ABSTRACT

On Rings with Distinguished Ideals and Their Modules

Joshua Buckner, B.S., M.S.

Advisor: Manfred H. Dugas, Ph.D.

Let S be an integral domain, R_S an S algebra, and $\mathscr{F}$ a family of left ideals of R. Define $End_S(R, \mathscr{F}) = \{\varphi \in End_S(R^+) : \varphi(X) \subseteq X \text{ for all } X \in \mathscr{F}\}$. In 1967, H. Zassenhaus proved that if R is a ring such that R^+ is free of finite rank, then there is a left R module M such that $R \subseteq M \subseteq \mathbb{Q}R$ and $End_{\mathbb{Z}}(M) = R$. This motivates the following definitions: Call $R_{\mathbb{Z}}$ a Zassenhaus ring with module M if the conclusion of Zassenhaus' result holds for the ring R and module M. It is easy to see that if $R_{\mathbb{Z}}$ is a Zassenhaus ring then R has a family $\mathscr{F}$ of left ideals such that $End_{\mathbb{Z}}(R, \mathscr{F}) = R$. (If $\mathscr{F}$ has this property, then call $\mathscr{F}$ a Zassenhaus family (of left ideals) of the ring R.) While the converse doesn't hold in general, this dissertation examines examples of rings R for which the converse does hold, i.e. R has a Zassenhaus family $\mathscr{F}$ of left ideals that can be used to construct a left R module M such that $R \subseteq M \subseteq \mathbb{Q}R$ and $End_{\mathbb{Z}}(M) = R$.

On Rings with Distinguished Ideals and Their Modules

by

Joshua Buckner, B.S., M.S.

A Dissertation

Approved by the Department of Mathematics

_____

Lance L. Littlejohn, Ph.D., Chairperson

Submitted to the Graduate Faculty of
Baylor University in Partial Fulfillment of the
Requirements for the Degree
of
Doctor of Philosophy

Approved by the Dissertation Committee

_____

Manfred H. Dugas, Ph.D., Chairperson

_____

David M. Arnold, Ph.D.

_____

Gregory A. Benesh, Ph.D.

_____

Markus Hunziker, Ph.D.

_____

Robert Piziak, Ph.D.

Accepted by the Graduate School
May 2007

_____

J. Larry Lyon, Ph.D., Dean

Page bearing signatures is kept on file in the Graduate School.

TABLE OF CONTENTS

ACKNOWLEDGMENTS v

1 Introduction 1

2 Zassenhaus Rings have Zassenhaus Families 4

3 Examples of Rings with Zassenhaus Families 6

4 Rings of Algebraic Integers with Zassenhaus Families 17

5 Some Dedekind Domains have Zassenhaus Families 23

6 From Zassenhaus Families to Zassenhaus Rings 27

7 An Alternate Proof of Zassenhaus's Result 36

8 Integer Matrix Rings are Zassenhaus Rings 42

9 Some PIDs are not Zassenhaus Rings 45

10 Conclusion: A Ring with a Zassenhaus Family that is not a Zassenhaus Ring 53

BIBLIOGRAPHY 54

ACKNOWLEDGMENTS

Thanks to my mentor, Manfred Dugas, and to everyone in Department of Mathematics of Baylor University for their kind direction, assistance, and encouragement.

CHAPTER ONE

Introduction

In [24], Hans Zassenhaus showed that for a ring R with a finite rank, free additive group, there is a group G such that the rank of G is equal to the rank of R and $\mathrm{End}_{\mathbb{Z}}(G) = R$. From [1, page 2], the rank of an abelian group G is the dimension of the rational vector space $\mathbb{Q} \otimes_{\mathbb{Z}} G$. On the other hand, in [10], A. L. S. Corner gave an example of a ring R with a torsion free, finite rank, free additive group, such that there is a group G with $\operatorname{rank} G = 2(\operatorname{rank} R)$ and $\mathrm{End}(G) = R$ but there is no group of smaller rank with this property. These two results motivate the following definition: A ring R with $1 \in R$ and additive group R^+ torsion free is a Zassenhaus ring if there is a left R-module ${}_RM$ so that $R \subseteq M \subseteq \mathbb{Q}R$ and $\mathrm{End}_{\mathbb{Z}}(M) = R$. In this case, $\operatorname{rank} M = \operatorname{rank} R$. Henceforth, all rings R are assumed to have an identity element 1_R sometimes denoted as 1.

The notion of a Zassenhaus ring represents a generalization of a more recent notion, that of an E-ring. A ring R with additive group R^+ is an E-ring if and only if each endomorphism of R^+ is multiplication on the left by some element of R, i.e. $End_{\mathbb{Z}}(R) = R$. E-rings play a noteworthy role in the theory of torsion-free abelian groups of finite rank (tffr groups); see the survey [22] on E-rings and their generalizations.

To show that a particular ring is a Zassenhaus ring, it is often useful to look for a family of left ideals of the ring from which to construct the necessary module. This construction method motivates the search for a family of ideals of R such that maps leaving the constituent ideals invariant turn out to be merely multiplications by elements of R. To that end, let R be an algebra over a commutative ring S. Let $\mathscr{F}$ be a family of left ideals of R and define $\mathrm{End}_S(R^+, \mathscr{F}) = \{\varphi \in \mathrm{End}_S(R^+) : \varphi(X) \subseteq X \text{ for all } X \in \mathscr{F}\}$. Call $\mathscr{F}$ a Zassenhaus family for R if

$\mathrm{End}_S(R^+, \mathscr{F}) = R$. In general, a Zassenhaus family for an S-algebra depends on S. Note that R is an E-ring if and only if the empty set is a Zassenhaus family for the $\mathbb{Z}$-algebra R.

Chapter Two shows that every Zassenhaus ring has a Zassenhaus family. If R is a Zassenhaus ring, one can construct the ideals for a Zassenhaus family for R from the module that makes R a Zassenhaus ring.

Chapter Three exhibits several rings for which it is easy to construct concrete Zassenhaus families. A Zassenhaus family can be constructed for each of the following: $\mathrm{End}_S(F)$ where S is a commutative ring and F is a free S-module, a matrix ring, and a ring of polynomials in one indeterminate over an infinite field. This chapter shows that if the divisible hull of a torsion free ring has a Zassenhaus family, then from that family, one can construct a Zassenhaus family for the ring. Conversely, if a ring has an additive group which is free of finite rank and the ring has a Zassenhaus family, then a Zassenhaus family for the divisible hull of the ring can be constructed. From these results, there is a Zassenhaus family for both polynomials with integer coefficients and a ring first exhibited by A. L. S. Corner. Finally, a Zassenhaus family for an incidence algebra over a field exists.

Chapter Four contains the construction of a Zassenhaus family over $\mathbb{Z}$ for an arbitrary ring R of algebraic integers of a finite degree, Galois field extension of the rationals. In this case, R^+ is a finitely generated free group. Hence, Zassenhaus' original result combined with the results of Chapter Two is enough to show that R has a Zassenhaus family. But this approach does not indicate the structure of the ideals in this Zassenhaus family. The construction of a natural and concrete example of a Zassenhaus family for R is exhibited.

Chapter Five proves that if R is in a large subclass of Dedekind domains then there are some necessary and sufficient conditions for R to have a Zassenhaus family over $\mathbb{Z}$.

Chapter Six shows that some rings with Zassenhaus families are Zassenhaus rings. This chapter contains a lemma that, in some cases, gives one a method to construct a module M from ideals of a Zassenhaus family for a ring R such that $\mathrm{End}_{\mathbb{Z}}(M) = R$ with $\operatorname{rank} M = \operatorname{rank} R$. This lemma is applied to the Zassenhaus families from Chapter Four for polynomials with integer coefficients, Corner's ring, and rings of algebraic integers.

Chapter Seven gives an alternate, more elementary, proof of Zassenhaus's original result. The proof uses only linear algebra and some elementary number theory.

Chapter Eight exhibits for the ring R of $n \times n$ matrices with integer entries, the construction of a module M with $\mathrm{End}_{\mathbb{Z}}(M) = R$, $\operatorname{rank} M = \operatorname{rank} R$, and M^+ a Butler group. Again, Zassenhaus' original result guarantees the existence of a module M, but tells us nothing about the structure of the module.

Chapter Nine proves that a certain subclass of PID's are not Zassenhaus rings. This result provides an example in Chapter Ten of a ring with a Zassenhaus family that is not a Zassenhaus ring. Thus having a Zassenhaus family is not equivalent to being a Zassenhaus ring. Many of the results in this dissertation have appeared in [6], [7], and [8].

CHAPTER TWO

Zassenhaus Rings have Zassenhaus Families

Denote by Π the set of prime numbers of $\mathbb{N}$. If $p \in \Pi$ and if G is an additive group then $t_p(G)$ denotes the set of all elements of G with order a power of p. For $n \in \mathbb{N}$, let $G[p^n] = \{g \in G : p^n g = 0\}$. That is, $g \in G[p^n]$ if and only if the order of $g = p^m$ with $m \leq n$.

For a ring R, let R^+ denote the additive group of R. Unless otherwise noted, identify R with the subring of $\mathrm{End}_{\mathbb{Z}}(R)$ in which each map is multiplication on the left by some element of R. Where convenient, write $R\cdot$ or even just R for this subring.

Definition 2.1. A ring R with identity whose additive group R^+ is torsion free is called a *Zassenhaus ring* if and only if there is a left R-module ${}_RM$ so that $R \subseteq M \subseteq \mathbb{Q}R$ and $\mathrm{End}_{\mathbb{Z}}(M) = R$. The module M is called the *Zassenhaus module* for the ring R.

Definition 2.2. Suppose that R is a ring with identity that is also an algebra over a (commutative) ring S. Let $\mathscr{F}$ be a family of some left ideals of R and define

$$\mathrm{End}_S(R^+, \mathscr{F}) = \left\{\varphi \in \mathrm{End}_S(R^+) : \varphi(X) \subseteq X \text{ for all } X \in \mathscr{F}\right\}.$$

Then $\mathscr{F}$ is called a *Zassenhaus family* for R if and only if $\mathrm{End}_S(R^+, \mathscr{F}) = R$. If $S = \mathbb{Z}$ then write $\mathrm{End}_{\mathbb{Z}}(R)$ and $\mathrm{End}(R^+, \mathscr{F})$ in place of $\mathrm{End}_{\mathbb{Z}}(R^+)$ and $\mathrm{End}_{\mathbb{Z}}(R^+, \mathscr{F})$.

Theorem 2.3. *If R is a Zassenhaus ring then R has a Zassenhaus family over $\mathbb{Z}$.*

Proof: Suppose that there is a left R-module ${}_RM$ so that $R \subseteq M \subseteq \mathbb{Q}R$ and $\mathrm{End}_{\mathbb{Z}}(M) = R$. Note that M/R is torsion because $\mathbb{Q}R/R$ is torsion. Let p be a prime number and $n \in \mathbb{N}$. Define $M_{p,n}$ by $M_{p,n}/R = (t_p(M/R))[p^n]$. So $M_{p,n}/R$ is the set of all elements $a + R$ of M/R such that there is a positive integer $m \leq n$ with $p^m(a + R) = R$. Alternatively, $M_{p,n}$ is the largest subgroup of M for which $p^n M_{p,n} \subseteq R$. Define $X_{p,n} = p^n M_{p,n} \subseteq R$.

To see that $X_{p,n}$ is a left ideal of R, suppose that $r \in R$ and $x \in X_{p,n}$. There is an $m \in M_{p,n}$ such that $x = p^n m$. Then $p^n(m + R) = R$, and thus $p^n m \in R$. Hence $rp^n m = p^n rm \in R$ and $p^n(rm + R) = R$. Therefore $rm \in M_{p,n}$. It follows that $rx = p^n rm \in p^n M_{p,n} = X_{p,n}$.

Note that $p^n R \subseteq X_{p,n} \subseteq R$. For, from the definitions, $R \subseteq M_{p,n}$. Hence $p^n R \subseteq p^n M_{p,n} = X_{p,n}$. It suffices to show that $\mathscr{F} = \{X_{p,n} : p \in \Pi, n \in \mathbb{N}\}$ is a Zassenhaus family for R. Suppose that $\varphi \in \mathrm{End}_{\mathbb{Z}}(R)$ so that $\varphi(X_{p,n}) \subseteq X_{p,n}$ for each $X_{p,n} \in \mathscr{F}$. The map φ has a unique extension $\psi \in \mathrm{End}_{\mathbb{Q}}(\mathbb{Q}R)$: For $q \in \mathbb{Q}$ and $a \in R$, define $\psi(qa) = q\varphi(a)$. Elementary calculation shows that this map is well defined. Under this definition, it is clear that $\psi|_R = \varphi$. Suppose that $\gamma \in \mathrm{End}(\mathbb{Q}R)$ such that $\gamma|_R = \varphi$. Let $qa \in \mathbb{Q}R$. Then $\gamma(qa) = q\gamma(a) = q\varphi(a) = \psi(qa)$.

To see that $\psi(M_{p,n}) \subseteq M_{p,n}$ for all $p \in \Pi$ and $n \in \mathbb{N}$, notice that $M_{p,n}$ in $\mathbb{Q}R$ is just $(1/p^n)X_{p,n}$ from the definition of $X_{p,n}$. Then

$$\begin{aligned}
\psi(M_{p,n}) &= \psi((1/p^n)X_{p,n}) \\
&= (1/p^n)\psi(X_{p,n}) \\
&= (1/p^n)\varphi(X_{p,n}) \\
&\subseteq (1/p^n)X_{p,n} = M_{p,n}.
\end{aligned}$$

Since $M = \sum_{p,n} M_{p,n}$, then $\psi(M) \subseteq M$. It follows that $\psi|_M$ is an element of $\mathrm{End}(M)$. But each of the elements of $\mathrm{End}(M)$ is just multiplication on the left by some element of R. So $\psi|_R = \varphi \in R$. $\square$

The converse of Theorem Ten may be stated as a question: Does every ring with a Zassenhaus family over $\mathbb{Z}$ have a Zassenhaus module? The answer to this question is no. That is, the converse of Theorem 2.3 does not hold in general. In Chapter Nine, results provide a whole class of counterexamples for the converse. In Chapter Ten a specific counterexample from that class is exhibited.

CHAPTER THREE

Examples of Rings with Zassenhaus Families

Theorem 3.1. *Let S be a ring and F a free S-module. Then* $\mathrm{End}_S(F)$*, the S-algebra of S-linear endomorphisms of F, has a Zassenhaus family over S.*

Proof: Let $E = \mathrm{End}_S(F)$. Fix a basis B over S for F. Given $x \in F$ and $b \in B$, define $\varphi_{x,b}$ and φ_x in E by

$$\varphi_{x,b}(c) = \begin{cases} x & \text{if } c = b, \\ 0 & \text{otherwise} \end{cases}$$

and $\varphi_x(c) = x$ for all $c \in B$. Let $J_b = \{\varphi_{x,b} : x \in F\}$ and $J = \{\varphi_x : x \in \mathscr{F}\}$.

For any finite subset I of B, define $\mathscr{O}_I = \{\varphi \in E : \varphi(I) = 0\}$. Then $\mathscr{O}_I$ is a left ideal of E. The set $\{\mathscr{O}_I : I \subseteq B,\ I \text{ finite}\}$ forms a basis of neighborhoods of the 0 map for the finite topology on E. It suffices to show that $\mathscr{F} = \{J\} \cup \{J_b : b \in B\} \cup \{\mathscr{O}_I : I \subseteq B,\ I \text{ finite}\}$ is a Zassenhaus family for E.

Let $\Phi \in \mathrm{End}_S(E)$ such that $\Phi(X) \subseteq X$ for all $X \in \mathscr{F}$. Then Φ also leaves invariant J and J_b for each $b \in B$. For each $x \in F$ it follows that $\Phi(\varphi_x) = \varphi_{\beta(x)}$ for some $\beta(x) \in F$. Note that if $x, y \in F$ and $c \in B$, then $(\varphi_x + \varphi_y)(c) = \varphi_x(c) + \varphi_y(c) = x + y = \varphi_{x+y}(c)$. So $\varphi_x + \varphi_y = \varphi_{x+y}$. Then $\varphi_{\beta(x+y)} = \Phi(\varphi_{x+y}) = \Phi(\varphi_x + \varphi_y) = \Phi(\varphi_x) + \Phi(\varphi_y) = \varphi_{\beta(x)} + \varphi_{\beta(y)} = \varphi_{\beta(x)+\beta(y)}$. Thus $\beta : F \to F$ preserves addition.

It will be seen that β is S-linear. For $s \in S$, $x \in F$, and $c \in B$, then $\varphi_{sx}(c) = sx = s\varphi_x(c)$. Thus $\varphi_{sx} = s\varphi_x$ for all $x \in F$ and for all $s \in S$. Let $s \in S$ and $x \in F$. Then $\varphi_{s\beta(x)} = s\varphi_{\beta(x)} = s\Phi(\varphi_x) = \Phi(s\varphi_x) = \Phi(\varphi_{sx}) = \varphi_{\beta(sx)}$ and so $s\beta(x) = \beta(sx)$. Therefore $\beta \in E$.

Let $b \in B$. There is a $\beta_b \in E$ similar to β above but related to the action of Φ on J_b instead of J. If $x \in F$ then $\Phi(\varphi_{x,b}) = \varphi_{\beta_b(x),b}$ for some $\beta_b(x) \in F$. Note that if $x, y \in F$ then $(\varphi_{x,b} + \varphi_{y,b})(b) = \varphi_{x,b}(b) + \varphi_{y,b}(b) = x + y = \varphi_{x+y,b}(b)$, and if $b \neq c \in B$

then $(\varphi_{x,b} + \varphi_{y,b})(c) = \varphi_{x,b}(c) + \varphi_{y,b}(c) = 0 = \varphi_{x+y,b}(c)$. So $\varphi_{x,b} + \varphi_{y,b} = \varphi_{x+y,b}$. Then $\varphi_{\beta_b(x+y),b} = \Phi(\varphi_{x+y,b}) = \Phi(\varphi_{x,b} + \varphi_{y,b}) = \Phi(\varphi_{x,b}) + \Phi(\varphi_{y,b}) = \varphi_{\beta_b(x),b} + \varphi_{\beta_b(y),b} = \varphi_{\beta_b(x)+\beta_b(y),b}$. Thus $\beta_b : F \to F$ preserves addition.

It will be seen that β_b is S-linear. If $s \in S$, $x \in F$, then $\varphi_{sx,b}(b) = sx = s\varphi_{x,b}(b)$, and if $b \neq c \in B$ then $\varphi_{sx,b}(c) = 0 = s{\cdot}0 = \varphi_{x,b}(c)$. Thus $\varphi_{sx,b} = s\varphi_{x,b}$ for all $x \in F$ and for all $s \in S$. Then $\varphi_{s\beta_b(x),b} = s\varphi_{\beta_b(x),b} = s\Phi(\varphi_{x,b}) = \Phi(s\varphi_{x,b}) = \Phi(\varphi_{sx,b}) = \varphi_{\beta_b(sx),b}$ and so $s\beta_b(x) = \beta_b(sx)$. Therefore $\beta_b \in E$.

