimal to itself. Also if this is not the case then for every x and y nonzero in F there exists an $n \in \mathbb{N}$ such that $|x| < |ny|$. This implies $x \prec ny$ in F which explains the terminology.

We have shown for an absolute value on F that being non-archimedean is completely determined by its behavior on the prime ring. This has as a consequence the following corollary.

Corollary 1.1.9. *Suppose F is a field with characteristic $p \neq 0$, then any absolute value on F is non-archimedean.*

Proof. Let F be a field with characteristic $p \neq 0$ and prime ring $\{n1 \mid n \in \mathbb{Z}\}$ then if $n1 \neq 0$ we have, $(n1)^{p-1} = 1$ so that, by Remark 1.1.5, $|n1| = 1$ and $|0| = 0$. This proves that $|.|$ is non-archimedean. □

1.2 Absolute values on the rationals

In this section we will characterize all absolute values on the rational field $\mathbb{Q}$. Actually it will turn out that there are only three types of equivalence classes for the relation in Proposition 1.1.7. This will be of particular interest when studying fields of characteristic 0 as they contain $\mathbb{Q}$.

Theorem 1.2.1. *Let $|.|$ be an archimedean absolute value on $\mathbb{Q}$. Then this is equivalent to the classical absolute value $|.|_\infty$.*

Proof. First take n and n' to be positive integers greater then 1. Rewriting n' in base n we obtain

$$n' = \sum_{i=0}^{k} a_i n^i, \qquad \text{with } k \in \mathbb{N}, i \in \{0, \ldots, k\} \text{ and } a_i \in \mathbb{N} \cap [0, n[. \tag{1.2}$$

Following a similar argument used in the proof of Proposition 1.1.8 we find

$$\begin{aligned} |n'| &< n(1 + |n| + \ldots + |n|^k) \\ &\leq n(k+1)\max\{1, |n|^k\}. \end{aligned}$$

Since $n' \geq n^k$ we see that $\log n' \geq k \log n$ and it follows that $\log n' / \log n \geq k$. So we can further estimate the previous inequality by

$$|n'| < n\left(\frac{\log n'}{\log n} + 1\right)\max\{1, |n|^{\log n' / \log n}\}.$$

Replacing n' by n'^r in (1.2) with r a positive integer yields

$$|n'^r| < \left(nr\frac{\log n'}{\log n} + n\right)\max\{1, |n|^{r \log n' / \log n}\}.$$

Consequently

$$|n'| < \left(rn\frac{\log n'}{\log n} + n \right)^{1/r} \max\{1, |n|^{\log n'/\log n}\}.$$

Using l'Hôpital's rule we find for any $a, b \in \mathbb{R}$ that the limit for r going to infinity of $1/r(ra+b)$ is equal to 0 so that $\lim_{r\to\infty}(ra+b)^{1/r} = 1$. This shows us that

$$|n'| \leq \max\{1, |n|^{\log n'/\log n}\}, \text{ for all } n, n' > 1. \tag{1.3}$$

Theorem 1.1.8 now tells us that there exists an integer $n' > 1$ such that $|n'| > 1$. It follows that $|n'| \leq |n|^{\log n'/\log n}$ and thus by the arbitrarity of n we see that $|n| > 1$ for all integers $n > 1$. We get for all $n, n' > 1$

$$|n'|^{1/\log n'} \leq |n|^{1/\log n},$$

and moreover by symmetry we see for all $n, n' > 1$

$$|n'|^{1/\log n'} = |n|^{1/\log n}.$$

For an n' fixed we now set

$$s = \frac{\log |n'|}{\log n'} = \frac{\log |n|}{\log n}.$$

We have $|n| = n^s$ for all integers $n > 1$, and by extension $|a| = |a|_\infty^s$ for all $a \in \mathbb{Q}_0$. Hence $|.|$ is equivalent to the classical norm $|.|_\infty$. □

So our first type of equivalence class is the one consisting of all absolute values which are equivalent to the classical absolute value. The two remaining classes will follow in the next theorem by Ostrowski.

Theorem 1.2.2 (Ostrowski)**.** *Let $|.|$ be a non trivial non-archimedean absolute value on $\mathbb{Q}$ then this is equivalent to a p-adic absolute value for some prime p.*

Proof. By the assumption we have $|n| \leq 1$ for every integer n. Suppose all $|n| = 1$ for $n \neq 0$, then $|.|$ is trivial which is a contradiction to the assumption. So define the following set

$$P = \{n \in \mathbb{Z} \mid |n| < 1\},$$

and we know this set contains nonzero elements. For any $p, q \in P$ and $n \in \mathbb{Z}$ we have

$$|p + q| \leq \max\{|p|, |q|\} < 1 \text{ and } |nq| = |n||q| < 1.$$

Thus P is an ideal in $\mathbb{Z}$ which is also prime since for any $n, n' \in Z$, $|n| = 1$ and $|n'| = 1$ implies $|nn'| = 1$. Hence for some p prime $P = (p)$. Now put $\gamma = |p| \in]0, 1[$. As in Example 1.1.3 we can write any $q \in \mathbb{Q}$ as $q = p^k a/b$ with $k \in \mathbb{Z}$ and $a, b \notin (p)$. Again because of the prime property $|a| = 1 = |b|$ so that

$$|q| = |p^k a/b| = |p|^k = \gamma^k = \gamma^{v_p(q)}.$$

Thus $|.|$ is a p-adic absolute value based on γ. □

This shows that the second class of absolute values on $\mathbb{Q}$ is made up off all the p-adic absolute values, where we run trough every possible prime p, while the third class consists only of the trivial absolute value.

1.3 Completion of a field

In metric, and more general, uniform topological spaces X, we have encountered particular sequences who seemingly inherit all properties of convergent sequences except that X does not contain its limit. Such sequences are called Cauchy. Spaces which do contain all these limits are called complete. When the space X is not complete it is possible to add these missing limits and in such a way make the space X as yet complete. We will now briefly elaborate on this for absolute valued fields F.

Definition 1.3.1 (Cauchy sequence)**.** *Let F be a field with absolute value $|.|$. A sequence $(a_i)_{i\in\mathbb{N}}$ in F is called a Cauchy sequence if for any $\epsilon > 0$, there exists a positive integer N such that for all $p, q \geq N$*

$$|a_p - a_q| < \epsilon$$

Stronger is saying that a sequence converges. For completeness' sake we add this definition.

Definition 1.3.2 (Convergent sequence)**.** *Let F be a field with absolute value $|.|$. A sequence $(a_i)_{i\in\mathbb{N}}$ in F is called a convergent sequence if there exists an $a \in F$ such that for any $\epsilon > 0$, there exists a positive integer N and for all $n \geq N$*

$$|a_n - a| < \epsilon$$

We say that $(a_i)_{i\in\mathbb{N}}$ converges to a and denote this by $a_n \to a$ or $\lim_n a_n = a$ or even just $\lim a_n = a$ if the indexing of the sequence is clear. Also we say that F is complete (relative to $|.|$) if every Cauchy sequence in F converges.

Clearly a convergent sequence is Cauchy. We should remark that the concept of convergence can be generalized to any topological space. The concept of a Cauchy sequence on the other hand can only be generalized to uniform spaces. More in depth information on the subject can be found in numerous textbooks like Nicolas Bourbaki's Elements of Mathematics [Bou66a, Chapter I & II]. That said, in the course of this text, we will specifically use fields which satisfy the conditions of Definition 1.3.2. To emphasize this choice we will use the term complete field.

As in the study of uniform topological spaces we now want to see when an "incomplete" field F with absolute value $|.|$ can be completed. Of course we first have to explain what is meant with a completion of a field. It is not enough to find a larger field $E \supseteq F$ that is complete. Obviously the absolute value on E has to coincide with $|.|$ on F. Also we want the topology on E to be close to the one induced on F. This is expressed by the density. Finally we want to know if a completion is unique.

Definition 1.3.3 (Completion of a field)**.** *Let F be a field with absolute value $|.|$ and E/F a field extension with $|.|'$ the absolute value on E, then we call E a completion of F if*

(1) $|.|'$ is an extension of $|.|$.

(2) E is complete, relative to the uniformity induced by $|.|'$.

(3) F is dense in E, relative to the topology induced by $|.|'$.

We now formally state the existence and uniqueness of the completion of a field F. Also, a complete proof is given, although the reader should be warned that this proof is very tedious and similar techniques can be found in any number of textbooks. This being said the reader can skip the details in favor of what follows afterwards.

Theorem 1.3.4. *If F is a field with absolute value $|.|$ then F has a completion $\hat{F}$. Furthermore if $\hat{F}_i, i = 1, 2$ are completions of F_i then any isometric isomorphism from F_1 to F_2 has a unique extension to an isometric isomorphism from $\hat{F}_1$ to $\hat{F}_2$. In particular a completion $\hat{F}$ is unique up to isometric isomorphism.*

Proof. We start by defining

$$C = \{a : \mathbb{N} \to F \mid \forall \epsilon > 0 \; \exists N \; \forall n, m \geq N : |a_n - a_m| < \epsilon\}$$

the set of all Cauchy sequences in F. Then take $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in C\backslash\{(0)_{n\in\mathbb{N}}\}$, where $(0)_{n\in\mathbb{N}}$ is the constant 0 sequence. Then for every ϵ there exists an $N > 0$ such that for any $m, n > N$

$$\begin{aligned} |(a_n + b_n) - (a_m + b_m)| &= |(a_n - a_m) + (b_n - b_m)| \\ &\leq |(a_n - a_m)| + |(b_n - b_m)| \\ &< \epsilon + \epsilon = 2\epsilon. \end{aligned}$$

Since $(0)_{n\in\mathbb{N}} \neq (a_n)_{n\in\mathbb{N}} \in C$ there also exists an M such that for all $n \geq M$, $a_n \neq 0$. Let $N' = \max\{N, M\}$ then for all $n, m \geq N'$

$$\begin{aligned} |(a_n b_n) - (a_m b_m)| &= |a_n(b_n - (a_m/a_n)b_m)| \\ &= |a_n||(b_n - (a_m/a_n)b_m)| \\ &= |a_n||(b_n - (a_m/a_n)b_m) + (b_m - b_{m)}| \\ &= |a_n||(b_n - b_m) - ((a_m/a_n) - 1)b_m| \\ &= |a_n||(b_n - b_m) - (a_m - a_n)(b_m/a_n)| \\ &\leq |a_n|\,(|(b_n - b_m)| + |(a_m - a_n)||(b_m/a_n)|) \\ &< |a_n|\epsilon + |b_m|\epsilon := \epsilon', \end{aligned}$$

where we notice that sequences $(c_n)_{n\in\mathbb{N}} \in C$ do not tend to infinity, i.e. $|c_n| \nrightarrow \infty$. We now see that the following two binary operations on C are well defined

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}} \qquad \textit{and} \qquad (a_n)_{n\in\mathbb{N}}(b_n)_{n\in\mathbb{N}} = (a_n b_n)_{n\in\mathbb{N}}.$$

These operations inherit the same properties as those on F which makes $(C, +, \cdot, (0)_{n\in\mathbb{N}}, (1)_{n\in\mathbb{N}})$ into a commutative ring. However, notice for example if $(a_n)_{n\in\mathbb{N}} \neq (0)_{n\in\mathbb{N}}$ is a Cauchy sequence then

$$0, a_1, a_2, a_3, \ldots, a_n, \ldots$$

is also a Cauchy sequence different from zero but for which no inverse exists, and hence C is not a field. We can also view F as a part of C by considering $\{F\}$, the set of constant sequences, in the following manner

$$i : F \hookrightarrow \{F\} \subseteq C : a \mapsto (a)_{n\in\mathbb{N}}.$$

Continuing on define

$$B = \{a : \mathbb{N} \to F \mid \forall \epsilon > 0 \; \exists N \; \forall n \geq N : |a_n| < \epsilon\},$$

the set of all null sequences. Now let $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in B$ and $(c_n)_{n\in\mathbb{N}} \in C$ then for any $\epsilon > 0$ there exists an N and for any $n \geq N$

$$\begin{aligned} |a_n + b_n| &\leq |a_n| + |b_n| \\ &< \epsilon + \epsilon = 2\epsilon, \end{aligned} \qquad \text{and} \qquad \begin{aligned} |c_n b_n| &= |c_n||b_n| \\ &< |c_n|\epsilon := \epsilon'. \end{aligned}$$

Again noticing that $|c_n| \nrightarrow \infty$ this shows that B is an ideal in C and since $B \cap \{F\} = \{(0)_n\}$ we have that B is a proper ideal of C.

Suppose now that B' is an ideal in C such that $B \subsetneq B'$ and take $(a_n)_{n\in\mathbb{N}} \in B'\backslash B$. This means that $(a_n)_{n\in\mathbb{N}}$ is a non-null Cauchy sequence and as such there exists a real number

$\eta > 0$ and an integer N such that $|a_n| > \eta$ for every $n \geq N$. Suppose this is not the case then for every $\eta > 0$, take for example $\eta = \epsilon/2$, and for every N their exists an $n > N$ such that $|a_n| \leq \eta = \epsilon/2$. But since $(a_n)_{n\in\mathbb{N}}$ is a Cauchy sequence, there also exists an N such that $|a_n - a_m| \leq \epsilon/2$ for every $n, m > N$. This implies that for every $n > N$

$$|a_n - 0| = |a_n - a_m + a_m| \leq |a_n - a_m| + |a_m| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

where $m > N$, a contradiction. Now define

$$b : \mathbb{N} \to F : n \mapsto \begin{cases} b_n = 1 & \text{if} \quad n < N \\ b_n = a_n & \text{if} \quad n \geq N. \end{cases}$$

Then $(a_n)_{n\in\mathbb{N}} - (b_n)_{n\in\mathbb{N}} := (c_n)_{n\in\mathbb{N}} \in B$. We also have for every $n, m \geq N$

$$|b_n^{-1} - b_m^{-1}| = |a_n^{-1} - a_m^{-1}| = |a_n^{-1}a_m^{-1}(a_m - a_n)| \leq \eta^{-2}\epsilon := \epsilon',$$

so that $(b_n^{-1})_{n\in\mathbb{N}} \in C$. We now obtain

$$(1)_{n\in\mathbb{N}} = (b_n^{-1})_{n\in\mathbb{N}}(b_n)_{n\in\mathbb{N}} = (b_n^{-1})_{n\in\mathbb{N}}(a_n)_{n\in\mathbb{N}} - (b_n^{-1})_{n\in\mathbb{N}}(c_n)_{n\in\mathbb{N}} \in B'.$$

This shows that $B' = C$ and more specifically that B is a maximal ideal.

Next we put $\hat{F} = C/B$. Then this is a field and again we can consider $\{F\} \cong F$ as a subfield as follows

$$j : F \hookrightarrow \hat{F} : a \mapsto a + B. \tag{1.4}$$

This makes $\hat{F}/F$ into a field extension.

We now want to introduce an absolute value on $\hat{F}$. Notice first that if $(a_n)_{n\in\mathbb{N}} \in C$ that

$$\begin{aligned} ||a_n| - |a_m||_\infty &\leq |a_n - a_m| \\ &< \epsilon. \end{aligned}$$

It follows that $(|a_n|)_{n\in\mathbb{N}}$ is a Cauchy sequence of real numbers and thus its limit exists in $\mathbb{R}$. Also if $(a_n)_{n\mathbb{N}} + B = (b_n)_{n\in\mathbb{N}} + B \in \hat{F}$ then $(a_n - b_n)_{n\in\mathbb{N}} \in B$ and $|a_n - b_n| \to 0$. Clearly this implies that $\lim_n |a_n| = \lim_n |b_n|$. We now have a map

$$|.|' : \hat{F} \to \mathbb{R}^+ : (a_n)_{n\in\mathbb{N}} + B \mapsto |(a_n)_{n\in\mathbb{N}} + B|' = \lim_n |a_n|$$

This map inherits the triangle inequality condition from $|.|$ because, for $(a_n)_{n\in\mathbb{N}} + B$ and $(b_n)_{n\in\mathbb{N}} + B$ in $\hat{F}$, we get

$$\begin{aligned} |((a_n)_{n\in\mathbb{N}} + B) + ((b_n)_{n\in\mathbb{N}} + B)| &= |(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} + B|' \\ &= |(a_n + b_n)_{n\in\mathbb{N}} + B|' \\ &= \lim_n |a_n + b_n| \\ &\leq \lim_n |a_n| + \lim |b_n| \\ &= |(a_n)_{n\in\mathbb{N}} + B|' + |(b_n)_{n\in\mathbb{N}} + B|'. \end{aligned}$$

Similarly we get the second multiplication condition. The first condition follows since $\lim |a_n| = 0$ if and only if $\lim a_n = 0$. Thus $|.|'$ is an absolute value on $\hat{F}$ which is clearly an extension of $|.|$ if we identify F as in (1.4).

To show that F is dense in $\hat{F}$ we need to take an element $(a_n)_{n\in\mathbb{N}} + B$ in $\hat{F}$ and show this is a limit of a sequence in F. Therefore consider the sequence $((a_m)_{n\in\mathbb{N}} + B)_{m\in\mathbb{N}}$ which we

can identify with the sequence $(a_m)_{m\in\mathbb{N}} \subseteq F$ via the map j. For any $\epsilon > 0$ we can now find an N such that for all $m \geq N$

$$\begin{aligned} |((a_m)_{n\in\mathbb{N}} + B) - ((a_n)_{n\in N} + B)|' &= |(a_m - a_n)_{n\in\mathbb{N}} + B|' \\ &= \lim_n |a_m - a_n| \\ &< \epsilon, \end{aligned}$$

for the latter we have used that $(a_n)_n$ is Cauchy.

Next we check whether $\hat{F}$ is complete. Therefore take a Cauchy sequence $((a_{mn})_{n\in N}+B)_{m\in\mathbb{N}}$ in $\hat{F}$. This implies that for all $\epsilon > 0$ there exists an N such that for all $p, q \geq N$

$$\begin{aligned} \lim_n |a_{pn} - a_{qn}| &= |(a_{pn} - a_{qn})_{n\in\mathbb{N}} + B|' \\ &= |(a_{pn})_{n\in\mathbb{N}} + B - (a_{qn})_{n\in\mathbb{N}} + B|' \\ &< \epsilon, \end{aligned}$$

which implies for an N' and all $n, p, q \geq \max\{N', N\}$ that $|a_{pn} - a_{qn}| < \epsilon$. Because of the density there exists for every m an $a_m \in F$ such that

$$\begin{aligned} \lim_n |a_m - a_{mn}| &= |(a_m - a_{mn})_{n\in\mathbb{N}} + B|' \\ &= |((a_m)_{n\in\mathbb{N}} + B) - (a_{mn})_{n\in\mathbb{N}} + B)|' < \frac{1}{2^m}. \end{aligned}$$

Thus for every $\epsilon > 0$ there again exists an N'' and for all $n \geq N''$ we see that $|a_m - a_{mn}| < \frac{1}{2^m} + \epsilon$. So, by using that$((a_{mn})_{n\in\mathbb{N}} + B)_{m\in\mathbb{N}}$ is Cauchy, we obtain

$$\begin{aligned} |a_p - a_q| &= |a_p - a_{pn} + a_{pn} - a_q + a_{qn} - a_{qn}| \qquad (\text{with } n \geq \max\{N', N''\}) \\ &\leq |a_p - a_{pn}| + |a_q - a_{qn}| + |a_{pn} - a_{qn}| \\ &< \left(\frac{1}{2^p} + \epsilon\right) + \left(\frac{1}{2^q} + \epsilon\right) + \epsilon \\ &= \frac{1}{2^p} + \frac{1}{2^q} + 3\epsilon, \end{aligned}$$

for all $p, q, \geq N$. This shows that $(a_n)_{n\in\mathbb{N}}$ is a Cauchy sequence so we can consider the element $(a_n)_{n\in\mathbb{N}} + B$. We finally get for $m \geq N$

$$\begin{aligned} |(a_n)_{n\in\mathbb{N}} + B - (a_{mn})_{n\in\mathbb{N}} + B)|' &= |(a_n - a_{mn})_{n\in\mathbb{N}} + B|' \\ &= \lim_n |a_n - a_{mn}| \\ &= \lim_n |a_n - a_{nn} + a_{nn} - a_{mn}| \\ &\leq \lim_n |a_n - a_{nn}| + \lim_n |a_{nn} - a_{mn}| \\ &< \lim_n \frac{1}{2^n} + \epsilon. \end{aligned}$$

This shows that $\lim_m (a_{mn})_{n\in\mathbb{N}} + B = (a_n)_{n\in\mathbb{N}} + B$. So all of the above was used to show that our construction of $\hat{F}$ is a completion of F.

We will finish by showing that this completion is unique. More generally consider $\hat{F}_i$ the completion of F_i relative to $|.|_i$, $i = 1, 2$. Now consider the isometric isomorphism s (if it exists) between F_1 and F_2.

$$s : F_1 \to F_2 : a \mapsto s(a) \qquad \text{such that} \qquad |a|_1 = |s(a)|_2, \forall a \in F_1.$$

Because s is also a continuous map from F_1 to $\hat{F}_2$, and because all induced topologies are Hausdorff we get by the density of F_1 in $\hat{F}_1$ that s has a unique extension to a continuous

$$\begin{aligned}\hat{s}(a+b) &= \hat{s}(\lim_n a_n + \lim_n b_n) \\ &= \hat{s}(\lim_n a_n + b_n) \\ &= \lim_n s(a_n + b_n) \\ &= \lim_n s(a_n) + \lim_n s(b_n) \\ &= \hat{s}(\lim_n a_n) + \hat{s}(\lim_n b_n) \\ &= \hat{s}(a) + \hat{s}(b)\end{aligned} \qquad \text{and} \qquad \begin{aligned}\hat{s}(ab) &= \hat{s}(\lim_n a_n \lim_n b_n) \\ &= \hat{s}(\lim_n a_n b_n) \\ &= \lim_n s(a_n b_n) \\ &= \lim_n s(a_n) \lim_n s(b_n) \\ &= \hat{s}(\lim_n a_n)\hat{s}(\lim_n b_n) \\ &= \hat{s}(a)\hat{s}(b).\end{aligned}$$

map $\hat{s} : \hat{F}_1 \to \hat{F}_2$. To show that this is an isometric homomorphism let $a, b \in \hat{F}_1$ then there exists sequences in $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \subseteq F_1$ such that $\lim_n a_n = a$ and $\lim_n b_n = b$. We now see

By similar reasoning we can show that $\hat{s}$ is isometric and unique. If s^{-1} is the inverse of s we can prove, again by using a similar argument, that $\widehat{s^{-1}}$ is the inverse of $\hat{s}$. This completes the proof. □

We conclude this section with an example. More precisely we will construct the completion of $\mathbb{Q}$ relative to a p-adic absolute value. Actually we will show that the closure of $\mathbb{Z}$ in the completion $\hat{\mathbb{Q}}$ of $\mathbb{Q}$ must be equal to the p-adic integers $\mathbf{Z}_p$. Afterwards it will not be difficult to verify that $\hat{\mathbb{Q}}$ is the field of fractions of $\mathbf{Z}_p$ and thus equal to the p-adic numbers $\mathbf{Q}_p$.

Example 1.3.5 (p-adic numbers)**.** First let us look at the ring of p-adic integers $\mathbf{Z}_p$. An element a of $\mathbf{Z}_p$ can be considered as a sequence of residue classes $(a_1 + (p), a_2 + (p^2), a_3 + (p^3), \ldots)$ such that for $i \leq j$ we have that $a_i \equiv a_j \bmod p^i$. We can represent this sequence as $(a_1, a_2, a_3, \ldots)$ where again $a_i \equiv a_j \bmod p^i$ for $i \leq j$. Two sequences $(a_1, a_2, a_3, \ldots)$ and $(b_1, b_2, b_3, \ldots)$ now represent the same element if and only if $a_k \equiv b_k \bmod p^k$. Addition and multiplication of these sequences is component-wise. A more algebraic construction of the ring $\mathbf{Z}_p$ can be given by means of inverse limits. Without going into the details we again get

$$\mathbf{Z}_p = \varprojlim_{i\in\mathbb{N}_0} \mathbb{Z}_{p^i} = \left\{ a \in \prod_{i\in\mathbb{N}\setminus\{0\}} \mathbb{Z}_{p^i} \mid a_i \equiv a_j \bmod p^i \text{ for all } i \leq j \in \mathbb{N}\setminus\{0\} \right\}.$$

A categorical definition by means of the universal property can also be used. Next recall that every $a \in \mathbb{Z}$ can be written as $a = r_0 + r_1 p + r_2 p^2 + \ldots + r_n p^n$ with $0 \leq r_i < p$. As a consequence $(r_0, r_0 + r_1 p, r_0 + r_1 p + r_2 p^2, \ldots, a, a, a, \ldots)$ is a representation of an element in $\mathbf{Z}_p$ and thus we can consider $\mathbb{Z}$ as a subring of $\mathbf{Z}_p$. As an example the number 159 will be represented in $\mathbf{Z}_5$ as $(4, 9, 34, 159, 159, \ldots)$. Notice that $\mathbf{Z}_p$ has no zero divisors, hence it has a field of fractions which we denote as $\mathbf{Q}_p$, the field of p-adic numbers.

Consider now $\hat{\mathbb{Z}}$ the closure of $\mathbb{Z}$ in the completion $\hat{\mathbb{Q}}$ of $\mathbb{Q}$ relative to the absolute value $|.|_p$. An element $a \in \hat{\mathbb{Z}}$ is the limit in $\hat{\mathbb{Q}}$ of a sequence of integers a_i. Since in particular this sequence is a Cauchy sequence for the p-adic absolute value we can assume, by removing elements if necessary, that $a_i \equiv a_j \bmod p^i$ for every $i \leq j \in \mathbb{N}$. We thus have a map

$$s : \hat{\mathbb{Z}} \to \mathbf{Z}_p : \lim a_i \mapsto (a_1, a_2, a_3, \ldots),$$

which is clearly an isomorphism. Observe that since $\{|a|_p \mid a \in \mathbb{Q}\}$ is closed in $\mathbb{R}$, this set is equal to $\{|a|_p \mid a \in \hat{\mathbb{Q}}\}$. Now take $\beta \neq 0$ in $\hat{\mathbb{Q}}$, then there exists an e in $\mathbb{Z}$ such that $|\beta|_p = |p^e|_p$. In other words $\alpha = \beta p^{-e}$ has absolute value equal to 1. As a consequence $\alpha = \lim a_i$ where $a_i = b_i/c_i$ with $(b_i, p) = 1 = (c_i, p)$. There now exists a sequence $(x_i)_i$ of element in $\mathbb{Z}$ such that $x_i c_i \equiv b_i \bmod p^i$. We then have $|x_i - b_i/c_i|_p = |p^i|_p$ and thus

$\alpha = \lim x_i \in \hat{\mathbb{Z}} = \mathbf{Z}_p$. Because β was chosen arbitrary we see that every element in $\hat{\mathbb{Q}}$ has the form αp^e with $\alpha \in \mathbf{Z}_p$. As $\mathbf{Z}_p(p^{\mathbb{Z}})$ is a field encompassed by the field of fractions of $\mathbf{Z}_p$ these fields are also equal and we can conclude that $\hat{\mathbb{Q}} = \mathbf{Q}_p$. This last approach can be viewed as the analytical manner of constructing the p-adic numbers. △

1.4 Galois extension of complete fields

Given an absolute valued field F. If E/F is a finite dimensional field extension, one could ask whether or not the absolute value $|.|$ can be extended to an absolute value on E. One could also wonder if this extension is unique. We will give a partial answer to these questions in the case that F is complete and the extension is Galois. Our main goal is then to use this results to determine the fields which are complete relative to an archimedean norm. It will turn out that the only possibilities are $\mathbb{R}$ and $\mathbb{C}$. This last result is due to Ostrowski and was proved around 1917. First we will give an elementary definition needed to state the uniqueness theorem.

Definition 1.4.1 (Galois norm/trace)**.** *Let E/F be a Galois field extension and suppose $\mathrm{Gal}(E/F) = \{\eta_1 = 1, \eta_2, \ldots, \eta_n\}$. We define the Galois norm as follows*

$$N = N_{E/F} : E \to F : u \mapsto N_{E/F}(u) = \prod_{i=1}^{n} \eta_i(u).$$

The Galois trace is defined as

$$T = T_{E/F} : E \to F : u \mapsto N_{E/F}(u) = \sum_{i=1}^{n} \eta_i(u).$$

Theorem 1.4.2. *Let F be a field with a non-trivial absolute value $|.|$ such that F is complete relative to this absolute value. Also let E/F be a Galois extension. Suppose that $|.|$ can be extended to an absolute value $|.|'$ on E. Then this can be done in only one way which is given by the formula*

$$|u|' = |N_{E/F}(u)|^{1/[E:F]} \tag{1.5}$$

for every $u \in E$. Moreover E is complete.

Proof. Let $(v_1, \ldots, v_r)$ be a base for the F-vector space E. Every element in the sequence $(u_i)_{i\in\mathbb{N}}$ can be written as $u_i = \sum_{j=1}^{r} \alpha_{ij} v_j$, with every $\alpha_{ij} \in F$ for $i \in \mathbb{N}$ and $1 \leq j \leq r$. We will first prove that $(u_i)_{i\in\mathbb{N}}$ is a Cauchy sequence in E if and only if all the r sequences $(\alpha_{ij})_{i\in\mathbb{N}}$ are Cauchy in F. Clearly it is sufficient that every $(\alpha_{ij})_{i\in\mathbb{N}}$ is Cauchy for $(u_i)_i$ to be Cauchy. Unfortunately we require that it is necessary. To prove this, assume that $(u_i)_{i\in\mathbb{N}}$ is a Cauchy sequence. If $r = 1$ then the equivalence is self-evident. This gives us a basis for induction. We thus continue with proving the induction step. Assume now the statement holds for $r-1$ and that $(\alpha_{ir})_{i\in\mathbb{N}}$ is not a Cauchy sequence. Then there exists a real $\epsilon > 0$ such that for every positive integer N there exist integers $p, q \geq N$ such that $|\alpha_{pr} - \alpha_{qr}| > \epsilon$. More precisely there exists a sequence of pairs $((p_i, q_i))_{i\in\mathbb{N}}$ with $p_1 < p_2 < \ldots$ and $q_1 < q_2 < \ldots$ such that $|\alpha_{p_i r} - \alpha_{q_i r}| > \epsilon$. Now define the sequence $(w_i)_{i\in\mathbb{N}}$ in E as follows

$$w_i = (\alpha_{p_i r} - \alpha_{q_i r})^{-1}(u_{p_i} - u_{q_i}) \qquad \text{with } i \in \mathbb{N}.$$

Since $|(\alpha_{p_i r} - \alpha_{q_i r})|^{-1} < \epsilon^{-1}$ and $(u_{p_i} - u_{q_i}) \to 0$ we obtain that $w_i \to 0$. By construction the r-th coefficient of all these elements is equal to 1. As a consequence we have $w_i = c_i + v_r$ where c_i is of the form $\sum_{j=1}^{r-1} \beta_{ij} v_j$. Clearly c_i converges tot $-v_r$ and thus is $(c_i)_{i\in\mathbb{N}}$ a Cauchy sequence. By the induction hypothesis we readily obtain that the $r-1$ sequences $(\beta_{ij})_{i\in\mathbb{N}}$ are Cauchy and, by the completeness of F, they each converge to a $\beta_j \in F$ for every $1 \leq j \leq r-1$. This shows that also $c_i \to \sum_{j=1}^{r-1} \beta_j v_j$ and by the uniqueness of limits we get

$$\sum_{j=1}^{r-1} \beta_j v_j = -v_k.$$

Clearly this is contradictory to the linear independence of the base $(v_1, \ldots, v_r)$. This proves that every $(\alpha_{ij})_{i\in\mathbb{N}}$ is Cauchy, as desired. We now use this fact to remark that, by the completeness of F relative to the absolute value $|.|$, all the sequences $(\alpha_{ij})_{i\in\mathbb{N}}$ converge in F to an $\alpha_j \in F$ for every $1 \leq j \leq r$ and as a consequence every Cauchy $(u_i)_{i\in\mathbb{N}}$ converges to a element $u = \sum_{j=1}^{k} \alpha_j v_j$. This proves that also E is complete.

It remains to prove formula (1.5). Suppose to the contrary that the formula does not hold. Then we can find a $u = \sum_{j=1}^{r} \alpha_j v_j$ such that $|u^r|' \neq |N_{E/F}(u)|$, where $r = [E : F]$. This inequality also holds for u^{-1}. So we can assume, by replacing u with u^{-1} if necessary, that $|u^r|' < |N_{E/F}(u)|$. Now put $w = u^r N_{E/F}(u)^{-1}$. Then $|w|' < 1$ and $N_{E/F}(w) = 1$. Also $w^n \to 0$. Again we can write $w^n = \sum_{j=1}^{r} \beta_{nj} v_j$ and we know that every $\beta_{nj} \to 0$ for every $1 \leq j \leq r$. But the norm map is a polynomial function from E to F, which is clearly continuous. Hence this implies that $1 = N_{E/F}(w^n) \to 0$ and this results in our final contradiction. □

Next we will show it is always possible to extend the absolute value $|.|$ on F to an absolute value $|.|'$ on the field E as long as the field extension is minimal, i.e. of second degree. If the $|.|$ is non-archimedean then extending is always possible as long as the extension is finite. For a proof of this fact see [Jac89, Theorem 9.12].

Lemma 1.4.3. *Let F be a field of characteristic $\neq 2$ which is complete relative to an absolute value $|.|$ and let E be a quadratic field extension of F. Then*

$$|u|' = |N_{E/F}(u)|^{1/2} \qquad \text{for every } u \in E \tag{1.6}$$

defines an absolute value of E which is an extension of $|.|$.

