CIRCULANTS (Extract)

Alun Wyn-jones

Last revised in December 2013.

Chapter 4.
The Supercirculants, $\mathbf{circ}_\infty$

This chapter describes the algebra $\mathbf{circ}_\infty$ (see example *(iii)* of §3.6).

We hold $\mathbf{circ}_\infty$ (and its extensions) to be the most natural generalization of circulants in that the algebra $\mathbf{circ}_\infty(R)$ subsumes every circulant algebra over a ring R. For this reason, we call $\mathbf{circ}_\infty(R)$ the **supercirculant algebra** over the ring R, and we call its members **supercirculants**.

This is a good point to discuss the supercirculants because many of the homomorphisms between circulants introduced in the last chapter assume particularly simple forms when generalized to the supercirculants. Also, the supercirculant algebra will be useful later in the chapter on tensor products of circulant algebras.

We originally identified $\mathbf{circ}_\infty(R)$ with the group ring $R[\mathbb{Q}/\mathbb{Z}]$. A typical member of $\mathbb{Q}/\mathbb{Z}$ is the fractional part of a rational, $\{m/n\}$ and the group product is addition modulo 1. We shall still use this representation of $\mathbf{circ}_\infty(R)$ where it is useful, but there is a representation which provides a more natural correspondence between the circulant algebras and the supercirculants. For this reason, we shall replace the group $\mathbb{Q}/\mathbb{Z}$ with another (but isomorphic) group consisting of an amalgam of the standard circulant bases $U_\infty := \{\mathrm{u}_m^n \vdash m, n \in \mathbb{Z}\}$.

4.1.1 **Definition** The group U_∞ is the set $\{\mathrm{u}_r^s \vdash r, s \in \mathbb{Z}, r \neq 0\}$ obeying the relations

(i) $\mathrm{u}_r^s \mathrm{u}_t^u = \mathrm{u}_{rt}^{st+ru}$

(ii) $\mathrm{u}_{rs}^{st} = \mathrm{u}_r^t$

(iii) $\mathrm{u}_r^s = 1$ iff $r \,|\, s$.

Clearly, $U_\infty \approx \mathbb{Q}/\mathbb{Z}$.

4.1.2 **Definition** $\mathbf{circ}_\infty(R) := R[U_\infty]$.

There is a copy of $\mathbf{circ}_n(R)$ in $\mathbf{circ}_\infty(R)$ for every n. The embedding is $\Upsilon_{1/n} : \mathbf{circ}_n(R) \hookrightarrow \mathbf{circ}_\infty(R)$ (see Proposition 3.6.4). In replacing $\mathbb{Q}/\mathbb{Z}$ with U_∞ we can identify $\mathbf{circ}_n$ with its copy, $\Upsilon_{1/n}(\mathbf{circ}_n) \subset \mathbf{circ}_\infty$. That is, the embedding is now viewed as a subset map. This identification leads to some intuitive and easily proved observations which follow.

4.1.3 **Proposition** Regarding $\mathbf{circ}_n(R) \subset \mathbf{circ}_\infty(R)$ for all $n = 1, 2, \ldots$,

(i) $\mathbf{circ}_m(R) \cap \mathbf{circ}_n(R) = \mathbf{circ}_{\gcd(m,n)}(R)$

(ii) $\mathbf{circ}_m(R) \vee \mathbf{circ}_n(R) = \mathbf{circ}_m(R)\mathbf{circ}_n(R) = \mathbf{circ}_N(R)$ where $N = \mathrm{lcm}(m, n)$.

(iii) $\mathbf{circ}_{mn}(R)$ is a free $\mathbf{circ}_n(R)$-module of rank m.

□

4.1.4 **Proposition** Every finite subset of $\mathbf{circ}_\infty(R)$ is in $\mathbf{circ}_N(R)$ for some N.

Proof.