Let I be a finite subset of B. If $x \in F$ and $c \in I$ then $(\varphi_x - \sum_{b\in I} \varphi_{x,b})(c) = \varphi_x(c) - \varphi_{x,c}(c) = x - x = 0$. So $\varphi_x - \sum_{b\in I} \varphi_{x,b} \in \mathscr{O}_I$ for all $x \in F$. Then $\Phi(\varphi_x - \sum_{b\in I} \varphi_{x,b}) = \varphi_{\beta(x)} - \sum_{b\in I} \varphi_{\beta_b(x),b} \in \mathscr{O}_I$ for all $x \in F$. Note that the finite topology is Hausdorff. It follows that the maps $\sum_{b\in I} \varphi_{\beta_b(x),b}$ indexed over all finite I define a net that converges to $\varphi_{\beta(x)}$ in the finite topology. Hence, for $c \in B$, it must follow that $\beta(x) = \varphi_{\beta(x)}(c) = \sum_{b\in B} \varphi_{\beta_b(x),b}(c) = \varphi_{\beta_c(x),c}(c) = \beta_c(x)$. Therefore $\beta(x) = \beta_b(x)$ for all $x \in F$ and for all $b \in B$.

If $\eta \in E$, then $\eta - \sum_{b\in I} \varphi_{\eta(b),b} \in \mathscr{O}_I$ for all finite subsets I of B. Note that $\Phi(\eta) - \sum_{b\in I} \Phi(\varphi_{\eta(b),b}) = \Phi(\eta) - \sum_{b\in I} \varphi_{\beta_b\circ\eta(b),b} = \Phi(\eta) - \sum_{b\in I} \varphi_{\beta\circ\eta(b),b}$. Since Φ preserves the $\mathscr{O}_I$, it follows that $\Phi(\eta) - \sum_{b\in I} \varphi_{\beta\circ\eta(b),b} \in \mathscr{O}_I$ for all finite subsets I of B. Hence, for all $c \in B$, it must be the case that $\Phi(\eta)(c) = \sum_{b\in B} \varphi_{\beta\circ\eta(b),b}(c) = \varphi_{\beta\circ\eta(c),c}(c) = \beta \circ \eta(c)$. So $\Phi(\eta) = \beta \circ \eta$. Therefore Φ is multiplication on the left by $\beta \in E$ and so $\mathscr{F}$ is a Zassenhaus family for E. $\square$

If F is finitely generated over S, linear algebra can be used to find a Zassenhaus family. Such an approach is taken for next result.

Proposition 3.2. *Let S be a ring with identity, and let $R = \mathrm{Mat}_{n\times n}(S) = \mathrm{End}_S(S^n)$ be the ring of $n \times n$ matrices over S. Then there is a Zassenhaus family $\mathscr{F} = \{J_i : 1 \leq i \leq n+1\}$ of left ideals of the S-algebra R such that $R = \oplus_{i=1}^n J_i$ and $J_{n+1} \cap (\oplus_{1\leq j\neq i\leq n} J_i) = \{0\}$ for all $1 \leq j \leq n$.*

Proof: Define $\varepsilon_{ij} \in R$ be the matrix with 1 in the (i,j) position and 0 everywhere else, $\varepsilon_i = \varepsilon_{ii}$, and $J_i = R\varepsilon_i = \oplus_{1\leq\alpha\leq n} S\varepsilon_{\alpha i}$. Note that J_i is the collection of matrices from R with nonzero entries possible only in the i-th column and zeros everywhere else. Of course $R = \oplus_{i=1}^{n} J_i$. Define $\varepsilon^{(i)} = \sum_{j=1}^{n} \varepsilon_{ij}$ a matrix with ones in the i-th row and zeros everywhere else. Then set $J_{n+1} = R\varepsilon^{(1)}$ in which is collected the matrices where each row has the same value in every position, i.e. each row is constant. So $J_{n+1} = \oplus_{i=1}^{n} S\varepsilon^{(i)}$. If $M \in J_{n+1}$ and zero appears anywhere in the i-th row, then the whole i-th row must be zero. Let $1 \leq j \leq n$. Then $J_{n+1} \cap (\oplus_{1\leq i\neq j\leq n} J_i) = \{0\}$ since the elements of $\oplus_{1\leq i\neq j\leq n} J_i$ have only zero entries in the j-th column.

Suppose that $r = (r_{\alpha\beta}) \in R$. Then $r\varepsilon_{ij} = (c_{\alpha\beta})$ where $c_{\alpha\beta} = \sum_k r_{\alpha k}(\varepsilon_{ij})_{k\beta}$. But $(\varepsilon_{ij})_{k\beta}$ is zero unless $k = i$ and $\beta = j$. Then $c_{\alpha j} = r_{\alpha i}$, and for $\beta \neq j$, $c_{\alpha\beta} = 0$. It follows that $r\varepsilon_{ij} = \sum_{\alpha=1}^{n} r_{\alpha i}\varepsilon_{\alpha j}$.

To show that there is a Zassenhaus family, let $\varphi \in End_S(R^+)$ such that $\varphi(J_i) \subseteq J_i$ for all $1 \leq i \leq n+1$. Since the ε_{ij} form an S-basis of R, there are $t_{ij,\alpha\beta} \in S$ such that $\varphi(\varepsilon_{ji}) = \sum_{1\leq\alpha,\beta\leq n} t_{ji,\alpha\beta}\varepsilon_{\alpha\beta}$. Since $\varphi(J_i) \subseteq J_i$, $\varphi(\varepsilon_{ji}) \in J_i$. The entries of $\varphi(\varepsilon_{ji})$ not in the i-th column are all zero. Thus $t_{ji,\alpha\beta} = 0$ for all $\beta \neq i$. It follows that

$$\begin{aligned}
\varphi\left(\varepsilon^{(i)}\right) &= \varphi\left(\sum_{j=1}^{n} \varepsilon_{ij}\right) = \sum_{j=1}^{n} \varphi(\varepsilon_{ij}) \\
&= \sum_{j=1}^{n} \left(\sum_{\alpha=1}^{n} t_{ij,\alpha j}\varepsilon_{\alpha j}\right) = \sum_{\alpha=1}^{n} \left(\sum_{j=1}^{n} t_{ij,\alpha j}\varepsilon_{\alpha j}\right) \\
&= \sum_{\alpha=1}^{n} c_{i\alpha}\varepsilon^{(\alpha)} = \sum_{\alpha=1}^{n}\sum_{j=1}^{n} c_{i\alpha}\varepsilon_{\alpha j}
\end{aligned}$$

for some $c_{i\alpha} \in S$. Then $t_{ij,\alpha j} = c_{i\alpha}$ for all $1 \leq j \leq n$, i, and α. Hence

$$\varphi(\varepsilon_{ji}) = \sum_{1\leq\alpha,\beta\leq n} t_{ji,\alpha\beta}\varepsilon_{\alpha\beta} = \sum_{1\leq\alpha\leq n} t_{ji,\alpha i}\varepsilon_{\alpha i} = \sum_{1\leq\alpha\leq n} c_{j\alpha}\varepsilon_{\alpha i}.$$

Comparing the final expression in our string of equalities to the usual definition of matrix multiplication, $\varphi = (c_{i\alpha}) \in R$. $\square$

Proposition 3.3. *The K-algebra $K[x]$ of all polynomials in indeterminate x over an infinite field K has a Zassenhaus family over K.*

Proof: Enumerate distinct elements a_j of K for all $0 < j \in \mathbb{N}$. Then define $a_0 = 0$. Put $\mathscr{F} = \{(a_j + x^n)K[x] : n \in \mathbb{N}, j > 0\}$ for our candidate for a Zassenhaus family.

Suppose that $\varphi \in \mathrm{End}_K(K[x])$ with $\varphi(X) \subseteq X$ for each $X \in \mathscr{F}$ and $\varphi(K) = \{0\}$. Then there are polynomials $g_{n,j}$ so that $\varphi(a_j + x^n) = (a_j + x^n)g_{n,j}$ for all n and j. But

$$\begin{aligned}\varphi(a_j + x^n) &= \varphi(a_j) + \varphi(x^n) \\ &= 0 + \varphi(x^n) = \varphi(x^n) \\ &= x^n g_{n,0}\end{aligned}$$

for all n and $j > 0$. It follows that $(a_j + x^n)g_{n,j} = x^n g_{n,0}$ for all n and $j > 0$.

Note that $\gcd(a_j + x^n, x^n) = 1$ for all $j > 0$. Then the polynomial $a_j + x^n$ divides $g_{n,0}$ for all $j > 0$. The only possibility is that $g_{n,0} = 0$ for all n. It follows from the linearity of φ that $\varphi = 0$.

Suppose that $\psi \in \mathrm{End}_K(K[x])$ so that $\psi(X) \subseteq X$ for all $X \in \mathscr{F}$. Consider $\varphi(a) = \psi(a) - \psi(1) \cdot a$. Then $\varphi(K) = \{0\}$. The preceding arguments show that $\varphi = 0$ and so $\psi = \psi(1)$. Therefore $\mathscr{F}$ is a Zassenhaus family for the K-algebra $K[x]$. $\square$

The next two propositions deal with restrictions and extensions. Let R be a torsion free ring. Define the $\mathbb{Q}$-algebra $A = \mathbb{Q} \otimes_{\mathbb{Z}} R$. Proposition 3.4 shows that if A has a Zassenhaus family $\mathscr{F}$ over $\mathbb{Q}$, then the family of restrictions $X \cap R$ of $X \in \mathscr{F}$ to R is a Zassenhaus family over $\mathbb{Z}$ for R. Proposition 3.6 shows that if R^+ is a free group that has finite rank, if R has an Zassenhaus family $\mathscr{F}$, and if each $X \in \mathscr{F}$ is pure in R, then the family of extensions $\mathbb{Q} \otimes_{\mathbb{Z}} X$ of $X \in \mathscr{F}$ to $\mathbb{Q} \otimes_{\mathbb{Z}} R$ is a Zassenhaus family for A.

Proposition 3.4. *Suppose that R is a torsion free ring with identity such that the $\mathbb{Q}$-algebra $A = \mathbb{Q}\otimes_{\mathbb{Z}} R$ has a Zassenhaus family $\mathscr{F}$ over $\mathbb{Q}$. Then $\mathscr{F}' = \{X \cap R : X \in \mathscr{F}\}$ is a Zassenhaus family over $\mathbb{Z}$ for the ring R.*

Proof: Identify R with $1 \otimes R$. Let $X \in \mathscr{F}$ and $x \in X$. Then $x = qr$ for some $q \in \mathbb{Q}$ and $r \in R$. Since $q^{-1} = q^{-1}1_R \in \mathbb{Q}R$ and X is an ideal of $\mathbb{Q}R$, $r = q^{-1}x \in X$ and so $r \in X \cap R$. Thus $X \subseteq \mathbb{Q}(X \cap R)$. The inclusion $\mathbb{Q}(X \cap R) \subseteq X$ holds since $\mathbb{Q}(X \cap R) \subseteq \mathbb{Q}X = X$. Therefore $X = \mathbb{Q} \otimes (X \cap R)$.

Suppose that $\varphi \in \mathrm{End}_{\mathbb{Z}}(R)$ so that $\varphi(X \cap R) \subseteq X \cap R$ for all $X \in \mathscr{F}$. Note that $\psi = \mathrm{id}_{\mathbb{Q}} \otimes \varphi \in \mathrm{End}_{\mathbb{Q}}(A)$ with $\psi|_R = \varphi$. Then $\psi(X) = \psi(\mathbb{Q} \otimes (X \cap R)) = \mathbb{Q} \otimes \varphi(X \cap R) \subseteq \mathbb{Q} \otimes X \subseteq X$. Since $\mathscr{F}$ is a Zassenhaus family for A, it follows that $\psi = a\cdot$ for some $a \in A$. But $\varphi(1)$ is in R and $\varphi(1) = \psi(1 \otimes 1) = a(1 \otimes 1) = a$. Hence φ is just left multiplication by $a \in R$. $\square$

Recall the following definition from abelian group theory; e.g., see [1].

Definition 3.5. A subgroup H of a group G is *pure* in G if and only if $H \cap nG = nH$ for each integer n.

Proposition 3.6. *Suppose that R is a ring such that R^+ free of finite rank. If R has a Zassenhaus family $\mathscr{F}$ over $\mathbb{Z}$ with the property that each $X \in \mathscr{F}$ is pure in R, then $\mathscr{F}' = \{\mathbb{Q}X : X \in \mathscr{F}\}$ is an Zassenhaus family over $\mathbb{Q}$ for the $\mathbb{Q}$-algebra $\mathbb{Q}R$.*

Proof: Since R^+ is free of finite rank, there are $r_i \in R$ such that $R^+ = r_1\mathbb{Z} \oplus \cdots \oplus r_n\mathbb{Z}$ for some $n \in \mathbb{N}$. Let $\psi \in End_{\mathbb{Q}}(\mathbb{Q}R, \mathscr{F}')$. Then $\psi(r_i) = \sum_{k=1}^{n} q_{i,k}r_k$ for some $q_{i,k} \in \mathbb{Q}$. For $1 \leq i \leq n$, denote by m_i the least common multiple of the denominators of the $q_{i,k}$ ranging over k. Then $m_i\psi(r_i) = \sum_{k=1}^{n}(m_iq_{i,k})r_k$ where $m_iq_{i,k} \in \mathbb{Z}$. So $m_i\psi(r_i) \in R$. Denote by m the product of the m_i. For $1 \leq i \leq n$, $m\psi(r_i) \in R$. It follows that $m\psi(R) = m\psi(r_1)\mathbb{Z} \oplus \cdots \oplus m\psi(r_n)\mathbb{Z} \subseteq R$.

Now $m\psi(X) \subseteq R$ and $m\psi(X) \subseteq \mathbb{Q}X$ so that $m\psi(X) \subseteq \mathbb{Q}X \cap R$. From purity, one argues that $\mathbb{Q}X \cap R = X$. It is clear that $X \subseteq \mathbb{Q}X \cap R$. Let $r \in \mathbb{Q}X \cap R$. Then

one can assume that r is of the form $(a/b)r'$ for some $a/b \in \mathbb{Q}$ and some $r' \in X$. So $br = ar'$. Since X is pure in R^+, there is an $x \in X$ such that $bx = ar'$. Hence $x = (a/b)r' = r$ and $r \in X$. Therefore $\mathbb{Q}X \cap R = X$ and $m\psi(X) \subseteq X$. Since $\mathscr{F}$ is a Zassenhaus family for R, $m\psi|_R = t \in R$. Since $m\psi$ is $\mathbb{Q}$–linear, $m\psi$ is multiplication by t on all of $\mathbb{Q}R$. Thus $\psi = (1/m)t \in \mathbb{Q}R$. $\square$

In the foregoing proposition, the hypothesis that R^+ is free of finite rank cannot be dropped. If this hypothesis is weakened to merely finite rank, one can only say that $\psi(R) \subseteq \psi(r_1)\mathbb{Q} \oplus \cdots \oplus \psi(r_n)\mathbb{Q}$. In this case, an infinite number of $x \in \psi(R)$ may require a distinct m_x to achieve $m_x\psi(x) \in R$. There may be no least common multiple m available so that $m\psi(R) \subseteq R$.

Lemma 3.7. *The ring $\mathbb{Z}[x]$ of integer polynomials has a Zassenhaus family $\mathscr{F}$ over $\mathbb{Z}$ such that all members of $\mathscr{F}$ are direct summands of the additive group of $\mathbb{Z}[x]$.*

Proof: Note that $A = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[x]$ is a $\mathbb{Q}$-algebra. Moreover, A is isomorphic to $\mathbb{Q}[x]$, the $\mathbb{Q}$-algebra of all polynomials in indeterminate x over the infinite field $\mathbb{Q}$. By Proposition 3.3, A has a Zassenhaus family. Proposition 3.4 provides the Zassenhaus family for $\mathbb{Z}[x]$.

It remains to show that each member of this family is a direct summand of the free abelian group $(\mathbb{Z}[x])^+$. A member X of the family for A from Proposition 3.3 has the form $X = (q + x^n)\mathbb{Q}[x]$ for some $q \in \mathbb{Q}$. This member is used in Proposition 3.4 to provide the member $Y = X \cap \mathbb{Z}[x]$ of the family for $\mathbb{Z}[x]$.

It will be seen that $Y = \mathbb{Z}[x] \cap (q + x^n)\mathbb{Q}[x] = (a + bx^n)\mathbb{Z}[x]$ where a and b are the numerator and denominator of q respectively. Note that if $f(x) \in \mathbb{Z}[x]$ then $(a+bx^n)f(x) = (q+x^n)bf(x) \in (q+x^n)\mathbb{Q}[x]$. Hence $(a+bx^n)\mathbb{Z}[x] \subseteq \mathbb{Z}[x] \cap (q+x^n)\mathbb{Q}[x]$. Let $g(x) = (q+x^n)f(x) \in \mathbb{Z}[x] \cap (q+x^n)\mathbb{Q}[x]$. Then $(q+x^n)f(x) = (a+bx^n)(1/b)f(x)$. This means that the binomial $a + bx^n$ divides the polynomial $g(x)$ in the ring $\mathbb{Q}[x]$. Note that $g(x) = qf(x) + x^n f(x) \in \mathbb{Z}[x]$. If $g(x) = \sum_{i=0}^{m} g_i x^i$ and $f(x) = \sum_{i=0}^{\ell} f_i x^i$,

then $qf(x) + x^n f(x) = \sum_{i=0}^{\ell+n} f_i' x^i$ where either $f_i' = qf_i$ or $f_i' = 0$ for $i < n$. It follows that $qf_i \in \mathbb{Z}$ for $0 \leq i < \ell$. Then b divides each f_i in $\mathbb{Z}$ and $(1/b)f(x) \in \mathbb{Z}[x]$. Thus $(a + bx^n)$ divides $g(x)$ in the ring $\mathbb{Z}[x]$. Therefore $(a + bx^n)\mathbb{Z}[x] = \mathbb{Z}[x] \cap (q + x^n)\mathbb{Q}[x]$.

To see that Y is a direct summand of the free group of $\mathbb{Z}[x]$, note that for any polynomial $p(x)$ in $\mathbb{Z}[x]$, the Euclidean Algorithm guarantees that $p(x) = r(x) + (a + bx^n)g(x)$ where $r(x)$ and $g(x)$ are unique in $\mathbb{Z}[x]$ but $r(x)$ is not in Y. $\square$

Next, consider a ring that was introduced by A. L. S. Corner to obtain torsion free abelian groups without indecomposable summands [12, page 145].

Definition 3.8. A *semigroup* is a set that is closed under an associative binary operation. In general, a semigroup need not be closed with respect to inverses of elements.

Definition 3.9. Suppose that R is a ring and Λ is a semigroup. Then the *semigroup ring* $R\Lambda = \oplus_{a \in \Lambda} Ra$ is the set of all finite sums $\sum_i r_i a_i$ with each $r_i \in R$ and each $a_i \in \Lambda$. Define addition term-wise, in the usual manner for direct sums. Define ring multiplication for $a = \sum_i r_i a_i$ and $b = \sum_j s_j b_j$ in RS as $ab = \sum_{i,j} (r_i s_j)(a_i b_j)$.

Definition 3.10. Let $\Lambda = \{\gamma : 0 \leq \gamma \in \mathbb{Q}\}$. Define a semigroup structure on Λ by setting $\alpha\beta = \max\{\alpha, \beta\}$ for all $\alpha, \beta \in \Lambda$.