Proof. The extension is of degree 2 and thus Galois. Let now $u \mapsto \tilde{u}$ be the automorphism that is not equal to the identity. We obtain $T_{E/F}(u) = u + \tilde{u}$ and $N_{E/F}(u) = u\tilde{u}$. Also $u^2 - T_{E/F}(u)u + N_{E/F}(u) = 0$. First let us show that the formula (1.6) indeed yields an extension of $|.|$. Therefore take $a \in F$ so that

$$|a|' = |N_{E/F}(a)|^{1/2} = |a^2|^{1/2} = |a|.$$

Remains to be shown that $|.|'$ is an absolute value. Clearly for every $u \in E$ we have that $|u|' \geq 0$ and also $|u|' = 0$ if and only if $u = 0$. Condition $|uw|' = |u|'|w|'$ follows from the multiplicative property of the Galois norm. Remains to prove the (weak) triangle inequality. Therefore take $u \in E$ such that $u \notin F$. As the field extension is quadratic $E = F(u)$ and the minimal polynomial of u over F is $(x - u)(x - \tilde{u})$ which is equal to

$$x^2 - T_{E/F}(u)x + N_{E/F}(u). \tag{1.7}$$

Simple calculations will also give that $N_{E/F}(u+1) = (u+1)(\tilde{u}+1) = N_{E/F}(u)+T_{E/F}(u)+1$. By Remark 1.1.2 it remains to show that $|N_{E/F}(u+1)|^{1/2} \leq |N_{E/F}(u)|^{1/2} + 1$ and by the previous this is equivalent to

$$|1 + T_{E/F}(u) + N_{E/F}(u)| \leq 1 + 2|N_{E/F}(u)|^{1/2} + |N_{E/F}(u)|.$$

We know the triangle inequality holds for elements in F so it remains to show that $|T_{E/F}(u)| \leq 2|N_{E/F}(u)|^{1/2}$ and this will follow if $|T_{E/F}(u)|^2 \leq 4|N_{E/F}(u)|$. So suppose this is not the case and

$$|T_{E/F}(u)|^2 > 4|N_{E/F}(u)|. \tag{1.8}$$

We will then show that u must be in F which is in contradiction with our specific choice of $u \notin F$.

For this consider the more general equation

$$x^2 - \alpha x + \beta = 0 \qquad \text{with } \alpha, \beta \in F \text{ and } |\alpha|^2 > 4|\beta| > 0. \tag{1.9}$$

Clearly (1.7) is of this form under the assumption (1.8). The equation is equivalent to $x = \alpha - \beta x^{-1}$. To find a solution for this equation define a sequence $(\gamma_i)_{i\in\mathbb{N}}$ of elements in F recursively by

$$\gamma_1 = \frac{1}{2}\alpha \qquad \gamma_{i+1} = \alpha - \beta\gamma_i^{-1}.$$

This definition can only make sense if none of the $\gamma_i = 0$. This is true for γ_1 as its norm is equal to $\frac{1}{2}|\alpha| \geq 0$. Now assume that $|\gamma_i| \geq \frac{1}{2}|\alpha|$. We then have

$$|\gamma_{i+1}| = |\alpha - \beta\gamma_i^{-1}| \geq |\alpha| - |\beta||\gamma_i^{-1}| \geq |\alpha| - 2|\beta||\alpha|^{-1} \geq |\alpha| - \frac{1}{2}|\alpha|^2|\alpha|^{-1} = \frac{1}{2}|\alpha|.$$

Hence every $\gamma_i \neq 0$. Observe now

$$|\gamma_{i+1} - \gamma_{i+2}| = |\beta\gamma_{i+1}^{-1}\gamma_i^{-1}(\gamma_{i+1} - \gamma_i)| \leq \frac{4|\beta|}{|\alpha|^2}|\gamma_{i+1} - \gamma_i|.$$

Setting $r = \frac{4|\beta|}{|\alpha|^2} < 1$ we obtain $|\gamma_{i+2} - \gamma_{i+1}| \leq r^i|\gamma_2 - \gamma_1|$ which clearly implies that $(\gamma_i)_{i\in\mathbb{N}}$ is a Cauchy sequence. Hence, due to the completeness of F with respect to $|.|$, $\gamma = \lim \gamma_i$ exists in F. Now taking the limit in both sides of the recursive definition of γ_{i+1} we obtain that $\gamma = \alpha - \beta\gamma^{-1}$. This shows that γ is a solution of (1.9) in F. This completes the proof. □

As promised we conclude this section with a classification of all the complete fields relative to an archimedean absolute value. The essential part of the following proof will be to show that there does not exist a field with archimedean absolute value such that it strictly encompasses the complex numbers.

Ostrowski's Theorem. *The only fields which are complete relative to an archimedean absolute value are* $\mathbb{R}$ *and* $\mathbb{C}$*.*

Proof. Let F be a field which is complete relative to an archimedean absolute value $|.|$. We know F must have characteristic 0 and so F contains $\mathbb{Q}$. Also its closure $\hat{\mathbb{Q}}$ is encompassed by F, i.e $\hat{\mathbb{Q}} \subseteq F$. Now the only archimedean absolute value on $\mathbb{Q}$ is the classical $|.|_\infty$. This shows that the closure of the rationals can be identified with the reals $\mathbb{R}$. We have thus established that either $F = \mathbb{R}$ or it is larger.
Suppose now F contains an element i such that $i^2 = -1$. Then F contains $\mathbb{R}(i)$ that can be identified with the complex numbers. Also, by the uniqueness of the extension, the norm on this subfield is equivalent with the classical $|.|_\infty$. If F does not contain such an element we can adjoin it to F to obtain $E = F(i)$. Since this is a quadratic field extension we uniquely extend the absolute value $|.|$ on F to one on E. Similar to our previous remarks, we now see E contains $\mathbb{C}$ with the classical absolute value. If we can now prove that $E = \mathbb{C}$ it will follow that $F = \mathbb{R}$. Hence the proof is reduced to showing that if F satisfies the hypothesis and F contains $\mathbb{C}$ with the restriction of $|.|$ to $\mathbb{C}$ equivalent to $|.|_\infty$, then $F = \mathbb{C}$.

Suppose know that $\mathbb{C} \subsetneq F$ and let $a \in F \setminus \mathbb{C}$. Consider the map $x \mapsto |x - a|$ of $\mathbb{C}$ into $\mathbb{R}$. Clearly by all previous remarks the topologies on these fields are the classical ones and so this map is continuous. Let $r = \inf_{\gamma\in\mathbb{C}} |\gamma - a|$. We claim this infimum is in fact a minimum which is obtained for some complex number γ_0. Clearly we can restrict the infimum to all γ such that $|\gamma - a| \leq r + 1$ without changing the value. Denoting the set of all these gamma by Γ we still obtain $\inf_{\gamma\in\Gamma} |\gamma - a| = r$. Let γ_1 and γ_2 be elements of Γ then $|\gamma_1 - \gamma_2| \leq 2r + 2$ which proves that Γ is closed and bounded in $\mathbb{C}$. By the continuity of $x \mapsto |x - a|$ we see that there exists a γ_0 such that $|\gamma_0 - a| = r$. In this way we obtain the following non empty, closed and bounded set

$$D = \{\gamma' \in \mathbb{C} \mid |\gamma' - a| = r\}.$$

We shall now show that this set is also open, which will cause a contradiction. This can be done by proving that if $\gamma' \in D$ then every γ in the open ball with radius r is completely contained in D. For notational ease define the non-complex field number $b = a - \gamma'$ and the complex number $c = \gamma - \gamma'$. We get $a - \gamma = (a - \gamma') - (\gamma - \gamma') = b - c$. We thus need to proof that if $|b| = r$ and $|c| < r$, then $|b - c| = r$. Note that still for every complex number $c' \in \mathbb{C}$

$$|b - c'| = |a - \gamma' - c'| = |a - (c' + \gamma')| \geq r.$$

And thus in essence b has taken on the role of a. Let now n be in $\mathbb{N}$ and consider $b^n - c^n$ which is equal to $(b - c)(b - \epsilon c) \dots (b - \epsilon^{n-1} c)$ where ϵ is a primitive n-th root of unity in $\mathbb{C}$. Then

$$\begin{aligned} |b - c||b - \epsilon c| \dots |b - \epsilon^{n-1} c| &= |b^n - c^n| \\ &\leq |b|^n + |c|^n. \end{aligned}$$

Since still $|b - \epsilon^k c| \geq r$ for every $1 \leq k \leq n - 1$, this implies

$$|b - c| r^{n-1} \leq r^n + |c|^n = r^n \left(1 + \frac{|c|^n}{r^n}\right).$$

It follows that $|b - c| \leq r(1 + |c|^n / r^n)$. Using now that $|c| < r$ we find $\lim(1 + (|c|/r)^n) = 1$ and thus $|b - c| \leq r$. Hence $|b - c| = r$. This proves that D is open as well as closed and non empty so that by the connectedness of $\mathbb{C}$ it follows that $D = \mathbb{C}$. If we now take two elements γ_1 and γ_2 in $\mathbb{C}$ we find that

$$|\gamma_1 - \gamma_2| \leq |\gamma_1 - a| + |a - \gamma_2| = 2r,$$

an outcome which is clearly impossible for all complex numbers. With this contradiction we see that F must be equal to the complex numbers and as such in general F can only be $\mathbb{R}$ or $\mathbb{C}$, and the proof is complete. □

1.5 Characterizing all archimedean locally compact fields

In this last section of our first chapter we will use the accumulated knowledge to characterize all fields F with an archimedean absolute value such that the induced topology is *locally compact*. Actually we will just show that in the archimedean case the concept of *locally compact* and complete coincide. We will do this by proving that all locally compact fields which are archimedean form a subclass of the class of all archimedean complete fields. By Ostrowski's theorem the latter consists only of the real and complex numbers which are both *locally compact*. For more information on the subject we again refer to [Bou66a]. First we will give a formal definition of *locally compact* fields.

Definition 1.5.1 (locally compact)**.** *Suppose F is a field with an absolute value $|.|$. We say that the induced topology $\mathcal{T}_{|.|}$ on F is locally compact if and only if every $a \in F$ has a neighborhood with compact closure.*

If the topology on F is clear and there is no risk for confusion we will simply say that F is locally compact. Furthermore the definition does not make use of the absolute value, neither does it utilize any of the operations defined on F. Therefore the definition can also be stated in general for every topological space. That said, in the course of this text, by "locally compact field" we will specifically mean a field which satisfies the conditions in Definition 1.5.1.

Proposition 1.5.2. *Let F be a field with non-trivial absolute value $|.|$. If F is locally compact then every closed and bounded set A in F is compact.*

Proof. Let A be any closed and bounded set in F. The boundedness implies that A is contained in an open ball $B(0,r)$ where we can assume the radius r to be larger than 1. Now let W a neighborhood of 0 such that its closure $\overline{W}$ is compact. Then W contains an open ball $B(0,\epsilon)$. Furthermore since $|.|$ is non trivial and because of Remark 1.1.5 we can find a $b \in F$ such that $|b| > r/\epsilon$. We now use the fact that $x \mapsto bx$ is a continuous function from F to itself to remark that $b\overline{W}$ is again compact. Also

$$A \subseteq B(0,r) \subseteq b\overline{W},$$

where we use that for every $c \in F$ such that $|c| < r$ we have that $|c/b| < \epsilon$ so that $c/b \in B(0,\epsilon) \subseteq W \subseteq \overline{W}$. If we now take a sequence $(a_i)_{i\in\mathbb{N}}$ in A then this is also a sequence in $b\overline{W}$ and thus it has a convergent subsequence $(a_{i_j})_{j\in\mathbb{N}}$. Finally since A is closed, the limit of this subsequence is contained in A which proves that A is compact. □

We would like to point out that if F is equipped with the trivial absolute value, then F is automatically locally compact. Evidently F is closed and contained in the closed ball $\overline{B(0,1)}$ and thus bounded. However in this specific case F can only be compact if and only if it is finite. This shows that the above property can not hold for the trivial absolute value in the case where F is infinite.

Proposition 1.5.3. *Every locally compact field is complete*

Proof. Let F be a locally compact field. If the induced topology is discrete then F is obviously complete. So suppose $|.|$ is non trivial. Let now $(a_i)_{i\in\mathbb{N}}$ be a Cauchy sequence with elements in F. We will first show that this sequence is bounded. Since the sequence is Cauchy there exists an $N \in \mathbb{N}$ such that for every $p, q \geq N$

$$|a_p - a_q| < 1.$$

Now take $M = \max_{0\leq i\leq N} |a_i|$. It follows that for every $i \in \mathbb{N}$

$$|a_j| = |a_j - a_N + a_N| \leq |a_j - a_N| + |a_N| \leq 1 + M$$

so that our sequence is contained in the closed ball $\overline{B(0, M+1)}$. By Property 1.5.2 we see that $\overline{B(0, M+1)}$ is compact and as a consequence $(a_i)_{i\in\mathbb{N}}$ has a convergent subsequence. This in turn implies that $(a_i)_{i\in\mathbb{N}}$ is convergent and F is complete. □

This last proposition also holds in general for topological groups. A more fundamental proof without the use of metrics can be found in [Bou66a, Corrollary III.3.3.1]. This concludes our categorization of all locally compact fields with archimedean absolute value.

Chapter 2

Valuation theory

In the previous chapter we introduced so called non-archimedean absolute values. These are absolute values which fulfill a much stronger requirement than the ordinary triangular inequality, i.e. they satisfy $|a+b| \leq \max\{|a|,|b|\}$. Notice that in this case none of the requirements make use of the addition in $\mathbb{R}$, only the multiplication and order relation on the non-negative reals is used. This observation makes it possible to generalize the concept of a non-archimedean absolute value to that of a *valuation*. This is a function, from the field F to an ordered abelian group adjoint with 0, satisfying the usual properties. The concept was first introduced by Krull in 1934. We will show that a *valuation* in the sense explained above is equivalent to the concept of a *valuation ring* and also a so called *place*. In this text we will only elaborate on Krull's *valuations* from a field F into an ordered abelian group and *valuation rings*.

Again our purpose will be to provide an introduction to this theory with as main goal to characterize all locally compact fields relative to an absolute value. As we have already handled the case where the absolute value is archimedean we can now fully concentrate on the case where $|.|$ is non-archimedean, this through the use of valuation theory. More specifically we will do this by examining the so called *local fields* which are actually nothing else then non-archimedean non-trivial locally compact fields. We again note that most of the proofs given here where originally found in [Jac89, Chapter 9].

2.1 Ordered abelian groups

Take G an abelian group. Suppose this group has a binary relation $\leq$ defined on it which is reflexive, transitive, antisymmetric and total, in other words a total order relation. Furthermore suppose this order relation is compatible with the multiplication, i.e. if $g_1 \leq g_2$ then $gg_1 \leq gg_2$ for every $g, g_1, g_2 \in G$. Now define the following subsets of G

$$H = \{h \in G \mid h < 1\} \qquad \text{and} \qquad H^{-1} = \{h^{-1} \mid h \in H\}.$$

First take h_1, h_2 elements in H, then clearly $h_1 h_2 < 1$ which proves that the set H is multiplicatively closed in G. The same can be shown for H^{-1} if we notice that this set is equal to $\{h \in G \mid 1 < h\}$. If g is an arbitrary element in $G \setminus \{1\}$ then either $g < 1$ or $g > 1$. The latter is equivalent with $g^{-1} < 1$. It follows that G is the disjoint union of the subsets H,$\{1\}$ and H^{-1}. This explains the relevance of the following definition.

Definition 2.1.1 (Ordered abelian group)**.** *Let G be an abelian group with subset H such that*

(1) G is the disjoint union $H \cup \{1\} \cup H^{-1}$ where $H^{-1} = \{h^{-1} \mid h \in H\}$.

(2) H is multiplicatively closed in G.

The pair (G, H) is then called an ordered abelian group.

In the following, when there is no risk of confusion, we will just speak of the *ordered abelian group G* or the *group G ordered by H*. Notice that if G is ordered by H it is also ordered by H^{-1}. The order induced by H^{-1} is called the reverse order, with respect to the original ordered group (G, H).

Remark 2.1.2 (Order relation)**.** *If G is an ordered abelian group we can define a binary relation $\preccurlyeq$ by specifying that $g_1 \prec g_2$ if $g_1 g_2^{-1} \in H$. Take g_1, g_2 and g_3 in G. Suppose $g_1 \prec g_2$ and $g_2 \prec g_3$ then $g_1 g_2^{-1} \in H$ and $g_2 g_3^{-1} \in H$. Since this set is multiplicatively closed in G we get that $g_1 g_3^{-1} \in H$ so that $g_1 \prec g_3$. This shows our relation is transitive. Also if $g_1 \preccurlyeq g_2$ and $g_2 \preccurlyeq g_1$ then, if $g_1 \neq g_2$, both $g_1 g_2^{-1}$ and $g_2 g_1^{-1} = (g_1 g_2^{-1})^{-1}$ are in H which is clearly a contradiction to H and H^{-1} being disjoint. It follows that g_1 must be equal to g_2 and the antisymmetry is proven. The same arguments show that $\preccurlyeq$ is reflexive. The totality of the relation is an obvious consequence of G being the union of H and H^{-1} with $\{1\}$. Remains to show that the relation behaves nicely in the sense that the multiplication is preserved. So if $g_1 \prec g_2$ then $g_1 g_2^{-1} = g_1 g_3 g_3^{-1} g_2^{-1} = g_1 g_3 (g_2 g_3)^{-1}$ is an element of H which shows that $g_1 g_3 \prec g_2 g_3$.*

Suppose now there is a compatible total order $\leq$ defined on G and take $H = \{h \in G \mid h < 1\}$ as was previously the case. We can again use this H to define $\preccurlyeq$. If $g_1 < g_2$ then $g_1 g_2^{-1} < 1$ as a consequence $g_1 g_2^{-1} \in H$ so that $g_1 \prec g_2$. On the other hand if $g_1 \prec g_2$ then $g_1 g_2^{-1}$ is again an element of H and we see $g_1 < g_2$. This shows the equivalence of an ordered abelian group and the notion of a total order relation which is compatible with the group multiplication.

Notice that in all of the above we never made use of the abelian property. As a consequence the definition can be generalized to all groups. This does however not imply that every group, or as a matter of fact every abelian group, can be ordered. For this take G a non-trivial ordered abelian group. To show this we can use a similar argument as we did earlier for fields in Remark 1.1.5. Without loss of generality we can assume G contains an element g such that $1 < g$. By multiplying both sides with g we get that $g < g^2$. Repeating this action we obtain an ascending chain

$$1 < g < g^2 < g^3 < \ldots < g^n < \ldots.$$

This chain can never stabilize and thus G cannot contain a non-trivial element g such that $g^n = 1$. This shows that no group with torsion elements can be ordered, which more specifically excludes all finite groups from being ordered.

Definition 2.1.3 (Order homomorphism)**.** *Let (G, H) and (G', H') be ordered abelian groups then a homomorphism from G to G' such that H is mapped into H' is called a order homomorphism.*

If now (G, H) is an ordered abelian group we automatically have the order homomorphism

$$(.)^{-1} : G \to G : g \mapsto g^{-1}.$$

which maps H into H^{-1}. As a consequence the order is reversed under this map.

We now construct some ordered abelian groups starting from others. An easy example can be found when an ordered abelian group (G, H) has a subgroup G_1. Then G_1 is ordered by $H_1 = G_1 \cap H$. A more elaborate example will be discussed in the following remark.

Remark 2.1.4 (Construction of ordered abelian groups)**.** *Let (G_i, H_i), with $1 \leq i \leq n$, be ordered abelian groups. We now want to find a way to order the abelian group $G = G_1 \times G_2 \times \ldots \times G_n$. A naive approach would be to order G by $H = H_1 \times H_2 \times \ldots \times H_n$.*

However if $n > 1$ and at least one group G_i is non trivial then G cannot be the disjoint union of H, H^{-1} and $\{1\}$. This because, for $h_i \in H_i$, the element $(1, 1, \ldots, 1, h_i, 1, \ldots, 1)$ is not an element of H nor is it an element of H^{-1}. In other words this method can only work if either $n = 1$ or every group G_i with $1 \leq i \leq n$ is trivial.

Let us now define H as the set consisting of all element of the form

$$(1, \ldots, 1, h_i, g_{i+1}, \ldots, g_n),$$

where h_i is an element of H_i and g_j is arbitrary, $i < j \leq n$. One now sees that

$$(g_1, g_2, \ldots, g_n) < (g_1', g_2', \ldots, g_n')$$

if an only if for some $1 \leq i \leq n$ we have $g_1 = g_1', g_2 = g_2', \ldots, g_{i-1} = g_{i-1}'$ and $g_i < g_i'$. We call this the lexicographic order on G corresponding to the given index $i \mapsto G_i$.

Let us now look at two examples. First observe $(\mathbb{R}, +)$. If we order this group by the negative reals $\mathbb{R}_0^-$ we obtain the classical order on $\mathbb{R}$. An other example would be to take the group $(\mathbb{R}_0^+, .)$ and order this group by $]0, 1[$. However the map $x \mapsto e^x$ is clearly an order isomorphism which shows that both ordered groups are "the same". Therefore let us consider the following example.

Example 2.1.5. Take $n > 1$ and $\mathbb{Z}^n$ the additive groups of n-tupels of integers ordered lexicographically. Now define $g_1 = (0, 1, 1, \ldots)$ and $g_2 = (1, 1, 1, \ldots)$. Clearly there does not exist an integer m, which we identify by $(m, m, \ldots, m) \in \mathbb{Z}^n$, such that $mg_1 > g_2$. As a consequence $\mathbb{Z}^n$ does not satisfy Archimedes' axiom. However the additive group of real numbers does have this property which proves that $\mathbb{Z}^n$ is not order isomorphic to a subgroup of $\mathbb{R}$. △

2.2 Valuation rings and the canonical valuation

We now have the necessary tools to define the concept of a valuation of a field F into an ordered abelian group G. The only thing missing is an image for $0 \in F$. To solve this problem we simply adjoin a 0 to G. Formally we set $V = G \cup \{0\}$ and define $00 = 0$ and for any $g \in G$ we set $g > 0$ and $0g = 0 = g0$.

Definition 2.2.1 (Valuation)**.** *Suppose F is a field and V an ordered abelian group adjoint with 0, then we define a V-valuation on F as a map $\varphi : F \to V : a \mapsto \varphi(a)$ such that*

(1) $\varphi(a) = 0$ if and only if $a = 0$.

(2) $\varphi(ab) = \varphi(a)\varphi(b)$.

(3) $\varphi(a + b) \leq \max\{\varphi(a), \varphi(b)\}$.

If φ is a valuation of F we denote by F^*, as usual, the multiplicative group of non-zero elements of F. Now $\varphi(F^*)$ is a subgroup of the given ordered abelian group G. We call this the *value group* of F, relative to φ. Also we can replace G by the value group $\varphi(F^*)$ without changing any of the structure. If we now take V to be the non-negative reals, then the definition of a V-valuation is nothing more then a non-archimedean absolute value. However to find an example of a V-valuation which is not an absolute value one usually defines the equivalent concept of an *exponential V'-valuation*. Here V' is again an ordered abelian group G' except the order is reversed and the group operation is written as an addition. Instead of adding 0 we now adjoint ∞ such that $\infty + \infty = \infty$ and for every $g \in G'$ we get $\infty > g$ and $\infty + g = \infty = g + \infty$.

Definition 2.2.2 (Exponential valuation)**.** *Let F be a field and V' an ordered abelian group adjoint with ∞, then we define an exponential V'-valuation on F as a map $\phi : F \to V' : a \mapsto \phi(a)$ such that*

(1') $\phi(a) = \infty$ *if and only if* $a = 0$.

(2') $\phi(ab) = \phi(a) + \phi(b)$.

(3') $\phi(a + b) \geq \min\{\phi(a), \phi(b)\}$.

From earlier remarks on reversing the order of a group we see that this definition is equivalent with that of a V-valuation.

Example 2.2.3. To construct an example of a valuation which is not an absolute value we first extend the definition of a valuation to a domain D. Note this can be done as we never made use of any inverse elements, though $ab = 0$ implies that $0 = \varphi(ab) = \varphi(a)\varphi(b)$. The latter implies that $\varphi(a) = 0$ or $\varphi(b) = 0$ in V. It follows that either $a = 0$ or $b = 0$. If now φ is a V-valuation on a domain D then φ can uniquely be extended to a V-valuation φ' on the field of fractions by setting $\varphi'(ab^{-1}) = \varphi(a)\varphi(b)^{-1}$. It is not difficult to see this map is indeed a V-valuation which clearly is an extension of φ. The uniqueness follows from the fact that $\varphi'(ab^{-1}) = \varphi'(a)\varphi'(b)^{-1}$. Now take F a field with exponential V-valuation ϕ. By the previous, to define an exponential valuation on $F(x)$, we need only to define one on $F[x]$. So for every

$$f(x) = x^k(a_0 + a_1x + \ldots + a_nx^n) \in F[x] \qquad \text{where } k \geq 0 \text{ and } a_0 \neq 0,$$

we define the V'-valuation $\phi'(f) = (k, \phi(a_0))$ where $V' = G' \cup \{\infty\}$ and $G' = \mathbb{Z} \oplus G$ which is ordered lexicographically. Again it is not difficult to see this is an exponential valuation. Finally if F is equipped with the trivial exponential valuation, the previous shows us how to define an exponential $\mathbb{Z}$-valuation on $F(x)$. Successive steps give us a way of defining an exponential $\mathbb{Z}^n$-valuation ϕ^n on $F(x_1, \ldots, x_n)$. More precisely if

$$f(x_1, \ldots, x_n) = x_1^{i_1}x_2^{i_2}\ldots x_n^{i_n}\frac{k(x_1, \ldots, x_n)}{l(x_1, \ldots, x_n)} \qquad \text{where } x_j \nmid k \text{ and } x_j \nmid l \neq 0,$$

for every $1 \leq j \leq n$. Then the above steps give us that $\phi^n(f) = (i_n, \ldots, i_1) \in \mathbb{Z}^n$. As remarked earlier the latter ordered abelian group is not isomorphic to a subgroup of $\mathbb{R}$ and thus we have constructed a valuation which can not be an absolute value if $n > 1$. For more extensive information see [Jac89] Section 9.6. △

Just as an ordered abelian group (G, H) was an equivalent way of defining an abelian group G equipped with a total order $\leq$ which is compatible with the multiplication on G we can find an equivalent concept of a valuation on a field through valuation rings. First let φ be a V-valuation of a field F and define

$$R = \{a \in F \mid \varphi(a) \leq 1\},$$

then R is a subring of F called *the valuation ring of the valuation* φ. To see this is a ring take $a, b \in R$. Then clearly $\varphi(a - b) \leq \max\{\varphi(a), \varphi(b)\} \leq 1$ and $\varphi(ab) = \varphi(a)\varphi(b) \leq 1$. Also $0, 1 \in R$. Now notice that similar to ordered abelian groups if $a \notin R$ then $\varphi(a) > 1$ and $\varphi(a^{-1}) = \varphi(a)^{-1} < 1$ so that $a^{-1} \in R$. This motivated us to define the following concept of a valuation ring, in F.

Definition 2.2.4 (Valuation ring)**.** *Let F be a field. A valuation ring in F is a subring R of F such that every element of F is either contained in R or is the inverse of an element in R.*

Now take R a valuation ring in F. Define U as the set of units of R and P the set of non-units. As before F^* is the multiplicative group of non-zero element in F, $R^* = R \cap F^*$ and $P^* = P \cap F^*$. As U is a (normal) subgroup of F^* we can form the factor group $G' = F^*/U$. Further put

$$H' = \{aU \mid a \in P^*\} \subset G'.$$

If we take $b, c \in P^*$ then bc is an element of R and $(bc)^{-1}$ is not, otherwise $(bc)^{-1}b = c^{-1}b^{-1}b = c^{-1}$ would be in R and thus c would be a unit. This shows that P^* is multiplicatively closed and hence so is H'. Also if $a \in F^*$ is not in R then a^{-1} is an element of P. Otherwise again a^{-1} would be a unit and then $a \in R$ which is a contradiction. This shows that F^* is the disjoint union $P^* \cup U \cup (P^*)^{-1}$. Clearly we now have that (G', H') forms an ordered abelian group. We now adjoin 0 to obtain $V' = G' \cup \{0\}$. Finally define the map

$$\varphi' : F \to V' : a \mapsto \begin{cases} 0 & \text{if} \quad a = 0, \\ aU & \text{if} \quad a \neq 0. \end{cases}$$

Remains to show this is a V'-valuation on F. The first two conditions are clearly satisfied. To prove the last condition take $a, b \in F$. If one is equal to zero then the inequality is easy. So suppose $a \neq 0$ and $b \neq 0$. Then either $ab^{-1} \in R^*$ or $ba^{-1} \in R^*$ (or both). Assume the first, then $\varphi'(ab^{-1}) \leq 1$ in G' as $R^* = U \cup P^*$. It follows that $\varphi'(a) \leq \varphi'(b)$. We also have that $ab^{-1} + 1 \in R$ so that $\varphi'(ab^{-1} + 1) \leq 1$. We now have

$$\varphi'(a + b) = \varphi'(b)\varphi'(ab^{-1} + 1) \leq \varphi'(b) = \max\{\varphi'(a), \varphi'(b)\}.$$

This shows that φ' is V'-valuation of F and moreover since $\varphi'(a) \leq 1$ if and only if $a \in R$, we see that R is the valuation ring associated with φ'. We call φ' the *canonical valuation* of the valuation ring R.

In closure again consider an arbitrary valuation φ on F into $V = G \cup \{0\}$ where G is an abelian group ordered by H. Let R be the corresponding valuation ring and φ' the canonical valuation of F determined by R. We now have a homomorphism $a \mapsto \varphi(a)$ from F^* into G. For $a \in U$ we have that $\varphi(a) \leq 1$ and also $\varphi(a)^{-1} = \varphi(a^{-1}) \leq 1$ which by the second conditions for valuations implies that $\varphi(a) = 1$. Since for every $b \in F^*$, $\varphi(b) = 1$ implies that $\varphi(b^{-1}) = 1$, this shows that U is the kernel of previous homomorphism. We obtain a monomorphism $\varphi'(a) \mapsto \varphi(a)$ from G' to G, which is an isomorphism form G' onto the value group $\varphi(F^*)$ of φ. Also if $bU \in H'$ then $b \in P^*$ and $\varphi(b) < 1$. As a consequence $\varphi'(a) \mapsto \varphi(a)$ is order-preserving. This shows the relevance of stating the following definition.

Definition 2.2.5 (Equivalent valuation)**.** *Suppose φ_1 and φ_2 are two valuations on a field F, then they are called equivalent if there exists an order isomorphism η of the value group $\varphi_1(F^*)$ onto the value group $\varphi_2(F^*)$ such that $\varphi_2 = \eta\varphi_1$.*

From the previous if φ_1 and φ_2 are equivalent this implies they have the same valuation rings. Moreover we have shown that any valuation φ is equivalent with the canonical valuation φ' determined by the valuation ring R of φ. This proves the following proposition.

Proposition 2.2.6. *Two valuations φ_1 and φ_2 on a field F are equivalent if and only if they have the same valuation ring.*

Finally let R be a valuation ring in F, we may assume that R is the subset of elements in F which satisfy $\varphi(a) \leq 1$ for a valuation φ of F. Since for every non-zero element a of F, either a itself or a^{-1} is contained in R we see that F is the field of fractions of R. As we have noticed earlier if we take u a unit in R then there exists a v in R such that $uv = 1$. It follows that $\varphi(u)\varphi(v) = 1$ and since these values are bounded by 1 this shows that $\varphi(u) = 1$. Conversely if $\varphi(u) = 1$ then $\varphi(u^{-1}) = 1$ and this shows that both u and u^{-1} are contained in R so that u is a unit in R. As concluded before this shows that

$$U = \{a \in R \mid \varphi(a) = 1\}.$$

Also the set P of non-units of R can then be seen as the set of elements b in F which satisfy $\varphi(b) < 1$. If we now take $b, c \in P$ then $\varphi(c+b) \leq \max\{\varphi(c), \varphi(b)\} < 1$ and if $a \in R$, $\varphi(ab) = \varphi(a)\varphi(b) < 1$. This shows that P is an ideal in R. Consequently R is a local ring with P its unique maximal ideal. This implies that $\overline{R} = R/P$ is a field called the *residue field* of R.

We remark that in the case of exponential valuations the valuation ring R is taken as the subring of elements $a \in F$ with $\phi(a) \geq 0$ and P will be the unique maximal ideal of element $b \in F$ such that $\phi(b) > 0$, where the value group $\phi(F^*)$ is written additively.

2.3 Discrete valuations and local fields

In this last introductory section we will try to characterize the remaining locally compact fields. For this we introduce the concept of a discrete valuation, i.e. a non trivial valuation φ whose value group is cyclic. Here we should point out that many textbooks define a discrete valuation as a non trivial (exponential) valuation from a field F to the additive integers. Although this is clearly equivalent to our definition, as $\varphi(F^*)$ is necessarily infinite cyclic, we prefer not to use this approach as the generator of $\mathbb{Z}$ equals 1 which is confusing with our notation for the identity in the value group. Naturally this is just due to the additive notion used which again we chose to ignore in favor of the *more intuitive* multiplicative notion. This because now $\varphi(0) = 0$ and $\varphi(1) = 1$ which is just plain easier to remember. As a setback we have to introduce extra notion by denoting g_φ the *small generator* of $\varphi(F^*)$, i.e. $\varphi(F^*) = \langle g_\varphi \rangle$ and $g_\varphi < 1$.

So let now φ be a discrete valuation with valuation ring R in the field F. Clearly this last field contains an element π such that $\varphi(\pi) = g_\varphi < 1$. We now have that π is an element of R. So let x be an element in R then $\varphi(x) = g_\varphi^n$ for a necessarily positive integer n. Thus $\varphi(x\pi^{-n}) = 1$ so that $x = u\pi^n$ with u a unit in R. Also if π is a product of two non-units $x = u\pi^n$ and $y = v\pi^m$, with $n, m \in \mathbb{N}_0$ and $u, v \in U$ then $\pi = uv\pi^{n+m}$. It follows that $g_\varphi = \varphi(\pi) = \varphi(\pi^{n+m}) = \varphi(\pi)^{n+m} = g_\varphi^{n+m}$ which is impossible as $\varphi(F^*)$ is torsion free. This already shows that R is a unique factorization domain with a unique irreducible element π, up to multiplication by a unit.
Let us now just assume this last part and take I a proper ideal in R. Then every element x in this ideal is of the form $u\pi^n$ with u a unit and n a positive integer uniquely determined by x. If we now take n_0 the lowest such integer occurring in I then we see that $I = (\pi^{n_0})$. Also (π) is a unique maximal ideal in R so that R is a local principal ideal domain but not a field.
Finally if R is a local PID which is not a field, take F the field of fractions of R and ab^{-1} a typical element of F which is not in R. This means that b, which is an element of R, can not be a unit of R. Thus it is contained in the unique maximal ideal (π) and $b = \pi^n$ for some positive integer n. Now suppose $(ab^{-1})^{-1} = ba^{-1}$ is also not contained in R then similarly again $a = \pi^m$ for some positive integer m. Let us assume that $n > m$ then $ba^{-1} = \pi^{n-m} \neq 1$. Since $n - m$ is positive $ba^{-1} \in R$ which is a contradiction. This shows that R is a valuation ring of F and it is not difficult to see that the $\varphi'(F^*) = \langle \varphi'(\pi) \rangle$. We have shown that the following are equivalent

(a) R is a valuation ring with a cyclic value group.