The general element of a group ring $R[G]$ is $\sum_{g \in X} a_g g$ where X must be a finite subset of G. Therefore we can write the general element of $\mathbf{circ}_\infty(R)$ as

$$\sum_{m/n \in X} a_{m/n} \mathrm{u}_n^m = b_0 + b_1 \mathrm{u}_N + b_2 \mathrm{u}_N^2 + \cdots + b_i \mathrm{u}_N^i + \cdots + b_{N-1} \mathrm{u}_N^{N-1} \tag{1}$$

where $N = \mathrm{lcm}\,\{n \vdash m/n \in X, \gcd(m, n) = 1\}$, and $b_i = \begin{cases} a_{i/N} & \text{if } i/N \in X \\ 0 & \text{otherwise} \end{cases}$

Let there be a finite subset $\{a, b, c, \ldots\} \subset \mathbf{circ}_\infty$. Then, by the above, there exist $A, B, C, \ldots \in \mathbb{N}$ such that $a \in \mathbf{circ}_A$, $b \in \mathbf{circ}_B$, $c \in \mathbf{circ}_C$, etc. Set $N = \mathrm{lcm}\{A, B, C, \ldots\}$, then by Proposition 4.1.3 *(ii)*, $\{a, b, c, \ldots\} \in \mathbf{circ}_N$. □

4.1.5 **Proposition** Let $R[G]$ be a group ring, let H be a subgroup of G, and let τ be a group endomorphism on G.

(i) τ extends to an R-algebra endomorphism, τ' on $R[G]$
where $\tau'(rf + sg) = r\tau(f) + s\tau(g),\ \forall r, s \in R,\ \ \forall f, g \in G.$

(ii) $\ker \tau' = R[\ker \tau]$

(iii) $R[H]$ is an R-subalgebra of $R[G]$. □

In the case of $R[G] = \mathbf{circ}_\infty(R)$, let us call the endomorphism of the type described in parts *(i)* and *(ii)* an **extended group endomorphism**, and let us call the subring of the type in part *(iii)* a **subgroup ring**. The extended group endomorphisms and the subgroup rings are interesting because they are automatically R-linear and R-subalgebras, respectively. To find all such endomorphisms and subalgebras of $\mathbf{circ}_\infty(R)$ we need more facts on the group U_∞.

4.1.6 **Theorem**

(i) The group U_∞ is pure torsion.

(ii) U_∞ is a divisible group, and so has the injective property.

(iii) $U_\infty = \prod_p \sigma(p^\infty)$ where the direct product is over all p-primary components of U_∞.

Proof. These are standard facts about the group $\mathbb{Q}/\mathbb{Z}$. See [Rot]. □

The injective property on U_∞ assures us that β exists whenever α exists in the map diagram below (where H and K are abelian groups.) Typically, $H \subset K$, and then the theorem says that there is an extension of α to K.

$$\begin{array}{ccccc} & & & & U_\infty \\ & & & \overset{\alpha}{\nearrow} & \uparrow \beta? \\ 0 & \to & H & \to & K \end{array}$$

Part *(iii)* of the theorem is perhaps better illustrated in the group $\mathbb{Q}/\mathbb{Z}$ taking the interval $[0,1) \cap \mathbb{Q}$ as a transversal for the rationals modulo 1. The p-primary component of $\mathbb{Q}/\mathbb{Z}$ is the set of all fractions whose denominators are powers of p. The direct sum decomposition of a general fraction in the interval $[0,1)$ is performed thus: Let $a/mn \in [0,1)$ with m, n coprime. Then, there exists a unique partial fraction decomposition of $a/mn = b/m + c/n$ where $b, c \in \mathbb{N}$ and $b/m,\ c/n \in [0,1)$. We proceed thus until the denominators of all partial fractions are prime powers.

4.1.7 **Proposition**

(i) Each finitely-generated subgroup of U_∞ is cyclic generated by u_n for some n.

(ii) The endomorphisms of U_∞ are direct products of endomorphisms on the p-primary components.