Lemma 3.11. *Let $R = S\Lambda$ be the semigroup ring of Λ over a commutative ring S. Then $\mathscr{F} = \{R\gamma : \gamma \in \Lambda\} \cup \{R(1-\gamma) : \gamma \in \Lambda\}$ is a Zassenhaus family for the S-algebra R. Moreover, each member of $\mathscr{F}$ is a direct summand of the S-module R^+.*

Proof: Let $\varphi \in \mathrm{End}_S(R)$ such that $\varphi(S) = \{0\}$ where φ leaves each member of $\mathscr{F}$ invariant. There is a column-finite $\Lambda \times \Lambda$-matrix $M = [s_{\alpha,\beta}]_{\alpha,\beta \in \Lambda}$ with entries in S such that $\varphi(\alpha) = \sum_{\beta \in \Lambda} \beta s_{\beta,\alpha}$ for all $\alpha \in \Lambda$.

For $\alpha, \beta \in \Lambda$, β divides α if and only if $\alpha \geq \beta$. Since $R\gamma = \oplus_{\gamma \leq \alpha \in \Lambda} S\alpha$ is invariant under φ for all $\gamma \in \Lambda$, $s_{\beta,\gamma} = 0$ for all $0 \leq \beta < \gamma$. In particular, $s_{\beta,0} = 0$ for all $\beta \in \Lambda$.

If $\beta, \gamma \in \Lambda$ such that $\beta > \gamma$, then $\beta - \beta\gamma = \beta - \beta = 0$. For $\gamma \in \Lambda$, expand $R(1-\gamma)$ in terms of direct summands:

$$\begin{aligned} R(1-\gamma) &= \langle \beta - \beta\gamma : \beta \in \Lambda \rangle_S \\ &= \langle \beta - \gamma : 0 \leq \beta < \gamma \rangle_S \\ &= \oplus_{0 \leq \beta < \gamma} S(\beta - \gamma). \end{aligned}$$

These ideals are invariant under φ for all $0 < \gamma \in \Lambda$. It follows that

$$\varphi(1-\gamma) = \varphi(-\gamma) = \sum_{\beta \geq \gamma} -\beta s_{\beta,\gamma} = \sum_{0 \leq \beta < \gamma} (\beta - \gamma) t_{\beta,\gamma}$$

for some $t_{\beta,\gamma} \in S$. Equating coefficients for the terms of the two sums yields $-s_{\gamma,\gamma} = \sum_{0 \leq \beta < \gamma} t_{\beta,\gamma}$ and $t_{\beta,\gamma} = 0$ for $0 \leq \beta < \gamma$. Taken together, these results for the coefficients imply that $s_{\gamma,\gamma} = 0$ for all $\gamma > 0$ as well as $s_{\beta,\alpha} = 0$ for all $\beta > \gamma$. Thus M is the zero matrix and $\varphi = 0$.

Suppose that $\psi \in \mathrm{End}_S(R)$ such that the members of $\mathscr{F}$ are invariant under ψ. Define $\varphi(x) = \psi(x) - \psi(1) \cdot x$ for each $x \in R$. Then $\varphi(S) = 0$. By the preceding argument, $\varphi = 0$ so that $\psi(x) = \psi(1) \cdot x$ for each $x \in R$. Therefore $\mathscr{F}$ is a Zassenhaus family for R.

Let $\gamma \in \Lambda$. Then $\gamma = \max\{\gamma, \gamma\} = \gamma \cdot \gamma$. Thus γ is an idempotent of the commutative ring R. By [14, Lemma 14.8], $R = R\gamma \oplus R(1-\gamma)$. $\square$

Definition 3.12. [21, Definition 1.1.7] A partially ordered set X is *locally finite* if and only if for any $a, b \in X$ the interval $[a, b] = \{x \in X : a \leq x \leq b\}$ is finite.

Definition 3.13. [21, Definition 1.2.1] Let X be a partially ordered set and R a commutative ring with identity. Define elements of the *incidence algebra*:

$$I(X, R) = \{f : X \times X \to R : f(x, y) = 0 \text{ if } x \not\leq y\}$$

Define operations for $f, g \in I(X, R)$; $r \in R$; and $a, b, x \in X$:

$$(f+g)(a,b) = f(a,b) + g(a,b)$$
$$(f \cdot g)(a,b) = \sum_{a \leq x \leq b} f(a,x) \cdot g(x,b)$$
$$(rf)(a,b) = r \cdot f(a,b)$$

Theorem 3.14. *Let K be a field and X a finite partially ordered set. Then the incidence K–algebra $R = I(X, K)$ has a Zassenhaus family over K.*

Proof: Denote by $\succeq$ the partial order on X. Without loss, one can label the elements of X as $\{1, 2, \ldots, n\}$. By [21, Lemma 1.2.5], the labels can be applied such that if $a, b \in X$ with $b \succeq a$ then $b \geq a$. By applying an isomorphism from [21, Proposition 1.2.7] and then a transpose, one may take $R = \oplus_{n \geq \alpha \succeq \beta \geq 1} K e_{\alpha\beta}$ with $e_{\alpha\beta}$ the $n \times n$ matrix with the identity of K in the (α, β) position and zeros everywhere else.

Proceed by induction on n. If $n = 1$ then R is K itself. In this case, let $\varphi \in \mathrm{End}_K(K)$. For $r \in K$, $\varphi(r) = r\varphi(1)$. So φ is just multiplication on the right by $\varphi(1) \in K$. The empty set serves as a Zassenhaus family since the algebra and ring coincide.

Suppose that for partially ordered sets Y of cardinality less than n, $I(Y, K)$ has a Zassenhaus family. This time, take the candidate for a Zassenhaus family for R to be the collection of all left ideals of R. Let $\varphi \in \mathrm{End}_K(R)$ so that $\varphi(1) = 0$ and $\varphi(J) \subseteq J$ for every left ideal J of R. Note that for $j \in X$, $Re_{jj} = \oplus_{\alpha \succeq j} K e_{\alpha j}$. So Re_{jj} is the collection of matrices in R with entries in the j-th column and zeros everywhere else. Define $S = \oplus_{j=2}^{n} Rejj$. Then $R = Re_{11} \oplus S$. Since R is lower triangular, the 1 row of any element of S has only zero entries. So S is isomorphic to the collection of lower triangular $n-1 \times n-1$ matrices. Using the transpose and [21, Proposition 1.2.7], S is isomorphic to $I(X^*, K)$ where $X^* = X - \{1\}$. Since Re_{11} and S are direct

summands of R, they are left ideals of R. Then $\varphi(Re_{11}) \subseteq Re_{11}$ and $\varphi(S) \subseteq S$. Then $\widetilde{\varphi} = \varphi|_S$ is a K–linear endomorphism of S.

Let J be a left ideal of S. If r is a matrix of J then define r^* to be the matrix resulting from attaching a row of all zeros as the 1 row and a column of all zeros in the 1 column. Define $J^* = \{r^* : r \in J\} \subseteq R$. Let $r \in R$ and $t \in J$. Then $r = r_1 + s^*$ for some $r_1 \in Re_{11}$ and $s \in S$. So $rt^* = (r_1 + s^*)t^* = r_1 t + s^* t^*$. Simple matrix multiplication is enough to show that $s^* t^* = (st)^*$. Since r_1 has nonzero entries only in the first column and the first row of t is zero, $r_1 t^* = 0$. Since J is a left ideal of S, $st \in J$ and $(st)^* \in J^*$. Thus $rt^* \in J^*$. Therefore J^* is a left ideal of R.

Since J^* is a left ideal of R, $\varphi(J^*) \subseteq J^*$. But $J^* \cap Re_{11} = 0$. So $J^* \subseteq S$ if one views S in the strictest sense as a direct summand of R. Then it has been shown that $\widetilde{\varphi}(J) \subseteq J$. Therefore $\widetilde{\varphi}$ leaves invariant any left ideal of S. By the induction hypothesis, S has a Zassenhaus family, so $\widetilde{\varphi}$ is multiplication on the left by $\widetilde{\varphi}(1_S) \in S$. Recall that $\widetilde{\varphi}(1_S) = 0$. Hence $\widetilde{\varphi} = 0$. Note that $1_S = \sum_{i=2}^{n} e_{ii}$ and $1_R = e_{11} + 1_S$. It was assumed that $\varphi(1_R) = 0$. It follows that $\varphi(e_{11}) = 0$. For $n \geq i, j \geq 2$, since $\widetilde{\varphi} = 0$ and $e_{ij} \in S$, $\varphi(e_{ij}) = 0$.

Fix $n \geq k \geq 2$ such that $k \succeq 2$ and $k \succeq 1$. Define $J_k = R(e_{k1} + e_{kk})$. Let $r = (r_{ij}) \in R$. Then re_{k1} is the matrix whose 1 column is the k-th column of r, but zeros everywhere else. Also, re_{kk} is the matrix with the same k-th column as r, but zeros everywhere else. Hence $J_k = R(e_{k1} + e_{kk}) = \oplus_{\alpha \succeq k} K(e_{\alpha 1} \oplus e_{\alpha k})$. By definition, J_k is a left ideal of R. Then $\varphi(J_k) \subseteq J_k$. Note that $k \succeq 2$ and $\alpha \succeq k$ implies that $\alpha \geq 2$. In this case, $\varphi(e_{\alpha k}) = 0$ for all $k \succeq 2$ and $\alpha \succeq k$. Hence $\varphi(J_k) = \oplus_{\alpha \succeq k} K(\varphi(e_{\alpha 1}) \oplus \varphi(e_{\alpha k}) = \oplus_{\alpha \succeq k} K\varphi(e_{\alpha 1})$. Since $\oplus_{\alpha \succeq k} K\varphi(e_{\alpha 1}) = Re_{11}$ is a left ideal of R, $\oplus_{\alpha \succeq k} K\varphi(e_{\alpha 1}) \subseteq Re_{11}$. It follows that $\varphi(J_k) \subseteq Re_{11}$. Thus $\varphi(J_k) \subseteq J_k \cap Re_{11} = \{0\}$. Since $e_{k1} + e_{kk} \in J_k$ and $e_{kk} \in S$, $0 = \varphi(e_{k1} + e_{kk}) = \varphi(e_{k1}) + \varphi(e_{kk}) = \varphi(e_{k1})$. Therefore $\varphi(e_{k1}) = 0$ for each $k \geq 2$ such that $k \succeq 1$. So $\varphi(Re_{11}) = 0$. Thus φ is zero on all of R.

Let $\psi \in \mathrm{End}_K(R^+)$ and define $\varphi(r) = \psi(r) - \psi(1_R) \cdot r$. Then $\varphi(1_R) = 0$ and the foregoing argument shows that ψ is multiplication on the left by $\psi(1_R) \in R$. Therefore the collection of left ideals of R contains a Zassenhaus family for R. By induction, $R = I(X, K)$ has a Zassenhaus family whenever X is finite. $\square$

CHAPTER FOUR

Rings of Algebraic Integers with Zassenhaus Families

Rings of algebraic integers provide more examples of rings with Zassenhaus families over $\mathbb{Z}$. For the following discussion, fix some notation.

Notation 4.1. Suppose that S is the ring of algebraic integers of a Galois field extension F over $\mathbb{Q}$ with degree n. Denote by $G = \{g_1, g_2, ..., g_n\}$ the finite Galois group for F over $\mathbb{Q}$, and set $g_1 = \mathrm{id}_F$.

Recall some basic definitions from [15, Chapter 1, Section 6].

Definition 4.2. A prime ideal P of S *lies above* a prime number p if and only if $P \cap \mathbb{Z} = p\mathbb{Z}$.

Definition 4.3. The *ramification index* of a prime ideal P of S over the prime number $p \in \mathbb{Z}$ is the power of P that appears in the prime factorization of pS.

Definition 4.4. A prime ideal P of S is *ramified* over a rational prime $p \in \mathbb{Z}$ if either the ramification index of P is greater than one or if the field S/P is not separable over $\mathbb{Z}/p\mathbb{Z}$.

Definition 4.5. A prime number $p \in \mathbb{Z}$ is *ramified* in S if and only if pS is divisible by some ramified prime ideal of S.

Definition 4.6. Suppose that a prime ideal P of S lies over a prime number p. The *relative degree* of P over p is the dimension of S/P over $\mathbb{Z}/p\mathbb{Z}$.

Lemma 4.7. *If* $SG = \{\sum_{i=1}^{n} s_i g_i : s_i \in S\}$, *then* $\mathbb{Q} \otimes SG = \mathbb{Q} \otimes \mathrm{End}(S^+) = \mathrm{End}_{\mathbb{Q}}(F^+)$.

Proof: Field automorphisms map roots to conjugate roots. Then each element of G maps S back into S. So $SG \subseteq \mathrm{End}(S^+)$.

Taking an argument from [4, Lemma 2.2.7], it will be seen that F has a basis contained in S. Since F as an extension over $\mathbb{Q}$ has finite degree n, there is a basis $\{x_1, x_2, \ldots, x_n\}$ for F. Since F is a finite Galois extension, each of the x_i are algebraic over $\mathbb{Q}$. Let $1 \leq i \leq n$. For x_i, there is an $m_i \in \mathbb{N}$ and there are $z(i,k) \in \mathbb{Q}$ for $0 \leq k \leq m_i$ such that $z(i,m_i)x_i^{m_i} + z(i,m-1)x_i^{m_i-1} + \ldots + z(i,1)x_i + z(i,0) = 0$. One can assume that the $z(i,k)$ are in $\mathbb{Z}$ (multiply the equation by a common denominator if necessary). Allow us to supress the i for now to write z_k for $z(i,k)$ and m for m_i. Then

$$\begin{aligned} z_m^{m-1}(x_i^m + z_{m-1}x_i^{m-1} + \ldots + z_1x_i + z_0) &= 0 \\ z_m^m x_i^m + z_{m-1}z_m^{m-1}x_i^{m-1} + \ldots + z_1z_m^{m-1}x_i + z_0z_m^{m-1} &= 0 \\ (z_mx_i)^m + z_{m-1}(z_mx_i)^{m-1} + \ldots + z_1z_m^{m-2}(z_mx_i) + z_0z_m^{m-1} &= 0. \end{aligned}$$

Since, as has just shown, z_mx_i is the root of a monic polynomial with coefficients in $\mathbb{Z}$, $z_mx_i \in S$. Define the set $Y = \{y_1, y_2, \ldots, y_n\} \subseteq S$ where $y_i = z(i,m_i)x_i$. Since the x_i are linearly independent, so must be the y_i. Thus Y forms a basis for F. It follows that Y forms a basis for S. This shows that F^+/S^+ is torsion. The fact that for each $f \in F$ there is a number $\ell \in \mathbb{N}$ so that $\ell f \in S$ is used in the future. Note that $\mathbb{Q} \otimes F = \mathbb{Q} \otimes S$.

By the preceding argument S^+ is free abelian of rank n. Hence $\mathrm{End}(S^+)$ is isomorphic to $\mathrm{Mat}_{n\times n}(\mathbb{Z})$. Then $\mathrm{End}(S^+)$ is a rank n^2 free abelian group and must have a basis with n^2 elements. By [13, Lemma V.7.5], G is a linearly independent collection of maps in $\mathrm{End}(S^+)$. It is easy to see that $\{y_ig_j : 1 \leq i, j+1 \leq n\}$ is linearly independent in $\mathrm{End}(S^+)$ and has cardinality n^2. Therefore this set is a basis for both $\mathrm{End}(S^+)$ and SG so $SG = \mathrm{End}(S^+)$.

From [19, Lemma 2.4], $\mathrm{End}(F^+) = FG$ where $FG = \{\sum_{i=1}^n f_ig_i : f_i \in F\}$. Suppose that $f = \sum_{i=1}^n f_ig_i \in FG$. Then the f_i are elements of F. There is an $m_i \in \mathbb{N}$ so that $m_if_i \in S$. Let $m = lcm_im_i$. Then $mf_i \in S$ for each i. It follows

that $mf \in SG$. Therefore $\mathbb{Q} \otimes FG = \mathbb{Q} \otimes SG$. At this point, it has been shown that $\mathbb{Q} \otimes SG = \mathbb{Q} \otimes \mathrm{End}(S^+) = \mathrm{End}(F^+)$.

Any $\mathbb{Q}$-linear endomorphism of F^+ is also $\mathbb{Z}$-linear. Hence $\mathrm{End}_{\mathbb{Q}}(F^+) \subseteq \mathrm{End}(F^+)$. Let $\varphi \in \mathrm{End}(F^+)$, $q \in \mathbb{Q}$, and $x \in F$. Say q has numerator a and denominator b. By definition F is an extension of $\mathbb{Q}$ so that $b^{-1}x \in F$. Then $\varphi(qx) = a\varphi(b^{-1}x) = q\varphi(bb^{-1}x) = q\varphi(x)$. Hence $\mathrm{End}(F^+) = \mathrm{End}_{\mathbb{Q}}(F^+)$. Finally, $\mathbb{Q} \otimes SG = \mathbb{Q} \otimes \mathrm{End}(S^+) = \mathrm{End}_{\mathbb{Q}}(F^+)$. $\square$

Theorem 4.8. *S has a Zassenhaus family $\mathscr{F} = \{L_i : i < \omega\}$ of prime ideals such that each L_i lies above a prime number p_i and $(i \longmapsto p_i)$ is a one-to-one correspondence of the ideals in $\mathscr{F}$ to the set of all prime numbers p such that some ideal of $\mathscr{F}$ lies over p.*

Proof: First construct $\mathscr{F}$. Note that $F = \mathbb{Q}[\pi]$ for some π with minimial polynomial $m_F(x) \in \mathbb{Z}[x]$ of degree n. Denote by $\mathbb{P}$ the set $\mathbb{P}$ of rational primes $p \in \mathbb{Z}$ such that $m_F(x) \pmod p$ has a root. From [9, Proposition on page 298], the set $\mathbb{P}$ is infinite.

By [15, Theorem 1.7.3], the prime numbers that ramify in S are the prime numbers p such that $p\mathbb{Z}$ contains the discriminant ideal I [15, Section 7] of S over $\mathbb{Z}$. $I = \mu\mathbb{Z}$ for some $\mu \in \mathbb{Z}$. Then $\mu\mathbb{Z} \subseteq p\mathbb{Z}$ means that p divides μ. Only a finite number of rational primes divide μ. Exclude these primes from $\mathbb{P}$. Then $\mathbb{P}$ is still infinite, and p is not ramified for each $p \in \mathbb{P}$.

Let $p \in \mathbb{P}$ and $\overline{m}_F(x) = m_F(x) \pmod p$. Let $\overline{m}_F(x) = g_1(x)^{a_1} \cdots g_t(x)^{a_t}$ for some distinct irreducible polynomials $g_i(x)$ over $\mathbb{Z}/p\mathbb{Z}$. By Kummer's Theorem [15, Theorem 1.7.4], $pS = Q_1^{a_1} Q_2^{a_2} \cdots Q_t^{a_t}$ for some distinct prime ideals Q_i of S such that the relative degree of Q_i is the degree of g_i. Since p is not ramified, each $a_i = 1$. Then $pS = Q_1 Q_2 \cdots Q_t$. Since $p \in \mathbb{P}$, there is a root a of $\overline{m}_F(x)$ in $\mathbb{Z}/p\mathbb{Z}$. It follows that $g_k(x) = (x - a)$ for some $1 \leq k \leq t$. So Q_k has relative degree 1. By [15, Theorem

1.6.8], the prime ideals $Q_1, Q_2, \ldots, Q_t$ lying above p each have the same ramification index e and relative degree f such that $eft = n$. In this case, $e = 1$. Since Q_k has relative degree 1, $f = 1$. Thus $t = n$ and pS factors into n distinct prime ideals.