(b) R is a unique factorization domain (UFD) with unique irreducible element, up to multiplication by units.

(c) R is a local principal ideal domain (PID).

A ring R satisfying one, and thus necessarily all, of the above criteria is called a Discrete Valuation Ring (DVR). This gives us a general idea what the structure of a field equipped with a discrete valuation looks like.

Let us now assume F has a non-archimedean absolute value $|.|$ defined on it such that the induced topology is locally compact. By Proposition 1.5.3 we already know F is complete. Also $R = \{a \in F \mid |a| \leq 1\}$ is closed and bounded and thus compact. Since the cosets of P yield an open cover of R the residue field $\overline{R}$ is finite. Moreover for any real number $0 < r < 1$

$$P_r = \{a \in F \mid |a| < r\},$$

is again an open ideal of R and again we see that R/P_r is finite. This shows that there are only finitely many different values in the value group $|F^*|$ between r and 1. In particular $|F|$ takes on a unique largest value $g_{|.|}$ lower than 1 and we see that this element is the small generator of $|F^*|$. This means that the valuation $|.|$ is discrete and it proves F fulfills the requirements of the following definition.

Definition 2.3.1 (Local field)**.** *Let F be a field with absolute value $|.|$. Then F is called a local field if*

(1) $|.|$ is non-archimedean discrete and non trivial.

(2) F is complete relative to $|.|$.

(3) The residue field of $|.|$ is finite.

It should be noted that some other authors use a more general definition of a local field in that they only assume that the residue field is perfect. Also the requirement that $|.|$ is non-archimedean is sometimes omitted. Nevertheless honoring the above definition it can be shown that a local field is also locally compact. For a proof of this converse implication we refer to [Bou72, Proposition VI.5.1.2]. The proof is based on topological features of inverse limits and since going into the subject would be to much of a deviation of our goal we will leave the verification up to the reader. Also it is not difficult to verify that all properties (1),(2) and (3) carry over to finite dimensional extension fields. Hence if F is local and E a finite dimensional field over F, such that the absolute value on E coincides with the one defined on F, then E is also local. This makes it easy to classify all local fields. We first state the following key lemma.

Hensel's Lemma. *Let F be complete relative to a discrete valuation $|.|$, R the valuation ring, P the unique maximal ideal and $\overline{R} = R/P$ the residue field. Suppose $f(x)$ is a monic polynomial in $R[X]$ such that $\overline{f}(x) = \overline{\gamma}(x)\overline{\delta}(x)$ in $\overline{R}[x]$ where $\overline{\gamma}(x), \overline{\delta}(x)$ are monic and $gcd(\overline{\gamma}(x), \overline{\delta}(x)) = 1$. Then $f(x) = g(x)h(x)$ in $R[x]$ where $g(x), h(x)$ are monic and $\overline{g}(x) = \overline{\gamma}(x), \overline{h}(x) = \overline{\delta}(x)$.*

For a proof see [Jac89, p593]. Notice if $\overline{f}(x) = (x-\overline{\rho})\overline{\delta}(x)$ with $\overline{\delta}(\rho) \neq 0$ then Hensel's lemma implies that $f(x) = (x-r)h(x)$ with $\overline{r} = \overline{\rho}$ and $\overline{h}(x) = \overline{\delta}(x)$. In other words if $\overline{f}(x)$ has $\overline{\rho}$ as a simple root in $\overline{R}[x]$ then $f(x)$ has a root r in R such that $\overline{r} = \overline{\rho}$ which in turn implies that r is a simple root of $f(x)$. This brings us to our first lemma.

Lemma 2.3.2. *Let F be a local field and let the order $o(\overline{R})$ of $\overline{R}$ be equal to N. Then R contains a set $\Lambda = \{\zeta_1, \zeta_2, \ldots, \zeta_N\}$ consisting of N distinct roots of $x^N = x$ and these elements constitute a set of representatives of the cosets of P in the additive group R.*

Proof. First of all as $\overline{R}$ is a finite field it has characteristic p and $N = p^n$ for some positive integer n. Also $\overline{R}$ is a splitting field of $f(x) = x^N - x$ over the prime field $\mathbb{Z}_p$. So let $\overline{\zeta'}$ be a random element in $\overline{R}$. Then by Hensel's lemma there exists a $\zeta_1 \in R$ such that $\zeta_1^N = \zeta_1$ and $\zeta_1 + P = \overline{\zeta'}$. If $\overline{\zeta''} \neq \overline{\zeta'}$ is another element of $\overline{R}$ then we can again find a $\zeta_2 \in R$ such that $\zeta_2^N = \zeta_2$ and $\zeta_2 + P = \overline{\zeta''}$. Also $\zeta_1 + P \neq \zeta_2 + P$ and we can thus obtain N distinct elements $\zeta_1, \zeta_2, \ldots, \zeta_N \in R$ such that $\zeta_i^N = \zeta_i$ and the cosets $\zeta_i + P$ are distinct. □

In light of this lemma suppose F is a local field, R the valuation ring, $P = (\pi)$ the unique maximal ideal in R and $\Lambda = \{\zeta_1, \zeta_2, \ldots, \zeta_N\}$ as in Lemma 2.3.2. As noticed before $|\pi|$ equals the small generator $g_{|.|}$ of the value group $|F^*|$. Let $a \in F^*$. We now claim we can write

$$a = \lambda_{k_1}\pi^{k_1} + \lambda_{k_2}\pi^{k_2} + \lambda_{k_3}\pi^{k_3} + \ldots + \lambda_{k_i}\pi^{k_i} + \ldots \tag{2.1}$$

where $\lambda_{k_i} \in \Lambda \setminus \{0\}$ and $k_1 < k_2 < \ldots$. To prove this let $|a| = g_{|.|}^{k_1} = |\pi^{k_1}|$. Then $a\pi^{-k_1}$ has absolute value equal to 1 and so is an element of $R \setminus P$. So there exists an element $\lambda_{k_1} \neq 0$ in Λ such that $a\pi^{-k_1} \equiv \lambda_{k_1}(\bmod P)$. Since now $a\pi^{-k_1} - \lambda_{k_1}$ is an element of P and $a\pi^{-k_1}$ a unit in R we obtain

$$|a| > |a - \lambda_{k_1}\pi^{k_1}|.$$

If now $a = \lambda_{k_1}\pi^{k_1}$ we have (2.1). Otherwise repeat the argument on $a - \lambda_{k_1}\pi^{k_1}$. By induction we obtain, by reordering the k_i's if necessary, $k_1 < k_2 < \ldots$ and $\lambda_{k_1}, \lambda_{k_2}$ non-zero in Λ such that

$$|a| > |a - \lambda_{k_1}\pi^{k_1}| > |a - \lambda_{k_1}\pi^{k_1} - \lambda_{k_2}\pi^{k_2}| > \ldots.$$

Since the absolute value $|.|$ is discrete we again obtain (2.1). Clearly the λ_i's such that (2.1) holds are uniquely determined. Also it is clear that $a \in R$ if and only if $0 \leq k_1$. We now proceed to our second lemma.

Lemma 2.3.3. *Let F be a local field and F_0 a subfield of F such that*

(1) $\Lambda \subseteq F_0$.

(2) F_0 is closed in the topology of F.

(3) $F_0 \cap P \neq \emptyset$.

Let π be an element of R such that $P = (\pi)$. Then $F = F_0(\pi)$ and π is algebraic over F_0.

Proof. Clearly F_0 is a local subfield of F. So let $P_0 = (\pi_0)$, be the unique maximal ideal in the valuation ring R_0 in F_0. Then $|\pi_0| = |\pi|^e$ with e clearly greater or equal to 1. Now if $k \in \mathbb{Z}$ we have $k = eq + r$ where $q \in \mathbb{Z}$ and $0 \leq r \leq e - 1$. It we now take $\pi_k = \pi_0^q \pi^r$ then $|\pi_k| = |\pi^k|$ and similar to what we did previously we can write every $a \in F^*$ as

$$a = \lambda_{k_1}\pi_{k_1} + \lambda_{k_2}\pi_{k_2} + \lambda_{k_3}\pi_{k_3} + \ldots + \lambda_{k_i}\pi_{k_i} + \ldots$$

where $\lambda_{k_i} \in \Lambda \setminus \{0\}$ and $k_1 < k_2 < \ldots$. Rewriting this series we obtain

$$a = a_0 + a_1\pi + a_2\pi^2 + \ldots + a_{e-1}\pi^{e-1} \tag{2.2}$$

where each a_i is of the form $\sum \lambda_q \pi_0^q$ and consequently an element in F_0. Now $|a_i\pi^i|$ has the form $|\pi|^{eq+i}$. Hence $|a_i\pi^i| \neq |a_j\pi^j|$ if $i \neq j$ for $0 \leq i, j \leq e - 1$. So suppose now $\sum_{i=0}^{e-1} a_i\pi^i = 0$ and $a_k \neq 0$ for some $0 \leq k \leq e - 1$. Then $|\sum_{i \neq k} a_i\pi^i| = |a_l\pi^l|$ for some $l \neq k$ and $0 \leq l \leq e - 1$. But this implies that $|a_k\pi^k| = |a_l\pi^l|$ which is impossible. Hence necessarily every $a_i = 0$ for $0 \leq i \leq e - 1$ and as a consequence $\{1, \pi, \pi^2, \ldots, \pi^{e-1}\}$ forms a basis for the F_0-vector space F and hence $F = F_0(\pi)$. Moreover writing $a = \pi^e$ as in (2.2) shows that π is algebraic over F_0. □

In closure we obtain the final theorem characterizing all local fields.

Theorem 2.3.4. *Let F be a local field then F is either the field of formal Laurent series over a finite field F_0 or a finite algebraic extension of the field $\mathbb{Q}_p$ of the p-adic numbers.*

Proof. Assume first F has finite characteristic p. Then $\overline{R} = R/P$ necessarily has as order an N which is a power of p. Let $\Lambda = \{\lambda_1, \ldots, \lambda_N\}$ be a set of element in F, as in Lemma 2.3.2, such that $\lambda_i^N = \lambda_i$. Since N is a power of the characteristic, it follows that Λ is a finite subfield of F. Now if we let $P = (\pi)$ then as before we see that every element a of F has the form

$$a = \sum_{i \leq k} \lambda_i \pi^i$$

for some $k \in \mathbb{Z}$ and $\lambda_i \in \Lambda$. Also this expression is unique. It follows that $F = \Lambda((\pi))$. Suppose now F has characteristic 0. Then F contains $\mathbb{Q}$ and the valuation is non trivial on $\mathbb{Q}$ since R/P is finite. This implies that $\mathbb{Q} \cap P \neq \emptyset$. Also F contains $\mathbb{Q}_p$ for some prime p. If we take Λ as before and set $F_0 = \mathbb{Q}_p(\Lambda)$, then F_0 fulfills the requirements of Lemma 2.3.3, so $F = F_0(\pi)$ is an algebraic extension of F_0. This implies that F is algebraic over $\mathbb{Q}_p$. □

To conclude these first two introductory chapters we summarize all possible fields whom a locally compact field F can be isomorphic to.

(1) If $|.|$ archimedean and

  (1a) if $\mathrm{char}(F) = 0$ then F is either the real numbers $\mathbb{R}$ or the complex number $\mathbb{C}$.

(2) If $|.|$ non-archimedean and

  (2a) if $\mathrm{char}(F) = 0$ then F is a finite algebraic field extension of the p-adic numbers $\mathbb{Q}_p$, for some prime p or

  (2b) if $\mathrm{char}(F) = p$ then F is the field of formal Laurent series over a finite field $\mathrm{GF}(q^n)$.

Chapter 3

Free products in linear groups

We now start with our main goal which is to discuss Gonçalves' and Passman's joint work on *Linear groups and groups rings*. Specifically our aim in this third chapter will be to find criteria that guarantee the product of some specifically chosen subgroups in linear groups is free. The core tool we will use for this is Klein's *famous* Ping-pong Lemma. More important however are the techniques needed to yield this power which are attributed to Tits [Tit72] and later generalized by Gonçalves and Passman [GP06].

To explain this a little more thoroughly let G be a group with non identity subgroups G_1 and G_2. We would like to know whether or not the subgroup $\langle G_1, G_2 \rangle$ generated by these two subgroups is naturally isomorphic to the free product $G_1 * G_2$. A sufficient requirement for this can be found in the elementary, although surprisingly powerful, Ping-pong Lemma. It states that if G acts on a set P which contains nonempty subsets P_1 and P_2 such that P_2 "attracts" the elements of P_1 under the action by $G_1^{\#}$ and vice versa, we then have what we require. The problem is thus more or less reduced to finding this duo of "attracting and repulsing sets".

So suppose V is a normed vector space over a suitable field F and $GL(V)$ is the general linear group of V. Now take S a nonsingular diagonalizable linear operator on V. Then V is a direct sum of eigenspaces of S and we say that $V = S_+ \oplus S_0 \oplus S_-$ is an *S-decomposition* of V if there exist real numbers $s > r > 0$ with $S_+ \neq \{0\}$ spanned by the eigenspaces of S corresponding to the eigenvalues of absolute values greater or equal then s, $S_- \neq \{0\}$ spanned by the eigenspaces of S corresponding to the eigenvalues of absolute values smaller or equal then r, and S_0 the span of the remaining eigenspaces. If m is now a sufficiently large positive integer, then surely the eigenvectors of S^m in S_+ will dominate those in $S_0 \oplus S_-$. As a consequence, given a vector v, the image vector $S^m(v)$ will tend to have large *components* in S_+. So $S^m(v)$ might not be in S_+ but it will be *attracted* towards it such that its falls into a neighborhood of S_+. Unfortunately this is too much wishful thinking as this is not quite true in reality. Two obstacles still remain.

(I) If v is a vector in $S_0 \oplus S_-$ then for every m the component of $S^m(v)$ in S_+ will be zero.

(II) A vector v might have large component in $S_0 \oplus S_-$, for the metric defined on V, to start with. Consequently it will never get close to S_+ for traditional norms.

The first problem shows us we have to avoid vectors in $S_0 \oplus S_-$ as these vectors will be blocked from getting closer to S_+ under the action of S. Secondly to control the total size of all components we need to work in the projective space $\mathcal{P}(V)$, or perhaps in the unit sphere of V. Only, to obtain a suitable metric on $\mathcal{P}(V)$, we will need that the unit sphere is compact a requirement which will be fulfilled if the underlying field F, and consequently V itself, is locally compact.

To conclude suppose T is another nonsingular diagonalizable operator with $V = T_+ \oplus T_0 \oplus T_-$ the T-decomposition of V. Again for a large enough positive integer n, T_+ will attract vectors, not in $T_0 \oplus T_-$, under the action by T^n. If we could now ping-pong elements "close" to S_+ to a projective neighborhood of T_+ under the action by T^n and vice versa under the action by S^m, then we can apply Klein's lemma to show that $\langle S^m, T^n \rangle$ is naturally isomorphic to the free product $\langle S^m \rangle * \langle T^n \rangle$. It is not difficult to see, and it will be explained in full detail, that in order to do this we will need certain intersection to be trivial. For example $S_+ \cap T_0 \oplus T_-$ has to be trivial as we want the *attractor* S_+ of S to be a *repulser* of T in order for its elements to fall into T_+ under the action of T. Reversed the *attractor* T_+ of T will need to be an *repulser* of S and we will require that $T_+ \cap S_0 \oplus S_-$ is trivial. Furthermore we will also need to find *attractors* and *repulsers* for the negative powers of T and S, as such that their vectors can also be tennised back and forth. So it seems we have our work cut out for us.

3.1 Finite-dimensional vector space over a locally compact field

In the remainder of this chapter let F be a field equipped with a non trivial absolute value $|.|$ such that the induced topology is locally compact. Also let $V = F^m$ be the vector space of m-tuples of F, then V is naturally equipped with the function

$$\|.\| : V \to \mathbb{R}^+ : v \mapsto \|v\| = \max\{|a_i| \mid i = 1, \ldots, m\}, \tag{3.1}$$

where $v = (a_1, a_2, \ldots a_m)$. It is easily checked that for every $a \in F$ and $v, w \in V$

(i) $\|v\| = 0$ if and only if $v = 0$,

(ii) $\|av\| = |a|\|v\|$,

(iii) $\|v + w\| \leq \|v\| + \|w\|$,

which makes $\|.\|$ into a norm on the F-vector space V. Also if $|.|$ is non-archimedean we again obtain the stronger property

(iv) $\|v + w\| \leq \max\{\|v\|, \|w\|\}$,

which shows that in this case $\|.\|$ is a non-archimedean norm on V. Continuing forward, since V is a finite-dimensional vector space over F we can generalize all observations made in Remark 1.1.6, that is $\|.\|$ induces a topology $\mathcal{T}_{\|.\|}$ where for every $v \in V$ and $r \in \mathbb{R}^+$ the spherical neighborhoods

$$B_r(v) = \{w \in V \mid \|w - v\| < r\}$$

form a basis for the neighborhood system of this topology. Similarly we have that this is the coarsest topology on V such that the norm $\|.\|$ is continuous and which is compatible with the structure of the vector space in the sense that

(i) the addition $+ : V \times V \to V$ is a continuous map and

(ii) the scalar multiplication $\cdot : F \times V \to V$ is a continuous map,

where $V \times V$ is again equipped with the product topology. Moreover if $\|.\|'$ is another norm defined on V with respect to the same absolute value $|.|$ on F then this norm is topologically equivalent to our norm $\|.\|$ in the sense that it induces the same topology on V. Also if $v = (a_1, a_2, \ldots a_m)$ is an element of V then for every a_i, with $1 \leq i \leq m$ we can find a $W_i \subset F$ which is a neighborhood of a_i with compact closure. It is then easily shown that $W_1 \times \ldots \times W_m$ is a neighborhood of v in V whose closure is compact. This shows that V endowed with the induced topology $\mathcal{T}_{\|.\|}$ is locally compact. Furthermore using similar, although subtly different, techniques as in Proposition 1.5.2 we can show that every closed and bounded set in V is compact as long as the absolute value on F is not trivial. To prove

this more easily note that the subsets $\|V\|$ and $|F|$ of $\mathbb{R}^+$ are equal as sets. Moreover if $|.|$ is archimedean then F is equal to $\mathbb{R}$ or $\mathbb{C}$ and as a consequence $\|V\| = |F| \subset F$. This concludes our brief analysis of the structure on V. Actually these properties will help us in defining a new metric on $\mathcal{P}(V)$ called the projective distance. But before we can go on doing this we first need to specify what is meant with a projective set in V.

Definition 3.1.1 (projective subset)**.** *Let V be a F-vector space. A subset $X \subseteq V$ which contains a nonzero vector and is closed under multiplication by F, that is $FX \subseteq X$, is called a projective subset of V. Clearly these projective subsets correspond in a one-to-one manner to the nonempty subsets of $\mathcal{P}(V)$, the projective space of V. As a consequence of this fact we say the two projective subsets X and Y are disjoint if $X \cap Y = \{0\}$.*

Previous remarks show that the unit sphere $\mathbf{S} = \{v \in V \mid \|v\| = 1\}$ is compact in V. Also if v is a nonzero element of V then there exists an $a \in F$ such that $\|v\| = |a|$. In particular v/a has norm 1 and hence $Fv \cap \mathbf{S} \neq \emptyset$. This shows that any projective subset X will intersect the unit sphere $\mathbf{S}$. This permits us to define a "distance", on the unit sphere, between two projective subsets X and Y and this will be done as follows.

$$d(X, Y) = \inf\{\|x - y\| \mid x \in X \cap \mathbf{S}, y \in Y \cap \mathbf{S}\}.$$

Also if $0 \neq v, w \in V$ we set

$$d(v, w) = d(Fv, Fw) = \inf\{\|av - bw\| \mid a, b \in F, \|av\| = 1 = \|bw\|\}.$$

To be complete we also specify the mixed distance

$$d(X, w) = d(X, Fw) = \inf\{d(x, w) \mid x \in X\}.$$

Clearly d can never be a metric on V since for two different vectors v, w with $w \in Fv$ we get that $d(v, w) = 0$. As such d can only be a pseudometric on V. However using the fact that the unit sphere is compact we do obtain that d is a metric on $\mathcal{P}(V)$. Moreover this metric *bounds* the projective space as it will at most have the same diameter as the unit sphere which in our case will be 2. We prove these claims in the following lemma.

Lemma 3.1.2. *Let F be a locally compact field and V be a finite-dimensional F-vector space. Also let d be defined as above. We then have*

(i) If X and Y are nonzero subspaces of V, then there exist $x_0 \in X \cap \mathbf{S}$ and $y_0 \in Y \cap \mathbf{S}$ such that $d(X, Y) = \|x_0 - y_0\|$. In particular if X and Y are disjoint, then $d(X, Y) > 0$.

(ii) The distance function d defines a metric on the projective space $\mathcal{P}(V)$. Also, with respect to this metric, the projective space of V has diameter lower or equal then 2. Moreover if the absolute value defined on F is non-archimedean, then the diameter is lower or equal then 1.

(iii) If v, w are two distinct vectors in V then $d(v, w) \leq 2\|v - w\|/\|v\|$. Again if $|.|$ is non-archimedean then $d(v, w) \leq \|v - w\|/\|v\|$.

Proof. (i) Since F is complete and V is a finite-dimensional vector space over F, every subspace of V is closed in V. It follows that $X \cap \mathbf{S}$ and $Y \cap \mathbf{S}$ are compact. By the continuity of the norm $\|.\|$ and the addition we see that the set $\{\|x - y\| \mid x \in X \cap \mathbf{S}, y \in Y \cap \mathbf{S}\}$ is also compact in $\mathbb{R}^+$ so that the infimum of this set is in fact a minimum.
(ii) First let u and v correspond to distinct points in $\mathcal{P}(V)$, i.e. $Fu \neq Fv$ and hence $Fu \cap Fv = \{0\}$. It follows from (i) that $d(v, u) = d(u, v) > 0$. Now let u, v, w be nonzero vectors in V. By (i), there exists $a, b, b', c' \in F$ such that $\|au\| = \|bv\| = \|b'v\| = \|c'w\| = 1$, $d(u, v) = \|au - bv\|$ and $d(v, w) = \|b'v - c'w\|$. It follows that $|b| = |b'|$ so if we set $c = (b/b')c' \in F$, then $\|cw\| = 1$ and $d(v, w) = \|bv - cw\|$. This last equality follows from the observation that $\|(b/b')(b'v - c'w)\| = \|b'v - c'w\|$. We thus obtain the triangle inequality

$$d(u, w) \leq \|au - cw\| \leq \|au - bv\| + \|bv - cw\| = d(u, v) + d(v, w).$$

Finally, for $0 \neq u, v \in V$ we have, as above, that $d(u,v) = \|au - bv\| \leq \|au\| + \|bv\| = 2$. So $\mathcal{P}(V)$ has diameter at most 2. In the non-archimedean case, $d(u,v) = \|au - bv\| \leq \max\{\|au\|, \|bv\|\} = 1$.
(iii) First assume that $|.|$ is archimedean then $\|V\| = |F| \subset F$ and it makes sense to write $v/\|v\|$ and $w/\|w\|$ for $v, w \in V$. Clearly both these elements have norm 1 and we note that

$$\begin{aligned} u = \frac{v}{\|v\|} - \frac{w}{\|w\|} &= \frac{v}{\|v\|} - \frac{w}{\|v\|} - \frac{w}{\|w\|} + \frac{w}{\|v\|} \\ &= \frac{v-w}{\|v\|} - \frac{w}{\|w\|}\left(1 - \frac{\|w\|}{\|v\|}\right) \\ &= \frac{v-w}{\|v\|} - \frac{w}{\|w\|}\left(\frac{\|v\|}{\|v\|} - \frac{\|w\|}{\|v\|}\right) \\ &= \frac{v-w}{\|v\|} - \frac{w}{\|w\|}\frac{\|v\| - \|w\|}{\|v\|} = u' - u'' \end{aligned}$$

where $\|u'\| = \|v - w\|/\|v\|$ and $\|u''\| = |\|v\| - \|w\|| / \|v\| \leq \|v - w\|/\|v\|$. It follows that

$$d(v,w) \leq \|u\| \leq \|u'\| + \|u''\| \leq 2\frac{\|v-w\|}{\|v\|}.$$

Otherwise if we suppose that $|.|$ is non-archimedean, for $\|v\| \neq \|w\|$ (ii) yields

$$d(v,w) \leq 1 \leq \frac{\max\{\|v\|, \|w\|\}}{\|v\|} = \frac{\|v-w\|}{\|v\|}.$$

Alternatively if $\|v\| = \|w\|$, choose $a \in F$ with $|a|$ equal to the norm of v and w. Then

$$d(v,w) \leq \left\|\frac{v}{a} - \frac{w}{a}\right\| = \frac{\|v-w\|}{|a|} = \frac{\|v-w\|}{\|v\|}$$

which concludes our proof of this lemma. □

Remark 3.1.3. *As mentioned in item (ii) the distance function d is indeed a metric on the points of the projective space $\mathcal{P}(V)$. Even more so we also have, for every projective subset X and Y of V and every vector $w \in V$, a more general triangle inequality given by*

$$d(X,Y) \leq d(X,w) + d(w,Y).$$

However as pointed out by Ángel del Río and explained in [GP07] if X and Y are projective subsets of V such that $d(X,Y) > 0$ then $Z = X \cup Y$ is also a projective subset of V such that

$$d(X,Y) > d(X,Z) + d(Z,Y) = 0.$$

Now suppose $|.|$ is an archimedean absolute value. Again F is then equal to either the real or complex numbers and $|.|$ is the classical absolute value. As we have chosen $\|.\|$ to be the maximum norm on V we can find two elements $a = (1,1,1,0,\ldots,0)$ and $b = (1,-1,0,0,\ldots,0)$ which are both elements of the unit sphere $\mathbf{S}$ and where $a \notin Fb$. It follows that $d(a,b) = 2$ and as such the bound in (ii) can be reached. Similarly if $|.|$ is non-archimedean these same two elements are still part of the units sphere but $d(a,b) = 1$ which was the bound for the non-archimedean case.

In closure if W is another finite-dimensional vector space over F with norm $\|.\|'$ and $\sigma : V \to W$ a linear transformation then this function is continuous. We now define

$$\|\sigma\|'' = \sup\{\|\sigma(v)\|' \mid v \in \mathbf{S}\}$$

which is a norm on the F-vector space $\mathcal{L}(V,W)$. Now since the unit sphere $\mathbf{S}$ is compact and the norm $\|.\|'$ is also continuous we get that $\{\|\sigma(v)\|' \mid v \in \mathbf{S}\}$ is also compact such that the supremum is in fact a maximum and in particular there exists a $v_0 \in \mathbf{S}$ such that $\|\sigma\|'' = \|\sigma(v_0)\|'$. Furthermore, $\|\sigma(v)\|' \leq \|\sigma\|''\|v\|$ for all $v \in V$. In the following we shall simply denote all these norms with $\|.\|$.

3.2 Attractors of generalized transvections and diagonalizable operators

As explained in the chapter introduction we are now faced with finding attractors, and corresponding repulsers, for diagonalizable operators. So suppose $T : V \to V$ is such a diagonalizable operator. This implies that T is semisimple and its eigenvalues are contained in F. Furthermore suppose V contains a proper subspace I spanned by the eigenspaces corresponding to the eigenvalues of maximal absolute value. Then we would like to show that a proper projective neighborhood $\overline{I} = \overline{\mathfrak{N}}_\epsilon(I)$ will be an "attractor" under the action of T, i.e. the image of a certain well chosen subspace X of V, the so-called "repulser", will fall into $\overline{I}$ under T. Actually we will need that the same holds not just for X but also for a projective neighborhood $\overline{X} = \overline{\mathfrak{N}}_\kappa(X)$ of X in order to be able to apply the Ping-pong Lemma.

It should be noted that not every diagonalizable operator has such a proper subspace I. For instance if $T = \mathrm{diag}(a, \ldots, a)$ with $a \in F$, then the subspace I spanned by the eigenspaces corresponding to the eigenvalues of maximal absolute value will be equal to V. Clearly for our purpose we will desire proper attractors. First we will need the following technical result providing us with a relative, although useful, lower and upper bound for the images of diagonalizable operators.

Lemma 3.2.1. *Let F be a locally compact field and V be a finite-dimensional F-vector space. Suppose $T : V \to V$ is a diagonalizable operator.*

(i) If all eigenvalues of T have absolute values lower or equal then r, then there exists a real constant $k > 0$ such that $\|T^n(v)\| \leq kr^n\|v\|$ for all $v \in V$ and $n \in \mathbb{N}$.

(ii) If all eigenvalues of T have absolute values greater or equal then s, then there exists a real constant $k' > 0$ such that $\|T^n(v)\| \geq k's^n\|v\|$ for all $v \in V$ and $n \in \mathbb{N}$.

Proof. Since T is diagonalizable, V has a basis consisting of eigenvectors of T and we denote this set by $\{v_1, v_2, \ldots v_m\}$. Each eigenvector v_i corresponds to an eigenvalue λ_i where we may assume that $s \leq |\lambda_i| \leq r$. Now every $v \in V$ can uniquely be written as $v = \sum_{i=1}^m \pi_i(v)v_i$, where $\pi_i : V \to F$ is a nonzero linear functional. Continuing on let us now define a new norm on V as follows

$$\|.\|' : V \to \mathbb{R}^+ : v \mapsto \|v\|' = \max\{|\pi_i(v)| \mid 1 \leq i \leq m\}.$$

Since V is finite dimensional this norm is equivalent to $\|.\|$. Now we have

$$T^n(v) = T^n\left(\sum_{i=1}^m \pi_i(v)v_i\right) = \sum_{i=1}^m \pi_i(v)T^n(v_i) = \sum_{i=1}^m \pi_i(v)\lambda_i^n v_i$$

and we see that

$$\|T^n(v)\|' = \max_{1\leq i\leq m}(|\lambda_i^n\pi_i(v)|) \leq r^n \max_{1\leq i\leq m}(|\pi_i(v)|) = r^n\|v\|'.$$

Similarly $\|T^n(v)\|' \geq s^n\|v\|'$. Now, as noted, the two norms $\|.\|$ and $\|.\|'$ are equivalent, i.e there exist positive real constants a and b such that $b\|v\|' \leq \|v\| \leq a\|v\|'$ for every $v \in V$. Thus

$$\|T^n(v)\| \leq a\|T^n(v)\|' \leq ar^n\|v\|' \leq \frac{a}{b}r^n\|v\|,$$

and again in a analogues fashion

$$\|T^n(v)\| \geq b\|T^n(v)\|' \geq bs^n\|v\|' \geq \frac{b}{a}r^n\|v\|.$$

The proof is now finished is we set $k = a/b$ and $k' = b/a$. □

This lemma enables us to put some weight behind our previous exertions, concerning attractors and repulsers of diagonalizable operators, and prove the following result.

Proposition 3.2.2. *Let F be a locally compact field and V be a finite-dimensional F-vector space. Suppose $T : V \to V$ is a diagonalisable nonsingular operator and*

(1) $I \neq \{0\}$ is the subspace of V spanned by the eigenspaces of T corresponding to the eigenvalues of absolute value greater or equal than some $r > 0$.

(2) $K \neq \{0\}$ is the subspace of V spanned by the remaining eigenspaces.

Suppose X is subspace of V disjoint from K, let κ be a positive real number smaller or equal to $d(X, K)/2$ and let $\epsilon > 0$. If we set

(3) $\overline{X} = \overline{\mathfrak{N}}_\kappa(X) = \{v \in V\backslash\{0\} \mid d(v, X) \leq \kappa\} \cup \{0\}$ and

(4) $\overline{I} = \overline{\mathfrak{N}}_\epsilon(I) = \{v \in V\backslash\{0\} \mid d(v, I) \leq \epsilon\} \cup \{0\}$,

then there exists an $N > 0$ such that for every $n \geq N$ we have that $T^n(\overline{X}) \subseteq \overline{I}$.