Proof. We shall prove the proposition for the group $\mathbb{Q}/\mathbb{Z}$, and we shall take as representatives the rationals in the interval $[0,1)$.

(i) Let x/y be any reduced fraction in $(0,1)$. Then, $kx/y \bmod 1 \in A$ for all $k \in \mathbb{N}$. Setting k to the inverse residue of $x \pmod y$, we see that $1/v \in A$.

Now, suppose that A is a finitely generated subgroup of $\mathbb{Q}/\mathbb{Z}$. By part *(i)* of the theorem, A is finite; let $u/v \in [0,1) \cap \mathbb{Q}$ be its smallest reduced fraction. By the above, $1/v \in A$. $\therefore u = 1$. Let x/y be any reduced fraction in A, then $1/y \in A$. By considering $a/v + b/y$ where $a, b \in \mathbb{Z}$, we see that $1/\mathrm{lcm}(v,y) \in A$. By the minimality of $1/v$, $\mathrm{lcm}(v,y) \le v$ which means $y \mid v$. That is, A consists entirely of the fractions with denominators dividing v, and hence is cyclic generated by $1/v$. QED *(i)*.

(ii) Let $\alpha : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ be non-trivial with $\alpha(x) \neq 0$. Let P_p be the projection homomorphism onto $\sigma(p^\infty)$ with p chosen so that $P_p(x) \neq 0$. (This must exist since $\alpha(x) \neq 0 \ \Rightarrow\ x \neq 0$.) Let $P_p^\perp = 1 - P_p$ be the complementary projection of P_p. Hence, $x = y \oplus z$ where $y = P_p(x)$, and $z = P_p^\perp(x)$.

Consider first $\alpha(y)$. Since α is a homomorphism, $\alpha(y)$ must have order dividing the order of $y \in \sigma(p^\infty)$. Therefore, $\alpha(y) \in \sigma(p^\infty)$. Similarly, $\alpha(z)$ must have order dividing the order of z which is in the direct product of all q-primary subgroups where $q \neq p$. This means that the order of $\alpha(z)$ cannot be divisible by p.

We have shown that $\alpha = \alpha_p \oplus \alpha_p^\perp$ where $\alpha_p = P_p \alpha P_p$, and $\alpha_p^\perp = P_p^\perp \alpha P_p^\perp$. We now apply the same reasoning to z eventually obtaining a complete decomposition of α into its actions on all the p-primary components of x, and all such actions are endomorphisms of their respective components. □

4.1.8 **Corollary** Each subgroup ring of $\mathbf{circ}_\infty(R)$ with a finite basis is $\mathbf{circ}_n(R)$ for some n. □

The proposition shows that every supercirculant endomorphism is specified by endomorphisms on the p-primary components. Let $\alpha_p : \sigma(p^\infty) \to \sigma(p^\infty)$. How is α_p specified? Let C_n be the subgroup of $\sigma(p^\infty)$ generated by $1/p^n$ (again using the $[0,1] \cap \mathbb{Q}$ representation). One can easily show that α_p must be an endomorphism on C_n for every n. This gives another simple corollary to Proposition 4.1.8.

4.1.9 **Corollary** Every endomorphism of $\mathbb{Q}/\mathbb{Z}$ is an endomorphism of every subgroup $C_n^{(p)} = \{a/p^n \vdash 0 \leq a < p^n\}$, and the action on $C_n^{(p)}$ is $x \to k_n^{(p)} x \bmod 1$ for some integer $k_n^{(p)}$.