Also by Kummer's Theorem, G transitively permutes the n prime ideals. Since G has order n, only id_F fixes all of the Q_i lying over p. Let $\mathbb{P} = \{p_i : i < \omega\}$. Let $i < \omega$ and let $k = (i \bmod n) + 1$. Pick a single prime ideal Q_i lying above p_i such that $g_k(Q_i) \neq Q_i$. Define a candidate $\mathscr{F}$ for a Zassenhaus family for S as $\mathscr{F} = \{Q_i : i < \omega\}$.

Let $\{a_1, a_2, ..., a_n\}$ be an integral basis of S. By Lemma 4.7, $\mathbb{Q} \otimes SG = \mathbb{Q} \otimes \mathrm{End}(S^+) = \mathrm{End}_{\mathbb{Q}}(F^+)$. Define an $n \times n$-matrix Δ over S by $\Delta = (g_i(a_j))_{1 \leq i,j \leq n}$. Then $\det(\Delta) \neq 0$ since $\det(\Delta)$ is a linear combination of basis elements for the linear transformations of S^+. Then there is a matrix Δ^{-1} with entries in F. It follows that $\Delta^{-1} \in \mathrm{End}_{\mathbb{Q}}(F^+)$. From Lemma 4.7, $\mathrm{End}_{\mathbb{Q}}(F^+) = \mathbb{Q} \otimes \mathrm{End}(S^+)$ so $\Delta^{-1} \in \mathbb{Q} \otimes \mathrm{End}(S^+)$. It follows that there is a number $m_\Delta \in \mathbb{N}$ such that $m_\Delta \Delta^{-1} \in \mathrm{End}(S^+) = \mathrm{Mat}_{n \times n}(S)$. That is, $m_\Delta \Delta^{-1}$ has entries in S.

Let $\varphi \in \mathrm{End}(S^+)$ such that $\varphi(P) \subseteq P$ for all $P \in \mathscr{F}$. Lemma 4.7 promises some $m \in \mathbb{N}$ such that $m\varphi = \sum_{i=1}^{n} s_i g_i \in SG$. Borrowing a technique from [19, Lemma 2.5]:

Let $f = m\varphi$. Then $f(P) \subseteq P$ for all $P \in \mathscr{F}$. Observe that

$$\begin{aligned}(f(a_1), ..., f(a_n)) &= \left(\sum_{i=1}^{n} s_i g_i(a_1), ..., \sum_{i=1}^{n} s_i g_i(a_n) \right) \\ &= (s_1, s_2, ..., s_n)\Delta.\end{aligned}$$

Let $x \in P$ for some $P \in \mathscr{F}$. Then

$$\begin{aligned}(f(xa_1), ..., f(xa_n)) &= \left(\sum_{i=1}^{n} s_i g_i(xa_1), ..., \sum_{i=1}^{n} s_i g_i(xa_n) \right) \\ &= \left(\sum_{i=1}^{n} s_i g_i(x) g_i(a_1), ..., \sum_{i=1}^{n} s_i g_i(x) g_i(a_n) \right) \\ &= (s_1 g_1(x), ..., s_n g_n(x))\Delta \in P \times P \times ... \times P.\end{aligned}$$

Recall that $m_\Delta \Delta^{-1}$ is a matrix with entries in S. Thus

$$(f(xa_1), ..., f(xa_n))m_\Delta \Delta^{-1} = m_\Delta(s_1 g_1(x), ..., s_n g_n(x))$$
$$\in P \times P \times ... \times P.$$

It follows that $m_\Delta s_i g_i(P) \subseteq P$ for all $1 \leq i \leq n$. If p divides m_Δ then exclude p from $\mathbb{P}$. Since only a finite number of primes divide m_Δ, $\mathbb{P}$ is still infinite.

Suppose that $p \in \mathbb{P}$ with $P \in \mathscr{F}$ the corresponding prime ideal lying over p. Note that $pS \subseteq P$ so that S/P is a torsion p-group. Also, $m_\Delta s_i g_i(P) \subseteq P$. From $\gcd(p, m_\Delta) = 1$ it follows that $s_i g_i(P) \subseteq P$.

Let $2 \leq i \leq n$. For $k = (i \bmod n) + 1$, $p_k \in \mathbb{P}$ with corresponding $P = P_k \in \mathscr{F}$ such that $g_i(P) \neq P$. Recall that P has relative degree 1 over p. Then S/P is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ a field and so P is a maximal ideal of S. It follows that $S = g_i(P) + P$ and $1 = g_i(a) + b$ for some elements a and b of P. This implies that $s_i = s_i g_i(a) + s_i b \in P + P = P$. Then $s_i \in P$ for all $P \in \mathscr{F}$. It follows that s_i is not a unit.

If $s_i \neq 0$, then $s_i S$ is a nontrivial, proper ideal of S such that $s_i S \subseteq P_k$ for all $P_k \in \mathscr{F}$ such that $k = (i \bmod n) + 1$. Since $\mathbb{P}$ is infinite, there are infinitely many such P_k. Then $s_i S$ factors into an infinite number of distinct prime ideals of S. This is a contradiction.

From this contradiction, one can conclude that $s_i = 0$ for $2 \leq i \leq n$. Thus $f = m\varphi = s_1 \,\mathrm{id}_F$. Then $\varphi(1) = s_1/m \in F$. But $\varphi(1) \in S$ so $s_1/m \in S$. Therefore φ is multiplication on the left by an element in S. $\square$

A direct application of the preceding theorem leads to the following corollary.

Corollary 4.9. *Let S be the ring of algebraic integers of the quadratic number field $F = \mathbb{Q}[\sqrt{m}]$. Then S has a Zassenhaus family of prime ideals all lying over distinct primes.*

Let F, S, and m be as in the preceding corollary. One can actually construct the Zassenhaus family for S using the techniques developed in the proof of the preceding theorem. Let $G = \{\mathrm{id}_F, \sigma\}$ be the Galois group of F.

First, suppose that $m > 0$. By Dirichlet's Arithmetic Progression Theorem [18, Theorem 6.21], the set $\Gamma = \{p \in \Pi : p \equiv 1 \bmod 4m\}$ is infinite. Note that each of 4 and m is a divisor of $4m$. From [16, page 19], $p \equiv 1 \bmod 4$ and $p \equiv 1 \bmod m$ for all $p \in \Gamma$. Since $1^2 \equiv 1 \bmod m$, each $p \in \Gamma$ is a quadratic residue $\bmod m$. By Gauss's Quadratic Reciprocity Theorem [16, Proposition II.2.5] and [16, Proposition II.2.3], it follows that m is a quadratic residue $\bmod p$ for all $p \in \Gamma$.

Now suppose that $m < 0$. Since $p \equiv 1 \bmod 4m$, then $(p-1)/2$ is an even integer. The [16, Proposition II.2.3] implies that -1 is a quadratic residue $\bmod p$.

Then any $m \in \mathbb{Z}$ is a quadratic residue $\bmod p$ for all $p \in \Gamma$. Define Γ' the set of all primes $p \in \Gamma$ such that p is not ramified in S. By the second paragraph of the proof of 4.8, Γ' is cofinite in Γ and has infinite cardinality. Also by the second paragraph of the proof of Theorem 4.8, $pS = P_pQ_p$ with distinct prime ideals P_p and Q_p of S. Since G operates transitively on the set $\{P_p, Q_p\}$, $\sigma(P_p) = Q_p$ for all $p \in \Gamma'$. The family $\mathscr{F} = \{P_p : p \in \Gamma'\}$ now has the properties required to apply the proof of Theorem 4.8. Note that by [15, Theorem 1.9.2], $S = \mathbb{Z}[d]$ where

$$d = \begin{cases} \sqrt{m} & \text{if } d \equiv 2, 3 \mod 4, \\ \frac{1+\sqrt{m}}{2} & \text{if } d \equiv 1 \mod 4. \end{cases}$$

CHAPTER FIVE

Some Dedekind Domains have Zassenhaus Families

Lemma 5.1. *[19, Lemma 2.5] Let R be an integral domain such that R^+ is torsion free and let D be the field of fractions of R. Let Λ be a finite set of ring automorphisms of R, let $s_\sigma \in R$ for each $\sigma \in \Lambda$, and let $f = \sum_{\sigma\in\Lambda} s_\sigma\sigma \in \mathrm{End}_{\mathbb{Z}}(R)$. If X is an ideal of R such that $f(X) \subseteq X$, then there is a nonzero $s_\Lambda \in R$ such that s_Λ only depends on Λ and $s_\Lambda s_\sigma\sigma(X) \subseteq X$ for each $\sigma \in \Lambda$.*

Proof: Let λ be an ordinal such that $\{a_\nu : \nu < \lambda\}$ a maximal $\mathbb{Z}$-independent set in R^+. Equivalently, $\{a_\nu : \nu < \lambda\}$ is maximal such that $\oplus_{\nu<\lambda} a_\nu\mathbb{Z} \subseteq D$ and $R/(\oplus_{\nu<\lambda} a_\nu\mathbb{Z})$ is torsion. Note that each $\sigma \in \Lambda$ extends uniquely to an automorphism of D. Abusing notation, call that map σ as well. Enumerate Λ as $\Lambda = \{\sigma_i : 1 \le i \le n\}$. For each $1 \le i \le n$ define an element $\Delta_i \in R^\lambda$, the cartesian product of λ many copies of R, by $\Delta_i = (\sigma_i(a_\nu))_{\nu<\lambda}$.

Define the $n \times \lambda$ matrix over R by

$$\Delta = \begin{bmatrix} \Delta_1 \\ \Delta_2 \\ \vdots \\ \Delta_n \end{bmatrix}$$

To see that the rows of Δ are independent over D, assume that there are $x_i \in D$ such that $0 = \sum_{i=1}^n x_i[(\sigma_i(a_\nu))_{\nu<\lambda}]$. Summing the terms of each sequence,

$$\left(\sum_{i=1}^n x_i\sigma_i\right)(a_\nu) = 0 \text{ for each } \nu < \lambda$$

Let $r \in R$. From earlier comments, there is a natural number m_r such that $m_r r$ is a linear combination of a finite number of the a_ν. It follows that

$$0 = \left(\sum_{i=1}^n x_i\sigma_i\right)(m_r r) = m_r\left(\sum_{i=1}^n x_i\sigma_i\right)(r)$$

Since R^+ is torsion-free and m_r is nonzero,

$$0 = \left(\sum_{i=1}^{n} x_i \sigma_i \right) (r)$$

It follows that $\sum_{i=1}^{n} x_i \sigma_i$ is the zero map on R. The proof of Lemma 7.5 in [Hungerford, page 291] can easily be modified to show that automorphisms of R are linearly independent over D from which one can conclude that $x_i = 0$ for $1 \leq i \leq n$. Therefore the rows of Δ are independent. Thus one can perform elementary row operations over D on Δ that, after finitely many steps, yield the "row reduced echelon form" of Δ. Since the rows of Δ are linearly independent over D, there is some $n \times n$ matrix M over D such that $M\Delta$ has n "pivot columns". Thus, a permutation of the ordinals less than λ can be performed such that, after this adjustment of the enumeration of $\{a_\nu : \nu < \lambda\}$, then $M\Delta = [I_n \vdots \Psi]$ where I_n is the $n \times n$ identity matrix. This means that $\Delta = [\Delta_1 \vdots \Delta_2]$ and $M\Delta = [M\Delta_1 \vdots M\Delta_2] = [I_n \vdots \Psi]$ and so $M = \Delta_1^{-1}$ is invertible. Since Δ_1 has entries in R, M has entries in D. The matrix M has a finite number of entries so there is a nonzero $s_\Lambda \in R$ such that $s_\Lambda M$ has entries in R.

Note that $(f(a_\nu))_{\nu<\lambda} = (\sum_{j=1}^{n} s_j \sigma_j(a_\nu))_{\nu<\lambda} = (s_1, s_2, \ldots, s_n)\Delta$. Let $x \in X$. Then

$$\begin{aligned}
(f(xa_\nu))_{\nu<\lambda} &= (\sum_{j=1}^{n} s_j \sigma_j(xa_\nu))_{\nu<\lambda} \\
&= (\sum_{j=1}^{n} s_j \sigma_j(x)\sigma_j(a_\nu))_{\nu<\lambda} \\
&= (s_1\sigma_1(x), \ldots, s_n\sigma_n(x))\Delta \in X^{(n)}.
\end{aligned}$$

where $X^{(n)}$ denotes the Cartesian product of n copies of X. Let

$$\begin{bmatrix} \Delta_1^{-1} \\ 0 \end{bmatrix}$$

denote the $\lambda \times n$ matrix with the $n \times n$ block Δ_1^{-1} above a block whose entries are all zero. Then

$$(s_1\sigma_1(x), \ldots, s_n\sigma_n(x))\Delta = (s_1\sigma_1(x), \ldots, s_n\sigma_n(x))[\Delta_1 \vdots \Delta_2] \in X^{(n)}$$

So

$$(s_1\sigma_1(x),\ldots,s_n\sigma_n(x))[\Delta_1|\Delta_2]\begin{bmatrix}\Delta_1^{-1}\\0\end{bmatrix}\in X^{(n)}\begin{bmatrix}\Delta_1^{-1}\\0\end{bmatrix}$$

which is equivalent to

$$(s_1\sigma_1(x),\ldots,s_n\sigma_n(x))I_n\in X^{(n)}\Delta_1^{-1}.$$

It follows that

$$s_\Lambda(s_1\sigma_1(x),\ldots,s_n\sigma_n(x))I_n\in X^{(n)}s_\Lambda\Delta_1^{-1}\subseteq X^{(n)}.$$

Therefore $s_\Lambda s_\sigma\sigma(X)\subseteq X$ for each $\sigma\in\Lambda$. $\square$

Theorem 5.2. *Let R be a Dedekind domain such that R^+ is torsion free, $\mathbb{P}$ the set of all prime ideals of R, and D the field of fractions of R. Moreover, let $K_{\mathbb{P}}$ be the kernel of the natural map $Aut(R)\to S_{\mathbb{P}}$ where $S_{\mathbb{P}}$ is the group of permutations of $\mathbb{P}$, and assume that $End(R^+)\subseteq D[Aut(R)]$. Then R has a Zassenhaus family of ideals if and only if $K_{\mathbb{P}}=\{id_R\}$.*

Proof: Assume that $\sigma\in K_{\mathbb{P}}$ and $\sigma\neq id_R$. This means that $\sigma(P)=P$ for all $P\in\mathbb{P}$ and since R is Dedekind, $\sigma(X)=X$ for all ideals X of R. If $\sigma\in R\cdot$ then $\sigma=\sigma(1)\cdot=1\cdot=id_R$, a contradiction. This shows that $R\subsetneqq\{\varphi\in\mathrm{End}_{\mathbb{Z}}(R):\forall X\trianglelefteq R(\varphi(X)\subseteq X)\}$ and R has no Zassenhaus family of ideals.

Now assume that $K_{\mathbb{P}}=\{id_R\}$. It follows that for any $id_R\neq\sigma\in Aut(R)$, there is some $P\in\mathbb{P}$ such that $\sigma(P)=Q\in\mathbb{P}$ but $Q\neq P$. Let $\{\beta_n:n<\omega\}$ be an increasing, unbounded sequence of natural numbers. Define $X_{\sigma,n}=PQ^{\beta_n}$. Then for $0\neq s$,

$$s\sigma(X_{\sigma,n})=sQ\sigma(Q)^{\beta_n}\subseteq PQ^{\beta_n}$$

only if $sQ\subseteq Q^{\beta_n}$.

Assume that there is a k such that $sQ \subseteq Q^{\beta_k}$. Since $sRQ \subseteq sQ$, the factorization of sR into prime ideals must contain a factor Q^{α} such that $\alpha \geq \beta_k - 1$. Since $\{\beta_n : n < \omega\}$ increases without bound, there is an index m such that $\beta_m > \alpha$. Then $sQ \not\subseteq Q^{\beta_m}$. It has been shown that for any $0 \neq s \in R$, there is an index m such that $s\sigma(X_{\sigma,m}) \not\subseteq X_{\sigma,m}$.

Suppose that $\varphi \in End(R^+)$ such that $\varphi(X_{\sigma,n}) \subseteq X_{\sigma,n}$ for each $\sigma \in Aut(R)$ and each $n \in \mathbb{N}$. Since $\varphi(R) \subseteq R$, it follows that $s\varphi = \sum_{i=1}^{k} s_i\sigma_i$ for some $s, s_i \in R$ and some $\sigma_i \in Aut(R)$.

Let $1 \leq i \leq k$. By the preceding lemma, $s_i\sigma_i(X_{\sigma,n}) \subseteq X_{\sigma,n}$ for each $\sigma \in Aut(R)$ and each $n \in \mathbb{N}$. In particular, $s_i\sigma_i(X_{\sigma_i,n}) \subseteq X_{\sigma,n}$ for each $n \in \mathbb{N}$. By the construction of the $X_{\sigma_i,n}$, it must be the case that $\sigma_i = id_R$ for all i. Therefore $s\varphi = t$ where $t = \sum_i s_i$. Then φ is the multiplication by $s^{-1}t \in D$. But $s^{-1}t = \varphi(1) \in R$ and it follows that $\varphi \in R$. This shows that $\mathscr{F} = \{X_{\sigma,n} : \sigma \in Aut(R), n \in \mathbb{N}\}$ is a Zassenhaus family of R. $\square$

CHAPTER SIX

From Zassenhaus Families to Zassenhaus Rings

For particular rings with Zassenhaus families, Lemma 6.8 below allows us to construct modules from the Zassenhaus families to satisfy the definition of a Zassenhaus ring. That is, various partial converses for Theorem 2.3 follow from this lemma. Recall the following definitions from abelian group theory; see, for example, [1]. Abelian groups in this section are presumed torsion free unless noted otherwise. From Definition 3.5, a subgroup H of a group G is *pure* in G if and only if $H \cap nG = nH$ for each integer n.

Definition 6.1. Suppose that H is a subgroup of a torsion free abelian group G. Then the *purification* of H in G is $H_* = \{g \in G : \exists n \in \mathbb{Z}(ng \in H)\}$.

Lemma 6.2. *H_* is pure in G.*

Proof: Let $n \in \mathbb{Z}$ and $g \in G$ such that $ng \in H_*$. Then there is an $m \in \mathbb{Z}$ so that $(mn)g = m(ng) \in H$. Hence $g \in H_*$ and $ng \in nH_*$. So $H_* \cap nG = nH_*$ for any $n \in \mathbb{Z}$. Therefore H_* is pure in G. $\square$

Definition 6.3. Suppose that G is an abelian group and that p is a prime number. Define a function $h_p^G : G \to \mathbb{N} \cup \{\infty\}$ as follows. If there is an $n \in \mathbb{N}$ so that g is divisible by p^n but not p^k for $k > n$, then set $h_p^G(g) = n$. Otherwise, set $h_p^G(g) = \infty$. The value $h_p^G(g)$ is called the *p-height* of g in G. For each $g \in G$, the *height sequence* $(h_p^G(g))_{p \in \prod}$ can be considered.