Proof. First of all it is clear that both $\overline{X}$ and $\overline{I}$ are projective subset of $V = I \oplus K$. Also since K and X are disjoint it follows from Lemma 3.1.2(i) that $d(X, K) > 0$. This shows we can find an element $\kappa > 0$ as in the statement of this proposition. So, if $0 \neq u$ is an arbitrary vector in $\overline{X}$, then by the definition of κ and $\overline{X}$ we have

$$\kappa + d(u, K) \geq d(X, u) + d(u, K) \geq d(X, K) \geq 2\kappa,$$

which shows that $d(u, K) \geq \kappa$ and hence also $d(\overline{X}, K) \geq \kappa$ and $\overline{X}$ is disjoint from K. Moreover since $\mathcal{P}(V)$ has diameter at most 2 we have that $\kappa \leq 1$. Now take $0 \neq v \in \overline{X}$ and write $v = x + y \in V$ with $x \in I$ and $y \in K$. If $y = 0$ then $v \in I$ so $T^n(v) \in I$ for all n and there is nothing to prove. So suppose $y \neq 0$. By Lemma 3.1.2(iii) we have

$$\kappa \leq d(\overline{X}, K) \leq d(v, K) \leq d(v, y) \leq \frac{2\|v - y\|}{\|v\|} = \frac{2\|x\|}{\|v\|}$$

so that $\|x\| \geq (\kappa/2)\|v\|$ and $x \neq 0$. Now let $\pi : V \to K$ be the natural projection of V into K with kernel I. Then $y = \pi(v)$, so if we set $h = \|\pi\|$ we get that $\|y\| \leq h\|v\|$. Next by the definition of r and the fact that I is spanned by the eigenspaces of T corresponding to the eigenvalues of absolute value $\geq r$, using Lemma 3.2.1(ii), we see that $\|T^n(x)\| \geq k'r^n\|x\|$ for some positive constant k'. Also if s is the maximum absolute value of all the eigenvalues of the restriction of T to K, then $s < r$, and again using Lemma 3.2.1(i) we see that $\|T^n(y)\| \leq ks^n\|y\|$ for some positive constant k.
Finally since $T^n(v)$ and $T^n(x)$ are not equal to 0 and $T^n(x) \in I$, Lemma 3.1.2(iii) yields

$$d\left(T^n(v), I\right) \leq d\left(T^n(v), T^n(x)\right) \leq \frac{2\|T^n(v - x)\|}{\|T^n(x)\|} = \frac{2\|T^n(y)\|}{\|T^n(x)\|}.$$

We can further blow up this inequality, using $\|T^n(y)\| \leq ks^n\|y\| \leq khs^n\|v\|$ in the numerator and $\|T^n(x)\| \geq k'r^n\|x\| \geq k'r^n(\kappa/2)\|v\|$ in the denominator, to obtain

$$d\left(T^n(v), I\right) \leq \frac{2\|T^n(y)\|}{\|T^n(x)\|} \leq \frac{4kh}{k''\kappa}\left(\frac{s}{r}\right)^n.$$

Clearly this last sequence goes to zero if n goes to infinity. This means that for an n sufficiently large every $d(T^n(v), I)$ can be made smaller then ϵ. In other words $T^n(v) \in \overline{I}$ for all sufficiently large n, were the bound depends on T, X and κ, but not on the choice of v. In closure we thus get that $T^n(\overline{X}) \subseteq \overline{I}$ for n large. □

Now let $T : V \to V$ be a nonsingular diagonalizable operator with eigenvalues $\lambda_1, \ldots, \lambda_n$. Then it is very easy to see that T^{-1} is also a nonsingular diagonalizable operator with eigenvalues $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$. Moreover if I is the subspace of V spanned by the eigenspaces of T corresponding to the eigenvalues of absolute values greater or equal then $r > 0$ then I is clearly also spanned by the eigenspaces of T^{-1} corresponding to the eigenvalues of absolute value smaller or equal then $r^{-1} > 0$. By this remark, interchanging T and T^{-1} in the previous proof we obtain an attractor for T^{-1}.

Proposition 3.2.3. *Let F be a locally compact field and V be a finite-dimensional F-vector space. Suppose $T : V \to V$ is a diagonalisable nonsingular operator such that*

(1) $I \neq \{0\}$ is the subspace of V spanned by the eigenspaces of T corresponding to the eigenvalues of absolute value lower or equal then $s > 0$.

(2) $K \neq \{0\}$ is the subspace of V spanned by the remaining eigenspaces.

Suppose X is subspace of V disjoint from K, let κ be a positive real number smaller or equal to $d(X, K)/2$ and let $\epsilon > 0$. If we set

(3) $\overline{X} = \overline{\mathfrak{N}}_\kappa(X) = \{v \in V \backslash \{0\} \mid d(v, X) \leq \kappa\} \cup \{0\}$ and

(4) $\overline{I} = \overline{\mathfrak{N}}_\epsilon(I) = \{v \in V \backslash \{0\} \mid d(v, I) \leq \epsilon\} \cup \{0\}$,

then there exists an $N > 0$ such that for every $n \geq N$ we have that $T^{-n}(\overline{X}) \subseteq \overline{I}$.

Although it would make life easier, not every operator we will encounter is diagonalizable. For instance the operators occurring in Santov's Theorem will certainly not be diagonalizable. Rather they are generalized transvections. Specifically, they are of the form $S = 1 + a\sigma$ where a is a nonzero element of F and $\sigma : V \to V$ is a nonzero operator of square 0. Clearly if $|a|$ is large then $a\sigma$ should *dominate* S. Using the same reasoning as with the diagonalizable operators given a vector v, the image vector $S(v) = v + a\sigma(v)$ should have large components in $I = \text{im } \sigma = \sigma(V)$. Again v itself could have large components in the complement of $\sigma(V)$ to start with which is why we will again need to use the projective distance. Furthermore if v is an element in the kernel but not in the image of σ then $S(v) = v \notin I$. So we will have to avoid vectors in $\ker \sigma$. We thus obtain similar criteria as for diagonalizable operators which we state in the following result.

Proposition 3.2.4. *Let F be a locally compact field and V be a finite-dimensional F-vector space. Suppose $S = 1 + a\sigma$ is a generalized transvection, i.e $a \in F_0$ and $\sigma : V \to V$ is nonzero and has square 0. Now set*

(1) $\{0\} \neq I = \text{im } \sigma = \sigma(V)$ the image of σ and

(2) $\{0\} \neq K = \ker \sigma$ the kernel of σ

Suppose X is a subspace in V with $V = X \oplus K$, let κ be a positive real number smaller or equal to $d(X, K)/2$ and let $\epsilon > 0$. If we set

(3) $\overline{X} = \overline{\mathfrak{N}}_\kappa(X) = \{v \in V \backslash \{0\} \mid d(v, X) \leq \kappa\} \cup \{0\}$ and

(4) $\overline{I} = \overline{\mathfrak{N}}_\epsilon(I) = \{v \in V \backslash \{0\} \mid d(v, I) \leq \epsilon\} \cup \{0\}$,

then for all suitably large $|a|$ we will have that $S(\overline{X}) \subset \overline{I}$.

Proof. Again we see that both $\overline{X}$ and $\overline{I}$ are projective subset of $V = X \oplus K$. Furthermore completely similar to the proof of Proposition 3.2.2 we see that for $0 \neq u$ an arbitrary vector in $\overline{X}$

$$\kappa + d(u, K) \geq d(X, u) + d(u, K) \geq d(X, K) \geq 2\kappa,$$

which shows that $d(u, K) \geq \kappa$ and hence also $d(\overline{X}, K) \geq \kappa$ which implies that $\overline{X}$ is disjoint form K. Again κ will be lower or equal than 1. Now let $0 \neq v \in \overline{X}$ and write $v = x + y \in V$

with $x \in X$ and $y \in K$. As $\overline{X} \cap K = \{0\}$, we have that $x \neq 0$. Now suppose $y = 0$, then $x = v$ so $\|x\| \geq (\kappa/2).\|v\|$. In the other case where $y \neq 0$ we have by using Lemma 3.1.2(iii) that

$$\kappa \leq d(\overline{X}, K) \leq d(v, K) \leq d(v, y) \leq \frac{2\|v - y\|}{\|v\|} = \frac{2\|x\|}{\|v\|},$$

which again yields $\|x\| \geq (\kappa/2)\|v\|$. Continuing we remark that $I \cong V/K \cong X$ and $X \cap K = \{0\}$, so if we restrict σ to X we obtain an isomorphism $\tau : X \to I$. Let $\tau^{-1} : I \to X$ be the inverse of this isomorphism τ and set $t = \|\tau^{-1}\|$. Suppose $z = \sigma(x) = \tau(x)$ then $x = \tau^{-1}(z)$ and hence $\|x\| \leq \|\tau^{-1}\|\|z\| = t\|\sigma(x)\|$ and we can conclude that $\|\sigma(x)\| \geq t^{-1}\|x\| \geq \kappa/(2t)\|v\|$.
Finally note that $S(v) = v + a\sigma(v) = v + a\sigma(x + y) = v + a\sigma(x)$. Since $S(v)$ and $a\sigma(x)$ are nonzero and since $a\sigma(x) \in I$, Lemma 3.1.2(iii) yields

$$d(S(v), I) \leq d(S(v), a\sigma(x)) \leq \frac{2\|S(v) - a\sigma(x)\|}{\|a\sigma(x)\|} = \frac{2\|v\|}{\|a\sigma(x)\|}.$$

But $\|a\sigma(x)\| = |a|\|\sigma(x)\| \geq |a|(\kappa/2t)\|v\|$, so that

$$d(S(v), I) \leq \frac{2\|v\|}{\|a\sigma(x)\|} \leq \frac{4t}{\kappa|a|}.$$

This means that if $|a| \geq 4t/(\kappa\epsilon)$ we obtain $d(S(v), I) \leq \epsilon$. Again note that this lower bound $4t/(\kappa\epsilon)$ depends on σ, X and κ but not upon the choice of $v \in \overline{X}$ and we again conclude that $S(\overline{X}) \in \overline{I}$. □

It may be interesting to point out a striking difference between the attractors, and repulsers, of generalized transvections and diagonalizable operators. Of course in both cases the attractor I will attract itself as this is crucial, but with diagonalizable operators also projective sets X which are essentially already close to the attractor will be drawn into $\overline{I}$ and as such X is a repulser. This is because in this case the "blockade" K, i.e. the subspace whose elements are blocked from getting close to I under the action by the operator, is projectively distant from I. Contrary to the generalized transvections where the attractor I is a subspace of the blockade K and only projective sets X which are essentially far away from I will be a repulser.

3.3 The Ping-pong Lemma applied to linear groups

Now that we have found our attracting and repulsing duo the questions still remains how exactly this will help us with finding free products of subgroups in a linear group. More generally if G is a group with non identity subgroups G_1 and G_2 we want to know when every element in $\langle G_1, G_2 \rangle$ can uniquely be written as a finite alternating product of element in $G_1^{\#}$, the non identity elements of G_1, and $G_2^{\#}$. Without further ado let us proceed to Klein's Lemma.

Ping-pong Lemma. *Let G be a group with non identity subgroups G_1 and G_2 and suppose that G acts on a set P having distinct nonemtpy subsets P_1 and P_2. If $G_1^{\#} P_1 \subseteq P_2$, $G_2^{\#} P_2 \subseteq P_1$ and $o(G_2) > 2$ then $\langle G_1, G_2 \rangle$ is naturally isomorphic to the free product $G_1 * G_2$.*

Proof. Clearly it suffices to prove that $1 \in G$ cannot be written as a nonempty alternating product of elements in $G_1^{\#}$ and $G_2^{\#}$. So suppose by way of contradiction that such a product exists and 1 is equal to

$$h_1 h_2 \dots h_n \tag{3.2}$$

with $n \geq 2$. First if both h_1 and h_n are elements in $G_1^{\#}$, then by conjugating expression (3.2) by an non identity element of G_2 we obtain a similar expression which now starts and ends in $G_2^{\#}$ and clearly is still equal to 1. Alternatively suppose h_1 is an element of $G_1^{\#}$ but

$h_n \in G_2^{\#}$. Because $o(G_2) > 2$ there exists and element h in $G_2^{\#}$ different form h_n^{-1} so that conjugation expression (3.2) by h again obtains an expression starting and ending in $G_2^{\#}$ equal to 1. Clearly we can use the same argument when $h_1 \in G_2^{\#}$ and $h_n \in G_1^{\#}$, and we can therefore assume that in the expression of 1 both h_1 and h_2 are elements of $G_2^{\#}$. But since P_1 and P_2 are ping-ponged back and forth under the action of $G_1^{\#}$ and $G_2^{\#}$ we obtain that

$$1P_2 = P_2 \text{ such that } P_2 = h_1 h_2 \dots h_n P_2 \subset P_1.$$

Alternatively if g is a non identity element of $G_1^{\#}$, then

$$g1g^{-1}P_1 = P_1 \text{ such that } P_1 = gh_1h_2 \dots h_n g^{-1} P_1 \subset P_2.$$

This shows that $P_1 = P_2$ which is a contradiction. As a consequence our assumption that 1 is equal to expression (3.2) is invalid and the lemma is proved. □

Notice that the assumption that at least one of the subgroups has order greater than 2 is essential. To show this suppose $G = \langle G_1, G_2 \rangle$ with $o(G_1) = o(G_2) = 2$. Then clearly $G_1 = \langle g_1 \mid g_1^2 = 1 \rangle$ and $G_2 = \langle g_2 \mid g_2^2 = 1 \rangle$ such that both these subgroups are isomorphic to $\mathbb{Z}_2$. Also G acts on the set $P = \{1, 2\}$ by interchanging the subset $P_1 = \{1\}$ and $P_2 = \{2\}$, i.e $g_1(1) = 2$ and $g_2(2) = 1$. Obviously G can be any finite dihedral group

$$\begin{aligned} D_{2n} &= \langle g_1, g_2 \mid g_1^2 = 1, g_2^2 = 1, (g_1 g_2)^n = 1 \rangle \\ &= \langle x = g_1, y = g_1 g_2 \mid x^2 = 1, y^n = 1, xyx^{-1} = y^{-1} \rangle \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2 \end{aligned}$$

including Klein's four-group $K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, or even an infinite dihedral group

$$\begin{aligned} D_\infty &= \langle g_1, g_2 \mid g_1^2 = 1, g_2^2 = 1 \rangle \cong \mathbb{Z}_2 * \mathbb{Z}_2 \\ &= \langle x = g_1, y = g_1 g_2 \mid x^2 = 1, xyx^{-1} = y^{-1} \rangle \cong \mathbb{Z} \rtimes \mathbb{Z}_2 \end{aligned}$$

while $G_1 * G_2$ can only be the infinite dihedral group, which shows that the assumption $o(G_2) > 2$ is crucial. Let us now put the Ping-pong Lemma to good use by giving an example. We will naively yield its power to prove Sanov's Theorem.

Sanov's Theorem. *Let* $\mathrm{SL}_2(\mathbb{C})$ *be the special linear group over the complex vector space* $\mathbb{C}^2$ *and suppose*

$$g_1 = \begin{bmatrix} 1 & a_1 \\ 0 & 1 \end{bmatrix} \qquad \textit{and} \qquad g_2 = \begin{bmatrix} 1 & 0 \\ a_2 & 1 \end{bmatrix}$$

are two unipotent elements in this group. If $|a_1|, |a_2| \geq 2$*, then* g_1 *and* g_2 *generate a free subgroup of* G *of rank 2.*

Proof. First note that both $G_1 = \langle g_1 \rangle$ and $G_2 = \langle g_2 \rangle$ are isomorphic to $\mathbb{Z}$ and we want to show that $\langle G_1, G_2 \rangle = G_1 * G_2$. Now observe that G acts on $P = \mathbb{C}^2$, the two dimensional complex vector space consisting of vectors $(r, s) = [r, s]^T$. Now define

$$P_1 = \{(r, s) \mid |r| < |s|\} \qquad \text{and} \qquad P_2 = \{(r, s) \mid |r| > |s|\}.$$

If $(r, s) \in P_1$ and $g_1^n \in G_1^{\#}$ where n is some nonzero integer then $g_1^n(r, s) = (r + na_1 s, s)$. Since $|na_1| \geq 2$ and $|s| > |r|$ we have

$$\begin{aligned} |r + na_1 s| = |na_1 s - (-r)| &\geq ||na_1 s| - |-r|| \\ &\geq |na_1||s| - |r| \\ &\geq 2|s| - |r| \\ &> 2|s| - |s| = |s|, \end{aligned}$$

which shows that $G_1^{\#}P_1 \subseteq P_2$. Similarly if $(r,s) \in P_2$ and $g_2^m \in G_2^{\#}$ where again m is some nonzero integer then $g_1^m(r,s) = (r, ma_2r + s)$. Now $|ma_2| \geq 2$ and $|r| > |s|$. We obtain

$$\begin{aligned} |ma_2r + s| = |ma_2r - (-s)| &\geq ||ma_2r| - |-s|| \\ &\geq |ma_2||r| - |s| \\ &\geq 2|r| - |s| \\ &> 2|r| - |r| = |r|, \end{aligned}$$

and we see that $G_2^{\#}P_2 \subseteq P_1$. By this the criteria of the Ping-pong Lemma are met and the wanted result follows. □

Again we note that some assumption on the size of a_1 and a_2 is required. If for example $a_1 = a_2 = 1$ then

$$g_1^{-1}g_2g_1^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

and we easily see that

$$\left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right) \left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right) = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

This shows that $g_1^{-1}g_2g_1^{-1}$ has order 4 and hence $\langle g_1, g_2 \rangle$ cannot be free.

From the proof of Sanov's Theorem we see that a size of at least 2 will suffice in making the proof work. However this does not completely explain how this lowerbound is obtained, nor does it give a constructive way of finding these sets P_1 and P_2 necessary to utilize the Ping-pong Lemma. So let us analyze this problem more closely. First notice that

$$g_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + a_1 \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \qquad \text{and} \qquad g_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + a_2 \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix},$$

where both $\sigma = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $\tau = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ have square zero. This shows that $g_1 = 1 + a_1\sigma$ and $g_2 = 1 + a_2\tau$ are in fact generalized transvections with

$$I_1 = \text{im }(\sigma) = \begin{bmatrix} \mathbb{C} \\ 0 \end{bmatrix} = \ker(\sigma) = K_1 \qquad \text{and} \qquad I_2 = \text{im }(\tau) = \begin{bmatrix} 0 \\ \mathbb{C} \end{bmatrix} = \ker(\tau) = K_2.$$

Evidently $I_1 \oplus I_2 = \mathbb{C}^2$ so if we would set $X_1 = I_2 = K_2$ and $X_2 = I_1 = K_1$ the conditions of Proposition 3.2.4 are met for both g_1 and g_2 simultaneously. Now notice that $d(X_1, K_1) = d(I_2, I_1) = d(K_2, X_2) = 1$ so the largest possible value we can give κ_1 according to this proposition is $1/2$ and by the symmetry of this example this value is also equal to ϵ_2, κ_2 and ϵ_1. Studying the proof of Proposition 3.2.4 we find that for $|a_1|$ and $|a_2|$ greater or equal than 16

$$g_1(\overline{\mathfrak{N}}_{1/2}(X_1)) \subseteq \overline{\mathfrak{N}}_{1/2}(I_1) = \overline{\mathfrak{N}}_{1/2}(X_2) \text{ and } g_2(\overline{\mathfrak{N}}_{1/2}(X_2)) \subseteq \overline{\mathfrak{N}}_{1/2}(I_2) = \overline{\mathfrak{N}}_{1/2}(X_1).$$

It again follows that $\langle g_1, g_2 \rangle$ is isomorphic to the free group. The drawback of this method is clearly the greater constriction imposed on the absolute values of a_1 and a_2. However we do obtain a constructive way of finding this duo of attracting and repulsing sets necessary to apply the Ping-pong Lemma. Also note that, using some basic calculation, we obtain

$$\overline{\mathfrak{N}}_{1/2}(X_1) = \overline{\mathfrak{N}}_{1/2}(I_2) \subseteq P_1 \qquad \text{and} \qquad \overline{\mathfrak{N}}_{1/2}(X_2) = \overline{\mathfrak{N}}_{1/2}(I_1) \subseteq P_2$$

Remark 3.3.1. *It should be noted that if we set $\kappa_1 = \epsilon_2 = 1 = \epsilon_1 = \kappa_2$ and take projective neighborhoods of the form*

(1) $\hat{X_1} = \mathfrak{N}_1(X_1) = \{v \in V \backslash \{0\} \mid d(v, X_1) < 1\} \cup \{0\}$ *and*

(2) $\hat{X_2} = \mathfrak{N}_1(X_2) = \{v \in V \backslash \{0\} \mid d(v, X_2) < 1\} \cup \{0\}$,

we are able to obtain the bound $|a_1|, |a_2| > 2$, this by rewriting the proof for this specific case. This will clearly not work in general but it shows that the technique, although being more general, is just as powerful as the original proof.

Unfortunately to use this method for other generalized transvections $S = 1 + a\sigma$ and $T = 1 + b\tau$ on a vector spaces F^n with F locally compact we do need to check two extra conditions. First in order to apply Klein's Lemma we need to ensure that the group generated by T or S has order greater then 2. Since $S^n = 1 + na\sigma$ and $T^m = 1 + mb\tau$ this condition is clearly satisfied if and only if $\mathrm{char}(F) \neq 2$. Also we need to be certain that the disjoint attractors found for T and S are also attractors for S^n and T^m. Overgoing the proof of Proposition 3.2.4 we see that this will be the case if $|na| = |n||a| \geq |a|$, i.e. if $|n| \geq 1$ for every $n \in 1\mathbb{Z} \backslash \{0\} \subset F$. From the introductory chapters we know this condition will fail if and only if F is an algebraic field extension of the p-adic numbers. Thus we need to exclude this particular case. We now formally obtain the following result.

Theorem 3.3.2. *Let F be a locally compact field and V a finite-dimensional F-vector space. Suppose $S, T : V \to V$ are two generalized transvection, i.e. $S = 1 + a\sigma$ and $T = 1 + b\tau$ where $\sigma, \tau : V \to V$ are nonzero operators with square zero. Assume that $|n| \geq 1$ for every $n \in 1\mathbb{Z} \setminus \{0\}$ and $\mathrm{char}(F) \neq 2$. Set*

(1) $I = \sigma(V) = \mathrm{im}\ (\sigma)$ *and* $K = \ker(\sigma)$,

(2) $J = \tau(V) = \mathrm{im}\ (\tau)$ *and* $L = \ker(\tau)$.

If the intersection $I \cap L$ and $J \cap K$ are both trivial, then for all $a, b \in F$ with $|a|$ and $|b|$ sufficiently large we have $\langle S, T \rangle = \langle S \rangle * \langle T \rangle$.

Proof. Since both $I \cap L$ and $J \cap K$ are trivial, by Lemma 3.1.2(i), the distances $d(I, L)$ and $d(J, K)$ are both strictly larger then 0. Now let $2\kappa > 0$ be the smaller of these two distances and define

$$P = \overline{\mathfrak{N}}_\kappa(I) \qquad \text{and} \qquad Q = \overline{\mathfrak{N}}_\kappa(J).$$

Since I is an attractor of S and $|n| \geq 1$ for every $n \in 1\mathbb{Z} \backslash \{0\}$ it follows from Proposition 3.2.4 that $\langle S \rangle^\# Q \subset P$ for all $a \in F$ with sufficiently large absolute value. Similarly $\langle T \rangle^\# P \subset Q$ for all $b \in F$ with sufficiently large absolute value. Clearly $I \subseteq P$ and also $I \subseteq K$ such that $I \cap Q = \{0\}$. Thus $P \neq Q$ and since $\mathrm{char}(F) \neq 2$, both S and T have order at least 3. This allows us the apply the Ping-pong Lemma as intended and the result is proved. □

Clearly this technique can be used to yield similar results for diagonalizable operators T and S. The constraints on the characteristic of F and the size of the prime ring elements will surely not be necessary in this case but as explained in the introductory we will still need some intersections to be trivial in order to apply Propositions 3.2.2 and 3.2.3. In fact we will require this for both the positive and negative powers of T and S, as such we will obtain four times as many intersection requirements. In order to avoid repetition we will formally state what is meant by a T-decomposition of V.

Definition 3.3.3 (T-decomposition)**.** *Let T be a nonsingular diagonalizable operator on a vector space V. If there exists real numbers $r > s > 0$ and*

(1) $T_+ \neq \{0\}$ is the subspace of V spanned by the eigenspaces of T corresponding to the eigenvalues of absolute value larger or equal to r,

(2) $T_- \neq \{0\}$ is the subspace of V spanned by the eigenspaces of T corresponding to the eigenvalues of absolute value smaller or equal to s and

(3) T_0 the span of the remaining eigenspaces,

then $V = T_+ \oplus T_0 \oplus T_-$ is called a T-decomposition of V.

As said earlier not every nonsingular diagonalizable operator T induces a T-decomposition on V. This will cause us to induce yet another restraint on the operators T and S. On the up-side all restrictions on the locally compact field F are gone.

Theorem 3.3.4. *Let F be a locally compact field and V a finite-dimensional F-vector space. Suppose $S, T : V \to V$ are two nonsingular diagonalizable operators such that $V = S_+ \oplus S_0 \oplus S_-$ and $V = T_+ \oplus T_0 \oplus T_-$ are an S- and a T-decomposition of V. If the eight intersections $S_\pm \cap (T_0 \oplus T_\pm)$ and $T_\pm \cap (S_0 \oplus S_\pm)$ are all trivial, then there exists positive integers n and m such that $\langle S^m, T^n \rangle = \langle S^m \rangle * \langle T^n \rangle$.*

Proof. Since all eight intersections $S_\pm \cap (T_0 \oplus T_\pm)$ and $T_\pm \cap (S_0 \oplus S_\pm)$ are trivial we have, by Lemma 3.1.2(i), that all eight distances $d(S_\pm, T_0 \oplus T_\pm)$ and $d(T_\pm, S_0 \oplus S_\pm)$ are strictly larger than 0. So let us take $2\kappa > 0$ as the smallest of these eight distances. Afterwards define

$$P = \overline{\mathfrak{N}}_\kappa(S_-) \cup \overline{\mathfrak{N}}_\kappa(S_+) \qquad \text{and} \qquad Q = \overline{\mathfrak{N}}_\kappa(T_-) \cup \overline{\mathfrak{N}}_\kappa(T_+).$$

Propositions 3.2.2 and 3.2.3 tell us that S_+ is an attractor for S and S_- is an attractor of S^{-1}. It follows that under the assumptions of this theorem $\langle S^m \rangle^\# Q \subset P$ where m is a sufficiently large positive integer. Similarly $\langle T^n \rangle^\# P \subset Q$ where now n is sufficiently large. In order to apply Klein's Lemma it remains to notice that since $\{0\} \neq S_+ \subseteq P$ and $S_+ \cap Q = \{0\}$ we have that $P \neq Q$. Clearly both $\langle S^m \rangle$ and $\langle T^n \rangle$ have infinite order which finishes this proof □

One can now wonder if a mixed situation is possible. Clearly the answer is positive as long as the necessary intersection requirements are fulfilled. Also since we will be using a generalized transvection we will have to induce the usual restriction on the locally compact field F as well.

Theorem 3.3.5. *Let F be a locally compact field and V be a finite-dimensional F-vector space. Suppose $S, T : V \to V$ are two nonsingular operators. Specifically S is diagonalizable with $V = S_+ \oplus S_0 \oplus S_-$ an S-decomposition of V. Furthermore $T = 1 + b\tau$ is a generalized transvection with $\tau : V \to V$ a nonzero operator with square 0. Also set $I = \tau(V) = \text{im}\ (\tau)$ and $K = \ker(\tau)$. Also assume that $|n| \geq 1$ for every $n \in 1\mathbb{Z}\backslash\{0\}$. If now the four intersections $S_\pm \cap K$ and $I \cap (S_0 \oplus S_\pm)$ are trivial then for a sufficiently large integer m and $b \in F$ with sufficiently large absolute value, we have $\langle S^m, T \rangle = \langle S^m \rangle * \langle T \rangle$.*

Proof. Complete similar to the proof of Theorems 3.3.2 and 3.3.4 set $2\kappa > 0$ the smallest of the four distances $d(I, S_0 \oplus S_\pm)$ and $d(S_\pm, K)$. Now define

$$P = \overline{\mathfrak{N}}_\kappa(S_+) \cup \overline{\mathfrak{N}}_\kappa(S_-) \qquad \text{and} \qquad Q = \overline{\mathfrak{N}}_\kappa(I).$$

By the triviality of the second two intersections $\langle S^m \rangle^\# Q \subset P$ with m sufficiently large and by the triviality of the first to intersections $\langle T \rangle^\# P \subset Q$, where now $a \in F$ has sufficiently large absolute values. Finally we again notice that $\{0\} \neq I \subset Q$ and $I \cap P = \{0\}$ such that $P \neq Q$. It was also observed in the previous theorem that $\langle S^m \rangle^\#$ is infinite cyclic such that the Ping-pong lemma is once more applicable. □

3.4 Free product of linear subgroups with operators having attractors

In the previous section we have extensively investigated when a group generated by two specific nonsingular operators is naturally isomorphic to the free product of the two cyclic groups generated by both operators. Now a final question arrises whether or not this can be generalized even further. For example if $S = 1 + a\sigma$ is a generalized transvection and G is a finite subgroup of the general linear group $\mathrm{GL}(V)$, can we find a positive integer n such that $\langle S^n, G\rangle$ is naturally isomorphic to $\langle S^n\rangle * G$, a non-abelian free group? For this we would again like to apply the Ping-pong Lemma and lift the criteria found there to obtain necessary conditions such that the answer to our question is possitive. Again S has an attractor I, where $I = \mathrm{im}\ \sigma$, and a "blockade" $K = \ker \sigma$. Now g is an operator in G then we trivially have that gI is an attractor of g with I as a repulser. As this is automatically the case no intersection requirement will have to be bestowed on I. However we will need gI to be a repulser of S and therefore $gI \cap K$ needs to be trivial. This requirements needs to be fulfilled for every $g \in G$ in order to apply the Ping-pong Lemma on S and G. The exact mathematical computations of this idea will be the subject of this section. First to ensure that elements close to I in a projective sense are also repulsed close to gI we will need the following lemma.

Lemma 3.4.1. *Let F be a locally compact field and V be a finite-dimensional F-vector space. Suppose $T : V \to V$ is a nonsingular linear transformation and let X and Y be projective subsets of V. Then*

$$d(T(X), T(Y)) \leq 2d(X, Y)\|T\|\|T^{-1}\|.$$

In particular, if $0 \neq x \in V$, then

$$d(T(x), T(Y)) \leq 2d(x, Y)\|T\|\|T^{-1}\|.$$

Proof. Take $x \in X \cap \mathbf{S}$ and $y \in Y \cap \mathbf{S}$ arbitrary . Then

$$d(T(X), T(Y)) \leq d(T(x), T(y)) \leq \frac{2\|T(x-y)\|}{\|T(x)\|},$$

where we again used Lemma 3.1.2(iii). Now $\|T(x-y)\| \leq \|T\|\|x-y\|$, and $x = T^{-1}(T(x))$ which implies that $1 = \|x\| \leq \|T^{-1}\|\|T(x)\|$. It follows that

$$d(T(X), T(Y)) \leq 2\|x-y\|\|T\|\|T^{-1}\|.$$

Because x, respectively y, was chosen arbitrarily in $X \cap \mathbf{S}$, respectively $Y \cap \mathbf{S}$, and since $d(X, Y) = \inf\{\|x-y\| \mid x \in X \cap \mathbf{S}, y \in Y\mathbf{S}\}$ we now see that

$$d(T(X), T(Y)) \leq 2d(X, Y)|\|T\|\|T^{-1}\|.$$

The second inequality now follows from this one which proves the lemma. □

This enables us to prove our fist mixed situation where G is a finite subgroup of the general linear group and S is a generalized transvection.

Theorem 3.4.2. *Let F be a locally compact field and V be a finite-dimensional F-vector space. Suppose G is a non identity finite subgroup of the general linear group $\mathrm{GL}(V)$. Furthermore let $S = 1 + a\sigma$ be a generalized transvection where $\sigma = V \to V$ is a nonzero operator of square 0. Assume that $o(G) > 2$ when $\mathrm{char}\, F = 2$ and that $|n| \geq 1$ for every $n \in 1\mathbb{Z} \setminus \{0\}$. Now set $I = \sigma(V) = \mathrm{im}\ (\sigma)$ and $K = \ker(\sigma)$. If all the intersections $gI \cap K$ are trivial for all $g \in G^{\#}$, then for all $a \in F$ with sufficiently large absolute value, we have $\langle G, S\rangle = G * \langle S\rangle$.*

Proof. Let 2κ be the minimum of the finitely many distances $d(gI, K)$ for all $g \in G^{\#}$. Then again using Lemma 3.1.2(i) we see that $\kappa > 0$. Now let $r = \max\{2\|g\|\|g^{-1}\| \mid g \in G^{\#}\}$ and take $\epsilon = \kappa/r$. We then again define a duo of attracting and repulsing sets by setting

$$P = \bigcup_{g \in G^{\#}} \overline{\mathfrak{N}}_{\kappa}(gI) \qquad \text{and} \qquad Q = \overline{\mathfrak{N}}_{\epsilon}(I).$$

Now let g be a non identity of G and $v \in Q$. Then $d(v, I) \leq \epsilon$. Therefore, using the previous lemma, we have

$$d(gv, gI) \leq 2\|g\|\|g^{-1}\|\epsilon \leq r\epsilon = k,$$

so $gv \in \overline{\mathfrak{N}}_\kappa(gI) \subseteq P$, which shows that $G^\# Q \subseteq P$. Also from Proposition 3.2.4 we know that I is an attractor of S and for all the finitely many subspace gI, with $g \in G^\#$ we see that there exists a positive real number s_g such that if $|a| \geq s_g$ then $S\overline{\mathfrak{N}}_\kappa(gI) \subseteq \overline{\mathfrak{N}}_\epsilon(I) = Q$. Thus if we take $|a| \geq s$ where $s = \max\{s_g \mid g \in G^\#\}$ we find that $SP \subset Q$. Even more since $S^n = 1 + na\sigma$ and $|na| \geq |a|$ for all $n \in 1\mathbb{Z} \setminus \{0\}$, we have $\langle S\rangle^\# P \subset Q$. Finally noticing that $I \subseteq Q$ but $I \cap P = \{0\}$ by the definition of κ and the fact that $I \subseteq K$, we obtain that $P \neq Q$. Also either G or $\langle S\rangle$ has order strictly larger then 2 such that we can conclude from the Ping-pong Lemma that $\langle G, S\rangle = G * \langle S\rangle$ and the proof is finished. □

Clearly the same technique can be applied for the situation where T is a diagonalizable operator. For every non identity element g in G we will now have two distinct repulsers T_+ and T_- and hence two distinct attractors namely gT_+ and gT_-. Consequently again we will have double the intersection requirements but no conditions set on the locally compact field F itself. To conclude this section we have.