Proof. C_n is cyclic since it is generated by $1/p^n$. All endomorphisms of the cyclic group $\mathbb{Z}_N$ are of the form $x \mapsto mx \bmod N$ for some integer m, it follows that the action of α on C_n is multiplication (mod 1) by some constant integer. □

Hence, we can specify α_p by specifying $k_n^{(p)}$ for every n. For consistency on all subgroups of $\sigma(p^\infty)$, we must have $k_{n+i} \equiv k_n \pmod{p^n}$ for $i \geq 0$. We can guarantee consistency by defining k_n p-adically as

$$k_n = k_n^{(p)} = c_0^{(p)} + pc_1^{(p)} + p^2 c_2^{(p)} + \cdots + p^{n-1} c_{n-1}^{(p)} \qquad \text{where } 0 \leq c_i < p \tag{2}$$

This demonstrates that the number of endomorphisms on each p-primary component of U_∞ has the cardinality of $\mathbb{R}$. Furthermore, a complete specification of the full endomorphism, $\alpha : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$, requires the independent specifications of an infinity of sequences $\left(k_n^{(p)}\right)_{n=1,2,\cdots}$, one for each prime, p.

4.1.10 **Examples**

(i) Take $c_0^{(p)} = 1$ for some prime p, and set all other $c_i^{(q)} = 0$. We get the projection endomorphism $P_p : \mathbb{Q}/\mathbb{Z} \to \sigma(p^\infty)$.

(ii) Take $k_n^{(p)} = k$, a constant. This specifies the $\mathbb{Q}/\mathbb{Z}$ group endomorphism $\alpha(x) = kx$. On U_∞ the homomorphism is given by $\alpha(\mathrm{u}_n) = \mathrm{u}_n^k$.

(iii) Take $c_i^{(p)} = \pi_i^{(p)}$ where $\pi_i^{(p)}$ is the i^{th} digit of π ($= 3.14159\ldots$) in base p arithmetic. This is an example of a homomorphism which requires an infinity of parameters, but is nevertheless well-defined.

4.2 Supercirculant Endomorphisms.

We have obtained a full description of the endomorphisms of the group U_∞. The next proposition shows that such endomorphisms when extended to $\mathbf{circ}_\infty$ are automatically endomorphisms on the circulant subrings.

4.2.1 **Proposition** Let α be an extended group endomorphism of $\mathbf{circ}_\infty(R)$ then α is also an endomorphism of $\mathbf{circ}_n(R)$ for every n.

Proof. From Corollary 4.1.9, if α is an extended group endomorphism, α must map each p-primary subgroup of the type C_n into itself. Hence, α maps the set $\{\mathrm{u}_n^i \vdash 0 \leq i < n\}$ into itself, and so α must be an endomorphism of $\mathbf{circ}_n(R)$. □

We now return to example *(ii)* of §4.1.10 (where $k_n^{(p)} = k$). As a map on U_∞ this is the endomorphism $\mathrm{u}_n \mapsto \mathrm{u}_n^k$. When extended to $\mathbf{circ}_\infty(R)$ call this map H_k. Observe that $H_n|\mathbf{circ}_{mn}(R)$ maps u_{mn} to u_n, and so it must be the wrap-around map, $\Gamma^m_{mn} : \mathbf{circ}_{mn}(R) \to \mathbf{circ}_m(R)$. More generally, the proposition shows that H_k in an endomorphism on $\mathbf{circ}_n(R)$ for all n. Clearly, H_k can only be the map ν_k of §3.7. In other words, as supercirculant maps, $\Gamma^n_{mn} = \nu_n = H_n|\mathbf{circ}_{mn}(R)$. It is therefore hardly surprising that Γ^n_{mn} and ν_h commute (see Proposition 3.7.6).

Even more drastic is the fate of the injection map, $\tilde{\Gamma}^{mn}_m$, when extended to the supercirculants -- it becomes the identity map ! $\tilde{\Gamma}^{mn}_m : \mathrm{u}_m \to \mathrm{u}^n_{mn} = \mathrm{u}_m$. Hence, all commutation relations of $\tilde{\Gamma}^m_{mn}$ with every circulant map are trivial.