Definition 6.4. For a given height sequence $\alpha = (h_p^G(g))_{p \in \prod}$ define the type of α in G, denoted type(α), to be the collection of all height sequences β for elements of G such that β differs from α at only a finite number of entries by only a finite amount. If $g \in G$ then the type of g is just the type of its height sequence.

A brief inspection will confirm that, in an abelian group, types are equivalence classes. That is, the property of belonging to a type is transitive, reflexive, and symmetric within the context of elements and the group operation of an abelian group.

Definition 6.5. A group G is *homogenous* if and only if all nonzero elements have the same type.

Let $z \in \mathbb{Z}$. Then z is divisible by only a finite number of primes, and each prime divisor divides z only up to a finite power. If α is the height sequence for z in $\mathbb{Z}$, α differs from $0 = (0)_{p\in\Pi}$ at only a finite number of entries by, at most, a finite amount. Thus $\alpha \in \text{type}(0)$ (equivalently, g is of type 0). Therefore, $\mathbb{Z}$ is homogenous of type 0.

If $\alpha = (a_p)$ and $\beta = (b_p)$ are height sequences, then say $\alpha \leq \beta$ if and only if $a_p \leq b_p$ for all $p \in \Pi$. It is easy to show that this is a partial order (see [1, Section 1]). This partial order induces a partial order for the types. For types τ_0 and τ_1, say $\tau_0 \leq \tau_1$ if and only if there are height sequences $\alpha_0 \in \tau_0$ and $\alpha_1 \in \tau_1$ so that $\alpha_0 \leq \alpha_1$.

Definition 6.6. For a type τ, set $G(\tau) = \{g \in G : \text{type}(g) \geq \tau\}$.

Lemma 6.7. *If A is any abelian group, $a \in A$, and $n, m \in \mathbb{N}$ such that $\gcd(m, n) = 1$ and $ma \in nA$. Then $a \in nA$.*

Proof: There is a $b \in A$ so that $ma = nb$. There are integers r and s so that $1 = rn + sm$. Then $m = (1 - rn)/s$. Using our new identity for m,

$$(1 - rn)a = snb$$

$$a - rna = snb$$

$$a = n(ra + sb) \in nA.$$

□

Lemma 6.8. *Suppose that G is a torsion free abelian group that is homogeneous of type 0. Suppose further that there is a family $\{V_i : i \in I\}$ of at most countably many pure subgroups of G such that*

(1) $G = \sum_{i\in I} V_i$, and

(2) each G/V_i is homogeneous of type 0.

Let $\{P_i : i \in I\}$ be a family of disjoint infinite sets of primes, and set $R_i = \langle p^{-1} : p \in P_i\rangle \subseteq \mathbb{Q}$. Denote by τ_i the type of R_i for all $i \in I$. Define $M = \sum_{i\in I} R_i V_i$. Then $M(\tau_i) = (V_i)_*$. That is, the purification of V_i in M is just $M(\tau_i)$.

Proof: Lemma 6.7 shows that if A is any abelian group and $n, m \in \mathbb{N}$ such that $\gcd(m, n) = 1$, then $ma \in nA$ for some $a \in A$ implies $a \in nA$.

To see that M/G is torsion, let $a \in M$. Then $a = \sum_i p_i^{-1} v_i$ for some $p_i \in P_i$ and $v_i \in V_i$. A finite number of the terms in the summation are nonzero so there is a finite least common multiple ℓ for the p_i. For each $i \in I$, $\ell p_i^{-1} v_i \in V_i$. Thus $\ell a = \sum_i \ell p_i^{-1} v_i \in \sum_i V_i = G$. Therefore M/G is torsion.

Let $i \in I$ and $v \in V_i$. If $p \in P_i$, then $v = p(1/p)v$ and $(1/p)v \in M$. Thus $h_p^M(v) \geq h_p^M(1/p)$. If $p \notin P_i$ then any element of R_i is only finitely divisible by p and the same goes for v. Then, by the construction of M, $\text{type}(v) \geq \text{type}(\tau_i)$. Thus $V_i \subseteq M(\tau_i)$.

To see that $M(\tau_i)$ is pure in M, let $k \in \mathbb{Z}$ and $a \in M$ such that $ka \in M(\tau_i)$. For each $p \in \Pi$, $h_p^M(ka) \leq h_p^{\mathbb{Z}}(k) + h_p^M(a)$. Since $h_p^{\mathbb{Z}}(k)$ is nonzero for at most finitely many $p \in \Pi$, $\text{type}(a) = \text{type}(ka) \geq \tau_i$. Thus $a \in M(\tau_i)$ and $ka \in kM(\tau_i)$. It follows that $M(\tau_i)$ is pure in M.

Since $M(\tau_i)$ is pure in M and $V_i \subseteq M(\tau_i)$, it is clear that $(V_i)_* \subseteq M(\tau_i)$. To show that $M(\tau_i) \subseteq (V_i)_*$, let $s \in M(\tau_i)$. Since M/G is torsion, there is some $m \in \mathbb{N}$ such that $s' = ms \in G \cap M(\tau_i)$.

The set $P_i^{'} = \{p \in P_i : s' \in pM, s' \notin pG, \gcd(p,m) = 1\}$ is cofinite in P_i. For, if $p \notin P_i^{'}$ then one or more of $s' \notin pM$, $s' \in pG$, and $\gcd(p,m) \neq 1$ holds. So the complement of $P_i^{'}$ is the union of $C_0 = \{p \in P_i : s' \notin pM\}$, $C_1 = \{p \in P_i : s' \in pG\}$, and $C_2 = \{p \in P_i : \gcd(p,m) \neq 1\}$. It suffices to show that each of these sets is finite.

If $s' \notin pM$, then s' is not divisible by p in M. But $s' \in M(\tau_i)$ so the height sequence for s' in M has at most finitely many entries such that the entry is less than the corresponding entry for τ_i. Recall that τ_i is the type of R_i which is generated by the inverses of the primes of P_i. Let τ_i^p denote the p-th entry for τ_i. Then τ_i^p is not zero for $p \in P_i$. It follows that s' is not divisible by p for at most finitely many $p \in P_i$. Therefore C_0 is finite.

Note that $s' \in G$ and G is homogenous of type 0. Then the height sequence for s' in G has entries that differ from 0 in at most finitely many places. It follows that s' is divisible by at most finitely many $p \in P_i$ in G. Thus $s' \in pG$ for at most finitely many $p \in P_i$. Therefore C_1 is finite.

Since m is divisible by at most a finite number of primes, $\gcd(p,m) \neq 1$ for a finite number of $p \in \Pi$. Since P_i is infinite, $\gcd(p,m) \neq 1$ for a finite number of $p \in P_i$. Thus C_2 is finite. Then $P_i^{'}$ is cofinal in P_i.

Let Π_i be the set of all square-free natural numbers whose prime factors are contained in P_i. Let $p \in P_i^{'}$. By the definition of $P_i^{'}$, there is an $x \in M$ so that $px = s'$. From the construction of M, it follows that $x = \sum_j \frac{1}{q_j} v_j$ for some $v_j \in V_j$ and $q_j \in \Pi_j$. Let $q = \prod_{j \neq i} q_j$. Since $px = s' = \sum_j \frac{1}{q_j} v_j$ one can rewrite the summation so that no term has p in the denominator. One can assume that $\gcd(p,q) = 1$. Now

$$qx = q \sum_j \frac{1}{q_j} v_j = \sum_j \frac{q}{q_j} v_j = g + \frac{1}{q_i} v_i'$$

with $v_i' = q v_i'$ and g a linear combination of the v_j with $j \neq i$. Note that $g \in G$. This implies that $qs' = pqx = pg + \frac{p}{q_i} v_i'$. Then $pv_i' \in q_i G \cap V_i = q_i V_i$ since V_i is pure in G. Either p divides q_i or not.

Assume p does not divide q_i. Since $pv_i' \in q_iV$, then $v_i' \in q_iV_i$ and $v_i' = q_iv_i''$ for some $v_i'' \in V_i$. Thus $qs' = p(g + v_i'')$. Since $p \in P_i^{'}$ and $\gcd(p, q) = 1$, the element s' is in pG. This contradicts the definition of $P_i^{'}$.

Thus one can assume that $q_i = pt$ for some $t \in \mathbb{N}$. Since q_i is square-free, $\gcd(p, t) = 1$. It follows that $qts' = ptg + \dfrac{pt}{q_i}v_i' = ptg + v_i'$. Then $qt(s' + V_i) \in p(G/V_i)$. Since both q and t are relatively prime to p, $\gcd(p, qt) = 1$. It follows that $s' + V_i \in p(G/V_i)$ for all $p \in P_i^{'}$. This shows that $\text{type}(s' + V_i) \geq \tau_i > 0$. But G/V_i is homogeneous of type 0. The only possibility is that $s' + V_i = V_i$, and thus $s' \in V_i$. Since $ms = s' \in V_i$, $s \in (V_i)_*$. $\square$

Theorem 6.9. *Suppose that R is a ring such that R/pR has no nonzero nilpotent elements for any prime p, $\mathbb{Q}R$ has a Zassenhaus family $F^{'} = \{\mathbb{Q}V_i : i \in I\}$, and the V_i are ideals of R such that R^+ and $\{V_i : i \in I\}$ satisfy Lemma 6.8. Then R is a Zassenhaus ring.*

Proof: Let $R_i \subseteq \mathbb{Q}$ be as described in Lemma 6.8. Set $M = \sum_{i\in I} R_iV_i \subseteq \mathbb{Q}R$. For $i \in I$, Lemma 6.8 shows that $M(\tau_i) = (V_i)_*$.

Let $\varphi \in \text{End}_{\mathbb{Z}}(M)$ such that $\varphi(1) = 0$. Let $a \in M(\tau_i)$ and $p \in \Pi$. If $h_p^M(a) = n$, then $a = p^nz$ for some $z \in M$ with z not divisible by p. In this case, $\varphi(a) = p^n\varphi(z)$. If $h_p^M(a) = \infty$, then $\varphi(a)$ must be divisible by any power of p as well. It follows that the type of $\varphi(a)$ is greater than or equal to the type of a. Hence φ maps $M(\tau_i)$ into itself. Then

$$\varphi(V_i) \subseteq \varphi((V_i)_*) \subseteq \varphi(M(\tau_i)) \subseteq M(\tau_i) = (V_i)_*$$

the purification of V_i in M. Let $g \in (V_i)*$. Then there is an $n \in \mathbb{N}$ so that $ng \in V_i$. Hence $g = (1/n)(ng) \in \mathbb{Q}V_i$. Therefore $\varphi(V_i) \subseteq \mathbb{Q}V_i$.

Since $R \subseteq M \subseteq \mathbb{Q}R$, $\mathbb{Q}M = \mathbb{Q}R$. From [1, Section 0], there is a unique extension $\psi \in \text{End}_{\mathbb{Q}}(\mathbb{Q}M) = \text{End}_{\mathbb{Q}}(\mathbb{Q}R)$ of φ. Then $\psi(\mathbb{Q}V_i) = \mathbb{Q}\psi(V_i) \subseteq \mathbb{Q}V_i$. Since

F' is a Zassenhaus family, ψ is multiplication on the left by $\frac{r}{q}$ for some $r \in R$ and some $q \in \mathbb{N}$. Recall that $\psi(1) = \varphi(1) = 0$. So $\psi = \varphi = 0$.

Let $\gamma \in \mathrm{End}_{\mathbb{Z}}(M)$ and $i \in I$. Then $\gamma(M(\tau_i)) \subseteq M(\tau_i) = (V_i)_* = \mathbb{Q}V_i \cap M$ and so $\gamma(\mathbb{Q}V_i) \subseteq \mathbb{Q}V_i$. Then γ leaves invariant the member ideals of $\mathscr{F}'$. Hence γ is multiplication on the left by some element of $\mathbb{Q}R$. Since $m = \gamma(1) \in M$, $(\gamma - m\cdot)(1) = 0$. By the preceding paragraph, $(\gamma - m\cdot)$ is the zero map. Thus γ is multiplication on the left by m.

To conclude that R is a Zassenhaus ring, it suffices to show that $m \in R$. To this end, let $x + R \in M/R$. From Lemma 6.8, $x = \sum_{i=1}^{n}(1/q_i)v_i$ where each $v_i \in V_i$ and q_i is a product of distinct primes raised only to the first power from P_i. Recall that the P_i are mutually disjoint. Hence $q = \mathrm{lcm}_i\, q_i$ is a product of distinct primes raised only to the first power. Then $qx \in R$. It follows that the order $q = o(x + R)$ and is square free. Also, $x = (\sum_{i=1}^{n} a_i v_i)/q$ for appropriate $a_i \in \mathbb{N}$. Notice that the numerator is in R.

One can write $m = \frac{s}{q}$ with $s \in R$ and $q = o(m+R)$. Then $\varphi(m) = m\cdot m = \frac{s^2}{q^2} \in M$. Let p be a prime divisor of q and $q = pq'$. Since q is square free, $gcd(p, q') = 1$. So $(q')^2\frac{s^2}{q^2} = \frac{s^2}{p^2} \in M$. Thus $o\left(\frac{s^2}{p^2} + R\right)$ divides p^2 and is square-free. It must be the case that $p\frac{s^2}{p^2} = \frac{s^2}{p} \in R$. Then $p\frac{s^2}{p} = s^2 \in pR$. It follows that $(s + pR)^2 = 0 \in R/pR$ since R/pR has no nonzero nilpotent elements.

It has been shown that $s^2 \equiv 0 (\mathrm{mod}\, p)$. Thus p divides s^2. This can only be the case when p divides s. Then $s \in pR$. Since $q = o(m + R)$, the element $m = \frac{s}{q}$ cannot be reduced. But p is a divisor of both q and s. Hence q must not have any prime divisors, i.e. $q = 1$. Therefore φ is multiplication on the left by $s \in R$. $\square$

The next two corollaries apply Theorem 6.9 to obtain examples of Zassenhaus Modules constructed from Zassenhaus families. Note that in the next corollary, the ring $\mathbb{Z}[x]$ is considered. This ring does not have finite rank.

Corollary 6.10. *The ring $\mathbb{Z}[x]$ of polynomials with integer coefficients is a Zassenhaus ring.*

Proof: Let $R = \mathbb{Z}[x]$. For each prime p, if p does not divide $0 \neq g(x) \in \mathbb{Z}[x]$ then p does not divide $(g(x))^n$ for $n \in \mathbb{N}$. Hence R/pR has no nonzero nilpotent elements. By Proposition 3.3, $\mathscr{F}' = \{\mathbb{Q}V_i : i \in I\}$ is a Zassenhaus family of the $\mathbb{Q}$-algebra $\mathbb{Q}R$. Lemma 3.7 shows that R has a countable Zassenhaus family $\mathscr{F} = \{V_i : i \in I\}$ such that each V_i is a direct summand of R^+. That $R = \sum_{i\in I} V_i$ is clear by inspection. Let $R_i \subseteq \mathbb{Q}$ be as described in Lemma 6.8. Set $M = \sum_{i\in I} R_i V_i \subseteq \mathbb{Q}R$. It is easy to see that R is homogenous of type 0. Let $i \in I$. From [11], direct summands of abelian groups are pure. By Lemma 3.7, each element of our Zassenhaus family for $\mathbb{Z}[x]$ is pure in the additive group of $\mathbb{Z}[x]$. Each element of the Zassenhaus family of Lemma 3.7 is pure in the additive group of $\mathbb{Z}[x]$. Since the additive group of $\mathbb{Z}[x]$ is a direct sum of copies of $\mathbb{Z}$, $\mathbb{Z}[x]$ is homogenous of type 0. Then for each element Y of the Zassenhaus family for $\mathbb{Z}[x]$ from Lemma 3.7, $(\mathbb{Z}[x])/Y$ is homogeneous of type 0. So Lemma 6.8 applies. The assertion follows from Theorem 6.9. $\square$

Corollary 6.11. *Let $R = S\Lambda$ the ring defined in Lemma 3.11 with the additional hypotheses that S^+ is homogenous of type 0, S^+ is free of finite rank, and S/pS has no nonzero nilpotent elements for any prime p. In this case, R is a Zassenhaus ring.*

Proof: The Zassenhaus family of Lemma 3.11 is countable. The family $\mathscr{F} = \{V_i : i \in I\}$ can be enumerated with a countable index set I. From the definition, $R = \oplus_{\gamma\in\Lambda} \gamma S$. To apply Lemma 6.8, one needs to know that R is homogenous of type 0. This property follows directly from the fact that S is homogenous of type 0 and R is the direct sum of copies of S. By Lemma 3.11, R is the sum of all the V_i and each V_i is a direct summand of R. It follows that each V_i is pure in R and R/V_i

is isomorphic to a direct summand of R. Since direct summands of R are homogenous of type 0, R/V_i is homogenous of type 0. By Proposition 3.6, $\mathscr{F}' = \{\mathbb{Q}V_i : i \in I\}$ is a Zassenhaus family of the $\mathbb{Q}$–algebra $\mathbb{Q}R$. The hypotheses of Lemma 6.8 are satisfied. The assertion follows from Theorem 6.9. $\square$

The next result helps show that rings of algebraic integers are Zassenhaus rings.

Proposition 6.12. *Suppose that S is a ring with identity such that S^+ is a free abelian group of finite rank. Suppose that $\mathscr{F} = \{P_i : i < \omega\}$ is a Zassenhaus family of right ideals of S. Suppose further that for each $i < \omega$, there is a (unique) number p_i such that p_iS is properly contained in P_i and the ring $S_i = P_i/p_iS$ has the property that $x \in S_i$ with $x^2 = 0$ implies $x = 0$.*

Then there is a right S module M such that $S \subseteq M \subseteq \mathbb{Q}S$ and $\mathrm{End}_{\mathbb{Z}}(M^+) = S$. Moreover, $p(t_p(M/S)) = 0$ for all prime numbers p.

Proof: Define $M = \sum_{i<\omega} p_i^{-1}P_i \subseteq \mathbb{Q}S$. Let $\varphi \in \mathrm{End}_{\mathbb{Z}}(M^+)$. Note that S^+ is finitely generated, say by $\{s_1, s_2, \ldots, s_n\}$, and M/S is torsion. Then for each s_i there is a k_i such that $k_i\varphi(s_i) \in S$. Define $k = \mathrm{lcm}_i\, k_i$. Let $s \in S$. Then $s = z_1s_1 + z_2s_2 + \ldots + z_ns_n$ for some $z_i \in \mathbb{Z}$. So $\varphi(s) = z_1\varphi(s_1) + z_2\varphi(s_2) + \ldots + z_n\varphi(s_n)$. It follows that $k\varphi(s) \in S$. Therefore $k\varphi|_S = \psi \in \mathrm{End}_{\mathbb{Z}}(S^+)$.

Note that $t_{p_i}(M/S) = (p_i^{-1}P_i)/S$. Let $i < \omega$ and $p_i^{-1}s \in p_i^{-1}P_i$. Then $p_ik\varphi(p_i^{-1}s) + S = k\varphi(s) + S = S$. Hence $k\varphi(p_i^{-1}s) + S \in t_{p_i}(M/S)$. So $k\varphi(p_i^{-1}P_i) \subseteq p_i^{-1}P_i$. Therefore $\psi(P_i) = p_ik\varphi(p_i^{-1}P_i) \subseteq P_i$ for all $i < \omega$.