Theorem 3.4.3. *Let F be a locally compact field and V be a finite-dimensional F-vector space. Suppose G is a non identity finite subgroup of the general linear group* $\mathrm{GL}(V)$*. Furthermore let $T : V \to V$ be a nonsingular diagonalizable operator with $V = T_+ \oplus T_0 \oplus T_-$ a T-decomposition of V. If for every $g \in G^\#$ the intersections $gT_\pm \cap T_0 \oplus T_\pm$ are trivial, then for a sufficiently large integers n we have $\langle G, T^n\rangle = G * \langle T^n\rangle$.*

Proof. Let $2\kappa > 0$ be the minimum of the finitely many distances $d(gT_+, T_0 \oplus T_-)$, $d(gT_-, T_0 \oplus T_-)$, $d(gT_+, T_+ \oplus T_0)$ and $d(gT_-, T_+ \oplus T_0)$ for all $g \in G^\#$. Let $t = \max\{2\|g\|\|g^{-1}\| \mid g \in G^\#\}$ and set $\epsilon = \kappa/t$. Then define

$$P = \bigcup_{g \in G^\#} \overline{\mathfrak{N}}_\kappa(gT_+) \cup \bigcup_{g \in G^\#} \overline{\mathfrak{N}}_\kappa(gT_-) \qquad \text{and} \qquad Q = \overline{\mathfrak{N}}_\epsilon(T_+) \cup \overline{\mathfrak{N}}_\epsilon(T_-).$$

First let g be an arbitrary non identity element of G and $v \in Q$. Then v is either in $\overline{\mathfrak{N}}_\epsilon(T_+)$ or in $\overline{\mathfrak{N}}_\epsilon(T_-)$. Suppose the first then $d(v, T_+) \leq \epsilon$. By lemma 3.4.1 we obtain that

$$d(gv, gT_+) \leq 2\|g\|\|g^{-1}\|\epsilon \leq t\epsilon = \kappa.$$

This shows that gv is an element of $\overline{\mathfrak{N}}_\kappa(gT_+) \subseteq P$. Similarly if v would have been an element of $\overline{\mathfrak{N}}_\epsilon(T_-)$ we would have obtained that $gv \in \overline{\mathfrak{N}}_\kappa(gT_-)$. Since $g \neq 1$ was chosen arbitrarily we get that $G^\# Q \subseteq P$. From Propositions 3.2.2 and 3.2.3 we know that T_+ is an attractor for T while T_- is an attractor for T^{-1}. For each non identity element g in G we can find a positive n_g such that for every larger positive integer n we have that $T^n\overline{\mathfrak{N}}_\kappa(gT_\pm) \subseteq \overline{\mathfrak{N}}_\epsilon(T_+)$ and $T^{-n}\overline{\mathfrak{N}}_\kappa(gT_\pm) \subseteq \overline{\mathfrak{N}}_\epsilon(T_-)$. If we now take $n' = \max\{n_g \mid g \in G^\#\}$ we see that for every $n \geq n'$ we have that $\langle T^n\rangle^\# P \subseteq Q$. Also $\langle T^n\rangle$ is infinite cyclic and since $T_+ \subset Q$ and $T_+ \cap P = \{0\}$ so that $P \neq Q$. This allows to apply the Ping-pong Lemma one last time to obtain that $\langle G, T^n\rangle = G * \langle T^n\rangle$. □

3.5 Intersection requirements expressed via idempotent conditions

We spend the remainder of this chapter rewriting the requirements for diagonalizable operators in Theorem 3.3.4. First take a look at the intersections $S_+ \cap (T_0 \oplus T_+)$ and $T_- \cap (S_0 \oplus S_+)$. Since the first intersection is taken to be trivial this implies that $\dim S_+ \leq \dim T_-$. Conversely as also the second intersection is required to be trivial we also have $\dim S_+ \geq \dim T_-$. Using the other intersection requirements we see that $\dim S_+ = \dim S_- = \dim T_+ = \dim T_- = r$ which will refer to as the "dimensionality requirements". Secondly let us now define the

following four projections $\sigma_+ : V \to S_+$, $\sigma_- : V \to S_-$, $\tau_+ : V \to T_+$ and $\tau_- : V \to T_-$ clearly all of rank r. Let us once more observe the intersection $S_+ \cap (T_0 \oplus T_+)$. The triviality of this intersection also implies that $\tau_- \circ \sigma_+$ which we will denote by $\sigma_+\tau_-$ has rank r as $T_0 \oplus T_+$ is the kernel of τ_-. Using the seven other intersection requirements we obtain the eight "idempotent conditions" rank $\sigma_\pm\tau_\pm = r = \text{rank } \tau_\pm\sigma_\pm$. We will no show that these *dimensionality requirements* together with the *idempotent condition* will also imply the eight intersection in Theorem 3.3.4 to be trivial. These formulations will be more convenient to verify when looking at applications in integral group rings.

Corollary 3.5.1. *Let F be a locally compact field and V be a finite-dimensional F-vector space. Suppose $S, T : V \to V$ are two nonsingular diagonalizable operators such that $V = S_+ \oplus S_0 \oplus S_-$ and $V = T_+ \oplus T_0 \oplus T_-$ are an S- and a T-decomposition of V. Assume that $\dim S_+ = \dim S_- = r = \dim T_+ = \dim T_-$ and consider the four projections $\sigma_+ : V \to S_+$, $\sigma_- : V \to S_-$, $\tau_+ : V \to T_+$ and $\tau_- : V \to T_-$. If the eight idempotent conditions $\text{rank } \sigma_\pm\tau_\pm = r = \text{rank } \tau_\pm\sigma_\pm$ hold, then $\langle S^m, T^n \rangle = \langle S^m \rangle * \langle T^n \rangle$ for all sufficiently large positive integers m and n.*

Proof. We will show how one of the idempotent conditions will imply one of the intersection requirements. For instance assume that $\text{rank } \sigma_+\tau_+ = r = \text{rank } \tau_+\sigma_+$. This implies that $\tau_+(\sigma_+(V)) = V\sigma_+\tau_+ = V\tau_+ = \tau_+(V)$. Thus the restriction of $\tau_+ : V\sigma_+ \to V\tau_+$ is onto and by the finite dimensionality also one-to-one. This means that the kernel of τ_+ is zero in $V\sigma_+ = S_+$. In other words $S_+ \cap (T_0 \oplus T_-) = \{0\}$. By using the same method one can show that the remaining seven idempotent conditions will yield the remaining intersection requirements necessary for using Theorem 3.3.4. This concludes the proof. □

We can also find similar idempotent conditions based on suitable projections for Theorems 3.3.2 and 3.3.5, but these maps are not canonically defined. This concludes our study of free products of groups generated by operators.

Chapter 4

Representation of Bass cyclic units

This chapter will form a bridge between the constructions of free groups in linear groups found in the previous chapter and its applications to the unit group of an integral group $\mathbb{Z}[G]$. Specifically we would like to know if for "some types of groups" $\mathcal{U}(\mathbb{Z}[G])$ contains a "certain couple of units" such that the group generated by these two elements is free of rank 2. The units we will be studying are called Bass cyclic units. These are units of the form

$$u_{k,m}(g) = (1 + g + g^2 + \ldots + g^{k-1})^m + \frac{1-k^m}{d}(1 + g + g^2 + \ldots + g^{d-1}),$$

where g is an element of G having order $o(g) = d$, k is a strictly positive integer relatively prime to d and m is a multiple of the Euler function $\varphi(d)$. These latter two conditions imply that $k^m \equiv 1 \bmod d$. Clearly this shows that $u_{k,m}(g)$ is an element of $\mathbb{Z}\langle g\rangle \subseteq \mathbb{Z}[G]$. Next recall the augmentation map $g \mapsto 1$ from $\mathbb{Z}\langle g\rangle$ to $\mathbb{Z}$, then each $u_{k,m}(g)$ has augmentation 1 and we can write

$$u_{k,m}(g) = (1 + g + g^2 + \ldots + g^{k-1})^m + c\hat{g},$$

where $\hat{g} = \sum_{i=0}^{d-1} g^i$ and c is the unique integer such that this element has augmentation 1. Notice that $g^j\hat{g} = \hat{g}g^j = \hat{g}$ for every integer j, so that finally we can observe the inverse of $u_{k,m}(g)$ in $\mathbb{Z}[G]$ which will be equal to

$$\begin{aligned} u_{k,m}(g)^{-1} = u_{l,m}(g^k) &= (1 + g^k + g^{2k} + \ldots + g^{k(l-1)})^m + \frac{1-l^m}{d}\widehat{g^k} \\ &= (1 + g^k + g^{2k} + \ldots + g^{k(l-1)})^m + c'g^k\hat{g} \\ &= (1 + g^k + g^{2k} + \ldots + g^{k(l-1)})^m + c'\hat{g}, \end{aligned}$$

with $kl \equiv 1 \bmod d$. Now $\mathbb{Z}[G]$ is contained in the complex group algebra $\mathbb{C}[G]$ and the irreducible representations from this algebra are homomorphisms θ from $\mathbb{C}[G]$ to a suitable matrix ring $\mathrm{M}_n(\mathbb{C})$. If g is an element of G with order d then the order of $\theta(g) = \overline{g}$ will divide d and as such the polynomial $x^d - 1$ will kill $\overline{g}$. Moreover this implies that the minimal polynomial which annihilates $\overline{g}$ is a divisor of $x^d - 1$. We know this latter polynomial splits over $\mathbb{C}$ and it has distinct roots. Clearly the same then holds for the minimal polynomial and we see from [LN97, Lemma 2.57] that this implies $\overline{g}$ is diagonalizable. Even more so, since the characteristic polynomial and the minimal polynomial share the same roots up to a higher multiplicity, the eigenvalues of $\overline{g}$ are all dth roots of unity. It now follows that $\theta(u_{k,m}(g)) = u_{k,m}(\overline{g})$ is diagonalizable with eigenvalues equal to $u_{k,m}(\varepsilon)$ where ε runs trough the eigenvalues of $\overline{g}$. Now if $u_{r,s}(h)$ is another Bass cyclic unit which is mapped onto $u_{r,s}(\overline{h})$ under θ, then this operator is also diagonalizable and we could ask ourselves whether or not the group $\langle u_{k,m}(\overline{g}), u_{r,s}(\overline{h})\rangle$ generated by these two elements is naturally isomorphic to the non-abelian free group $\langle u_{k,m}(\overline{g})\rangle * \langle u_{r,s}(\overline{h})\rangle$. If this would be the case then

$\langle u_{k,m}(g), u_{r,s}(h)\rangle$ will surely also be free of rank 2. Fortunately we have readily acquired criteria for the image operators $T = u_{k,m}(\overline{g})$ and $S = u_{r,s}(\overline{h})$, the first requirement being that $\mathbb{C}^n$ has a T-decomposition $T_+ \oplus T_0 \oplus T_-$ and an S-decomposition $S_+ \oplus S_0 \oplus S_-$ such that $r = \dim T_+ = \dim T_- = \dim S_+ = \dim S_- \neq 0$. Since the constructions of these four spaces depend on the absolute values of the eigenvalues of both operators it is interesting to first study them. Clearly two questions of interest arrise.

(I) For which dth roots of unity ε is $|u_{k,m}(\varepsilon)|$ maximal and for which ones is this value minimal?

(II) If ε_1 and ε_2 are two dth roots of unity, when is $|u_{k,m}(\varepsilon_1)| = |u_{k,m}(\varepsilon_2)|$?

The first question (I) can aid us in knowing how low we can take the dimension r. The second one (II) can help answer the question wether or not it is possible to choose the dimensions of T_+, T_-, S_+ and S_- to be equal, let alone different from 0. The goal of this chapter will be to describe how this will all exactly pan out.

4.1 Construction of Bass cyclic units by means of cyclotomic units

We start by giving a structural description of Bass cyclic units as this gives some nice intuition how one came about defining these specific units. To show this we will first need to know the description of the rational group algebra $\mathbb{Q}\langle g\rangle$ where g has finite order. Afterwards we will use $\mathbb{Z}$-orders to show why Bass units are indeed units in $\mathbb{Z}[G]$. So let G be a finite group and g an element of order d. Now consider the map

$$\varphi : \mathbb{Q}[x] \to \mathbb{Q}\langle g\rangle : x \mapsto g.$$

This map is clearly a ring epimorphism and by the first isomorphism theorem we obtain

$$\mathbb{Q}\langle g\rangle \cong \frac{\mathbb{Q}[x]}{\ker \varphi}.$$

Even more using the fact that $\mathbb{Q}[x]$ is a principal ideal domain we can prove that $\ker \varphi = (x^d - 1)$. Moving on it is well know that $x^d - 1$ decomposes in $\mathbb{Q}[x]$ as a product of cyclotomic polynomials, i.e.

$$x^d - 1 = \prod_{\substack{1 \leq n \leq d \\ n|d}} \phi_n(x),$$

where $\phi_n(x) = \prod_{(k,n)=1, 1 \leq k < n}(x - \varepsilon_n^k)$ and $\varepsilon_n = e^{2\pi i/n}$ is a primitive nth root of unity. The Chinese remainder theorem now tells us

$$\mathbb{Q}\langle g\rangle \cong \prod_{\substack{1 \leq n \leq d \\ n|d}} \frac{\mathbb{Q}[x]}{\phi_n(x)}.$$

Finally one can now consider the ring epimorphism

$$\varphi' : \mathbb{Q}[x] \to \mathbb{Q}[\varepsilon_n] : x \mapsto \varepsilon_n.$$

then using the same remarks as earlier one shows that $\ker \varphi' = \phi_n(x)$. This now proves the following isomorphism of $\mathbb{Q}\langle g\rangle$ as a direct product of cyclotomic fields.

$$\mathbb{Q}\langle g\rangle \cong \prod_{\substack{1 \leq n \leq d \\ n|d}} \mathbb{Q}[\varepsilon_n].$$

As a corollary there exists an embedding s from $\mathbb{Z}\langle g\rangle$ to $\prod_{n|d,1\leq n\leq d}\mathbb{Z}[\varepsilon_n]$. Unfortunately this embedding s does not have to be an isomorphism in general. For example take $\mathbb{Q}\langle x\rangle$ where x has order 2 then from the above

$$\mathbb{Q}\langle x\rangle \cong \mathbb{Q}[1]\times\mathbb{Q}[-1]\cong\mathbb{Q}\times\mathbb{Q}.$$

However $\mathbb{Z}\times\mathbb{Z}$ contains a non trivial idempotent, for example $(0,1)$ while surely $\mathbb{Z}\langle x\rangle$ does not. To see this take $a+bx$ an element in $\mathbb{Z}\langle x\rangle$ such that $(a+bx)=(a+bx)^2=(a^2+b^2)+2abx$. It follows that $a^2+b^2=a$ and $2ab=b$ which can only be the case if $b=0$ and a is equal to 0 or 1, thus $a+bx=0$ or $a+bx=1$. So $\mathbb{Z}\langle x\rangle$ can not be isomorphic to $\mathbb{Z}\times\mathbb{Z}$. More generally one can show that $\mathbb{Z}[G]$, for G a finite group, contains no non-trivial idempotents. Continuing on, by identifying $\mathbb{Z}\langle g\rangle$ with its image under s, we can assume

$$R_1=\mathbb{Z}\langle g\rangle\subseteq\prod_{\substack{1\leq n\leq d\\ n|d}}\mathbb{Z}[\varepsilon_n]=R_2.$$

Since both of these rings are $\mathbb{Z}$-orders, see [PMS02, Definition 2.91], we know by Lemma 2.9.5 of [PMS02] that if we can find an element $u\in R_1$ which is invertible in R_2 then u is also invertible in R_1 and thus a unit. Now clearly u is a unit in the latter ring if and only if all of its projections are units in there respective components. So when searching for units in $Z\langle g\rangle$, in order to apply the techniques explained here, one first needs to search for units in $\mathbb{Z}[\varepsilon_n]$. Now if k is a natural number greater or equal to 1 and relatively prime to n then

$$u_k(\varepsilon_n)=\frac{\varepsilon_n^k-1}{\varepsilon_n-1}=1+\varepsilon_n+\ldots+\varepsilon_n^{k-1},$$

with $\varepsilon_n\neq 1$. Such a unit in $\mathbb{Z}[\varepsilon_n]$ is called a cyclotomic unit with inverse

$$u_k(\varepsilon_n)^{-1}=\frac{\varepsilon_n-1}{\varepsilon_n^k-1}=\frac{\varepsilon_n^{kl}-1}{\varepsilon_n^k-1}=1+\varepsilon_n^k+\ldots\varepsilon_n^{k(l-1)},$$

where $kl\equiv 1 \bmod n$. So we could take

$$u_k(g)=1+g+g^2+\ldots+g^{k-1},$$

in $\mathbb{Z}\langle g\rangle$ where k is relatively prime to d and thus to all divisors of d. From the previous it follows that $u_k(g)$ projects, in every component, to an element $1+\varepsilon_n+\ldots+\varepsilon_n^{k-1}\in\mathbb{Z}[\varepsilon_n]$ which is a unit when $\varepsilon_n\neq 1$. However in the first component where ε_n is equal to 1 the projection is in fact the augmentation map from R_2 to $\mathbb{Z}$ and it is clear that the augmentation of $u_k(g)$ equals k which is definitely not a unit in $\mathbb{Z}$. So in closure we consider the element

$$u_{k,m}(g)=(1+g+g^2+\ldots+g^{k-1})^m+\frac{1-k^m}{d}(1+g+g^2+\ldots+g^{d-1}),$$

where k is a strictly positive integer relatively prime to d and m is a multiple of the Euler function $\varphi(d)$. We now see that $(1+g+g^2+\ldots+g^{d-1})$ project to 0 in every component where $\varepsilon_n\neq 1$ such that the projection of $u_{k,m}(g)$ is still a unit in these components. Also by the choice of $c=\frac{1-k^m}{d}$ this element has augmentation 1 and this is also a unit in the first component, namely $\mathbb{Z}$. It follows that $u_{k,m}(g)$ is a unit in R_2 and by the aforementioned lemma also in $R_1=\mathbb{Z}\langle g\rangle\subseteq\mathbb{Z}[G]$. Moreover from the inverse element $u_k(\varepsilon_n)^{-1}$ in $\mathbb{Z}[\varepsilon_n]$ we readily see

$$u_{k,m}(g)^{-1}=u_{l,m}(g^k)=(1+g^k+g^{2k}+\ldots+g^{k(l-1)})^m+\frac{1-l^m}{d}\widehat{g^k}.$$

Let us now introduce some basic properties of Bass cyclic units which will be relevant for future calculations.

Proposition 4.1.1. *With the notation for Bass cyclic units as above, we have the following conditions on the parameters k,l, m and n.*

(i) $u_{k+d,m}(g) = u_{k,m}(g)$.

(ii) $u_{k,m}(g)u_{k,n}(g) = u_{k,(m+n)}(g)$.

(iii) $u_{k,m}(g)u_{l,m}(g^k) = u_{kl,m}(g)$.

(iv) $u_{1,m}(g) = 1$ *and* $u_{k,m}(g)^{-1} = u_{l,m}(g^k)$ *where* $kl \equiv 1 \bmod d$.

Proof. It is sufficient to proof the assertions for $u_{k,m}(\varepsilon)$ where ε is a primitive dth root of unity. The four equation now become clear since $u_{k,m}(\varepsilon) = ((\varepsilon^k - 1)/(\varepsilon - 1))^m$. For completeness' sake we will show why the first three equation *(i)*, *(ii)* and *(iii)* are valid. Equation *(iv)* is just a summary of the previous explanation.
(i) For the first equation we get

$$u_{k+d,m}(\varepsilon) = \left(\frac{\varepsilon^{k+d} - 1}{\varepsilon - 1}\right)^m = \left(\frac{\varepsilon^k - 1}{\varepsilon - 1}\right)^m = u_{k,m}(\varepsilon).$$

(ii) The second product formula is obtain by

$$u_{k,m}(\varepsilon)u_{k,n}(\varepsilon) = \left(\frac{\varepsilon^k - 1}{\varepsilon - 1}\right)^m \left(\frac{\varepsilon^k - 1}{\varepsilon - 1}\right)^n = \left(\frac{\varepsilon^k - 1}{\varepsilon - 1}\right)^{m+n} = u_{k,m+n}(\varepsilon).$$

(iii) To see why the third equation is valid notice that

$$u_{k,m}(\varepsilon)u_{l,m}(\varepsilon^k) = \left(\frac{\varepsilon^k - 1}{\varepsilon - 1}\right)^m \left(\frac{\varepsilon^{kl} - 1}{\varepsilon^k - 1}\right)^m = \left(\frac{\varepsilon^{kl} - 1}{\varepsilon - 1}\right)^m = u_{kl,m}(\varepsilon).$$

□

In view of *(i)* we see that $u_{k,m}(g)$ is determined by k modulo d so that we can assume that $1 \leq k \leq d-1$. Moreover $u_{1,m}(g) = 1$ and $u_{d-1,m}(g) = (-g^{(d-1)})^m$, so if we want non trivial units we take $2 \leq k \leq d-2$. Now since k has to be relatively prime to d this implies that $d \geq 5$. Finally notice that (ii) implies $u_{k,m}(g)^a = u_{k,ma}(g)$ for all strictly positive integers a. We now prove a fairly easy lemma stating that if we have a ring homomorphism $\theta : \mathbb{Z}[G] \to \mathbb{Z}[H]$ which is actually determined by the group epimorphism $\theta : G \to H$ then we can retract Bass cyclic units $u_{k,m}(y)$ found in $\mathbb{Z}[H]$ to obtain "nice" Bass cyclic units $u_{k,m'}(x)$ in our first integral group ring. Here *nice* means $u_{k,m'}(x)$ maps to a positive power of $u_{k,m}(y)$. This will be useful for finding free groups of rank 2 generated by two Bass cyclic units.

Lemma 4.1.2. *Let $\theta : \mathbb{Z}[G] \to \mathbb{Z}[H]$ be the group ring homomorphism determined by the group epimorphism $\theta : G \to H$, and let y be an element in H of order $o(y)$. If $u_{k,m}(y)$ is a Bass cyclic unit of $\mathbb{Z}[H]$, then there exists an element $x \in G$, whose order has the same prime factors as those of y, and a Bass cyclic unit $u_{k,m'}(x)$ of $\mathbb{Z}[G]$ such that $u_{k,m'}(x)$ maps to a positive integer power of $u_{k,m}(y)$.*

Proof. Take y an element of H with order $o(y) = p_1^{k_1} \dots p_n^{k_n}$. Since θ is a group epimorphism there exist a $z \in G$ such that $\theta(z) = y$. Then z has order $o(z)$ with $o(y) \mid o(z)$. Thus

$$o(z) = (p_1^{k'_1} \dots p_n^{k'_n})(p_{n+1}^{k'_{n+1}} \dots p_{n+s}^{k'_{n+s}}) = uv,$$

where $o(y) \mid u$. Since $\gcd(u, v) = 1$ we know there exists integers r and s such that $1 = ru + sv$. Thus $y = y^{ru}y^{sv} = y^{sv}$. Naturally $\theta(z^{sv}) = y^{sv} = y$ and $(z^{sv})^u = 1$. It follows that the order $o(z^{sv})$ divides u. We thus have that $x = z^{sv}$ is an element which maps onto y under θ such that its order $o(x)$ has the same prime factors as the order y. Now if $u_{k,m}(y)$ is a Bass

cyclic unit in $\mathbb{Z}[H]$ then $\gcd(k, o(y)) = 1$ and as such $\gcd(k, o(x)) = 1$. Clearly there now exists a positive integer a such that $\varphi(o(x))$ divides $m' = ma$. We now have that $u_{k,m'}(x)$ is a Bass cyclic unit and since $o(y) \mid o(x)$ we have that $\theta(\hat{x})$ is an integer multiple of $\hat{y}$. From the basic properties it follows that $\theta(u_{k,m'}(x))$ and $u_{k,m}(y)^a$ agree up to an integer multiple of $\hat{y}$, say $c\hat{y}$. Since both of these terms have augmentation 1, we conclude that $c = 0$, and both elements are equal as required. □

So assume we can find two Bass cyclic units $u_{k,m}(y)$ and $u_{r,s}(y')$ in $\mathbb{Z}[H]$ such that the group generated by these two elements is of rank 2. If this is the case we can find two Bass cyclic units $u_{k,m'}(x) \mapsto u_{k,m}(y)$ and $u_{r,s'}(x') \mapsto u_{r,s}(y')$ so that clearly $\langle u_{k,m'}(x), u_{k,m}(y)\rangle = \langle u_{k,m'}(x)\rangle * \langle u_{r,s'}(x')\rangle$. Thus the problem of finding Bass cyclic units in $\mathbb{Z}[G]$ such that the group generated by these elements is free of rank 2 is reduced to finding such units in the "smaller" integral group ring $\mathbb{Z}[H]$. This concludes our brief introduction.

4.2 Maximality condition for the absolute values of eigenvalues

We now start with addressing the first problem (I) mentioned in our introduction. We would like to know for which dth roots of unity ε the value $|u_{k,m}(\varepsilon)|$ is maximal/minimal. As mentioned earlier this could help us determine the dimensionality of the attractors. Before we can answer our question we will first need the following technical lemma. The original proof and the proof of all following lemma's where found in [GP06].

Lemma 4.2.1. *Let k be a real numbers with $2 \leq k$. Define the real-valued function*

$$f :]0, 1/2] \to \mathbb{R}^+ : z \mapsto \left| \frac{\sin(k\pi z)}{\sin(\pi z)} \right|.$$

Then for every $r \in]0, 1/(2k)]$ we have that $\max\{f(z) \mid z \in [r, 1/2]\} = f(r) > 1$.

Proof. Let us first examine the function f on the open interval $]0, 1/k[$. Clearly both the nominator and denominator are strictly positive so the absolute value can be omitted. Furthermore let z be an element of the half closed, half open interval $[1/(2k), 1/k[$. As z increases through this interval $x = k\pi z$ will increase through the interval $[\pi/2, \pi[$ and as a consequence the numerator $\sin x$ decreases. Also $y = \pi z$ will increase trough the interval $[\pi/(2k), \pi/k[\subseteq]0, \pi/2[$ which will imply that the denominator $\sin y$ will increase. It follows that f strictly decreases on the interval $[1/(2k), 1/k[$. On the other hand if $z \in]0, 1/(2k)[$ then

$$\begin{aligned} \frac{\partial f(z)}{\partial z} &= \frac{k\pi \cos(k\pi z)\sin(\pi z) - \pi \cos(\pi z)\sin(k\pi z)}{\sin^2(\pi z)} \\ &= \left(\frac{\pi \cos(k\pi z)\cos(\pi z)}{\sin(k\pi z)\sin(\pi z)} \right) (k \tan(\pi z) - \tan(k\pi z)) \end{aligned}$$

where the first term is strictly positive, since all trigonometric functions are positive, and, by looking at the Taylor expansions of tan around 0 and using the fact that $2 \leq k$, the second term is strictly negative. It again follows that f is strictly decreasing to 0 on the interval $]0, 1/(2k)[$ and as such by the first part on the entire interval $]0, 1/k[$. Since r is chosen in this interval we have that $f(r) > f(z)$ for all $z \in]r, 1/k[$. It thus remains to compare $f(r)$ with the values $f(z)$ where $z \in [1/k, 1/2]$. First from the Taylor expansion of sin around 0 we can see that for every $x \geq 0$ we have that $x \geq \sin x \geq x - x^3/6 = x(1 - x^2/6)$. This shows

$$\sin(k\pi r) \geq k\pi r \left(1 - \frac{(k\pi r)^2}{6}\right) \geq k\pi r \left(1 - \frac{\pi^2}{24}\right),$$

where we used that $kr \leq 1/2$. For de denominator we have $\sin \pi r \leq \pi r$ and we obtain

$$f(r) = \frac{\sin(k\pi r)}{\sin(\pi r)} \geq \frac{k\pi r(1-\pi^2/24)}{\pi r} = k\left(1 - \frac{\pi^2}{24}\right).$$

Using the fact that $2 \leq k$ we have $f(r) \geq 2(1-\pi^2/24) > 1.177 > 1$. On the other hand if $z \in [1/k, 1/2]$, then $|\sin k\pi z| \leq 1$ and

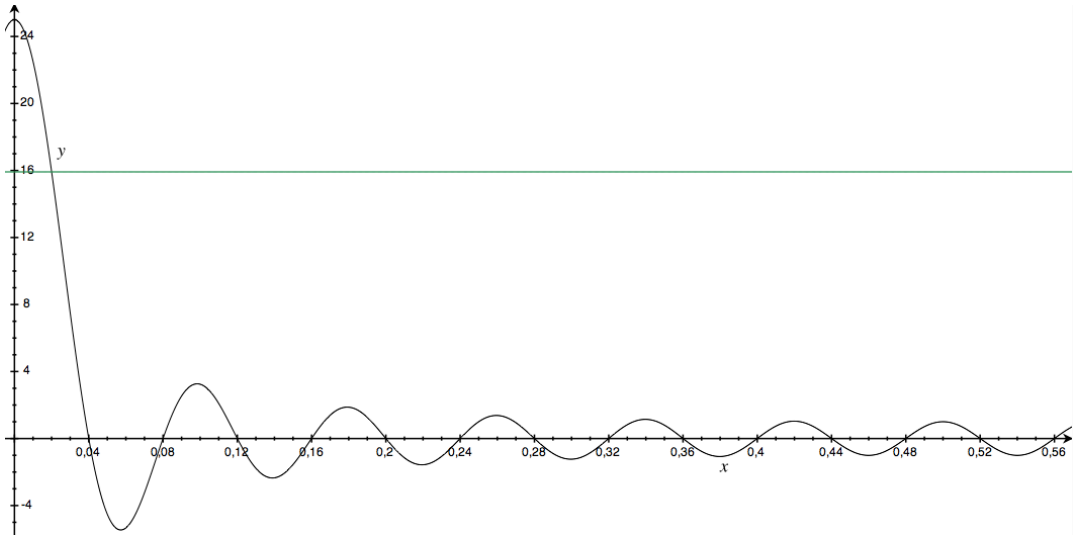
$$\sin(\pi z) \geq \sin\left(\frac{\pi}{k}\right) \geq \frac{\pi}{k}\left(1 - \frac{(\pi/k)^2}{6}\right) \geq \frac{\pi}{k}\left(1 - \frac{\pi^2}{24}\right),$$

again using the lower bound $2 \leq k$. We now have $\pi(1-\pi^2/24)^2 > 1.089 > 1$, we finally have

$$f(z) = \left|\frac{\sin(k\pi z)}{\sin(\pi z)}\right| \leq \frac{k}{\pi(1-\pi^2/24)} < k\left(1 - \frac{\pi^2}{24}\right) \leq f(r),$$

where $z \in [1/k, 1/2]$. This completes the proof of our lemma. □

The next image shows a computer plot of $f(z) = \sin(k\pi z)/\sin(\pi z)$ with $k = 25$. Clearly the function drops *rapidly* from $f(0) = k$ to $f(1/k) = 0$. Afterwards its stays relatively small in absolute value on the remaining interval $[1/k, 1/2]$. More precisely, in absolute value, it will be below the horizontal line which represents the value of $f(1/2k)$. Lemma 4.2.1 showed that this is a general phenomenon.



We now use this observation to prove our next lemma.

Lemma 4.2.2. *Let $\varepsilon = e^{2\pi i/d}$ be a primitive complex dth root of unity and let a be an integer. Assume that $2 \leq k \leq d-2$ and that $(k,d) = 1$.*

(i) $u_{k,m}(1) = 1$ and if $\varepsilon^a \neq 1$ then

$$|u_{k,m}(\varepsilon^a)| = \left|\frac{\varepsilon^{ak/2} - \varepsilon^{-ak/2}}{\varepsilon^{a/2} - \varepsilon^{-a/2}}\right|^m = \left|\frac{\sin(k\pi a/d)}{\sin(\pi a/d)}\right|^m$$

(ii) The largest absolute value $|u_{k,m}(\varepsilon^a)|$ occurs when $a \equiv \pm 1$ mod d.

(iii) The smallest absolute value $|u_{k,m}(\varepsilon^a)|$ occurs when $ak \equiv \pm 1$ mod d.

Proof. (i) First we have that $u_{k,m}(1) = k^m + (1-k^m)1$. So let $\varepsilon^a \neq 1$. Then clearly $\sum_{i=0}^{d-1}(\varepsilon^a)^i$ gives 0 and

$$u_{k,m}(\varepsilon^a) = \left(1 + (\varepsilon^a) + (\varepsilon^a)^2 + \ldots + (\varepsilon^a)^{k-1}\right)^m = \left(\frac{\varepsilon^{ak}-1}{\varepsilon^a - 1}\right)^m.$$

Now since $|\varepsilon^{a/2}| = 1$, this yields

$$|u_{k,m}(\varepsilon^a)| = \left|\frac{\varepsilon^{ak}-1}{\varepsilon^a-1}\right|^m = \left|\frac{\varepsilon^{ak/2}(\varepsilon^{ak/2}-\varepsilon^{-ak/2})}{\varepsilon^{a/2}(\varepsilon^{a/2}-\varepsilon^{-a/2})}\right|^m = \left|\frac{\varepsilon^{ak/2}-\varepsilon^{-ak/2}}{\varepsilon^{a/2}-\varepsilon^{-a/2}}\right|^m.$$

Note that numerator is twice the imaginary part of $\varepsilon^{ak/2}$ and the denominator twice the imaginary part of $\varepsilon^{a/2}$ so that by $\varepsilon^a = e^{2\pi i a/d} = \cos(2\pi a/d) + i\sin(2\pi a/d)$,

$$|u_{k,m}(\varepsilon^a)| = \left|\frac{\sin(k\pi a/d)}{\sin(\pi a/d)}\right|^m.$$

(ii) Again assume that $\varepsilon^a \neq 1$. Then by the symmetry of the sine function towards negatives we clearly have that $|u_{k,m}(\varepsilon^a)| = |u_{d-k,m}(\varepsilon^a)|$. This shows that, by replacing k by $d-k$ if necessary, we may assume $2 \leq k \leq d/2$. Furthermore since also

$$|u_{k,m}(\varepsilon^a)| = |u_{k,m}(\varepsilon^{-a})| = |u_{k,m}(\varepsilon^{d-a})| \tag{4.1}$$

we can take $a = 1, 2, \ldots, \lfloor d/2 \rfloor$. So let us consider the real-valued function

$$f :]0, 1/2] \to \mathbb{R}^+ : z \mapsto \left|\frac{\sin(k\pi z)}{\sin(\pi z)}\right|.$$

as in Lemma 4.2.1. We observe that $|u_{k,m}(\varepsilon^a)| = f(a/d)^m$ with $m > 0$. Furthermore if we set $r = 1/d$ then $rk = k/d \leq 1/2$ and a/d is contained in the closed interval $[r, 1/2]$. From the previous lemma we see that the maximum value of $f(z)$ on this interval is obtained for $z = r = 1/d$ which implies $a = 1$ and we also have $f(1/d) > 1$. So by keeping the equalities (4.1) in mind the largest absolute value of $|u_{k,m}(\varepsilon^a)|$ where $\varepsilon^a \neq 1$ occurs when $a \equiv \pm 1 \bmod d$. Since this absolute value is strictly larger then 1 and since $u_{k,m}(1) = 1$ we see that $|u_{k,m}(\varepsilon^{\pm 1})|$ is the maximum value of $|u_{k,m}(\varepsilon^a)|$ over all complex dth roots of unity ε^a.
(iii) Naturally the smallest value of $|u_{k,m}(\varepsilon^a)|$ occurs precisely when $|u_{k,m}(\varepsilon^a)^{-1}|$ takes on its largest value. Thus since $u_{k,m}(\varepsilon^a)^{-1} = u_{l,m}(\varepsilon^{ka})$ with $kl \equiv 1 \bmod d$ we see that $|u_{k,m}(\varepsilon^a)|$ is minimal when $|u_{l,m}(\varepsilon^{ka})|$ is maximal. Since $2 \leq l \leq d-2$, this will occur precisely when $ak \equiv \pm 1 \bmod d$, as required. □

We now see the maximal, respectively minimal, absolute value of $|u_{k,m}(\varepsilon)|$ taken over all complex dth roots of unity ε is obtained by precisely two of these roots. Moreover both these roots are complex conjugates. This shows that depending on the situations T_+ and T_- where $T = u_{k,m}(\overline{g})$ will have dimension at least 2.