Since $\mathscr{F}$ is a Zassenhaus family, $\psi = s\cdot \in S\cdot$ and $\varphi = \dfrac{s}{k} \in End_{\mathbb{Z}}(M^+)$. Note that $\varphi(1) = \dfrac{s}{k} \in M$. From the construction of M, there is a finite subset I of ω, there is a $u \in S$, and there are $b_i \in P_i - p_iS$ so that $\dfrac{s}{k} = \sum_{i\in I} \dfrac{b_i}{p_i} + u$.

Fix $j \in I$ and define $q = \displaystyle\prod_{i\in I-\{j\}} p_i$. Then $q\dfrac{s}{k} = \dfrac{qb_j}{p_j} + w$ for some $w \in S$. But the denominator p_j stops us short of the desired conclusion. So it can only be said

that $q\frac{s}{k}\cdot \in End_{\mathbb{Z}}(M^+)$. Then $\frac{b_j}{p_j}\cdot\frac{qs}{p_j}=\frac{qb_j^2}{p_j^2}+\frac{b_jw}{p_j}\in M$. All elements in M/S have square-free orders. But $p_j^2\frac{qb_j^2}{p_j^2}\in S$. So the order of $\frac{qb_j^2}{p_j^2}+S$ must be p_j. Thus $\frac{qb_j^2}{p_j}\in S$. Then $q(b_j+p_jS)^2=0\in S_j$. Recall that $\gcd(q,p_j)=1$. By our hypothesis, $b_j\in p_jS$ which contradicts the choice of b_j. Thus I is empty and so $\varphi=\frac{s}{k}\cdot\in S\cdot$ as desired. □

Corollary 6.13. *Let S be the ring of algebraic integers of either a quadratic number field or some Galois field extension field F over $\mathbb{Q}$ of finite degree. Then there is an $S\subseteq M\subseteq\mathbb{Q}S$ such that* $\mathrm{End}_{\mathbb{Z}}(M^+)=S$.

Proof: By Corollary 4.9 and Theorem 4.8, there is a Zassenhaus family $\mathscr{F}=\{P_i : i<\omega\}$ of right ideals of S. Since the $(i\to p_i)$ relation is injective, for each $i<\omega$, there is a unique number p_i such that p_iS is properly contained in P_i.

Fix $i<\omega$, and let $x\in S_i$ such that $x^2=0$. By Proposition 6.12, it suffices to show that $x=0$. Since $x\in S_i$, $x=q+p_iS$ for some $q\in P_i$. By hypothesis, $q^2\in p_iS$. Let $p_iS=Q_1Q_2\cdots P_i\cdots Q_k$ where $k\in\mathbb{N}$ and each Q_i is a prime ideal of S. Then $q^2\in Q_i$ for each $1\leq i\leq k$, and $q^2\in P_i$. Since these ideals are prime, $q\in Q_i$ for each $1\leq i\leq k$, and $q\in P_i$. Thus $q\in Q_1Q_2\cdots P_i\cdots Q_k=p_iS$. It follows that $x=0$. □

CHAPTER SEVEN

An Alternate Proof of Zassenhaus's Result

Zassenhaus's result from [24] is relevant to the topic of Zassenhaus rings, as one might expect. This chapter presents an alternate proof of this result that uses some ideas of Butler's from [9]. First, here are a few lemmas to help in the alternate proof.

Lemma 7.1. *Let R be a torsion free ring with identity. Let $\mathscr{F} = \{L_i : i < \mathbb{N}\}$ be a countable family of left ideals of R such that $L_i = Rb_i$ where $b_i \in R$ is not a zero divisor. Suppose that, for each $i < \mathbb{N}$, there is a prime number p_i, a nonzero natural number γ_i, and an integer δ_i such that $p_i^{\gamma_i}\delta_i R \subseteq L_i$, p_i and δ_i are relatively prime, and $(i \longmapsto p_i)$ is injective. Define $M = R + \sum_{i\in\mathbb{N}} p_i^{-\gamma_i} L_i \subseteq \mathbb{Q}R$. If $y \in M$ and $y\cdot \in \mathrm{End}_{\mathbb{Z}}(M)$, then $y \in R$.*

Proof: Note that $t_{p_i}(M/R) = (p_i^{-\gamma_i}L_i + R)/R$. Furthermore, $t_p(M/R) = 0$ for primes p not among the p_i. It follows that M/R is torsion. Let $y + R$ be an element of M/R. Then $y = \dfrac{v}{k}$ for some $v \in R$ and some product k of finitely many of the p_i. Choose k to be the order of $y + R$ in M/R. Since R is closed under addition, it suffices to prove the result for the case in which $k = p_i$ for some $i < \omega$.

Note that $(\dfrac{v}{p_i}p_i^{-\gamma_i}L_i + R)/R \subseteq t_{p_i}(M/R) = (p^{-\gamma_i}L_i + R)/R$. Then $p_i^{-(\gamma_i+1)}vL_i \subseteq p_i^{-\gamma_i}L_i + R$. Multiplying this last relation through by $p_i^{\gamma_i}\delta_i$, $p_i^{-1}\delta_i vL_i \subseteq \delta_i L_i + p_i^{\gamma_i}\delta_i R \subseteq L_i + L_i = L_i$. Then $v\delta_i L_i \subseteq p_i L_i$. Since p_i and δ_i are relatively prime, $vL_i \subseteq p_i L_i$. Since $L_i = Rb_i$, there is some $r \in R$ such that $vb_i = p_i r b_i$. Since b_i is not a zero divisor in R, $v = p_i r$. Therefore $y = r \in R$. $\square$

The proof of the following lemma uses some linear algebra. Basic definitions can be found in [13, Chapter VII]. Recall from [13, Page 356] the notion of an invariant subgroup of a free abelian group with respect to one of the group's endomorphisms.

Suppose that F is a free abelian group and $\varphi \in \mathrm{End}_{\mathbb{Z}}(F)$. Let $\rho \in \mathbb{Z}[x]$. Note that $\rho(\varphi) \in \mathrm{End}_{\mathbb{Z}}(F)$. For $a \in F$, define $a \cdot \rho = \rho \circ \varphi(a)$. In this manner, φ induces a $\mathbb{Z}[x]$ module structure on F. Using these definitions, let $e \in F$ and define $W = e\mathbb{Z}[\tau]$. By the obvious argument, it is easy to see that W is τ invariant.

Lemma 7.2. *Let F be a free abelian group of finite rank, let $0 \neq e \in F$, and let $\tau \in \mathrm{End}_{\mathbb{Z}}(F)$. Define $W = e\mathbb{Z}[\tau]$ as the τ invariant subgroup of F generated by e, and denote by W_* the purification of W in F. Then there is (a least) $k \in \mathbb{N}$ so that $kW_* \subseteq W$.*

Let $c \in \mathbb{Z}$ such that c is not an eigenvalue of τ, and let $\alpha \in \mathbb{N}$. If $\alpha e \in F(c-\tau)$ then $\det(c - \tau|_W)$ divides $k\alpha$.

Proof: Let $\chi_\tau(x) = \det(x - \tau)$ be the characteristic polynomial of τ. Then $\chi_\tau(x) \in \mathbb{Z}[x]$ and is monic [13, Page 366], i.e. $\chi_\tau(x)$ leading coefficient 1. Using [13, Theorem VII.4.1], one can say something about the structure of W. The minimal polynomial $m_\tau(x)$ of τ is in $\mathbb{Z}[x]$ and divides χ_τ. Thus m_τ is also monic. Let $f(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{Z}[x]$ be the minimal poynomial of $\tau|_W$. By the definition of m_τ, $m_\tau \circ \tau|_W = 0$. Then f divides m_τ. Hence f is monic and $a_m = 1$. Then $\mathbb{Z}[\tau|_W]$ is a ring extension of degree m over $\mathbb{Z}$. It follows that $\mathbb{Z}[\tau|_W] = \oplus_{i=1}^{m-1}\mathbb{Z}(\tau|_W)^i$. Since $e \in W$, $W = \oplus_{i=1}^{m-1} e\tau^i\mathbb{Z}$.

An easy consequence of [13, Theorem II.1.6] is that F/W_* is finitely generated. By [11, Corollary 28.3] since W_* is pure in F and F/W_* is finitely generated, W_* is a direct summand of F. Then $F = W_* \oplus C$ where C is just the complement of W_* in F. An elementary argument suffices to show that $\mathbb{Q}F = \mathbb{Q}W \oplus \mathbb{Q}C$.

Since c is not an eigenvalue of τ, there is no nonzero $a \in F$ so that $\tau(a) = ca$. That is, there is no nonzero $a \in F$ such that $(c - \tau)(a) = 0$. Hence $\ker(c - \tau) = 0$. Equivalently, 0 is not an eigenvalue of $c - \tau$. By [13, VII.5.4], the roots of the characteristic polynomial $\chi_{c-\tau}$ for $c - \tau$ are precisely the eigenvalues for $c - \tau$. Then $\chi_{c-\tau}(0) \neq 0$.

Since $c-\tau$ is a zero of $\chi_{c-\tau}$, $c-\tau$ is a root of a monic polynomial over $\mathbb{Z}$. Then there is a minimal polynomial $m_{c-\tau}(x) = \sum_{j=0}^{\ell} b_j x^j$ for $c-\tau$. Then $m_{c-\tau}(x)$ divides $\chi_{c-\tau}$. Hence 0 is not a root for $m_{c-\tau}(x)$ and so $m_{c-\tau}(0) = b_0 \neq 0$. The following calculations allow us to say something useful about $(c-\tau)^{-1}$.

$$b_0 = (c-\tau)\sum_{j=1}^{\ell} -b_j(c-\tau)^{j-1}$$

$$1 = (c-\tau)b_0^{-1}\sum_{j=1}^{\ell} -b_j(c-\tau)^{j-1}$$

$$(c-\tau)^{-1} = (m_{c-\tau}(0))^{-1}\sum_{j=1}^{\ell} -b_j(c-\tau)^{j-1}$$

In short, $(c-\tau)^{-1} \in (m_{c-\tau}(0))^{-1}\mathbb{Z}[c-\tau]$. Since c is just a constant integer, $\mathbb{Z}[c-\tau] \subseteq \mathbb{Z}[\tau]$. Then $(c-\tau)^{-1} \in (m_{c-\tau}(0))^{-1}\mathbb{Z}[\tau]$.

Suppose that $\alpha e \in F(c-\tau)$. Then $(\alpha e)(c-\tau)^{-1} \in m_{c-\tau}(0)^{-1}W_* \cap F = W_*$ since W_* is pure in F. It follows that $\alpha e \in W_*(c-\tau)$. Thus there is a $k \in \mathbb{N}$ so that $k\alpha e \in W(c-\tau) = \left(\oplus_{i=0}^{m-1} e\tau^i\mathbb{Z}\right)(c-\tau)$. Define the $m \times m$ matrix $C(f) = (u_{ij})_{1\leq i,j\leq m}$ where

$$u_{ij} = \begin{cases} 1 & \text{if } i = j+1,\ 1 \leq j \leq m-1 \\ -a_{i-1} & \text{if } j = m \\ 0 & \text{otherwise} \end{cases}$$

Graphically,

$$C(f) = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & \vdots & -a_1 \\ 0 & 1 & 0 & \vdots & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & -a_{m-1} \end{bmatrix}$$

The matrix $C(f)$ is called the companion matrix of the monic polynomial $f(x)$. Define

$B = cI_{m\times m} - C(f)$. Then

$$B = \begin{bmatrix} c & 0 & \cdots & 0 & a_0 \\ -1 & c & \cdots & \vdots & a_1 \\ 0 & -1 & c & \vdots & a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & -1 & c + a_{m-1} \end{bmatrix}$$

Suppose $k\alpha e = \left(\sum_{i=0}^{m-1} e\tau^i z_i\right)(c - \tau)$. Then

$$\begin{aligned} k\alpha e &= e\sum_{i=0}^{m-1}(cz_i\tau^i - z_i\tau^{i+1}) \\ &= e\left(\sum_{i=0}^{m-1} cz_i\tau^i - \sum_{i=1}^{m} z_{i-1}\tau^i\right) \\ &= e\left(cz_0 - z_{m-1}\tau^m + \sum_{i=1}^{m-1}(cz_i - z_{i-1})\tau^i\right) \end{aligned}$$

Equating coefficients of powers of τ yields $cz_0 = k\alpha$, $z_{m-1} = 0$, and $cz_i - z_{i-1} = 0$ for $1 \le i \le m-1$. Let

$$\overrightarrow{z} = \begin{bmatrix} z_0 \\ \vdots \\ z_{m-1} \end{bmatrix} \in \mathbb{Z}^m.$$

Elementary computations show that

$$B\overrightarrow{z} = \begin{bmatrix} cz_0 + a_0 z_{m-1} \\ -z_0 + cz_1 + a_1 z_{m-1} \\ -z_1 + cz_2 + a_2 z_{m-1} \\ \vdots \\ -z_{m-3} + cz_{m-2} + a_{m-2} z_{m-1} \\ -z_{m-2} + z_{m-1}(c + a_{m-1}) \end{bmatrix} = \begin{bmatrix} k\alpha \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{7.1}$$

and $\chi_{C(f)}(x) = \det(xI_m - C(f)) = f(x)$. Then $\chi_{C(f)}(c) = \det(B) = f(c)$. Recall from elementary linear algebra (see for example [13, Pages 352 and 353]) that B has a classical adjoint (or adjugate) $\mathrm{adj}(B)$ which is a matrix with the property that $\mathrm{adj}(B)B =$

$\det(B)I$. Multiplying (1) from the left by $adj(B)$, then $\det(B)z_{m-1} = c_{1m}k\alpha$ where c_{1m} is the $(1, m)$-cofactor of the matrix B, just the (1, m) entry of adj(B). By [13, Page 352], c_{1m} is $(-1)^{m+1}$ times the determinant of the matrix obtained by deleting the first row and m-th column from B. But this matrix is upper triangular with only -1 on the main diagonal. Thus the determinant for this matrix is a product of the -1 entries. So $c_{1m} = (-1)^{m+1}(-1)^m = (-1)^{2m+1} = -1$. Then $\det(B)z_{m-1} = -k\alpha$. Therefore $f(c) = \det(B)$ divides $k\alpha$. $\square$

With the aid of the above lemmas, an alternate proof to Zassenhaus's result can be given.

Theorem 7.3. *(Zassenhaus Theorem [24]) Let R be a ring with identity such that R^+ is free abelian of finite rank. Then there is a left R module M such that $R \subseteq M \subseteq \mathbb{Q}R$ and $\mathrm{End}_{\mathbb{Z}}(M) = R$. That is, every additive endomorphism of M is merely multiplication on the left by some element of R. Moreover $t_p(M/R)$ is bounded for all primes p.*

Proof: Define $\Sigma = \{\sigma \in \mathrm{End}_{\mathbb{Z}}(R) : 0 \neq \sigma \text{ and } \sigma(1) = 0\}$. Since R^+ is free and of finite rank, Σ is countable and can be enumerated as $\{\sigma_i : i < \omega\}$. Note that Σ is the collection of additive endomorphisms of R each of which cannot possibly be multiplication by some element of R. For each $i < \omega$, since at least $\sigma(1)$ is not zero, there is some $\tau_i \in R$ and some nonzero $e_i \in R$, such that $\sigma_i(-\tau_i) = e_i$.

Let $i < \omega$. Using the notation from Lemma 7.2, suppose that $c_i \in \mathbb{Z}$ such that c_i is not an eigenvalue of τ_i. Then there is no $\mu \in R$ so that $\tau_i \cdot \mu = c_i\mu$. In other words, there is no $\mu \in R$ so that $0 = (c_i - \tau_i) \cdot \mu$. Then $c_i - \tau_i$ has a trivial kernel and must be invertible. The image of $c_i - \tau_i$ may be a proper subgroup of R^+. However, the inverse of $c_i - \tau_i$ has a unique extension to $\mathbb{Q}R$. Thus this extension can be identified with the inverse, a member of End$(\mathbb{Q}R^+)$. By Lemma 7.2, there is some k_i such that if $\alpha e_i \in R(c_i - \tau_i)$, then $\det(c_i - \tau_i|_W) = f_i(c_i)$ divides αk_i.

There are infinitely many primes q such that $f_i(x) \bmod q$ has a root in $\mathbb{Z}/q\mathbb{Z}$. This is a well known result in number theory, an elementary proof of which is contained in [9, proposition on page 298]. Hence, for each $i \in \mathbb{N}$, one can pick such a prime p_i where p_i is not in $\{p_j : 0 \leq j \leq i-1\}$ and p_i does not divide k_i.

Fix $i \in \mathbb{N}$ and set $q = p_i$. Note that if an integer $c^{(t)}$ has the form $c^{(t)} = c + tq$ for some $t \in \mathbb{Z}$ then, $\bmod q$, $c^{(t)}$ is a root of $f_i(x)$. Thus the set $\{c \in \mathbb{Z} : f_i(c) \equiv 0 \bmod q\}$ is infinite. Since R has finite rank, τ_i has only finitely many eigenvalues. Therefore c_i can be chosen such that c_i is not an eigenvalue of τ_i and $f_i(c_i) \equiv 0 \bmod q$. Then $f_i(c_i) = \det(c_i - \tau_i|_W) = q^{\gamma_i}\delta_i$ for some nonzero $\gamma_i \in \mathbb{N}$ and some integer δ_i that q does not divide.

Since $c_i - \tau_i \in R$, the associated linear transformation is just a diagonal matrix. It is easy to see that the classical adjoint of this linear transformation must also be a diagonal matrix. It follows that there is some $\rho \in R$ such that $\rho(c_i - \tau_i) = q^{\gamma_i}\delta_i$. Thus $q^{\gamma_i}\delta_i R \subseteq R(c_i - \tau_i)$. Note that q divides $f_i(c_i) = \det(c_i - \tau|_W)$ but q does not divide $\delta_i k_i$. Recall that if $\delta_i e_i = \delta_i \sigma(-\tau_i) \in R(c_i - \tau_i)$, then $\det(c_i - \tau_i|_W) = f_i(c_i)$ divides $\delta_i k_i$. Therefore $\delta_i \sigma_i(c_i - \tau_i) = \delta_i \sigma_i(-\tau_i) \notin R(c_i - \tau_i)$.

Set $L_i = R(c_i - \tau_i)$, and switch back to p_i in place of q. Define $M = R + \sum_{i<\omega} p_i^{-\gamma_i} L_i \subseteq \mathbb{Q}R$. Let $\varphi \in \mathrm{End}_{\mathbb{Z}}(M)$. Since R^+ is finitely generated and M/R is torsion, there is some $m \in \mathbb{N}$ such that $m\varphi(R) \subseteq R$. In particular, $m\varphi(1) \in R$. Let $\sigma = m\varphi - (m\varphi(1))\cdot \in \mathrm{End}_{\mathbb{Z}}(R)$. Note that $\sigma(1) = 0$.