4.3 Equality condition for the absolute values of eigenvalues

We conclude with question (II). If ε_1 and ε_2 are two dth roots of unity, when is $|u_{k,m}(\varepsilon_1)| = |u_{k,m}(\varepsilon_2)|$? In the maximal and minimal situation we know from Lemma 4.2.2 that this will happen when either $\varepsilon_1 = \varepsilon_2$ or $\varepsilon_1 = \overline{\varepsilon_2}$. We will now prove that this is the case in general for dth roots of unity where d is power of a prime p.

Lemma 4.3.1. *Let p be a prime and set $d = p^n$*

(i) Suppose $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ and $\delta_1, \delta_2, \ldots, \delta_r$ are complex dth roots of unity that satisfy

$$\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_r = \delta_1 + \delta_2 + \ldots + \delta_r. \tag{4.2}$$

If $r \leq p-1$ then, by relabeling the δ_i's if necessary, we have $\varepsilon_i = \delta_i$ for all i.

(ii) Suppose $2 \leq k \leq d-2$ and let $\varepsilon = e^{2\pi i/d}$ be a primitive complex dth root of unity. If $p \geq 5$ and $|u_{k,m}(\varepsilon^a)| = |u_{k,m}(\varepsilon^b)|$, then $a \equiv \pm b \bmod d$.

Proof. (i) First let $\varepsilon = e^{(2\pi i)/(p^n)}$ be a primitive complex p^nth root of unity and set

$$K = \mathbb{Q}(\varepsilon) = \{a_0 + a_1\varepsilon + a_2\varepsilon^2 + \ldots + a_{p^n-1}\varepsilon^{p^n-1} \mid a_0, a_1, \ldots, a_{p^n-1} \in \mathbb{Q}\},$$

the p^nth cyclotomic field. Then

$$\begin{aligned} \mathrm{Gal}(K/\mathbb{Q}) &= \{\sigma_i : \varepsilon \mapsto \varepsilon^i \mid 1 \leq i \leq p^n \text{ and } (i, p^n) = 1\} \\ &\cong \mathcal{U}(\mathbb{Z}_{p^n}) \cong \mathrm{Aut}(\mathbb{Z}_{p^n}). \end{aligned}$$

If we set $\mathrm{tr}(e) = 1/(p^{n-1})T_{K/\mathbb{Q}}(e)$ for every $e \in K$. Then $tr(1) = (p^n - p^{n-1})/p^{n-1} = p-1$. Secondly let ζ be a primitive pth root of unity. We now calculate the scaled trace to obtain

$$\begin{aligned} \mathrm{tr}(\zeta) = \frac{1}{p^{n-1}}T_{K/\mathbb{Q}}(\zeta) &= \frac{1}{p^{n-1}} \sum_{(i,p^n)=1} \zeta^i \\ &= \frac{1}{p^{n-1}} \left(\sum_{i=1}^{p^n} \zeta^i - \sum_{(i,p^n)\neq 1} \zeta^i \right) \\ &= \frac{1}{p^{n-1}} \left(\frac{\zeta^{p^n}-1}{\zeta - 1} - \left(\zeta^p + (\zeta^p)^2 + \ldots + (\zeta^p)^{p^{n-1}} \right) \right) \\ &= \frac{1}{p^{n-1}} \left(0 - (p^{n-1}) \right) = -1 \end{aligned}$$

Though if ζ is a p^ath root of unity with $2 \leq a \leq n$ we get

$$\begin{aligned} \mathrm{tr}(\zeta) = \frac{1}{p^{n-1}}T_{K/\mathbb{Q}}(\zeta) &= \frac{1}{p^{n-1}} \sum_{(i,p^n)=1} \zeta^i \\ &= \frac{1}{p^{n-1}} \left(\sum_{i=1}^{p^n} \zeta^i - \sum_{(i,p^n)\neq 1} \zeta^i \right) \\ &= \frac{1}{p^{n-1}} \left(\frac{\zeta^{p^n}-1}{\zeta - 1} - \frac{\zeta^{p^{n+1}}-1}{\zeta^p - 1} \right) \\ &= 0 \end{aligned}$$

Let us now first prove that $\varepsilon_1 = \delta_i$ for some $i \in \{1, \ldots, r\}$. Notice that, by multiplying both sides of the equality by ε_1^{-1} if necessary, we may assume that $\varepsilon_1 = 1$. Now take trace tr of both sides of the equality (4.2). Recall $\mathrm{tr}(1) = (p-1)$. In the worst case scenario all other elements are pth roots of unity and as such they will all lower the overall value on the left-hand side. Since $r \leq p-1$ we get that

$$\mathrm{tr}(\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_r) \geq (p-1) - (p-2) > 0.$$

This shows that the trace tr of the right-hand side is also strictly positive and from the previous we see that only 1 has a positive contribution to this value. It follows that there must exist an δ_i equal to $1 = \varepsilon_1$. Clearly the result now follows by induction on r.

(ii) Now let ε be a primitive complex dth root of unity. Since d is odd these units are a square. Therefore to avoid having too many exponents we will replace a by $2a$ and b by $2b$. First suppose ε^{2a} and ε^{2b} are both not equal to 1. From the proof of Lemma 4.2.2*(i)* we know that $|u_{k,m}(\varepsilon)| = \pm(\varepsilon^k - \varepsilon^{-k})/(\varepsilon - \varepsilon^{-1})$ and by this the equality $|u_{k,m}(\varepsilon^{2a})| = |u_{k,m}(\varepsilon^{2b})|$ implies that

$$\frac{\varepsilon^{ak} - \varepsilon^{-ak}}{\varepsilon^a - \varepsilon^{-a}} = \kappa \frac{\varepsilon^{bk} - \varepsilon^{-bk}}{\varepsilon^b - \varepsilon^{-b}},$$

where $\kappa = \pm 1$. Here we used the fact that both sides are in the real axis. This last equality implies that

$$\begin{aligned} \varepsilon^{ak+b} - \varepsilon^{ak-b} - \varepsilon^{-(ak-b)} + \varepsilon^{-(ak+b)} &= \kappa\left(\varepsilon^{bk+a} - \varepsilon^{bk-a} - \varepsilon^{-(bk-a)} + \varepsilon^{-(bk+a)}\right) \\ &= \varepsilon^{bk+\kappa a} - \varepsilon^{bk-\kappa a} - \varepsilon^{-(bk-\kappa a)} + \varepsilon^{-(bk+\kappa a)}. \end{aligned}$$

And this clearly implies the equality

$$\varepsilon^{ak+b} + \varepsilon^{-(ak+b)} + \varepsilon^{bk-\kappa a} + \varepsilon^{-(bk-\kappa a)} = \varepsilon^{ak-b} + \varepsilon^{-(ak-b)} + \varepsilon^{bk+\kappa a} + \varepsilon^{-(bk+\kappa a)}. \tag{4.3}$$

As $p \geq 5$ we can apply the first part of this lemma to conclude that each of the left-hand exponents must match a right-hand exponent modulo d. Now d is odd and both $2a$ and $2b$ are not equal to 0 modulo d. Also $2 \leq k \leq d-2$. This implies that $ak+b \not\equiv \pm(ak-b) \bmod d$ as this would imply that either $2a \equiv 0 \bmod d$ or $2b \equiv 0 \bmod d$. We obtain

$$\begin{aligned} ak + b &\equiv \pm(bk + \kappa a) \quad \bmod d, \\ ak - b &\equiv \pm(bk - \kappa a) \quad \bmod d \end{aligned}$$

Suppose first the two $\pm$ signs above do not agree. We can then add both equations to obtain $2ak \equiv \pm 2\kappa a \bmod d$ which implies that $k \equiv \pm 1 \bmod d$ which is contradiction to $2 \leq k \leq d-2$. So the signs must agree and if we again add up both equation we have $2ak \equiv \pm 2bk \bmod d$ which implies that $2a \equiv \pm 2b \bmod d$ as required.
To conclude suppose $\varepsilon^{2b} = 1$, then the previous arguments can be radically simplified. Suppose $\varepsilon^{2a} \neq 1$. Then $|u_{k,m}(\varepsilon^{2a})| = |u_{k,m}(\varepsilon^{2b})| = 1$ yields

$$\frac{\varepsilon^{ak} - \varepsilon^{-ak}}{\varepsilon^a - \varepsilon^{-a}} = \kappa = \pm 1,$$

and so $\varepsilon^{ak} - \varepsilon^{-ak} = \kappa(\varepsilon^a - \varepsilon^{-a}) = \varepsilon^{\kappa a} - \varepsilon^{-\kappa a}$. We now get the much simpeler equality

$$\varepsilon^{ak} + \varepsilon^{-\kappa a} = \varepsilon^{-ak} + \varepsilon^{\kappa a}. \tag{4.4}$$

Part (i) of this proof now implies that $ka \equiv -ka \bmod d$ or $ka \equiv \kappa a \bmod d$ but both these cases are impossible by our choice of k and a. Thus we also have $\varepsilon^{2a} = 1$ such that $2a \equiv 0 \equiv \pm 2b \bmod d$ and the proof is completed. □

Clearly the converse of Lemma 4.3.1*(ii)* is also true. If $\varepsilon \neq 1$ is a dth root of unity then

$$|u_{k,m}(\varepsilon)| = \left|\frac{\varepsilon^k - 1}{\varepsilon - 1}\right|^m = \left|\frac{\varepsilon^k(1 - \overline{\varepsilon}^k)}{\varepsilon(1 - \overline{\varepsilon})}\right|^m = \left|\frac{\varepsilon^k}{\varepsilon}\right|^m \left|\frac{\overline{\varepsilon}^k - 1}{\overline{\varepsilon} - 1}\right|^m = \left|\frac{\overline{\varepsilon}^k - 1}{\overline{\varepsilon} - 1}\right|^m = |u_{k,m}(\overline{\varepsilon})|.$$

Chapter 5

Free product of Bass cyclic units in integral group rings

In this final chapter we will try to apply all our accumulated knowledge when searching for free products of units in integral group rings. Actually we would like to show that if G is a finite non-abelian group, whose order is relatively prime to 6, then $\mathbb{Z}[G]$ contains two Bass cyclic units $u_{k,t}(g)$ and $u_{r,s}(h)$ such that the group $\langle u_{k,t}(g), u_{r,s}(h)\rangle$ generated by these two units is free of rank 2. This is the main result found in [GP06]. Notice that if H would be a proper non-abelian subgroup of G such that the wanted result follows for H then surely the two free Bass cyclic units found in $\mathbb{Z}[H]$ also generate a free group of rank 2 in $\mathbb{Z}[G]$. Even more if $\overline{G}$ would be a proper non-abelian epimorphic image of G attaining the result then Lemma 4.1.2 could be used to retract the two free Bass cyclic units from $\mathbb{Z}[\overline{G}]$ to again obtain the result in $\mathbb{Z}[G]$. This somewhat reduces the problem to non-abelian groups G in which every proper subgroup is abelian and every proper epimorphic image is abelian, namely if we work by induction on the order of $o(G)$.

The idea is actually recycled from an earlier article by Gonçalves and Passman [GP04] where they show that the unit group $\mathcal{U}(\mathbb{Z}[G])$ of an integral group ring $\mathbb{Z}[G]$ contains a free product $\mathbb{Z}_p * \mathbb{Z}$ if and only if G has a non-central element of order p. Here they reduced the problem to so called p-critical groups. By sliming down the possible groups needed to be investigated, the number of relations increase and we have more structure to work with. So it is important to first thoroughly study the structure of these *minimal* non-abelian groups.

This is however only half of the argument. Knowing the group structure is one thing but in order to apply the techniques introduced in Chapter 3 one also needs to investigate which are the possible irreducible complex representations $\mathfrak{X}$ for these groups. First, due to the specific group structures, we will see that the degree of all nonlinear representations will be fixed. This obviously influences the number of eigenvalues in the representation of our Bass cyclic units. Consequently if the degree n equals 2 or 3 it might be possible that two of the eigenvalues in the representations of an element $g \in G$ are complex conjugate and the calculations from Chapter 4 then imply that the representation $S = \mathfrak{X}(u_{k,t}(g))$ of any given Bass cyclic unit $u_{k,t}(g)$ can not induce a suitable S-decomposition of the vectorspace $\mathbb{C}^n$, this due to the limited dimension of this space. As a consequence of the generality of the wanted result, we will need to assume that the order of G is relatively prime to 6.

Unfortunately this does not resolve all problems completely. It could still be possible that S contains the complex conjugate of the eigenvalue having the largest absolute value while it does not for the lowest. As a consequence $\dim S_+ = 2 \neq 1 = \dim S_-$. This is why it is important to know which eigenvalues are present in the representation of $\mathfrak{X}(g)$ and which matrices are used to diagonalize $\mathfrak{X}(g)$ and consequently also $S = \mathfrak{X}(u_{k,t}(g))$. Naturally we

will also need this knowledge in order to verify the idempotent conditions set in Chapter 3. For two of the group cases these calculations will follow fairly easy, while in the third case we will need to examine the group structure more intensively in order to obtain the wanted result. Ultimately we will be restricted in our choice of Bass cyclic units and irreducible complex representation for this last case. Now we have a general notion of the obstacle to come, it is time to go into more detail.

5.1 Non-abelian groups whose proper subgroups and epimorphic images are abelian

In this first section we will give a thorough description of these *minimal* non-abelian groups. We start of by describing non-nilpotent groups such that every proper subgroup is nilpotent. This will obviously aid us when looking at non-nilpotent groups having only abelian proper subgroups. Intuitively these groups are close to being nilpotent and in fact a central argument of the next theorem will be to show that they are solvable. This gives us two categories of interest to study, namely the nilpotent groups such that every proper subgroups is abelian and the solvable, non-nilpotent groups fulfilling the same criteria. With each step we will add more restrictions until in the end we will also assume that every proper epimorphic image of the groups is abelian.

As said we start by just assuming that every proper subgroup is nilpotent while the group itself is not. The original proofs of these first two theorems where found in Scott's book on Group theory [Sco64].

Theorem 5.1.1. *Let G be a finite non-nilpotent group such that all its proper subgroups are nilpotent. Then there exists an $X \in Syl_p(G)$ and $A \in Syl_q(G)$ where p and q are distinct primes such that*

(i) $G = A \rtimes X$,

(ii) X *is cyclic and*

(iii) G *is solvable.*

Proof. We proceed by induction on the order of G. First suppose G is simple and also assume that there is just one proper maximal subgroup H. Since for every $g \in G$ we get that gHg^{-1} is a subgroup of G we see that $gHg^{-1} \leq H$ and it follows that H is normal. Hence G contains at least two distinct proper maximal subgroups. Let H and K be two distinct maximal subgroups such that their intersection has maximal order among all interesections of two distinct maximal subgroups. Now suppose their intersection $H \cap K$ is not trivial. By the simplicity we get that the normalizer $N(H \cap K) = \{g \in G \mid g(H \cap K) = (H \cap K)g\}$ is a proper subgroup of G and therefore it is encompassed by a proper maximal subgroup $L \geq N(H \cap K)$. Now since L is nilpotent by assumption we get that $N(H \cap K) \cap H > H \cap K \cap H = H \cap K$ so that $L \cap H > H \cap K$. But we assumed that the intersection $H \cap K$ was maximal for all pairs of distinct proper maximal subgroups. It follows that $H = L$ and by the mirrored argument $L = K$, a contradiction. Hence any two distinct maximal subgroups intersect in $\{1\}$. If H is now a proper maximal subgroup of G, then $N(H) = H$ and the previous arguments shows that $H \cap H^g = \{1\} = H^g \cap H^{g'}$ for every $g, g' \notin H$. This shows that there are $[G : H]$ conjugates of $H^\#$ each containing $o(H) - 1$ elements. So the number of elements in conjugates of $H^\#$ is equal to

$$(o(H) - 1)[G : H] = o(G) - [G : H] \geq o(G) - o(G)/2 = o(G)/2,$$

where we used that $[G : H] \leq o(G)/2$. Also $[G : H] \geq 2$, so that by the above equation we see that there exists at least one element $x \neq e$ outside all conjugates of H and this elements is contained in a proper maximal subgroup K. By the intersection property all conjugates

of $K^{\#}$ are disjoint from all conjugates of $H^{\#}$, where again we use that $N(K) = K$, so that, including 1, we have at least $2(o(G)/2)+1$ elements in G, clearly an impossibility. Therefore G can not be simple. So there does exists a $\{1\} < K < G$ normal in G. Now all subgroups of G/K are nilpotent. If G is a group of minimal order fulfilling the requirements of this theorem then G/K is necessarily nilpotent and hence solvable. Otherwise we can use the induction hypothesis and again we see that G/K is solvable. Note that K is nilpotent by assumption and thus also solvable. Both observations together imply that G is solvable which proves *(iii)*. Now if all Sylow subgroups are normal then G would be nilpotent. So there exists a prime p and an $X \in Syl_p(G)$ such that X is not normal in G. Since G is solvable there exists a $H \lhd G$ such that $[G : H]$ is prime. Furthermore since H is again nilpotent any Sylow subgroup of H is characteristic in H and therefore normal in G. This implies that X can not be a subgroup of H otherwise it would also be a Sylow subgroup of H which contradicts X not being normal. We therefore get that $[G : H] = p$. Moreover all other Sylow q-subgroups Q with $q \neq p$ are contained in H and again using the same reasoning normal in G. So there exists an $A \in Syl_q(G)$ with $p \neq q$ such that $A \not\subseteq C(X) = \{g \in G \mid gx = xg \text{ for all } x \in X\}$, otherwise X would be normal in G. This shows that AX is a non-nilpotent subgroup of G and thus $AX = G$. Remember that Sylow p-subgroups are disjoint from Sylow q-subgroups, for $p \neq q$, so that G equals the semidirect product $A \rtimes X$ which proves *(i)*. Finally if X is not cyclic then for every $x \in X$ we have that $\langle x \rangle < X$. But then $A\langle x \rangle$ is a proper subgroup of G and thus nilpotent which implies $A \subset C(x)$ for every $x \in X$. We see that in this case $A \subseteq C(X)$ which is a contradiction. Hence X is cyclic so that *(ii)* also holds and the proof is finished. □

From now on suppose that every proper subgroup of G is abelian. If G itself is non-nilpotent then the previous theorem can be fine tuned. If G is nilpotent we will show that it is in fact a p-group.

Theorem 5.1.2. *Let G be a finite non-abelian group such that all its proper subgroups are abelian. Then either*

(a) G is a p-group for some prime p or

(b) $G = A \rtimes X$ is a semidirect product of

(i) a cyclic subgroup $X = \langle x \rangle$ where x has prime power order p^i and

(ii) a normal elementary abelian q-subgroup A where q is prime distinct from p.

Proof. First suppose G is nilpotent and that its order is divisible by at least two primes. Then G is the direct product of its proper Sylow subgroups and these are abelian by assumption. This would imply that G is also abelian which is a contradiction. Hence if G is nilpotent it is a p-group for some prime p which is case *(a)*. Otherwise when G is not nilpotent, Theorem 5.1.1 applies and in addition A is abelian. Now suppose A is not elementary. Let $X = \langle x \rangle$ and observe the homomorphism

$$\pi : X \to \mathrm{Aut}(A) : x \mapsto \pi_x = x(.)x^{-1}.$$

Any proper characteristic subgroup L of A is normal in G so that LX is a proper subgroup of G and thus abelian. Moreover this implies that $\pi_x \neq 1_A$ fixes the elements of L. Now A contains two of these characteristic subgroups namely A_1, the subgroup of all qth powers of elements in A, and A_2, the subgroups of all elements of order q or 1. Notice that both these subgroups are proper since A is not elementary by assumption. Now $A \not\subseteq C(X)$ so that $A \not\subseteq C(x)$. This allows us to locate an element y in $A \setminus C(x)$. Clearly y^q is an element of A_1. Since this subgroup is characteristic $\pi_x(y^q) = y^q$ which implies that $\pi_x(y)^q = y^q$. Now for every $z \in G$, we have that $y^q = z^q$ if and only if $z = yu$ where u is an element of order q or 1, i.e. in A_2. Furthermore let now yu be an element of yA_2. Then

$$\pi_x(yu)^q = \pi_x(y^q u^q) = \pi_x(y^q) = y^q,$$

which implies that $\pi_x(yu) = yv$ where v is an element of A_2. This shows that π_x permutes the elements of yA_2. Now $o(yA_2) = o(A_2) = q^i$ for some $i > 0$. Contrasting to this we know form Theorem 5.1.1 that X has order p^j for some $j > 0$ so that $\langle x^p \rangle$ is either a proper subgroup of X or equal to $\{1\}$. Whatever the case this implies that $A\langle x^p \rangle$ is abelian, and it is clear that π_x has order p. By this fact we see that π_x must fix at least one element $yu \in yA_2$ and we already know that π_x fixes all elements of A_2 by assumption so that π_x fixes $y = yuu^{-1}$, a contradiction. Hence A is elementary abelian and we obtain case *(b)*. This concludes the proof. □

Notice, as said in the introduction, that we have not made use yet of the fact that every proper epimorphic image of G is abelian. We will use this extra criteria to further investigate both situations. First we examen the p-group case, where we make use of arguments found in [GP04]. The main idea is to show that G contains a non-central element of prime order p. We note that the method used may not be the most efficient but it works nonetheless.

Lemma 5.1.3. *Let G be a finite non-abelian p-group for some prime p such that every proper subgroup and every proper epimorphic image is abelian then $G = A \rtimes X$ is a semidirect product of*

(1) a cyclic subgroup $X = \langle x \rangle$ where x has order p and

(2) a normal subgroup A where either

(2a) A is cyclic or

(2b) A is equal to $C_p \times C_p$

Proof. First of all since G is non-abelian it contains two elements x, y such that $xy \neq yx$. This implies that x and y generate a nonablian subgroup and since G does not contain such a proper subgroup it follows that $\langle x, y \rangle = G$. Moreover if x' is another generator of $\langle x \rangle$ and y' is another generator of $\langle y \rangle$ then also $x'y' \neq y'x'$ and again $G = \langle x', y' \rangle$. Next since G is non-abelian the commutator subgroup G' is nonempty and the center $Z(G)$ does not equal the whole group. Now $G/Z(G)$ is abelian by assumption which implies that G' is central. Also G' contains an element z of order p and since again $G/\langle z \rangle$ is abelian by assumption it clearly follows that $G' = \langle z \rangle$. In particular this implies that pth powers of elements in G are central. To see this take $g, h \in G$, we then have $gh = [g, h]hg$ and since G' is central $g^2h = [g, h]ghg = [g, h]^2hg^2$. By induction we obtain that $g^ph = [g, h]^phg^p = hg^p$ and the claim follows.
(1) We now want to prove that G contains a non-central element of order p. If either y or x has order p then the situation is easy. Otherwise both x and y have order strictly larger then p. Here we set $o(x) = p^{m+1}$ and $o(y) = p^{n+1}$ where $n, m \in \mathbb{N}_0$. Since $x^p \neq 1$ is central, $\langle x^p \rangle$ is normal in G and $G/\langle x^p \rangle$ is abelian by assumption. This implies that $z \in \langle x^p \rangle$ and more specifically, by switching the generator of $\langle x \rangle$ if necessary, we may assume that $z = x^{p^m}$. Similarly we find that $z = y^{p^n}$. So let us now observe the following subgroup

$$H = \langle x^p, y \rangle = \langle x^p, y \mid (x^p)^{p^m} = 1 = y^{p^{n+1}}, (x^p)^{p^{m-1}} = y^{p^n}, x^py = yx^p \rangle.$$

By the fundamental theorem of finite abelian groups one sees that this subgroup is cyclic. Now x^p is an element of $H = \langle c \rangle$ and moreover it cannot be a generator of this subgroup as this would imply that G itself is cyclic which is impossible. This shows that

$$G = \langle c, x \mid c^{p^r} = 1 = x^{p^{m+1}}, x^p = c^{ip}, \text{ where } 1 \leq i \leq p^{r-1} - 1 \rangle.$$

As a consequence of these equations xc^{-i} is easily seen to be a non-central element of G as it does not commute with y and it has order p.
So by renaming elements if necessary we may assume that x is our non-central element of order p and y is an element in G which does not commute with x. Furthermore set $X = \langle x \rangle$ and $A = \langle y, z \rangle$. Since A contains the commutator $A \lhd G$ and $G = AX$ as G is still generated

by x and y. Moreover $X \not\subseteq A$ so that $X \cap A = \{1\}$. This readily shows $G = A \rtimes X$.
(2a) Now suppose y has order strictly larger then p. Again by previous comments it is clear that $z \in \langle y \rangle$ and as a consequence A is cyclic.
(2b) Otherwise if y has order p then clearly $\langle y \rangle \cap \langle z \rangle = \{1\}$ so that $A = C_p \times C_p$ and all the results in the lemma are proven. □

To conclude let us further sharpen the result for non-nilpotent groups $G = A \rtimes X$. We will show that in this case X acts faithfully and irreducibly on A. This is due to the fact that the order of A is relatively prime to the order of X which is evidently not true with p-groups and moreover the result will also be false in this case. To see this notice from the proof of the previous lemma that the commutator subgroup G' which is a proper subgroup of A is central in G and as such X acts trivially on it. This will however not be possible in the next situation as a semisimplicity argument would then imply that G' has an X-invariant complement subgroup A_1. Since X can not act trivially on this A_1, otherwise G would be abelian, we have found a proper non-abelian subgroup $A_1 \rtimes X$ of G which is impossible.

Lemma 5.1.4. *Let G be a finite non-abelian group which is not a p-group such that every proper subgroup and every proper epimorphic image is abelian then $G = A \rtimes X$ is a semidirect product of*

(1) a cyclic subgroup $X = \langle x \rangle$ where x has order p and

(2) a normal elementary abelian q-subgroup A,

where q is a prime distinct from p. Moreover X acts faithfully and irreducibly on A.

Proof. Since G is not a p-group we know from Theorem 5.1.2*(b)* that $G = A \rtimes X$ where $X = \langle x \rangle$ is cyclic of prime power order p^n and A is an elementary abelian q-group. Now suppose $n \neq 1$, then $x^p \neq 1$ is either central or not. First suppose the latter. Then $A \rtimes \langle x^p \rangle$ is a proper non-abelian subgroup which is a contradiction to the assumptions. So $x^p \neq 1$ has to be central and in particular $\langle x^p \rangle$ is normal in G. It is now not difficult to see that this implies that $G/\langle x^p \rangle$ is a proper non-abelian epimorphic image of G which again yields a contradiction to the assumptions and as a result x must have prime order p.
Next X clearly acts faithfully on A as x can not act trivially on A otherwise G would be abelian. Also since A is an elementary abelian q-group it naturally posses the structure of a $GF(q)$-vector space where the subspaces in this structure correspond to subgroups in the group structure. Moreover it is easily seen that the action of $\langle x \rangle$ on A is $GF(q)$-linear. This implies that A can be seen a $GF(q)X$-module and this time the submodules correspond to subgroups of A which are invariant under the action of X. But since $\gcd(p, q) = 1$, Maschke's Theorem implies that $GF(q)X$ is semisimple and thus A is completely reducible as a $GF(q)X$-module. Clearly X cannot act trivially on all these irreducible components as otherwise A would be abelian. So let A_1 be an irreducible component such that X does not act trivially on it then from the previous remarks $A_1 \rtimes X$ is a non-abelian subgroup of G and since G does not contain such a subgroup it follows that $A = A_1$ and A is irreducible as a $GF(q)X$-module. More specifically X acts irreducibly on A and the proof is finished. □

Before ending this section we will summarize all useful results. We will also divide them into the three cases which will be studied in the next sections. So one more time if G is a finite non-abelian group such that every proper subgroup and every proper epimorphic image is abelian then $G = A \rtimes X$ is a semidirect product of

(1) a cyclic subgroup $X = \langle x \rangle$ where x has order p and

(2) a normal subgroup A where either

Case A: $A = \langle a \rangle$ is cyclic of prime power order or
Case B: A is equal to $C_p \times C_p$ or
Case C: A is an elementary abelian q-subgroup where
(i) q is prime distinct from p and
(ii) A has order strictly larger then q, i.e A is not cyclic, and
(iii) X acts faithfully and irreducibly on A.

It should be noted that there are some extra untold restrictions on the orders of the subgroups A and X. For example in **Case A** the order of X will have to be strictly smaller then the order of A and in **Case C** A can consist of at most $o(X) = p$ copies of C_q. The reason why this is true will become apparent from the different case studies.

5.2 Bass cyclic units in the integral group ring over a p-group and $C_{q^i} \rtimes C_p$

Before we go and prove the following representation lemma it might be useful to introduce an "orthogonality" property between two pth roots of unity where p is a prime. For this let $\varepsilon_n = e^{2\pi n/p}$ and $\varepsilon_m = e^{2\pi m/p}$ be two such pth roots of unity with $1 \leq n, m \leq p-1$. Then observe the following sum

$$\sum_{k=1}^{p} \overline{\varepsilon_n^k} \varepsilon_m^k = \sum_{k=1}^{p} e^{-2\pi kn/p} e^{2\pi km/p} = \sum_{k=1}^{p} e^{2\pi k(n-m)/p}.$$

If now $m = n$ then clearly every term is equal to 1 so that the sum is equal to p. Otherwise when $m \neq n$ this is the sum over all pth roots of unity which is equal to 0. This implies that

$$\sum_{k=1}^{p} \overline{\varepsilon_n^k} \varepsilon_m^k = p\delta_{n,m},$$

where δ denotes the Kronecker delta. We now prove the following lemma which gives a description of the nonlinear irreducible complex representations $\mathfrak{X}$ of G. We are specifically interested in the possible degree's of these representations and in the form of the matrices used to diagonalize the representation $\mathfrak{X}(g)$ of a random element $g \in G$.

Lemma 5.2.1. *Let $G = A \rtimes X$ be a semidirect product of a normal abelian subgroup A and a cyclic subgroup $X = \langle x \rangle$ where x has prime order p. Let $\mathfrak{X} : \mathbb{C}[G] \to M_n(\mathbb{C})$ be a complex irreducible representation of G of degree $n > 1$, with associated character $\chi : G \to \mathbb{C}$, and let $\mu : A \to \mathbb{C}$ be an irreducible constituent of the restriction of χ to A. We then have*

(i) n=p and we can assume that

$$\mathfrak{X}(a) = \begin{bmatrix} \mu(a) & & & \\ & \mu^x(a) & & \\ & & \ddots & \\ & & & \mu^{x^{p-1}}(a) \end{bmatrix}$$

for all $a \in A$ where $\mu^{x^i}(a) = \mu(x^i a x^{-i})$ and these p linear characters are all distinct. Furthermore $\mathfrak{X}(x)$ is the permutation matrix.

$$\mathfrak{X}(x) = \begin{bmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{bmatrix}.$$

(ii) Let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p$ be all the complex pth roots of unity, define

$$P = \frac{1}{\sqrt{p}} \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \varepsilon_1 & \varepsilon_2 & \ldots & \varepsilon_p \\ \vdots & \vdots & & \vdots \\ \varepsilon_1^{p-1} & \varepsilon_2^{p-1} & \ldots & \varepsilon_p^{p-1} \end{bmatrix}.$$

Let $Q = P^*$, were $*$ denotes transpose conjugate. Then P is a unitary matrix, $Q = P^{-1}$ and $Q\mathfrak{X}(x)P = \operatorname{diag}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p)$.

(iii) If $A = \langle a \rangle$ cyclic, then $\mu(a), \mu^x(a), \ldots, \mu^{x^{p-1}}(a)$ are all distinct and not equal to 1. If p is odd, then no two of these elements can be complex conjugates of each other.

Proof. (i) First since G is non-abelian there exists a nonlinear irreducible representation $\mathfrak{X} : G \to \mathrm{M}_n(\mathbb{C})$ which can be linearly extended to a representation $\mathfrak{X} : \mathbb{C}[G] \to \mathrm{M}_n(\mathbb{C})$ such that it is still irreducible and $n > 1$. Moreover if $\mathfrak{M} : A \to \mathrm{M}_n(\mathbb{C})$ is the restriction of $\mathfrak{X}$ to the normal abelian subgroup A then $\mathfrak{M}$ is necessarily no longer irreducible. It is however completely reducible and all of its irreducible constituents are linear. Clifford's Theorem [Isa76, Theorem 6.5] now tells us that all these characters are conjugate to each other. Also it is not difficult to see that the conjugating elements will come from X. Lastly using Itô's Theorem [Isa76, Theorem 6.15] we see that $n > 1$ divides $[G : A] = p$ such that $n = p$. It follows that we can assume

$$\mathfrak{X}(a) = \begin{bmatrix} \mu(a) & & & \\ & \mu^x(a) & & \\ & & \ddots & \\ & & & \mu^{x^{p-1}}(a) \end{bmatrix},$$

where μ is such an irreducible constituent of $\mathfrak{M}$ and $\mu^{x^i}(a) = \mu(x^i a x^{-i})$. Moreover if two of these characters μ^{x^i} and μ^{x^j} are equal then one easily sees that all of these conjugate characters are identical. But this would imply that $\mathfrak{X}(a) = \operatorname{diag}(\mu(a), \mu(a), \ldots, \mu(a))$, and as a consequence $\mathfrak{X}(A)$ is central in the matrix ring such that $\mathfrak{X}(G)$ is abelian which contradicts the assumption that n is strictly larger then 1. Furthermore we easily see that the matrix $\mathfrak{X}(x)$ is a permutation matrix and without loss of generality we may assume that is it of the form

$$\mathfrak{X}(x) = \begin{bmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{bmatrix}.$$

Also *(ii)* follows by direct computation of the aforementioned matrices. To quickly demonstrate this let us first look at the following matrix product

$$QP = \frac{1}{p} \begin{bmatrix} 1 & \overline{\varepsilon_1} & \ldots & \overline{\varepsilon_1^{p-1}} \\ 1 & \overline{\varepsilon_2} & \ldots & \overline{\varepsilon_2^{p-1}} \\ \vdots & \vdots & & \vdots \\ 1 & \overline{\varepsilon_p} & \ldots & \overline{\varepsilon_p^{p-1}} \end{bmatrix} \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \varepsilon_1 & \varepsilon_2 & \ldots & \varepsilon_p \\ \vdots & \vdots & & \vdots \\ \varepsilon_1^{p-1} & \varepsilon_2^{p-1} & \ldots & \varepsilon_p^{p-1} \end{bmatrix}.$$

Clearly the element on the nth row and mth colom of the resulting matrix will be determined by the sum

$$\frac{1}{p} \sum_{k=1}^{p} \overline{\varepsilon_n^k} \varepsilon_m^k = \frac{1}{p} p \delta_{n,m} = \delta_{n,m}$$

which shows the product QP is equal to the identity matrix. Secondly we look at the following matrix product

$$[Q\mathfrak{X}(x)]P = \frac{1}{p}\begin{bmatrix} \overline{\varepsilon_1^{p-1}} & 1 & \dots & \overline{\varepsilon_1^{p-2}} \\ \overline{\varepsilon_2^{p-1}} & 1 & \dots & \overline{\varepsilon_2^{p-2}} \\ \vdots & \vdots & & \vdots \\ \overline{\varepsilon_p^{p-1}} & 1 & \dots & \overline{\varepsilon_p^{p-2}} \end{bmatrix}\begin{bmatrix} 1 & 1 & \dots & 1 \\ \varepsilon_1 & \varepsilon_2 & \dots & \varepsilon_p \\ \vdots & \vdots & & \vdots \\ \varepsilon_1^{p-1} & \varepsilon_2^{p-1} & \dots & \varepsilon_p^{p-1} \end{bmatrix}.$$

Now the element on the nth row and mth column will be produced by the sum

$$\frac{1}{p}\sum_{k=1}^{p}\overline{\varepsilon_n^k}\varepsilon_m^{k+1} = \frac{1}{p}\varepsilon_m\sum_{k=1}^{p}\overline{\varepsilon_n^k}\varepsilon_m^k = \frac{1}{p}p\varepsilon_m\delta_{n,m} = \varepsilon_m\delta_{n,m}.$$

This time we obtain the matrix $\mathrm{diag}(\varepsilon_1,\dots,\varepsilon_p)$. Finally for *(iii)*, since $A = \langle a\rangle$ is cyclic the linear characters of A are completely determined by their value on a. In particular it must follows from *(i)* that $\mu(a), \mu^x(a), \dots, \mu^{x^{p-1}}(a)$ are all distinct. Furthermore if $\mu^{x^i}(a) = 1$ for some $i \in \{1,\dots,p-1\}$ then $\mu^{x^i} = 1_A$ and clearly $\mu^{x^j} = 1_A$ for every $j \in \{1,\dots,p-1\}$ which is certainly a contradiction. To conclude if $\mu^{x^i}(a)$ and $\mu^{x^j}(a)$ are complex conjugates of each other for some $i \not\equiv j \bmod p$ then x^{j-i} sends μ^{x^i} to its complex conjugate character and hence $x^{2(j-i)}$ fixes μ^{x^i}. If we now look at the form of the matrix $\mathfrak{X}(x)$ we see that this can only occur when $p = 2$. □

Let us put this information to practice and prove **Case A**. We are looking for two elements g and h in $G = A \rtimes X$ around which we would like to construct two Bass cyclic units $u_{k,t}(g)$ and $u_{r,s}(h)$ such that these units generate a free non-abelian group of rank 2 in $\mathcal{U}(\mathbb{Z}[G])$. Clearly g and h may not commute as otherwise the same holds for $u_{k,t}(g)$ and $u_{r,s}(h)$. So g and h can not both be in A or X. An easy choice would be to suppose $g \in A = \langle a\rangle$ (non-central) and $h \in X = \langle x\rangle$ and we could just take $g = a$ and $h = x$. Clearly one can always find a nonlinear irreducible representation $\mathfrak{X}$ as described in the previous lemma such that $\mathfrak{X}([g,h]) \neq 1$ if and only if $[g,h] \neq 1$. Also from Lemma 5.2.1 we know that the eigenvalues of $\mathfrak{X}(x)$ are all the pth roots of unity. As mentioned multiple times, Lemma 4.2.2 then tells us that two of the eigenvalues of $\mathfrak{X}(u_{k,t}(x))$ will have maximal absolute value and the same goes for those of minimal absolute value. So we would like a similar result for the eigenvalues of $\mathfrak{X}(u_{r,s}(a))$. Fortunately since A is cyclic the eigenvalues of $\mathfrak{X}(a)$ are easy to control and none of them are complex conjugates of each other. The dimension requirements will thus be fulfilled and the verifications of the idempotent conditions will also follow easily. We now formally prove the result for **Case A**. As with the other cases the original proofs can be found in [GP06].

Case A. *Let $G = A \rtimes X$ be a semidirect product of*

(1) a normal cyclic subgroup $A = \langle a\rangle$ where a has prime power order q^i and

(2) a cyclic subgroup $X = \langle x\rangle$ where x has prime order $p \geq 5$, where p not necessarily different form q.

then there exist Bass cyclic units $u_{k,tm}(a)$ and $u_{r,sn}(x)$ that generate a non-abelian free subgroup of the unit group of the integral group ring $\mathbb{Z}[G]$, where n and m are positive integers.

Proof. First observe the homomorphism

$$\pi : X \to \mathrm{Aut}(A) : x \mapsto \pi_x = x(.)x^{-1},$$

and notice that $o(\mathrm{Aut}(A)) = (q-1)q^{i-1}$. Now the order of π_x equals p and this shows that either p is equal to q or it divides $q-1$. Either way we have that $q \geq p \geq 5$. So choose two Bass cyclic units

$$u_{k,t}(a) \qquad \text{and} \qquad u_{r,s}(x),$$

with $k \not\equiv \pm 1 \bmod o(a)$ and $r \not\equiv \pm 1 \bmod o(x)$. Since both a and x have odd order greater or equal than 5 we can take $k = r = 2$.
Now we have chosen two Bass cyclic units let us find a suitable representation. Since G is non-abelian, there exists a nonlinear irreducible representation

$$\mathfrak{X} : \mathbb{Z}[G] \subseteq \mathbb{C}[G] \to \mathrm{M}_u(\mathbb{C}),$$

for some $u > 1$ with associated character $\chi : G \to \mathbb{C}$ and Lemma 5.2.1 tells us that $u = p$. Let us first look at $u_{r,s}(x)$. Again using the aforementioned lemma we can assume

$$\mathfrak{X}(x) = \begin{bmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{bmatrix}.$$

Also there exists a suitable described unitary matrix P with $P^{-1}\mathfrak{X}(x)P = \mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_p)$, where $\varepsilon_1, \ldots, \varepsilon_p$ are all the p distinct complex pth roots of unity written in any order we choose. So if we set $T = \mathfrak{X}(u_{r,s}(x))$ we obtain

$$P^{-1}TP = \mathrm{diag}(u_{r,s}(\varepsilon_1), \ldots, u_{r,s}(\varepsilon_p)).$$

This shows that T is diagonalizable and we know the eigenvalues of T. Even more, the calculations made in the previous chapter, more precisely in Lemma 4.2.2, show us precisely that two of these have the largest absolute value and two have the smallest absolute value. By its own this shows we can find a T-decomposition $V = T_+ \oplus T_0 \oplus T_-$ of $V = \mathbb{C}^p$ with $\dim T_+ = \dim T_- = 2$. By reordering the eigenvalues of $\mathfrak{X}(x)$ we can assume that $|u_{r,s}(\varepsilon_1)| = |u_{r,s}(\varepsilon_2)|$ is the maximal absolute value of all eigenvalues of T and $|u_{r,s}(\varepsilon_3)| = |u_{r,s}(\varepsilon_4)|$ is the minimal. If now τ_+ and τ_- are the corresponding projections of V into T_+ and T_-, respectively, then

$$\tau_+ = P(e_{1,1} + e_{2,2})P^{-1} \qquad \text{and} \qquad \tau_- = P(e_{3,3} + e_{4,4})P^{-1}.$$

Secondly let us take a closer look at $u_{k,t}(a)$. Again from Lemma 5.2.1 we know that

$$\mathfrak{X}(a) = \mathrm{diag}(\alpha_1, \ldots, \alpha_p),$$

for suitable distinct complex numbers α_i where no two of these are complex conjugates of each other. Moreover as $a^{q^i} = 1$ we know that $\alpha_1, \ldots, \alpha_p$ are distinct q^ith roots of unity. So if set

$$S = \mathfrak{X}(u_{k,t}(a)) = \mathrm{diag}(u_{k,t}(\alpha_1), \ldots, u_{k,t}(\alpha_p)),$$

we again see from earlier work, more precisely Lemma 4.3.1, that all the eigenvalues of S have distinct absolute value. This allows us to find an S-decomposition of $V = \mathbb{C}^p = S_+ \oplus S_0 \oplus S_-$ with $\dim S_+ = \dim S_- = 2 = \dim T_+ = \dim T_-$. Again we denote by σ_+ and σ_- the projections of V into S_+ and S_-, respectively. Clearly there now exist distinct subscripts i, j, i' and j' such that

$$\sigma_+ = e_{i,i} + e_{j,j} \qquad \text{and} \qquad \sigma_- = e_{i',i'} + e_{j',j'}.$$

Since both S and T are diagonalizable, in order for the group generated by some powers of these operators to be free, it remains to verify that the eight idempotent conditions of Corollary 3.5.1 are fullfiled. Let us show that the rank $\sigma_+\tau_- = \text{rank } \tau_-\sigma_+ = 2$. The six other products will follow in the same manner. First consider $\sigma_+\tau_- = (e_{i,i}+e_{j,j})P(e_{3,3}+e_{4,4})P^{-1}$. Clearly $\sigma_+\tau_-$ has the same rank as $(e_{i,i} + e_{j,j})P(e_{3,3} + e_{4,4})$. Furthermore this latter matrix has only four nonzero entries, namely on the intersection of the ith and jth row with the third and fourth column. Thus they form a 2×2 submatrix

$$M_{2\times 2} = \frac{1}{\sqrt{p}} \begin{bmatrix} \varepsilon_3^{i-1} & \varepsilon_4^{i-1} \\ \varepsilon_3^{j-1} & \varepsilon_4^{j-1} \end{bmatrix},$$

and this matrix has non-zero determinant since ε_3 is different from ε_4. This shows that $\sigma_+\tau_-$ has rank 2 as wanted. Looking at $\tau_-\sigma_+$ we first notice that P is a unitary matrix, i.e its inverse is equal to its transpose conjugate, so that clearly both σ_+ and τ_- are Hermetian, i.e. equal to its own transpose conjugate. It follows that $(\sigma_+\tau_-)^* = \tau_-^*\sigma_+^* = \tau_-\sigma_+$ and therefore rank $\tau_-\sigma_+ =$ rank $\sigma_+\tau_- = 2$.
Using the same technique for the remaining six idempotent conditions we know, using Corollary 3.5.1, that there exists positive integers m and n such that $\langle S^m, T^n\rangle = \langle S^m\rangle * \langle T^n\rangle$ is free of rank 2. Clearly this shows that $u_{k,t}(a)^m$ and $u_{r,s}(x)^n$ also generate a free group of rank 2 in the unit group of $\mathbb{Z}[G]$. Moreover we have that $u_{k,t}(a)^m = u_{k,tm}(a)$ and $u_{r,s}(x)^n = u_{r,sn}(x)$, by Proposition 4.1.1, and the result follows. □

Similarly **Case B** will again follow easily since the the eigenvalues of every non-central element a in A will be easy to control.

Case B. *Let $G = A \rtimes X$ be a semidirect product of*

(1) a normal subgroup A which is an elementary abelian p-group of order p^2 and

(2) a cyclic subgroup $X = \langle x\rangle$ where x has prime order $p \geq 5$.

then there exist Bass cyclic units $u_{k,tm}(a)$ and $u_{r,sn}(x)$, where $a \in A$ is a non-central element in G, that generate a non-abelian free subgroup of the unit group of the integral group ring $\mathbb{Z}[G]$, where n and m are positive integers.

Proof. The proof is completely similar to that of Case A, the only part that will differ is that we do not have a canonical choice for a. We will show that the same technique stills works if we choose $a \in A$ an element which is non-central in G. Therefore choose a Bass cyclic unit $u_{k,t}(a)$ where $k \not\equiv \pm 1 \bmod p$, for example $k = 2$. Again there exists a nonlinear irreducible representation

$$\mathfrak{X} : \mathbb{Z}[G] \subseteq \mathbb{C}[G] \to \mathrm{M}_u(\mathbb{C}),$$

for some $u > 1$ with associated character $\chi : G \to \mathbb{C}$ and, by Lemma 5.2.1, $u = p$. Also

$$\mathfrak{X}(a) = \mathrm{diag}(\alpha_1, \ldots, \alpha_p),$$

for suitable complex numbers α_i. Since now $a^p = 1$, these complex numbers are all the complex pth roots of unity. So if we set

$$S = \mathfrak{X}(u_{k,tm}(a)) = \mathrm{diag}(u_{k,t}(\alpha_1), \ldots, u_{k,t}(\alpha_p)),$$

the situation is identical as for x in the sense that Lemma 4.2.2(ii) and (iii) tells us that two of these eigenvalues have maximal absolute value and two have minimal absolute value. This allows us to find an S-decomposition $V = S_+ \oplus S_0 \oplus S_-$ of V where $\dim S_+ = \dim S_- = 2$. Clearly the proof now proceeds exactly as the proof of **Case A** and the result again follows. □

Notice that the first parameter of both Bass cyclic units is taken arbitrarily, i.e. no additional requirements where enforced. The second parameter has to fulfill just one new requirement. Instead of being a multiple of $\varphi(o(a))$, respectively $\varphi(o(x))$, it also has to be a multiple of n, respectively m. Also the choice of group elements to construct two Bass cyclic units could just as well have been any non-central element of A, respectively X. This somewhat implies that there are *a lot* of free pairs of Bass cyclic units in these two types of groups.

Unfortunately this will no not be true in our last case since in this case the eigenvalues of an element in A will be much more difficult to control and we will be forced to look at other specific group elements. This will not only force us to choose the group elements wisely but also restrict us in our choice or parameters. This will the subject of the next section.

5.3 Bass cyclic units in the integral group ring over a Frobenius group

A transitive permutation group G of a finite set P such that no non trivial element fixes more then one point of P is called a Frobenius group. The subgroup H consisting of all elements fixing one point of P is called the Frobenius complement while the normal subgroup K consisting of the identity element together with all elements which are not in any conjugate of H is called the Frobenius kernel. One can then show that $G = K \rtimes H$. An equivalent definition is saying that G has a non identity subgroup H, which will be equal to the Frobenius complement, such that $H \cap H^g = \{1\}$ for every $g \in G \setminus H$. Now if G is as in **Case C** then it is easily seen that X is a Frobenius complement since for every $1 \neq a \in A$ we have that $X \cap X^a = \{1\}$. If this intersection would not be trivial and h is a non identity element inhabiting this intersection then $aha^{-1}h^{-1}$ is an element of both A and X and therefore equal to 1. This would imply that $\langle a \rangle$ is X-invariant subgroup of A which is impossible. More information on the subject can be found in [Pas68]. This explains the sections header.

Before we can go on and prove the next lemma we are obligated to elaborate just a little bit more on the structure of $G = A \rtimes X$ for our **Case C**. Since A is an elementary abelian q-group consisting of a direct product of n copies of C_q it is easily seen that A can be viewed as the additive subgroup of the finite field $\mathrm{GF}(q^n)$. We have already pointed out in Lemma 5.1.4 that A is an irreducible $\mathrm{GF}(q)X$-module where we used the fact that $\mathrm{GF}(q)X$ is semisimple. Again using this observations we can construct the Wedderburn decomposition of this ring to obtain

$$\mathrm{GF}(q)X \cong \mathrm{M}_{n_1}(D_1) \oplus \mathrm{M}_{n_2}(D_2) \oplus \ldots \oplus \mathrm{M}_{n_r}(D_r),$$

where each D_j is a (finite) division ring and thus a finite field for every $1 \leq j \leq r$. This implies we have

$$\begin{aligned} \mathrm{GF}(q)X &\cong \mathrm{GF}(i_1) \oplus \mathrm{GF}(i_2) \oplus \ldots \oplus \mathrm{GF}(i_r) \\ &= A_1 \oplus A_2 \oplus \ldots \oplus A_r, \end{aligned}$$

and moreover each irreducible $\mathrm{GF}(q)X$-module is isomorphic to one of these component $A_j = \mathrm{GF}(i_j)$ with $1 \leq j \leq r$. Now A is such an irreducible $\mathrm{GF}(q)X$-module and is thus isomorphic to A_j for some $1 \leq j \leq r$, and also $\mathrm{GF}(i_j) = \mathrm{GF}(q^n)$. Now x acts on $\mathrm{GF}(q)X$ by right multiplication so each projection x_j of x acts by right multiplication on the component A_j for every $1 \leq j \leq r$. Thus if we identify x with its projection in A we can view x as an element of $A = \mathrm{GF}(q^n)$ acting by right multiplication on A.

This observation will be useful in the following lemma where for $a \in A$ and $x \in X$ we denote $a\pi_x(a) = axax^{-1} = aa^x$ by a^{1+x}.

Lemma 5.3.1. *Let $X = \langle x \rangle$ be a cyclic group of prime order p acting faithfully and irreducibly on an elementary abelian q-group A of order $o(A) \geq q^2$, where q is a prime distinct from p and $p \geq 5$, $q \geq 3$. If $1 \neq a \in A$ then the $p-1$ elements $a^{1+x}, a^{1+x^2}, \ldots, a^{1+x^{p-1}}$ cannot all be X-conjugate.*

Proof. First we will give two invariant subgroups of A for the action of X. The first one is $C_A(x) = \{a \in A \mid a = axax^{-1}\}$. Clearly this is a subgroup of A which is invariant under the action of X. Moreover this cannot be the full group otherwise X would act trivially on A and G would be abelian. So by the irreducibility of the action we conclude that

$$C_A(x) = \{1\}. \tag{5.1}$$

For the second invariant subgroup take $1 \neq a \in A$ and $a^{\langle x \rangle} = \langle a, a^x, a^{x^2}, \ldots, a^{x^{p-1}} \rangle$, i.e. the group generated by the orbit of a. This time the invariant subgroup contains a non trivial

element and as such

$$a^{\langle x\rangle} = A. \tag{5.2}$$

Now suppose, by way of contradiction, that $a^{1+x}, a^{1+x^2}, \ldots, a^{1+x^{p-1}}$ are all X-conjugate. By (5.2) and the faithfulness of the action we see that all these $p-1$ elements are distinct, otherwise $o(A) = p$ which contradicts the assumptions. Therefore if $b \in A$ is the pth element in this X-conjugacy class then

$$b\prod_{i=1}^{p-1} a^{1+x^i} \in C_A(x) = \{1\}.$$

Also $a^{1+x+x^2+\ldots x^{p-1}} \in C_A(x) = \{1\}$ so that $1 + x + x^2 + \ldots x^{p-1} = 0$ in its action on A. Otherwise said $x + x^2 + \ldots x^{p-1} = -1$ and we conclude $ba^{p-1}a^{-1} = 1$ so that $b = a^{2-p}$. It now follows that there exists a one-to-one function f from $\{1, 2, \ldots, p-1\}$ to itself such that

$$a^{(2-p)x^i} = b^{x^i} = a^{1+x^{f(i)}},$$

for all $1 \le i \le p-1$. In particular, again by (5.2) and the faithfulness of the action, we see $(2-p)x^i = 1 + x^{f(i)}$ as operators on A. But from previous remarks we know we can view A as the additive group of $\mathrm{GF}(q^n)$. Furthermore x can be viewed as element of order p in this field acting by right multiplication on A. Also, once more using $a^{\langle x\rangle} = A$ we see that x generates $\mathrm{GF}(q^n)$ over the prime subfield $\mathrm{GF}(q)$. This implies that the operator equation $(2-p)x^i = 1 + x^{f(i)}$ can in fact be viewed as an equation in the field. Also if $i = f(i)$ for some $1 \le i \le p-1$ then $x^i \in \mathrm{GF}(q)$ and thus also $x \in \mathrm{GF}(q)$. However this would imply that $n = 1$, contrary to our assumption. Now multiply both sides of our equation by x^{-i} to obtain, after setting $j \equiv -i \bmod p$,

$$(2-p) = x^j + x^{g(j)}, \tag{5.3}$$

where $g(j) = f(i) - i \not\equiv 0 \bmod p$. This last equality implies that g is also one-to-one from $\{1, 2, \ldots, p-1\}$ to itself. Now summing the above equation over all j, we obtain

$$(2-p)(p-1) \equiv (-1) + (-1) = -2 \bmod q.$$

Thus $p^2 \equiv 3p \bmod q$ and hence $p \equiv 3 \bmod q$ where we used that $p \neq q$. So in particular $q > 3$ so that $2 - p \equiv -1 \bmod q$. Looking back at (5.3) this gives $1 + x^j = -x^{g(j)}$ for every $1 \le j \le p-1$. Since p is odd and $x^p = 1$, this yields $(1 + x^j)^p = -1$.
In other words $x, x^2, \ldots, x^{p-1} \in \mathrm{GF}(q^n)$ are all roots of the polynomial equations $(1+\zeta)^p = -1$ and $\zeta^p = 1$ in $\mathrm{GF}(q)[\zeta]$. Hence they are roots of

$$2 + (1+\zeta)^p - \zeta^p,$$

a polynomial of degree $p-1$. It thus follows that this polynomial must be a scalar multiple of $1 + \zeta + \zeta^2 + \ldots + \zeta^{p-1}$. Considering the constant term we see that this scalar is 3. This shows that $\binom{p}{k} \equiv 3 \bmod q$ for every $1 \le k \le p-1$. However since $p \equiv 3 \bmod q$ and $p, q \ge 5$ we easily see that $\binom{p}{3} \equiv 1 \not\equiv 3 \bmod q$ so we finally obtain the required contradiction. □

Notice that we explicitly had to make use of the fact that $o(A) \ge q^2$. Also the assumptions on the primes are again necessary. For example if $p = 3$, then $1 + x + x^2 = 0$ in its action on A and

$$a^{1+x} = a^{-x^2} \quad \text{and} \quad a^{1+x^2} = a^{-x},$$

so that clearly these elements are X-conjugate. Next we isolate certain matrix computations from the proof of **Case C**. Just notice the involvement of the elements $a^{1+x}, a^{1+x^2}, \ldots, a^{1+x^{p-1}}$ where the failure of a certain matrix to reach rank 2 will cause (some) irreducible characters of these elements to be equal.

Lemma 5.3.2. *Assume that $G = A \rtimes X$, $\mathfrak{X}$, χ, P and $Q = P^*$ are as in Lemma 5.2.1. Again $\varepsilon_1, \ldots, \varepsilon_p$ are all the complex pth roots of unity. Now let $i \neq i'$ be subscripts such that $\varepsilon_{i'} = \overline{\varepsilon_i}$ and $j \neq j'$ subscripts with $\varepsilon_{j'} = \overline{\varepsilon_j}$. Furthermore, let $a \in A$ be an element whose order is relatively prime to p and assume that the matrix*

$$M = (e_{i,i} + e_{i',i'})Q\mathfrak{X}(a)P(e_{j,j} + e_{j',j'})$$

does not have rank 2. Then

(i) if $i = j$ or $i = j'$, we have that $\chi(a^{1+x^d}) = \chi(a^{1+x})$ for all $1 \leq d \leq p-1$ and

(ii) if $i \neq j$ and $i \neq j'$, then we obtain $\chi(a^{1+x^d}) = \chi(a^{1+x^{ud}})$ for all $1 \leq d \leq p-1$, where $u \not\equiv \pm 1 \bmod p$ and $\varepsilon_j/\overline{\varepsilon_i} = (\varepsilon_j/\varepsilon_i)^u$.

Proof. Suppose a has order q where by assumption q is relatively prime to p. Therefore, write $\mathfrak{X}(a) = \operatorname{diag}(\alpha_0, \alpha_1, \ldots, \alpha_{p-1})$, where each of the α_d is a qth root of unity and the subscripts can be viewed modulo p. Without loss of generality one can assume $\mathfrak{X}(x)^{-1}\mathfrak{X}(a)\mathfrak{X}(x) = \operatorname{diag}(\alpha_{p-1}, \alpha_0, \ldots, \alpha_{p-2})$ and it is then easily seen that

$$\mathfrak{X}(x)^{-d}\mathfrak{X}(a)\mathfrak{X}(x)^d = \operatorname{diag}(\alpha_{0-d}, \alpha_{1-d}, \ldots, \alpha_{p-1-d}).$$

It follows that

$$\mathfrak{X}(a^{1+x^d}) = \mathfrak{X}(aa^{x^d}) = \operatorname{diag}(\alpha_0\alpha_{0-d}, \alpha_1\alpha_{1-d}, \ldots, \alpha_{p-1}\alpha_{p-1-d}),$$

which implies $\chi(a^{1+x^d}) = \sum_{r=0}^{p-1} \alpha_r\alpha_{r-d}$. Continuing forward, if ρ is a pth root of unity, we set $\operatorname{Tr}(\rho, a) = \sum_{r=0}^{p-1} \rho^r\alpha_r$ to obtain

$$\begin{aligned}\operatorname{Tr}(\rho,a)\operatorname{Tr}(\rho^{-1},a) = \left(\sum_{r=0}^{p-1}\rho^r\alpha_r\right)\left(\sum_{s=0}^{p-1}\rho^{-s}\alpha_s\right) &= \sum_{s=0}^{p-1}\left(\rho^{-s}\alpha_s\sum_{r=0}^{p-1}\rho^r\alpha_r\right)\\ &= \sum_{s=0}^{p-1}\left(\sum_{r=0}^{p-1}\rho^{r-s}\alpha_r\alpha_s\right)\\ &= \sum_{d=0}^{p-1}\left(\sum_{r=0}^{p-1}\rho^d\alpha_r\alpha_{r-d}\right) = \sum_{d=0}^{p-1}\rho^d\chi(a^{1+x^d}).\end{aligned}$$

This gives us the necessary tools to start calculating with the matrix M. We first look at the middle matrices. Observe that the (i,j)th entry of $Q\mathfrak{X}(a)P$ is given by

$$\frac{1}{p}\sum_{r=0}^{p-1}\overline{\varepsilon_i}^r\alpha_r\varepsilon_j^r = \frac{1}{p}\operatorname{Tr}(\varepsilon_j/\varepsilon_i, a).$$

Also since $\varepsilon_{i'} = \overline{\varepsilon_i}$ and $\varepsilon_{j'} = \overline{\varepsilon_j}$, we see that the 2×2 submatrix corresponding to the intersection of the ith and i'th rows and jth and j'th columns is given by

$$M_{2\times 2} = \frac{1}{p}\begin{bmatrix}\operatorname{Tr}(\varepsilon_j/\varepsilon_i,a) & \operatorname{Tr}(\varepsilon_{j'}/\varepsilon_i,a)\\ \operatorname{Tr}(\varepsilon_j/\varepsilon_{i'},a) & \operatorname{Tr}(\varepsilon_{j'}/\varepsilon_{i'},a)\end{bmatrix} = \frac{1}{p}\begin{bmatrix}\operatorname{Tr}(\varepsilon_j/\varepsilon_i,a) & \operatorname{Tr}(\overline{\varepsilon_j}/\varepsilon_i,a)\\ \operatorname{Tr}(\varepsilon_j/\overline{\varepsilon_i},a) & \operatorname{Tr}(\overline{\varepsilon_j}/\overline{\varepsilon_i},a)\end{bmatrix}.$$

Clearly this matrix consists of the four nonzero values of M and as such it has the same rank as M. Now setting $\sigma = \varepsilon_j/\varepsilon_i$ and $\tau = \varepsilon_j/\overline{\varepsilon_i}$, we obtain that $\sigma \neq \tau, \overline{\tau}$ and

$$M_{2\times 2} = \frac{1}{p}\begin{bmatrix}\operatorname{Tr}(\sigma,a) & \operatorname{Tr}(\overline{\tau},a)\\ \operatorname{Tr}(\tau,a) & \operatorname{Tr}(\overline{\sigma},a)\end{bmatrix}.$$

Since rank $M \neq 2$ it is clear that $\det M_{2\times 2} = 0$. It follows that $\operatorname{Tr}(\sigma,a)\operatorname{Tr}(\overline{\sigma},a) = \operatorname{Tr}(\tau,a)\operatorname{Tr}(\overline{\tau},a)$ and the cleverly made calculations from above show that

$$\sum_{d=0}^{p-1}\sigma^d\chi(a^{1+x^d}) = \sum_{d=0}^{p-1}\tau^d\chi(a^{1+x^d}). \tag{5.4}$$

Now since a is an element of order q we can consider each $\chi(a^{1+x^d})$ as an element in $\mathbb{Q}[\delta]$ where δ is a primitive complex qth root of unity. In particular (5.4) is a polynomial in two variables satisfied by the two pth roots of unity σ and τ. Similar to the proof of the previous lemma we know, since $\gcd(p,q)=1$, that any such equation is a scalar multiple of $1+\zeta+\ldots+\zeta^{p-1}$.
(i) First suppose that $i=j$, then $\varepsilon_i=\varepsilon_j$ so that $\sigma=1$ and τ is a primitive pth root of unity. As (5.4) is a polynomial equation in τ of degree smaller or equal then $p-1$ we see from above arguments that the coefficients of the powers of τ must be equal. This clearly implies that $\chi(a^{1+x^d})=\chi(a^{1+x})$ for every $1\leq d\leq p-1$. Similarly, if $i=j'$, then $\tau=1$ and σ is a primitive pth root of unity and the same remarks apply.
(ii) So consider now the case where $i\neq j$ and $i\neq j'$. Then both σ and τ are primitive p roots of unity. It follows we can write $\tau=\sigma^u$ for some $1\leq u\leq p-1$. Moreover since $\tau\neq\sigma$ and $\tau\neq\overline{\sigma}$ we can take $2\leq u\leq p-2$. Remembering to view the exponents modulo p, equation (5.4) has the form

$$\sum_{d=0}^{p-1}\sigma^d\chi(a^{1+x^d})=\sum_{d=0}^{p-1}\sigma^{ud}\chi(a^{1+x^d}).$$

Since the coefficients match for $d=0$ this implies that all coefficients match and in particular $\chi(a^{1+x^d})=\chi(a^{1+x^{ud}})$ for all $1\leq d\leq p-1$. Clearly $\varepsilon_j/\overline{\varepsilon_i}=\tau=\sigma^u=(\varepsilon_j/\varepsilon_i)^u$. Thus all assertions of this lemma have now been proven. □

We will immediately start with the proof of our last case. As said earlier: notice the specific choice of our group elements and parameters in this proof.

Case C. *Let $G=A\rtimes X$ be a semidirect product of*

(1) a normal subgroup A which is an elementary abelian q-group of order at least q^2, where $q\geq 3$ and

(2) a cyclic subgroup $X=\langle x\rangle$ where x has prime order $p\geq 5$ and p is necessarily different from q,

then there exist Bass cyclic units $u_{k,tn}(x)$ and $u_{k,tn}(x^{a^{-1}})$, where $1\neq a\in A$, that generate a non-abelian free subgroup of the unit group of the integral group ring $\mathbb{Z}[G]$, where again n is a positive integers.