Assume that $0 \neq \sigma$. Then $\sigma \in \Sigma$ and $\sigma = \sigma_i$ for some $i < \omega$. Thus $\delta_i \sigma_i(c_i - \tau_i) \notin L_i$. Note that σ_i induces an endomorphism of M/R. It follows that $\sigma_i(p_i^{-\gamma_i} L_i) \subseteq p_i^{-\gamma_i} L_i + R$. Hence $\delta_i \sigma_i(L_i) \subseteq \delta_i L_i + p_i^{\gamma_i}\delta_i R \subseteq L_i + L_i = L_i$. This contradicts $\delta_i \sigma_i(c_i - \tau_i) \notin L_i$. Thus $\sigma_i = 0$ and so $\varphi = \varphi(1)\cdot \in End_{\mathbb{Z}}(M)$. Recall that $\varphi(1) \in M$. By Lemma 7.1, $\varphi(1) \in R$. $\square$

CHAPTER EIGHT

Integer Matrix Rings are Zassenhaus Rings

This chapter shows that the ring $\mathrm{Mat}_{n\times n}(\mathbb{Z})$ of $n \times n$ integer matrices, where $n \geq 2$, is a Zassenhaus ring.

Definition 8.1. [23, Example 2.3.3] For a prime number p, let $\mathbb{Z}(p^\infty) = \mathbb{Z}[1/p]/\mathbb{Z}$ be the divisible p-group.

Definition 8.2. [2, Chapter 3] A finite rank torsion free group G is *completely decomposable* if and only if $G = \oplus_{i=1}^{n} A_i$ where $n \in \mathbb{N}$ and each A_i is rank 1.

Definition 8.3. [2, Chapter 3] A finite rank torsion free group G is *Butler group* if and only if G is a pure subgroup of some completely decomposable group.

Definition 8.4. [11, Section 7] Let p be a prime number. The *p-adic* topology for a group A is the topology generated by defining the collection of neighborhoods of zero as $\{p^k A : k \in \mathbb{N}\}$.

Proposition 8.5. *Let $R = \mathrm{Mat}_{n\times n}(\mathbb{Z})$ be the ring of $n \times n$ integer matrices where $n \geq 2$. For $1 \leq i \leq n$, let p_i be distinct prime numbers. There is an R-module M such that $M/R \approx \oplus_{i=1}^{n+1}\mathbb{Z}(p_i^\infty)$ and M is a Zassenhaus module for R. Moreover, M is a torsion free finite rank Butler group.*

Proof: Let $\mathscr{F} = \{J_i : 1 \leq i \leq n+1\}$ be the Zassenhaus family from Proposition 3.2. Define $M = \sum_{i=1}^{n+1} J_i\mathbb{Z}[1/p_i]$. By construction, M is a sum of finitely many rank 1 subgroups so that M is a Butler group. To see that $M/R \approx \oplus_{i=1}^{n+1}\mathbb{Z}(p_i^\infty)$, note that $M = \oplus_{i=1}^{n+1} J_i\mathbb{Z}[1/p_i]$. Define $\sigma : M/R \to \oplus_{i=1}^{n+1}\mathbb{Z}(p_i^\infty)$ as follows. If $\alpha + R \in M/R$ then $\alpha = \sum_{i=1}^{n+1} J_i a_i$ for some $a_i \in \mathbb{Z}[1/p_i]$. Set $\sigma(\alpha + R) = \sum_{i=1}^{n+1}(a_i + \mathbb{Z})$. If $\alpha + R, \beta + R \in M/R$ are equal where $\beta = \sum_{i=1}^{n+1} J_i b_i$, then $a_i - b_i \in \mathbb{Z}$. In this case, $\sigma(\beta + R) = \sigma(\alpha + R)$. Thus σ is well defined. If $\alpha \in \ker\sigma$, then the a_i are each in

$\mathbb{Z}$. It follows that σ is monic; it is clearly epic. So σ is an isomorphism showing that $M/R \approx \oplus_{i=1}^{n+1}\mathbb{Z}(p_i^\infty)$.

Let $a + R \in M/R$ and $p_i^n a \in R$ for some i and some nonzero $n \in \mathbb{N}$. Then $a = r/p_i^n$ for some $r \in R$. In this case, the entries of the matrix a are in $\mathbb{Z}[1/p_i]$. Since the denominators of these entries must each be divisible by a power of p_i, a must be an element of $J_i\mathbb{Z}[1/p_i]$. Thus $t_{p_i}(M/R) = (J_i\mathbb{Z}[1/p_i] + R)/R$.

Let $\varphi \in \mathrm{End}(M)$. Note that R^+ is finitely generated and M/R is torsion. Then there is some $m \in \mathbb{N}$ such that $\psi = m\varphi \in \mathrm{End}(M)$ with $\psi(R) \subseteq R$. Let $x \in J_i$ for some $1 \leq i \leq n+1$. Then $p_i^n\psi(p_i^{-n}x) \in R$. Since x may have summands divisible by p_i^n, $\psi(p_i^{-n}x) \in p_i^{-n}R + R$. Since ψ is an endomorphism on M, $\psi(p_i^{-n}x) \in M \cap (p_i^{-n}R + R) = p_i^{-n}J_i + R$. Therefore $\psi(x) \in J_i + p_i^n R$ for all $n \in \mathbb{N}$. Then $\psi(J_i) \subseteq \cap_{k\in\mathbb{N}}(J_i + p_i^n R)$ for all $1 \leq i \leq n+1$. To show that $\psi(J_i) \subseteq J_i$ for all $1 \leq i \leq n+1$ some elementary topology is applied.

Suppose that the matrix $a \in \cap_{k\in\mathbb{N}} p_i^k R$. Then each of the entries of a has p_i-height ∞. But the entries of a are integers and so must have finite p_i height. Thus $\{0\} = \cap_{k\in\mathbb{N}} p_i^k R$. Therefore a convergent sequence in the p_i-adic topology of R converges to a unique limit.

Let $a \in R$ be a limit point of J_i. Then there is a sequence $(a_k)_{k\in\mathbb{N}}$ converging to a such that each $a_i \in J_i$. For each $k \in \mathbb{N}$, $a - a_k \in p_i^k R$. Let C be the complement of J_i in R. Then $a = b + c$ for some $b \in J_i$ and some $c \in C$. Fix $0 < k \in \mathbb{N}$ for the moment. Then $b + c = a_k + p_i^k r$ for some $r \in R$. Then $c = a_k - b + p_i^k$. There are $b' \in J_i$ and $c' \in C$ so that $r = b' + c'$. Hence $c = a_k - b + p_i^k(b' + c')$. Since $c \in C$, $c = p_i^k c'$. Thus c has infinite p_i height. Then $c = 0$ and $a = b$. This shows that $a \in J_i$. Therefore J_i is closed in the p_i-adic topology.

Suppose that $a \in \cap_{k\in\mathbb{N}}(J_i + p_i^k R)$. Note that J_i is not disjoint from $p_i^k R$ for each $k \in \mathbb{N}$. Then a is a limit point of J_i. Since J_i is closed, $a \in J_i$. Thus $J_i = \cap_{k\in\mathbb{N}}(J_i + p_i^k R)$ for all $1 \leq i \leq n+1$. Finally $\psi(J_i) \subseteq J_i$ for all $1 \leq i \leq n+1$.

Since $\mathscr{F}$ is a Zassenhaus family, $\psi = r\cdot$ for some $r \in R$. Thus $\varphi = \frac{r}{m}\cdot \in \mathrm{End}(M)$. Without loss, assume that $\frac{r}{m}$ is reduced. That is, $r \notin pR$ for any prime p dividing m.

To ultimately derive a contradiction, assume that $m = p_j$ for some $1 \leq j \leq n+1$. From the definition of M, $r \in J_j$. If $1 \leq j \leq n$, pick $1 \leq j \neq k \leq n$. Label the entries of r as $r = (r_{ij})_i$ disregarding the $r_{i\ell}$ where $\ell \neq j$ since these entries are zero. Then $r\varepsilon_{jk} = \sum_{\alpha=1}^{n} r_{\alpha j}\varepsilon_{\alpha k} \in J_k$. There is some β such that $r_{\beta j} \notin p_j R$ as otherwise $\frac{r}{m}$ would not be reduced. It follows that $\varphi(\varepsilon_{jk}) = \frac{r\varepsilon_{jk}}{p_j} \notin M$. Note that the numerator is in J_k but the denominator is different from p_k. Thus $\varphi(\varepsilon_{jk}) \notin M$ which is a contradiction.

If $j = n+1$ then $r = \sum_{\alpha=1}^{n} r_\alpha(\sum_{\beta=1}^{n} \varepsilon_{\alpha\beta})$ where $r_\alpha \in R$. Since $\frac{r}{m}$ is reduced there is some $1 \leq i \leq n$ such that $r_i \in R - p_{n+1}R$. Then $r\varepsilon_{ik} \in J_k$ and $r\varepsilon_{ik} = \sum_{\alpha=1}^{n} r_\alpha\varepsilon_{\alpha k} \in J_k - p_{n+1}R$. Similar to the previous case, $\varphi(\varepsilon_{ik}) = \frac{r\varepsilon_{ik}}{p_{n+1}} \notin M$, a contradiction.

Having exhausted the cases for which $m = p_j$ for some $1 \leq j \leq n+1$, it follows that $m = 1$ and φ is multiplication on the left by $r \in R$. Therefore M provide the module necessary to declare R a Zassenhaus ring. $\square$

CHAPTER NINE

Some PIDs are not Zassenhaus Rings

For the next theorem, a slight variation of [5, Corollary 10.18] is needed.

Lemma 9.1. *If R is a Noetherian integral domain and $\{b_nR : n \in N\}$ is an infinite strictly descending chain of principal ideals of R, then $\cap_n b_nR = \{0\}$.*

Proof: If $b_n = 0$ for all n then there is nothing to show. Suppose that the b_n are nonzero. Since $b_{n+1}R \subseteq b_nR$, it follows that $b_{n+1} = b_n s_n$. Let $0 \neq x \in \cap_k b_k R$. Since $0 \neq x \in b_nR$, there is a $0 \neq y_n \in R$ such that $x = b_n y_n$. Then $b_n y_n = b_{n+1} y_{n+1} = b_n s_n y_{n+1}$. Since the chain is strictly descending, $0 \neq b_n$. Then $b_n(y_n - s_n y_{n+1}) = 0$ implies that $y_n = s_n y_{n+1}$. It follows that $y_n \in y_{n+1}R$ and so $y_nR \subseteq y_{n+1}R$. Since R is Noetherian, there is a k such that $y_kR = y_{k+t}R$ for all $t \in \mathbb{N}$. Then $y_k = y_{k+1}s_n$ and $y_{k+1} = y_k r_k$ for some $r_k \in R$. Hence $y_k(1 - s_k r_k) = 0$ and so s_k, r_k are units in R. Since $b_{k+1} = b_k s_k$ and s_k is a unit, then $b_kR = b_{k+1}R$ contradicting the hypothesis that $\{b_nR : n \in N\}$ is a strictly descending chain. Therefore, $x = 0$. $\square$

Lemma 9.2. *Suppose R is a PID such that R^+ is torsion free, the set Π of prime ideals of R is finite, and R has a nontrivial ring automorphism. The set $\mathbb{P} = \{p \text{ prime} : pR \neq R\}$ is finite but nonempty.*

Proof: Identify each $\sigma \in Aut(R)$ with its unique extension $\sigma \in End_{\mathbb{Q}}(\mathbb{Q}R)$. Let $p \in \mathbb{Z}$ be a prime number such that $pR \neq R$. Then p is not a unit. Then the ideal (p) generated by p is contained in some maximal ideal P. Maximal ideals are prime so that $P \in \Pi$.

If q is a prime number distinct from p, then $q \notin P$. To see this, assume that $q \in P$. Since q and p are prime numbers, they are relatively prime. So there are

integers α and β such that $1 = \alpha p + \beta q$. Since P is a ring, $1 = \alpha p + \beta q \in P$. But then $P = R$. Therefore, there is at most one prime number contained in each $P \in \Pi$. It follows that there are only finitely many prime numbers p such that $pR \neq R$.

Define $\mathbb{P} = \{p \text{ prime } : pR \neq R\}$. By the preceding arguments, the cardinality of $\mathbb{P}$ is less than or equal to the cardinality of Π. Therefore $\mathbb{P}$ is finite. Let $\mathbb{P} = \{p_i : 1 \leq i \leq \ell\}$.

Let $p \in \mathbb{P}$. Then $pR \neq R$ implies that $p^n R \neq p^{n-1} R$ for $n \in \mathbb{N}$. So $\{p^n R : n \in \mathbb{N}\}$ is a strictly descending sequence of principle ideals. From the preceding lemma, $\cap_n p^n R = 0$.

Note that for every prime number $q \notin \mathbb{P}$, the ideal $qR = R$. Then $q^n R = R$ by a trivial inductive argument. If $0 \neq r \in R$, it has been shown that the p height of r is at most finite for $p \in \mathbb{P}$ and the q height of r is infinite for prime numbers $q \notin \mathbb{P}$. Therefore, the type of an element r in R is $(\alpha_p)_{p \text{ prime}}$ where $\alpha_p \in \mathbb{N}$ for the finite number of primes $p \in \mathbb{P}$ and $\alpha_p = \infty$ for $p \notin \mathbb{P}$. Therefore R^+ is homogenous of type $\tau_{\mathbb{P}}$ where

$$\tau_{\mathbb{P}}(p) = \begin{cases} 0 & \text{if } p \in \mathbb{P} \\ \infty & \text{otherwise} \end{cases}$$

If $\mathbb{P} = \emptyset$ then $pR = R$ for all primes p. Thus R^+ is divisible and $R^+ = \oplus_\kappa \mathbb{Q}$, a vector space over $\mathbb{Q}$. Then $\mathbb{Q}R = R$. In this case, $End(R)$ is the ring of linear transformations of a vector space over $\mathbb{Q}$. Hence if the rank of R is κ, $End(R)$ is the ring of $\kappa \times \kappa$ matrices with entries in $\mathbb{Q}$.

Suppose that R has a Zassenhaus module M. Since $\mathbb{Q}R = R$, then $M = R$. Suppose further that $R = End(M)$. Then $R = End(R)$ is the ring of endomorphisms of a $\mathbb{Q}$ vector space and thus not commutative for $\kappa > 1$. This shows that $\kappa = 1$ and $R = \mathbb{Q}$. But $\mathbb{Q}$ has no nontrivial automorphisms which contradicts one of our hypotheses about R. Therefore $\mathbb{P} \neq \emptyset$. $\square$

Lemma 9.3. *Suppose R is a PID such that R^+ is torsion free, the set Π of prime ideals of R is finite, and R has a nontrivial ring automorphism. If R has a Zassenhaus module M then there is a family of submodules $\{M_{p,n} : p \in \mathbb{P}, n \in \mathbb{N}\}$ such that*

$$M = \sum_{p\in\mathbb{P}} \bigcup_{n\in\mathbb{N}} M_{p,n}$$

and for $p \in \mathbb{P}$ and $n \in \mathbb{N}$, each submodule $M_{p,n}$ has the following properties

(1) $R \subseteq M_{p,n}$;

(2) $M_{p,n} \subseteq M_{p,n+1}$;

(3) $p^n M_{p,n} \subseteq R$;

(4) $pM_{p,n+1} \subseteq M_n$; and

(5) $M_{p,n+t} \cap p^{-n}R \subseteq M_{p,n}$ for all $t \in \mathbb{N}$.

Proof: Define $\mathbb{P} = \{p \text{ prime } : pR \neq R\}$. By Lemma 9.2, $\mathbb{P}$ is finite but nonempty. Let $p \in \mathbb{P}$. Note that since R is a PID, R is a Dedekind domain. Since $pR \neq R$, pR is a proper ideal of the Dedekind domain R and has a unique factorization into powers of the prime ideals of R. For $p \in \mathbb{P}$, it follows that the principle ideal $pR = \prod_{i=1}^{k} P_i^{a_{p,i}}$ for some $a_{p,i} \in \mathbb{N}$.

To see that M/R is a $\mathbb{P}$ group, let $m + R \in M/R$. Then $m = (a/b)r$ for some $a/b \in \mathbb{Q}$ and for some $r \in R$. For any prime $q \notin \mathbb{P}$, r is q divisible. Thus one can assume that b is a product of powers of primes from $\mathbb{P}$. Since $\mathbb{P}$ is finite, $\zeta = \prod_{p\in\mathbb{P}} p$ is an integer. Then $\zeta(a/b)r \in R$ so that $\zeta \cdot (m + R) = R$ in M/R.

Define $M_{p,n}$ as the submodule of M such that $M_{p,n}/R = (M/R)[p^n]$. That is, $M_{p,n}$ is the set of all $m \in M$ such that $p^n m \in R$. Set $M_{p,0} = R$. It follows that the structure of M can be given in terms of the newly defined submodules:

$$M = \sum_{p\in\mathbb{P}} \bigcup_{n\in\mathbb{N}} M_{p,n}.$$

As for the properties of each $M_{p,n}$:

(1) follows directly from the definition of $M_{p,n}$.

(2) Since $p^n M_{p,n} \subseteq R$, then $p^{n+1} M_{p,n} \subseteq R$. By definition $M_{p,n} \subseteq M_{p,n+1}$.

(3) follows directly from the definition of $M_{p,n}$.

(4) Note that $p^{n+1} M_{p,n+1} = p^n (p M_{p,n+1}) \subseteq R$. By definition $p M_{p,n+1} \subseteq M_{p,n}$.

(5) Let $t \in \mathbb{N}$ and $m \in M_{p,n+t} \cap p^{-n} R$. Since $m \in M_{p,n+t}$, $m \in M$. Since $m \in p^{-n} R$, $m + R \in (M/R)[p^n]$. Then $m + R \in M_{p,n}/R$. So $m + R = m' + R$ for some $m' \in M_{p,n}$. Then $m - m' \in R \subseteq M_{p,n}$. Thus $m \in M_{p,n}$. $\square$

Lemma 9.4. *Recalling the notation and hypotheses of Lemma 9.3: For $p \in \mathbb{P}$ define $X_{p,n} = p^n M_{p,n}$. Then each $X_{p,n} = \prod_{i=1}^{k} P_i^{e_{p,n}^{(i)}}$ for some prime ideals P_i of R and some integer exponents $e_{p,n}^{(i)}$. Furthermore*

(1′) $p^n R \subseteq X_{p,n}$.

(2′) $p X_{p,n} \subseteq X_{p,n+1}$.

(3′) $X_{p,n+1} \subseteq X_{p,n}$.

(4′) $X_{p,n+t} \cap p^t R \subseteq p^t X_{p,n}$ *for* $t \in \mathbb{N}$.

(5′) $p^t X_{p,n} \subseteq X_{p,n+t}$ *for* $t, n \in \mathbb{N}$.

(6′) $X_{p,n+t} \cap p^t R = p^t X_{p,n}$ *for* $t, n \in \mathbb{N}$.

Proof: Set $X_{p,0} = R$. From the definition of $M_{p,n}$, one can conclude that $X_{p,n}$ is an ideal of R. Since R is a Dedekind domain, each $X_{p,n}$ has a unique factorization into powers of the prime ideals of R. Let this factorization be given by $X_{p,n} = \prod_{i=1}^{k} P_i^{e_{p,n}^{(i)}}$. Define $e_{p,0}^{(i)} = 0$.

(1′) By (1), it follows that $R \subseteq M_{p,n}$. Then $p^n R \subseteq p^n M_{p,n+1} = X_{p,n}$.