Proof. We start off to proof this last case by taking an arbitrary $1\neq a\in A$. Readily checked in Lemma 5.3.1 we know that the elements $a^{1+x},a^{1+x^2},\ldots,a^{1+x^{p-1}}$ cannot all be X-conjugate to a^{1+x}. In other words there exists a u with $1\leq u\leq p-1$ such that a^{1+x^u} is not X-conjugate to a^{1+x}. Fortunately we know that $(a^{1+x})^{x^{-1}}=a^{1+x^{-1}}$ so we can clearly restrict u and assume $2\leq u\leq p-2$. Let us now choose Bass cyclic units

$$u_{k,t}(x)\qquad\text{and}\qquad u_{k,t}(x^{a^{-1}})=a^{-1}u_{k,t}(x)a.$$

Contrary to the previous cases the first parameters of both units are necessarily equal where we could have chosen them to differ in the previous cases, also we will not take k to be arbitrary, rather set

$$k\equiv\frac{u-1}{u+1}\bmod p.$$

Clearly $k\not\equiv 0 \bmod p$ and, since $u\equiv(1+k)/(1-k) \bmod p$ we also see $k\not\equiv\pm 1 \bmod p$ which shows that k fulfills our requirements for being a parameter of a proper Bass cyclic units, so we are allowed to assume $2\leq k\leq p-2$.
Now to again find a suitable representation of G, first notice that G acts on A as X does. This means that a^{1+x} and a^{1+x^u} are not G-conjugate and they are thus contained in different conjugacy classes of G. As a consequence there exists an irreducible representation $\mathfrak{X}$ of $\mathbb{C}[G]$, with corresponding character χ, such that $\chi(a^{1+x})\neq\chi(a^{1+x^u})$. Moreover taking complex

conjugates we also see that $\chi(a^{-(1+x)}) \neq \chi(a^{-(1+x^u)})$. Furthermore we know that X acts faithfully and irreducibly on A and since the commutor subgroup G' is an invariant subgroup of A we see that $A = G'$. But $\mathbb{C}$ is abelian so if $\mathfrak{X}$ would be linear then $\mathfrak{X}(A) = \{1\}$ and $\chi(a^{1+x}) = 1 = \chi(a^{1+x^u})$, a contradiction. So $\chi(1) \neq 1$ and Lemma 5.2.1 is applicable. In particular $\chi(1) = p$ and we can assume that $\mathfrak{X}(a)$ and $\mathfrak{X}(x)$ are described as in the lemma. Furthermore if we set $\varepsilon = e^{2\pi i/p}$, then we take $\varepsilon_l = \varepsilon^l$ in the description of the matrix P, for all $1 \leq l \leq p$.
From Lemma 5.2.1(ii) we get that $P^{-1}\mathfrak{X}(x)P = \operatorname{diag}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p)$ so again following the example of the previous cases we set $T = \mathfrak{X}(u_{k,s}(x))$ which is diagonalizable since

$$P^{-1}TP = \operatorname{diag}(u_{k,t}(\varepsilon_1), u_{k,t}(\varepsilon_2), \ldots, u_{k,t}(\varepsilon_p)).$$

So we know the eigenvalues of T and by our specific ordering of the primitive complex pth roots of unity we see from Lemma 4.2.2 that $u_{k,t}(\varepsilon_i)$ and $u_{k,t}(\varepsilon_{i'})$ are the two eigenvalues of T having the largest absolute value if and only if $i = 1$ and $i' = p-1$. Also $\varepsilon_{i'} = \overline{\varepsilon_i}$ as before. Furthermore $u_{k,t}(\varepsilon_j)$ and $u_{k,t}(\varepsilon_{j'})$ are the two eigenvalues having the smallest absolute value if and only if this time $j \equiv k^{-1} \bmod p$ and $j' \equiv -k^{-1} \bmod p$. Again $\varepsilon_{j'} = \overline{\varepsilon_j}$. We thus once more find a T-decomposition of $\mathbb{C}^p = V = T_+ \oplus T_0 \oplus T_-$ with $\dim T_+ = \dim T_- = 2$. Again suppose that τ_+ and τ_- are the corresponding projections of V into T_+ and T_-, respectively, then

$$\tau_+ = P(e_{i,i} + e_{i',i'})P^{-1} \qquad \text{and} \qquad \tau_- = P(e_{j,j} + e_{j',j'})P^{-1}.$$

Now let us take a look at our second Bass cyclic unit. Set

$$S = \mathfrak{X}(u_{k,t}(x^{a^{-1}})) = \mathfrak{X}(a)^{-1}\mathfrak{X}(u_{k,t}(x))\mathfrak{X}(a).$$

Then S and T are conjugate to each other and clearly $\mathbb{C}^p = V$ also has an S-decomposition $V = S_+ \oplus S_0 \oplus S_-$ with $\dim S_+ = \dim S_- = 2$. Furthermore this time the corresponding projections σ_+ and σ_- from V into S_+ and S_-, respectively, satisfy

$$\begin{aligned} \sigma_+ &= \mathfrak{X}(a)^{-1}\tau_+\mathfrak{X}(a) = \mathfrak{X}(a)^{-1}P(e_{i,i} + e_{i',i'})P^{-1}\mathfrak{X}(a) \qquad \text{and} \\ \sigma_- &= \mathfrak{X}(a)^{-1}\tau_-\mathfrak{X}(a) = \mathfrak{X}(a)^{-1}P(e_{j,j} + e_{j',j'})P^{-1}\mathfrak{X}(a). \end{aligned}$$

Again both S and T are diagonalizable, so in order for some powers of them to generate a free group of rank 2, it again remains to verify the eight idempotent conditions set in Corollary 3.5.1. However we can again simplify these verifications by noticing that both P and $\mathfrak{X}(a)$ are unitary. It follows that $\sigma_\pm$ and $\tau_\pm$ are Hermetian so that $(\tau_\pm\sigma_\pm)^* = \sigma_\pm^*\tau_\pm^* = \sigma_\pm\tau_\pm$ and therefore $\operatorname{rank} \tau_\pm\sigma_\pm = \operatorname{rank} \sigma_\pm\tau_\pm$. This reduces the number of ranks to check by half. So since P and $\mathfrak{X}(a)$ are nonsingular matrices we see that

$$\operatorname{rank} \sigma_\pm\tau_\pm = \operatorname{rank} (e_{r,r} + e_{r',r'})P^{-1}\mathfrak{X}(a)P(e_{s,s} + e_{s',s'}),$$

where $r = i$ or j and also $s = i$ or j. Clearly this is the part where the calculations in the previous lemma comes to good use.
(i) First of all if $r = s$ then we know from Lemma 5.3.2(i) that if these matrices do not have rank 2, then $\chi(a^{1+x}) = \chi(a^{1+x^d})$ for all $1 \leq d \leq p-1$ which is clearly a contradiction to our choice of irreducible representation which states that $\chi(a^{1+x}) \neq \chi(a^{1+x^u})$. This solves the first two cases.
(ii) Secondly observe that

$$\left[(e_{i,i} + e_{i',i'})P^{-1}\mathfrak{X}(a)P(e_{j,j} + e_{j',j'})\right]^* = (e_{j,j} + e_{j',j'})P^{-1}\mathfrak{X}(a^{-1})P(e_{i,i} + e_{i',i'}),$$

so it is sufficient to only look at the case $i = r \neq s = j$. So suppose

$$M = (e_{i,i} + e_{i',i'})P^{-1}\mathfrak{X}(a)P(e_{j,j} + e_{j',j'}),$$

and that this matrix does not have rank 2. Also let u' be defined such that $\varepsilon_j/\overline{\varepsilon_i} = (\varepsilon_j/\varepsilon_i)^{u'}$. Due to our specific ordering of the pth roots of unity used to construct P we have $\varepsilon_j/\overline{\varepsilon_i} =$

$\varepsilon^{k^{-1}+1}$ and $\varepsilon_j/\varepsilon_i = \varepsilon^{k^{-1}-1}$. Taking into account the choice of u' this shows that $u' \equiv (1+k)/(1-k) \equiv u \bmod p$. But Lemma 5.3.2(ii) tells us that $\chi(a^{1+x}) = \chi(a^{1+x^{u'}}) = \chi(a^{1+x^u})$ which again conflicts with our specific choice of the parameters u and k and the choice of irreducible representation in which $\chi(a^{1+x}) \neq \chi(a^{1+x^u})$. This shows that M does indeed have rank 2 and all idempotent conditions are satisfied.
By Corollary 3.5.1 there exists a positive integer n such that $\langle S^n, T^n\rangle = \langle S^n\rangle * \langle T^n\rangle$ is a free group of rank 2. Again this shows that $u_{k,t}(x^{a^{-1}})^n$ and $u_{k,t}(x)^n$ also generate a free group of rank 2 in the unit group of $\mathbb{Z}[G]$. Moreover we have that $u_{k,t}(x^{a^{-1}})^n = u_{k,tn}(x^{a^{-1}})$ and $u_{k,t}(x)^n = u_{k,tn}(x)$ by Proposition 4.1.1, and finally the result follows. □

All pieces of the puzzle have now been acquired. The explanations and remarks made up until this moment should make the claim of the main theorem clear. However we will still include a complete proof of Gonçalves's and Passman's result to show how these pieces complete the puzzle.

Main result. *Let G be a finite non-abelian group whose order is relatively prime to 6, then there exist two elements g and h in G of prime power order and two Bass cyclic units $u_{k,t}(g)$ and $u_{r,s}(h)$ such that $\langle u_{k,t}(g), u_{r,s}(h)\rangle$ is a non-abelian free subgroup of the unit group of the integral group ring $\mathbb{Z}[G]$.*

Proof. As mentioned earlier we proceed by induction on the order of G. So first assume G is a non-abelian group whose order is minimal and relatively prime to 6. Then clearly every proper subgroup of G is abelian and also every proper epimorphic image is abelian. Therefore G is as in one of the three cases and the result follows from the previous study of these three cases.
So let G be an arbitrary group, whose order is relatively prime to 6. If G has a proper non-abelian subgroup H then by induction this subgroup contains two Bass cyclic units $u_{k,t}(g)$ and $u_{r,s}(h)$ such that the group generated by these to units is free of rank 2 in $\mathcal{U}(\mathbb{Z}[H])$. Clearly these two elements are also units in $\mathbb{Z}[G]$ and as such the result again follows for G.
Otherwise suppose G has a proper epimorphic image $\overline{G}$ which is non-abelian. Then again by induction the result follows for $\overline{G}$ and it contains two Bass cyclic units $u_{k,t}(\overline{g})$ and $u_{r,s}(\overline{h})$ such that the group generated by these two units is free of rank 2 in $\mathcal{U}(\mathbb{Z}[\overline{G}])$. But Lemma 4.1.2 then shows us that G contains two units g and h with the same order as $\overline{g}$ and $\overline{h}$ such that $u_{k,t'}(g)$ and $u_{r,s'}(h)$ maps to powers of $u_{k,t}(\overline{g})$ and $u_{r,s}(\overline{h})$, respectively, under the natural homomorphism $\mathbb{Z}[G] \to \mathbb{Z}[\overline{G}]$. This shows that $\langle u_{k,t'}(g), u_{r,s'}(h)\rangle = \langle u_{k,t'}(g)\rangle * \langle u_{r,s'}(h)\rangle$ is the required free group of rank 2.
Finally if G does not have a proper non-abelian subgroup and it does not have a proper epimorphic image which is non-abelian then we are back in our thee studied cases and again the result follows from our previous work. This concludes the proof of our main theorem. □

Clearly the implication in this main theorem cannot be reversed. It is not because an integral groups ring $\mathbb{Z}[G]$ over a non-abelian group G contains two free Bass cyclic units that the order of G is relatively prime to 6. To see this just take a non-abelian group G such that $\gcd(o(G), 6) = 1$, then the free Bass cyclic units found in $\mathbb{Z}[G]$ clearly also generate a free group of rank 2 in the unit group of $\mathbb{Z}[G \times H]$ where H is any group, possibly having order $o(H)$ not relatively prime to 6. However these are not the only examples and using the techniques introduced in [GP06] we can construct others.

Example 5.3.3. Let us start by defining two groups

$$X = \langle x\rangle = C_5 \quad \text{and} \quad A = A_0 \times A_1 \times A_2 \times A_3 \times A_4,$$

where $A_i = \langle a_i\rangle = C_8$ with $i \in \mathbb{Z}_5$. We use these groups to define a non-abelian group $G = A \rtimes X$ in which $a_i^x = a_{i+1}$ and we remember to view these subscripts modulo 5. First choose two Bass cyclic units

$$u_{3,4}(a_0) \quad \text{and} \quad u_{3,4}(x)$$

in $\mathbb{Z}[G]$. Notice that all the parameters fulfill the necessary requirements. Next set $\varepsilon_i = e^{2\pi i/8}$ and $\delta_j = e^{2\pi j/5}$ with $i \in \mathbb{Z}_8$ and $j \in \mathbb{Z}_5$. Using these roots of unity we define a suitable representation $\mathfrak{X} : \mathbb{Z}[G] \to \mathrm{M}_5(\mathbb{C})$ by setting

$$\mathfrak{X}(a_0) = \begin{bmatrix} 1 & & & & \\ & \varepsilon_1 & & & \\ & & \varepsilon_3 & & \\ & & & \varepsilon_5 & \\ & & & & \varepsilon_7 \end{bmatrix} \quad \text{and} \quad \mathfrak{X}(x) = \begin{bmatrix} & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \\ 1 & & & & \end{bmatrix}.$$

Clearly all other elements are now uniquely determined using the relations in the group G and linearly extending the resulting representation to one on $\mathbb{Z}[G]$. Finally set

$$P = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \delta_1 & \delta_2 & \delta_3 & \delta_4 \\ 1 & \delta_2 & \delta_4 & \delta_1 & \delta_3 \\ 1 & \delta_3 & \delta_1 & \delta_4 & \delta_2 \\ 1 & \delta_4 & \delta_3 & \delta_2 & \delta_1 \end{bmatrix} \quad \text{to obtain} \quad P^{-1}\mathfrak{X}(x)P = \begin{bmatrix} 1 & & & & \\ & \delta_1 & & & \\ & & \delta_2 & & \\ & & & \delta_3 & \\ & & & & \delta_4 \end{bmatrix}.$$

From now on the arguments are almost exactly the same as in the proof of **Case A**. Nonetheless we continue on one last time and as to be expected we set $T = \mathfrak{X}(u_{3,4}(x))$. Again Lemma 4.2.2 tells us that $u_{3,4}(\delta_1)$ and $u_{3,4}(\delta_4)$ are the eigenvalues of T having the largest absolute value while $u_{3,4}(\delta_2)$ and $u_{3,4}(\delta_3)$ have the smallest absolute value. So we obtain a T-decomposition $V = T_+ \oplus T_0 \oplus T_-$ of $V = \mathbb{C}^5$ where $\dim T_+ = 2 = \dim T_-$. Moreover the projections τ_+ and τ_- of V onto T_+ and T_-, respectively, are canonically defined and given by

$$\tau_+ = P(e_{2,2} + e_{5,5})P^{-1} \qquad \text{and} \qquad \tau_- = P(e_{3,3} + e_{4,4})P^{-1}.$$

Continuing on the path set before us, we take $S = \mathfrak{X}(u_{3,4}(a_0))$. Due to our specific choice of representation we again see that two eigenvalues of S have the largest absolute value, namely $u_{3,4}(\varepsilon_1)$ and $u_{3,4}(\varepsilon_7)$, while two have the smallest absolute value, namely $u_{3,4}(\varepsilon_3)$ and $u_{3,4}(\varepsilon_5)$. So we also have a suitable S-decomposition $V = S_+ \oplus S_0 \oplus S_-$ of $V = \mathbb{C}^5$, i.e. $\dim S_+ = 2 = \dim S_-$. The projections σ_+ and σ_- from V into S_+ and S_-, respectively, are now given by

$$\sigma_+ = (e_{2,2} + e_{5,5}) \qquad \text{and} \qquad \sigma_- = (e_{3,3} + e_{4,4}).$$

So once more we need to check the idempotent conditions set in Corollary 3.5.1. First look at the ranks of the matrices $M^{i,i',j,j'} = (e_{i,i} + e_{i',i'})P(e_{j,j} + e_{j',j'})$ with $2 \leq i, i', j, j' \leq 5$ and both $i' \neq i, j$ and $j' \neq i, j$. But these matrices only have four nonzero elements namely on the intersection of the ith and i'th rows with the jth and j'th columns. Again these give rise to the submatrices

$$M^{i,i',j,j'}_{2\times 2} = \frac{1}{\sqrt{5}} \begin{bmatrix} \delta^i_{j-1} & \delta^i_{j'-1} \\ \delta^{i'}_{j-1} & \delta^{i'}_{j'-1} \end{bmatrix},$$

and since $(\delta_{j-1}/\delta_{j'-1})^i \neq (\delta_{j-1}/\delta_{j'-1})^{i'}$ we see these submatrices all have determinant different from 0. So all matrices $M^{i,i',j,j'}$ have rank 2 and we clearly have that the four ranks rank $\sigma_\pm\tau_\pm$ also have rank 2. Since the $\sigma_\pm$ and $\tau_\pm$ are all Hermetian we also see that $(\sigma_\pm\tau_\pm)^* = \tau_\pm\sigma_\pm$ so the four operators $\tau_\pm\sigma_\pm$ again have rank 2.
Corollary 3.5.1 now tells us that there exist positive integers m and n such that S^m and T^n generate a non-abelian free group of rank 2 and consequently the same holds for $u_{3,4}(a_0)^m = u_{3,4m}(a_0)$ and $u_{3,4}(x)^n = u_{3,4n}(x)$. △

Clearly the group in the previous example is a non-abelian groups whose order is not relatively prime to 6 and moreover it is not of the form $G \times H$ as in the remarks following the main theorem. This opens a door to many other examples and classes of groups $\mathcal{G}$ such that the unit group of the integral group ring over one of these groups in the class $\mathcal{G}$ contains a free pair of Bass cyclic units. One example being the next theorem which is given by Passman.

Theorem 5.3.4. *Let $p \geq 5$ be a prime and let $d = p^w$ be a power of p. Suppose x and y are two d-cycles in $G = S_n$, the symmetric group of permutations of a set of size n. If x and y are of the form*

$$x = (1\ 2 \dots k\ x_{k+1}\ x_{k+2} \dots x_d) \quad \text{and} \quad y = (1\ 2 \dots k\ y_{k+1}\ y_{k+2} \dots y_d),$$

such that $\{x_{k+1}, x_{k+2}, \dots, x_d\}$ and $\{y_{k+1}, y_{k+2}, \dots y_d\}$ are disjoint subsets of the set $\{k+1, k+2, \dots, n\}$ of remaining numbers, and $k \not\equiv 0, \pm 1 \bmod p$, then for all parameters s and s', there exists an m and m', so that the Bass cyclic units $u_{s,m}(x)$ and $u_{s',m'}(y)$ generate a non-abelian free subgroup of the unit group of $\mathbb{Z}[G]$.

Proof. [Pas08, Theorem 3.4] □

5.4 Free product of a Bass cyclic unit with a bicyclic unit

Up until now we have only stated results concerning two Bass cyclic units. For this we have utilized those theorems in Chapter 3 making use of only diagonalizable operators and not those making use of generalized transvections. Therefore we quickly take a look at bicyclic units. Let us first take a look at a subgroup H of the finite group G and denote by $\widehat{H} \in \mathbb{Z}[G]$ the sum of all elements of H in $\mathbb{Z}[G]$. Notice that for every $h \in H$, $(1-h)\widehat{H} = 0 = \widehat{H}(1-h)$. This shows that the group ring elements $(1-h)g\widehat{H}$, with $g \in G$, have square zero. Consequently $1 + (1-h)g\widehat{H}$ is a unit in the ring $\mathbb{Z}[G]$ with inverse $1 - (1-h)g\widehat{H}$. We note that $1 + \widehat{H}g(1-h)$ is also a unit having inverse $1 - \widehat{H}g(1-h)$. When $H = \langle h \rangle$ is cyclic then honoring the notation used in Chapter 4 we denote $\widehat{H}$ as $\hat{h}$. Elements of the form

$$\beta_{g,h} = 1 + (1-h)g\hat{h} \quad \text{and} \quad \gamma_{g,h} = 1 + \hat{h}g(1-h),$$

are called *bicyclic* units. It is not difficult to verify that $1 + (1-h)g\widehat{H} = 1$ if and only if $h^g \in H$ and hence if and only if $g \in N_G(H)$. In particular, if G is a Dedekind group, i.e. a group with every subgroup normal, then $\mathbb{Z}[G]$ has no non trivial bicyclic units. Now if $\mathfrak{X}$ is a (suitable) complex irreducible representation of G then

$$\beta_{g,h} \mapsto \mathfrak{X}(\beta_{g,h}) = 1 + \mathfrak{X}((1-h)g\hat{h}),$$

where $\mathfrak{X}((1-h)g\hat{h})$ is a (nonzero) matrix of square zero. This shows, via the correspondence between operators and matrices, that $\mathfrak{X}(\beta_{g,h})$ is a generalized transvection.

We conclude this master thesis by sketching the proof of a result found in [GdR08], which is due to Gonçalves and del Río in 2008. The techniques used are based on those introduced in [GP06] and described in the thesis.

Secondary result. *Let G be a finite non-abelian group whose order is relatively prime to 6, then $\mathbb{Z}[G]$ contains a bicyclic unit β and a Bass cyclic unit u such that β^t and u generate a non-abelian free group of the unit group $\mathcal{U}(\mathbb{Z}[G])$, for any sufficiently large integer t.*

Let us briefly describe the steps used to proof this result. As said earlier the complete proof can be found in [GdR08, Theorem 1.3].

Step 1: *Reducing the number of groups needed to be investigated.*

This secondary result will again be proven by induction on the order $o(G)$ of G. Following the reasoning in the main result, we can again assume that the non-abelian group G only has proper subgroups H which are abelian. For if H is non-abelian and the result holds then the Bass cyclic units u, respectively the bicyclic units β, found in $\mathbb{Z}[H]$ is again a Bass cyclic

unit, respectively bicyclic unit, of $\mathbb{Z}[G]$. Also because these two units form a free pair in $\mathbb{Z}[H]$ they also generate a free group of rank 2 in $\mathbb{Z}[G]$. Moreover we can once more assume that every proper epimorphic image $\overline{G}$ of G is abelian, this by again using the same arguments as in the proof of the main result. So every proper subgroup and epimorphic image of the non-abelian group G is abelian and these groups where classified in Section 5.1.

Step 2: *Choosing the right units.*

Now we need to find suitable group elements of G which we can use the construct a Bass cyclic unit u and bicyclic unit β, this for all three cases. From the definition we see β requires two group elements g and h such that $h^g \notin \langle h \rangle$. Since $G = A \rtimes X$ where $X = \langle x \rangle$ is not normal in G we readily see that there exists an $a \in A$ such that $x^a \notin X$. Specifically

Case A: A is cyclic and we can take a to be a generator of A,

Case B: $A = \langle y \rangle \times \langle z \rangle$ where $\langle z \rangle = G' = Z(G)$ and we can just take $a = y$,

Case C: $Z(G) = 1$ and we can take a to be any non trivial element of A.

After choosing a in each specific case we will fix it for the duration of the proof. It will also be used for the construction of the Bass cyclic unit u. So set

$$u = u_{k,m}(a) \quad \text{and} \quad \beta = \beta_{a,x} = 1 + (1 - x)a\hat{x},$$

where m is a multiple of $\varphi(q)$, where q is the order of a, and $2 \leq k \leq q - 2$. Additional conditions on m will be specified later.

Step 3: *Describing a suitable irreducible complex representation.*

Now the commutator $[a, x] \neq 1$ and we know there exists a necessarily nonlinear irreducible representation $\mathfrak{X}$ of G such that $\mathfrak{X}([a, x]) \neq 1$. Moreover, due to the specific structures of our groups, Lemma 5.2.1 gives a thorough description of these representations. What was not specified is that in **Case C** we may assume that $\mu(a) = 1$. This observation will be useful for the following. We know $\mathfrak{X}(a) = \operatorname{diag}(\alpha_0, \ldots, \alpha_{p-1})$ is a non-scalar matrix and if we set $\Lambda = \{\alpha_i \mid 0 \leq i \leq p - 1\}$ we know from the previous sections that

Case A: $o(\Lambda) = p$ and no two elements in Λ are complex conjugate to each other,

Case B: $o(\Lambda) = p$ and all pth roots of unity are represented,

Case C: $o(\Lambda) \neq p$ and Λ contains at least two elements including 1.

Now the representation of our units are given by

$$S = \mathfrak{X}(u) = \begin{bmatrix} u_{k,m}(\alpha_0) & & & \\ & u_{k,m}(\alpha_1) & & \\ & & \ddots & \\ & & & u_{k,m}(\alpha_{p-1}) \end{bmatrix} = \begin{bmatrix} u_0 & & & \\ & u_1 & & \\ & & \ddots & \\ & & & u_{p-1} \end{bmatrix}.$$

and $T = \mathfrak{X}(\beta) = 1 + \tau$ where

$$\tau = \begin{bmatrix} \alpha_0 - \alpha_1 & \alpha_0 - \alpha_1 & \ldots & \alpha_0 - \alpha_1 \\ \alpha_1 - \alpha_2 & \alpha_1 - \alpha_2 & \ldots & \alpha_1 - \alpha_2 \\ \vdots & \vdots & & \vdots \\ \alpha_{p-1} - \alpha_0 & \alpha_{p-1} - \alpha_0 & \ldots & \alpha_{p-1} - \alpha_0 \end{bmatrix}.$$

Notice that the same values α_i appear in both the representations of u and β. This is why the group element a was used to construct u rather then x.

Step 4: *Finding the attractors and repulsers.*

Following the reasoning of Chapter 3 we are now faced with finding the attractors and repulsers of the operators/matrices $\mathfrak{X}(u)$ and $\mathfrak{X}(\beta)$. Let us start with the second one. The attractor here is the image I of τ while the repulser is the kernel K. It is easily seen that

$$I = \operatorname{im} \tau = \tau(\mathbb{C}^p) = \mathbb{C}\Psi \quad \text{where} \quad \Psi = \begin{bmatrix} \alpha_0 - \alpha_1 \\ \alpha_1 - \alpha_2 \\ \vdots \\ \alpha_{p-1} - \alpha_0 \end{bmatrix},$$

and

$$K = \ker \tau = \left\{ \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{p-1} \end{bmatrix} : x_0 + \ldots + x_{p-1} = 0 \right\}.$$

The attractors and repulsers of (the positive powers of) $\mathfrak{X}(u)$ are the sets

(i) S_+ the subspace of $V = \mathbb{C}^p$ spanned by the eigenvectors of $S = \mathfrak{X}(u)$ corresponding to the eigenvalues u_i having maximal absolute value and

(ii) S_- the subspace of $V = \mathbb{C}^p$ spanned by the eigenvectors of $S = \mathfrak{X}(u)$ corresponding to the eigenvalues u_j having minimal absolute value.

As usual S_0 will denote the subspace spanned of the remaining eigenvalues. The observations made concerning the size and consistency of Λ in each of the cases show that $S_+ \neq V \neq S_-$ which implies that $S_+ \neq \{0\}$ and $S_- \neq \{0\}$ as needed.

Step 5: *Checking the intersection requirements.*

It seems logical now to prove that S and T satisfy the conditions of Theorem 3.3.5, i.e that the four intersections $S_\pm \cap K$ and $I \cap (S_0 \oplus S_\pm)$ are trivial. Unfortunately in **Case C** it might be possible, and in **Case B** it certainly is the case, that S_+, respectively S_-, has dimension two. Since K is a hyperplane this implies that $K \cap S_\pm \neq \{0\}$. This is the point where more criteria are imposed on the parameter m, specifically m is also taken to be a multiple of q, the order of a. As a consequence if $\varepsilon \neq 1$ is a qth root of unity then

$$u_{k,m}(\varepsilon) = \left(\frac{\varepsilon^k - 1}{\varepsilon - 1}\right)^m = \left(\frac{\varepsilon^k(1 - \overline{\varepsilon}^k)}{\varepsilon(1 - \overline{\varepsilon})}\right)^m = \left(\frac{\varepsilon^k}{\varepsilon}\right)^m \left(\frac{\overline{\varepsilon}^k - 1}{\overline{\varepsilon} - 1}\right)^m = \left(\frac{\overline{\varepsilon}^k - 1}{\overline{\varepsilon} - 1}\right)^m = u_{k,m}(\overline{\varepsilon}).$$

So now two eigenvalues u_i and u_j of $S = \mathfrak{X}(u)$ have equal absolute value if and only if they are equal. This implies that $W = (S_+ \cap K) \oplus (S_- \cap K)$ is invariant under the action of S and by this S and T induce endomorphisms $\overline{S}$ and $\overline{T}$ on the quotient space $\overline{V} = V/W$. The $\overline{S}$-decomposition of $\overline{V}$ is given by $\overline{V} = \overline{S_+} \oplus \overline{S_0} \oplus \overline{S_-}$. It is now not that difficult to show that $\overline{S}$ and $\overline{T}$ do fulfill the hypothesis of Theorem 3.3.5 and if follows that $\overline{S}^s$ and $\overline{T}^t$ generate a non-abelian free subgroup of $\mathrm{GL}(\overline{V})$, for any sufficiently large integers s and t. So $u_{k,ms}(a)$ and $\beta_{a,x}^t$ also generate a non-abelian free subgroup of the unit group $\mathcal{U}(\mathbb{Z}[G])$. This concludes our brief description of the proof of the secondary result.

Similar to the previous section we conclude by giving a secondary example of a group G whose order is not relatively prime to 6 such that the unit group of the integral group ring $\mathbb{Z}[G]$ still contains a free pair (u, β^t) consisting of a Bass cyclic unit u and a power of a bicyclic unit β.

Theorem 5.4.1. *Let $G = A_n$, receptively $G = S_n$, the alternating group of a finite set of order $n \geq 5$, respectively the symmetric group, then $\mathbb{Z}[G]$ contains a Bass cyclic unit u and a bicyclic unit β such that the subgroup generated by u and β^t is free of rank 2, for any sufficiently large integer t.*

Proof. [GdR08, Theorem 7.3] □

References

[Bou66a] Nicolas Bourbaki. *Elements of mathematics. General topology. Part 1.* Hermann, Paris, 1966.

[Bou66b] Nicolas Bourbaki. *Elements of mathematics. General topology. Part 2.* Hermann, Paris, 1966.

[Bou72] Nicolas Bourbaki. *Elements of mathematics. Commutative algebra.* Hermann, Paris, 1972. Translated from the French.

[Cay54] Arthur Cayley. On the theory of groups, as depending on the symbolic equation $\theta^n = 1$. *Philosophical Magazine*, 7(4):408–409, 1854.

[CJR58] Bomshik Chang, S. A. Jennings, and Rimhak Ree. On certain pairs of matrices which generate free groups. *Canad. J. Math.*, 10:279–284, 1958.

[Fer03] Raul Antonio Ferraz. Free subgroups in the units of $\mathbb{Z}[K_8 \times C_p]$. *Comm. Algebra*, 31(9):4291–4299, 2003.

[GdR08] Jairo Z. Gonçalves and Ángel del Río. Bicyclic units, Bass cyclic units and free groups. *J. Group Theory*, 11(2):247–265, 2008.

[GdR11] Jairo Z. Gonçalves and Ángel del Río. Bass cyclic units as factors in a free group in integral group ring units. *Internat. J. Algebra Comput.*, 21(4):531–545, 2011.

[Gou97] Fernando Q. Gouvêa. *p-adic numbers.* Universitext. Springer-Verlag, Berlin, second edition, 1997. An introduction.

[GP04] Jairo Z. Gonçalves and Donald S. Passman. Embedding free products in the unit group of an integral group ring. *Arch. Math. (Basel)*, 82(2):97–102, 2004.

[GP06] Jairo Z. Gonçalves and Donald S. Passman. Linear groups and group rings. *J. Algebra*, 295(1):94–118, 2006.

[GP07] Jairo Z. Gonçalves and Donald S. Passman. Erratum to: "Linear groups and group rings" [J. Algebra **295** (2006), no. 1, 94–118; mr2188853]. *J. Algebra*, 307(2):930–931, 2007.

[Her01] Martin Hertweck. A counterexample to the isomorphism problem for integral group rings. *Ann. of Math. (2)*, 154(1):115–138, 2001.

[Hig40] Graham Higman. The units of group-rings. *Proc. London Math. Soc. (2)*, 46:231–248, 1940.

[HP80] B. Hartley and P. F. Pickel. Free subgroups in the unit groups of integral group rings. *Canad. J. Math.*, 32(6):1342–1352, 1980.

[Isa76] I. Martin Isaacs. *Character theory of finite groups.* Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. Pure and Applied Mathematics, No. 69.

[Jac85] Nathan Jacobson. *Basic algebra. I.* W. H. Freeman and Company, New York, second edition, 1985.

[Jac89] Nathan Jacobson. *Basic algebra. II.* W. H. Freeman and Company, New York, second edition, 1989.

[JL93] Eric Jespers and Guilherme Leal. Generators of large subgroups of the unit group of integral group rings. *Manuscripta Math.*, 78(3):303–315, 1993.

[Lam01] Tsit Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[MM03] George A. Miller and H. C. Moreno. Non-abelian groups in which every subgroup is abelian. *Trans. Amer. Math. Soc.*, 4(4):398–404, 1903.

[Mol92] Theodor Molien. Über Systeme höherer complexer Zahlen. *Math. Ann.*, 41(1):83–156, 1892.

[MS97] Zbigniew S. Marciniak and Sudarshan K. Sehgal. Constructing free subgroups of integral group ring units. *Proc. Amer. Math. Soc.*, 125(4):1005–1009, 1997.

[Noe29] Emmy Noether. Hyperkomplexe Größen und Darstellungstheorie. *Math. Z.*, 30(1):641–692, 1929.

[Pas68] Donald S. Passman. *Permutation groups*. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Pas71] Donald S. Passman. *Infinite group rings*. Marcel Dekker Inc., New York, 1971. Pure and Applied Mathematics, 6.

[Pas77] Donald S. Passman. *The algebraic structure of group rings*. Pure and Applied Mathematics. Wiley-Interscience [John Wiley & Sons], New York, 1977.

[Pas04] Donald S. Passman. Free products in linear groups. *Proc. Amer. Math. Soc.*, 132(1):37–46 (electronic), 2004.

[Pas08] Donald S. Passman. Free subgroups in linear groups and group rings. In *Noncommutative rings, group rings, diagram algebras and their applications*, volume 456 of *Contemp. Math.*, pages 151–164. Amer. Math. Soc., Providence, RI, 2008.

[PMS02] César Polcino Milies and Sudarshan K. Sehgal. *An introduction to group rings*, volume 1 of *Algebras and Applications*. Kluwer Academic Publishers, Dordrecht, 2002.

[Rob82] Derek J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

[RS87] Klaus Roggenkamp and Leonard Scott. Isomorphisms of p-adic group rings. *Ann. of Math. (2)*, 126(3):593–647, 1987.

[San47] I. N. Sanov. A property of a representation of a free group. *Doklady Akad. Nauk SSSR (N. S.)*, 57:657–659, 1947.

[Sco64] William R. Scott. *Group theory*. Prentice-Hall Inc., Englewood Cliffs, N.J., 1964.

[Seh78] Sudarshan K. Sehgal. *Topics in group rings*, volume 50 of *Monographs and Textbooks in Pure and Applied Math.* Marcel Dekker Inc., New York, 1978.

[Seh93] S. K. Sehgal. *Units in integral group rings*, volume 69 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, Harlow, 1993. With an appendix by Al Weiss.

[Tit72] Jacques Tits. Free subgroups in linear groups. *J. Algebra*, 20:250–270, 1972.

Index