(2′) By (2), $p X_{p,n} = p^{n+1} M_{p,n} \subseteq p^{n+1} M_{p,n+1} = X_{p,n+1}$.

(3′) $X_{p,n+1} = p^{n+1}M_{p,n+1} = p^n(pM_{p,n+1}) \subseteq p^nM_{p,n} = X_{p,n}$ by (4).

(4′) $X_{p,n+t} \cap p^tR = p^{n+t}(M_{p,n+t} \cap p^{-n}R) \subseteq p^{n+t}M_{p,n} \subseteq X_{p,n}$ by (5).

(5′) For $t = 1$, the statement is just (2′). Suppose the claim holds for a $t \in \mathbb{N}$. Then $p^{t+1}X_{p,n} = p(p^tX_{p,n}) \subseteq pX_{p,n+t}$ by the induction hypothesis. By (2'), $pX_{p,n+t} \subseteq X_{p,n+t+1}$.

(6′) If $t, n \in \mathbb{N}$, then $X_{p,n+t} \cap p^tR = p^tX_{p,n}$. To see this, note that (4′) and the last claim imply that $X_{p,n+t} \cap p^tR \subseteq p^tX_{p,n} \subseteq X_{p,n+t} \cap p^tR$ for all $t, n \in \mathbb{N}$. □

Lemma 9.5. *Recall from Lemma 9.3:* $pR = \prod_{i=1}^{k} P_i^{a_{p,i}}$. *For the exponents* $e_{p,n}^{(i)}$ *defined in Lemma 9.4 the following properties hold:*

(i) $e_{p,n}^{(i)} \geq 0$.

(ii) $na_{p,i} \geq e_{p,n}^{(i)}$.

(iii) $e_{p,n}^{(i)} + a_{p,i} \geq e_{p,n+1}^{(i)}$.

(iv) $e_{p,n+1}^{(i)} \geq e_{p,n}^{(i)}$.

(v) If $p = p_j$ *then* $\max\{e_{p,n+t}^{(j)}, ta_{p,j}\} = e_{p,n}^{(j)} + ta_{p,j}$ *for* $t \in \mathbb{N}$.

(vi) If $p = p_i$ *then either* $e_{p,n+t}^{(i)} = e_{p,n}^{(i)} + ta_{p,i}$ *or* $e_{p,n}^{(i)} = 0$ *for* $t \in \mathbb{N}$.

Proof: (i) follows directly from the definition.

(ii) Let P_i be the unique prime ideal of R that lies over $p = p_i$. By (1′), $P_i^{na_{p,i}} = (pR)^n = p^nR \subseteq X_{p,n} = \prod_{j=1}^{k_p} P_j^{e_{j,n}}$. Then $P_i^{na_{p,i}} \subseteq P_i^{e_{p,n}^{(i)}}$. So $na_{p,i} \geq e_{p,n}^{(i)}$.

(iii) By (2′), $\prod_{i=1}^{k_p} P_i^{e_{p,n}^{(i)}+a_{p,i}} = \prod_{i=1}^{k_p} P_i^{a_{p,i}}P_i^{e_{p,n}^{(i)}} = pRX_{p,n} \subseteq pX_{p,n} \subseteq X_{p,n+1} = \prod_{i=1}^{k_p} P_i^{e_{p,n+1}^{(i)}}$. Then $P_i^{e_{p,n}^{(i)}+a_{p,i}} \subseteq P_i^{e_{p,n+1}^{(i)}}$. Hence $e_{p,n}^{(i)} + a_{p,i} \geq e_{p,n+1}^{(i)}$.

(iv) By (3′), $\prod_{i=1}^{k_p} P_i^{e_{p,n+1}^{(i)}} = X_{p,n+1} \subseteq X_{p,n} = \prod_{i=1}^{k_p} P_i^{e_{p,n}^{(i)}}$. Then $P_i^{e_{p,n+1}^{(i)}} \subseteq P_i^{e_{p,n}^{(i)}}$. Hence $e_{p,n+1}^{(i)} \geq e_{p,n}^{(i)}$.

(v) Let $t, n \in \mathbb{N}$. By (4′), $X_{p,n+t} \cap p^t R \subseteq p^t X_{p,n}$. Let $b_i = \max\{e^{(i)}_{p,n+t}, ta_{p,i}\}$. From the factorization into prime ideals of $X_{p,n+t}$ and $p^t R$, $P_i^{b_i} \subseteq X_{n+t} \cap p^t R$. From (4′) and the factorization of $p^t X_{p,n}$, it follows that $b_i \geq e^{(i)}_{p,n} + ta_{p,i}$. By (iii), $e^{(i)}_{p,n} + a_{p,i} \geq e^{(i)}_{p,n+1}$. By a trivial inductive argument, $e^{(i)}_{p,n} + ta_{p,i} \geq e^{(i)}_{p,n+t}$ for $t \in \mathbb{N}$. Clearly, $e^{(i)}_{p,n} + ta_{p,i} \geq ta_{p,i}$. Then $e^{(i)}_{p,n} + ta_{p,i} \geq b_i$. Therefore $b_i = e^{(i)}_{p,n} + ta_{p,i}$.

(vi) Note that from (v) it follows that $e^{(i)}_{p,n} + ta_{p,i}$ is either $e^{(i)}_{p,n+t}$ or $ta_{p,i}$. If $ta_{p,i} = e^{(i)}_{p,n} + ta_{p,i}$, then $e^{(i)}_{p,n} = 0$. $\square$

Lemma 9.6. *Suppose R is a PID such that R^+ is torsion free, the set Π of prime ideals of R is finite, and R has a nontrivial ring automorphism σ. If R is a Zassenhaus ring, then there are distinct prime ideals P and Q of R such that $\sigma(P) = Q$.*

Proof: Recall definitions and notations from Lemmas 9.2, 9.3, 9.4, and 9.5. Assume that $id \neq \sigma \in Aut(R)$ such that $\sigma(P) = P$ for each $P \in \Pi$. Since σ is an automorphism, $\sigma(pR) = p\sigma(R) = pR$.

From the above lemmas, if $p \in \mathbb{P}$ then the principle ideal $pR = \prod_{i=1}^{k} P_i^{a_{p,i}}$ for some $a_{p,i} \in \mathbb{N}$. Also

$$M = \sum_{p \in \mathbb{P}} \bigcup_{n \in \mathbb{N}} M_{p,n}$$

and $X_{p,n} = p^n M_{p,n} = \prod_{i=1}^{k} P_i^{e^{(i)}_{p,n}}$ for $p \in \mathbb{P}$ and $n \in \mathbb{N}$.

Then $\sigma(X_{p,n}) = \prod_{i=1}^{k} \sigma(P_i)^{e^{(i)}_{p,n}} = \prod_{i=1}^{k} P_i^{e^{(i)}_{p,n}} = X_{p,n}$. Note that $\sigma|_R : R \to R$ has a unique extension to $\sigma : \mathbb{Q}R \to \mathbb{Q}R$. So $\sigma(X_{p,n}) = \sigma(p^n M_{p,n}) = p^n \sigma(M_{p,n})$ is a well-defined statement. It follows that $p^n \sigma(M_{p,n}) = p^n M_{p,n} \subseteq R$. By definition, $\sigma(M_{p,n}) \subseteq M_{p,n}$. Therefore

$$\sigma(M) = \sum_{p \in \mathbb{P}} \bigcup_{n \in \mathbb{N}} \sigma(M_{p,n}) \subseteq \sum_{p \in \mathbb{P}} \bigcup_{n \in \mathbb{N}} M_{p,n} = M.$$

So $\sigma : M \to M$ and $\sigma \in End(M)$. Suppose that there is an $r \in R$ so that $\sigma(x) = r \cdot x$ for each $x \in R$. Then $\sigma(1) = r$. Since σ is a ring automorphism, $\sigma(1) = 1$.

Therefore $r = 1$ and $\sigma = id_R$. This contradicts the hypothesis that $id_R \neq \sigma$. Therefore σ cannot be multiplication by an element of R. Finally by our choice of M, R cannot be a Zassenhaus ring. $\square$

Theorem 9.7. *Suppose R is a PID such that R^+ is torsion free, the set Π of prime ideals of R is finite, and R has a nontrivial ring automorphism. Then R is not a Zassenhaus ring.*

Proof: Assume to the contrary that R has a Zassenhaus module M. Recall definitions and notations from Lemmas 9.2, 9.3, 9.4, and 9.5. By Lemma 9.6, for every nonidentity automorphism of R there are indexes $1 \leq i \neq e \leq k$ such that $\sigma(P_i) = P_e$.

Let $p \in \mathbb{P}$. Define $\mathcal{O}_p = \{i : 1 \leq i \leq k, e_{p,n}^{(i)} = 0 \text{ for all } n \in \mathbb{N}\}$ and $\Lambda_p = \{1, 2, \ldots, k\} - \mathcal{O}_p$. There are two cases, either Λ_p is empty or it is not.

Suppose that Λ_p is empty. In this case, for all $n \in \mathbb{N}$, the ring $R = X_{p,n} = p^n M_{p,n}$ so that $p^{-n}R = M_{p,n}$. Then $\sigma(M_{p,n}) = \sigma(p^{-n}R) = p^{-n}\sigma(R) = p^{-n}R = M_{p,n}$.

Suppose that Λ_p is not empty. Let $i \in \Lambda_p$. There is a least n_i such that $e_{p,n_i-1}^{(i)} = 0$ and $e_{p,n_i}^{(i)} \neq 0$. If $i \in \Lambda$ and $t \in \mathbb{N}$, then $e_{p,n_i+t}^{(i)} = e_{p,n_i}^{(i)} + ta_{p,i}$.

Let $i, j \in \Lambda_p$ such that $i \leq j$ and $n \in \mathbb{N}$. Then for some $t, r \in \mathbb{N}$, $n = n_i + t = n_j + r$. Note that $r = n_i - n_j + t$. If $i = j$ then $e_{p,n_i}^{(i)} - e_{p,n_j}^{(j)} = e_{p,n_i}^{(i)} - e_{p,n_i}^{(i)} = 0$. Otherwise

$$\begin{aligned} e_{p,n}^{(i)} - e_{p,n}^{(j)} &= e_{p,n_i+t}^{(i)} - e_{p,n_j+r}^{(j)} \\ &= e_{p,n_i}^{(i)} + ta_{p,i} - (e_{p,n_j}^{(j)} + ra_{p,j}) \\ &= e_{p,n_i}^{(i)} - e_{p,n_j}^{(j)} + ta_{p,i} - (n_i - n_j + t)a_{p,j} \\ &= e_{p,n_i}^{(i)} - e_{p,n_j}^{(j)} + t(a_{p,i} - a_{p,j}) + (n_i - n_j)a_{p,j} \end{aligned}$$

Note that the expression $e_{p,n_i}^{(i)} - e_{p,n_j}^{(j)} + (n_i - n_j)a_{p,j}$ does not depend on n.

For $P_i \in \Pi$, the image of P_i under σ is also a prime ideal. So σ induces a permutation σ on the indices $\{1, \ldots, k\}$. Then $\sigma(pR) = p\sigma(R) = pR$ so that $\sigma(\prod_{i=1}^{k_p} P_i^{a_{p,i}}) = \prod_{i=1}^{k_p} P_i^{a_{p,i}}$. Since σ is a ring automorphism, $\sigma(\prod_{i=1}^{k_p} P_i^{a_{p,i}}) = \prod_{i=1}^{k_p} \sigma(P_i)^{a_{p,i}} = \prod_{i=1}^{k_p} P_{\sigma(i)}^{a_{p,i}}$. Unique factorization implies that $P_{\sigma(i)}^{a_{p,i}} = P_{\sigma(i)}^{a_{p\sigma(i)}}$ and $a_{p,i} = a_{p\sigma(i)}$.

If $i, j \in \Lambda_p$ so that $\sigma(i) = j$ then $a_{p,i} = a_{p,j}$. Thus $e_{p,n}^{(i)} - e_{p,n}^{(j)} = e_{p,n_i}^{(i)} - e_{p,n_j}^{(j)} + (n_i - n_j)a_{p,j}$ which does not depend on n. For such pairs i, j define $D_{i,j} = e_{p,n_i}^{(i)} - e_{p,n_j}^{(j)} + (n_i - n_j)a_{p,j}$. There are a finite number of integers $D_{i,j}$ so one can pick a natural number D greater than all of them.

If $\sigma(i) = i$ then $P_{\sigma(i)}^{D+e_{p,n}^{(i)}} = P_i^{D+e_{p,n}^{(i)}} \subseteq P_i^{e_{p,n}^{(i)}}$. If $\sigma(i) = j$ then $P_{\sigma(i)}^{D+e_{p,n}^{(i)}} = P_j^{D+e_{p,n}^{(i)}}$. From $D > D_{i,j} = e_{p,n}^{(i)} - e_{p,n}^{(j)}$ it follows that

$$e_{p,n}^{(i)} - D_{i,j} = e_{p,n}^{(j)}$$

$$e_{p,n}^{(i)} + D > e_{p,n}^{(j)}$$

Therefore $P_j^{D+e_{p,n}^{(i)}} \subseteq P_j^{e_{p,n}^{(j)}}$.

Since R is a PID, there is an $s \in R$ such that $sR = \prod_{i=1}^{k_p} P_i^D$. Then

$$\begin{aligned} s\sigma(X_{p,n}) &= \prod_{i=1}^{k_p} P_i^D \prod_{i=1}^{k_p} P_{\sigma(i)}^{e_{p,n}^{(i)}} \\ &= \prod_{i=1}^{k_p} P_{\sigma(i)}^{D+e_{p,n}^{(i)}} \\ &\subseteq \prod_{i=1}^{k_p} P_i^{e_{p,n}^{(i)}} = X_{p,n} \end{aligned}$$

Thus $s\sigma(X_{p,n}) \subseteq X_{p,n}$. Now $s\sigma(M_{p,n}) = s\sigma(p^{-n}X_{p,n}) = p^{-n}s\sigma(X_{p,n}) \subseteq p^{-n}X_{p,n} = M_{p,n}$. Therefore $s\sigma(M_{p,n}) \subseteq M_{p,n}$. Since $id_R \neq \sigma$, the map $s\sigma$ is not multiplication by an element of R. It follows that R cannot be Zassenhaus ring. $\square$

CHAPTER TEN

Conclusion: A Ring with a Zassenhaus Family that is not a Zassenhaus Ring

The following example is a natural adaptation of the example from [20, page 987] to our Zassenhaus family and Zassenhaus ring terminology.

Denote by $R = \mathbb{Z}_{13}[i]$ the ring of polynomials in $i = \sqrt{-1}$ with coefficients from the ring integers localized at the prime ideal $13\mathbb{Z}$. The prime ideals of $\mathbb{Z}_{13}[i]$ are $(2+3i)R$ and $(2-3i)R$. The mapping $\sigma(a+bi) = a-bi$ is a nontrivial ring automorphism for R. By Theorem 9.7, R is not a Zassenhaus ring.

It is easy to show that $\mathrm{End}_{\mathbb{Z}}(R) \subseteq \mathbb{Q}[\mathrm{Aut}(R)]$. $\mathrm{Aut}(R) = \{\mathrm{id}_R, \sigma\}$ where σ is the map above. Since σ maps $(a+ib)R$ to $(a-ib)R$, $K_\pi = \{\mathrm{id}_R\}$. By Theorem 5.2, there is a Zassenhaus family for R. Therefore $\mathbb{Z}_{13}[i]$ has a Zassenhaus family but is not a Zassenhaus ring.

Zassenhaus families are used directly to construct modules sufficient for showing that several disparate classes of finite rank rings are Zassenhaus rings. The Zassenhaus families of $\mathbb{Z}[x]$, $S\Lambda$, rings of algebraic integers of finite degree Galois extentions of $\mathbb{Q}$, and $\mathrm{Mat}_{n\times n}(\mathbb{Z})$ provide modules which show that these rings are Zassenhaus rings. This is evidence for making the case that any finite rank ring with a Zassenhaus family is, in fact, a Zassenhaus ring. But it has been shown that such a definitive converse for our first theorem is not possible.

BIBLIOGRAPHY

[1] David M. Arnold, *Finite rank torsion free abelian groups and rings*, Lecture Notes in Mathematics, vol. 931, Springer-Verlag, Berlin, 1982.

[2] David M. Arnold *Abelian groups and representations of finite partially ordered sets*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, 2, Springer-Verlag, New York, 2000.

[3] Emil Artin, *Galois theory*, second ed., Dover Publications Inc., Mineola, NY, 1998, Edited and with a supplemental chapter by Arthur N. Milgram.

[4] Robert B. Ash, *A course in algebraic number theory*, online text: http://www.math.uiuc.edu/ r-ash/ANT.html, 2003.

[5] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley Series in Mathematics, Westview Press, Boulder, CO, 1969.

[6] Joshua Buckner and Manfred Dugas. Left rigid rings. To appear in Journal of Algebra.

[7] Joshua Buckner and Manfred Dugas. Quasi-localizations of $\mathbb{Z}$. To appear in Israel Journal of Mathematics.

[8] Joshua Buckner and Manfred Dugas. Co-local subgroups of abelian groups. In *Abelian groups, rings, modules, and homological algebra*, volume 249 of *Lect. Notes Pure Appl. Math.*, pages 29–37. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[9] M. C. R. Butler, *On locally free torsion-free rings of finite rank*, J. London Math. Soc. **43** (1968), 297–300.

[10] A. L. S. Corner, *Every countable reduced torsion–free ring is an endomorphism ring*, Proc. London Math. Soc. (3) **13** (1963), 687 – 710.

[11] László Fuchs, *Infinite abelian groups. Vol. I*, Pure and Applied Mathematics, Vol. 36, Academic Press, New York, 1970.

[12] László Fuchs, *Infinite abelian groups. Vol. II*, Academic Press, New York, 1973, Pure and Applied Mathematics. Vol. 36-II.

[13] Thomas W. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York, 1980, Reprint of the 1974 original.

[14] I. Martin Isaacs, *Algebra*, Brooks/Cole Publishing Co., Pacific Grove, CA, 1994.

[15] Gerald J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996.

[16] Neal Koblitz, *A course in number theory and cryptography*, second ed., Graduate Texts in Mathematics, vol. 114, Springer-Verlag, New York, 1994.

[17] Lee Lady, *Finite Rank Torsion Free Modules Over Dedekind Domains*, online text: http://www.math.hawaii.edu/ lee/book/index.html

[18] William J. LeVeque, *Fundamentals of number theory*, Dover Publications Inc., Mineola, NY, 1996, Reprint of the 1977 original.

[19] A. Mader and C. Vinsonhaler, *Torsion-free E-modules*, J. Algebra **115** (1988), no. 2, 401–411.

[20] J. D. Reid and C. Vinsonhaler, *A theorem of M. C. R. Butler for Dedekind domains*, J. Algebra **175** (1995), no. 3, 979–989.

[21] Eugene Spiegel and Christopher J. O'Donnell, *Incidence algebras*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 206, Marcel Dekker Inc., New York, 1997.

[22] C. Vinsonhaler, *E-rings and related structures*, Math. Appl., vol. 520, pp. 387–402, Kluwer Acad. Publ., Dordrecht, 2000.

[23] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994.

[24] H. Zassenhaus, *Orders as endomorphism rings of modules of the same rank*, J. London Math. Soc. **42** (1967), 180–182.