Next, let us consider the idempotent $\bar{\delta}^{n|mn}$ and its associated map, $x \mapsto \bar{\delta}^{n|mn}x$. Trivially, any idempotent in a subring is also an idempotent in the larger ring. So, $\bar{\delta}^{n|mn}$ is a supercirculant idempotent, and hence defines an endomorphism on $\mathbf{circ}_\infty$. By definition,

$$\bar{\delta}^{n|mn} \;:=\; \frac{1}{n}\sum_{i=0}^{n-1} \mathrm{u}^{im}_{mn} \;=\; \frac{1}{n}\sum_{i=0}^{n-1} \mathrm{u}^{i}_{n}$$

and so it is quite unambiguous to write $\bar{\delta}^n$ instead of $\bar{\delta}^{n|mn}$ because as a supercirculant, $\bar{\delta}^n$ truly depends only on n.

The circulant repeater map, Γ^{mn}_m was defined as $\Gamma^{mn}_m(\mathrm{u}_m) = \bar{\delta}^n \mathrm{u}_{mn}$. This definition stands except that Γ^{mn}_m no longer depends upon m. The value of $\Gamma^{mn}_m(x)$ is entirely determined by x and n. Our suspicions are confirmed; indeed, $\Gamma^m_{mn}(x) = \bar{\delta}^n x$. This and the above observations are collected below.

4.2.2 **Proposition** The Γ^s_r homomorphisms of chapter 3 have natural extensions to $\mathbf{circ}_\infty$ which are:

(i) $\Gamma^{mn}_m = \nu_n : \mathrm{u}_i \mapsto \mathrm{u}^n_i, \quad \forall i \in \mathbb{N}.$

(ii) $\tilde{\Gamma}^{mn}_m =$ identity map.

(iii) $\Gamma^m_{mn}(x) = \bar{\delta}^n(x).$

Proof. The first two statements are already clear.

For the third statement, note that $\bar{\delta}^n \mathrm{u}_n = \bar{\delta}^n$. Therefore, $\bar{\delta}^n \mathrm{u}_d = \bar{\delta}^n$ whenever $d \,|\, n$. Whence, $\bar{\delta}^n \mathrm{u}_m = \bar{\delta}^n \mathrm{u}_{m/d}$ where $d = \gcd(m, n)$. We now see that $\bar{\delta}^n \mathrm{u}_{mn} = \bar{\delta}^n \mathrm{u}^n$. But, $\Gamma^{mn}_m(\mathrm{u}_n) = \bar{\delta}^n \mathrm{u}_{mn} = \bar{\delta}^n \mathrm{u}_n$. The rest follows by linearity. □

4.3 Supercirculant Eigenvalues

In the Chapter 2 we saw that the R-linear circulant automorphisms are permutations of the circulant eigenvalues. We would therefore expect that R-linear automorphisms of supercirculants which were also endomorphisms of the circulant algebras would also be permutations of eigenvalues. But, first we must define eigenvalues for the supercirculants. The reader may ponder what definition might be appropriate before reading on, but will conclude that the one given below is the only definition which is an R-linear ring monomorphism from the supercirculant algebra into an algebra having componentwise multiplication and addition.

4.3.1 **Definition** The eigenvalue map $\lambda : \mathbf{circ}_\infty(R) \to \Lambda_\infty(R)$ is defined by $\lambda_i(\mathrm{u}_n) \;:=\; \zeta_n^i, \;\forall i \in \mathbb{N}$, and is then extended by additivity, multiplicativity, and R-linearity to the whole of $\mathbf{circ}_\infty(R)$.

The definition implies that $\Lambda_\infty(R)$ is a space of infinite sequences, and when R is a domain, $\Lambda_\infty(R)$ is an infinite dimensional vector space. That is, given any $c \in \mathbf{circ}_\infty$, $\lambda(c) = (\lambda_0(c), \lambda_1(c), \ldots, \lambda_i(c), \lambda_{i+1}(c), \ldots)$. Also, since $c \in \mathbf{circ}_n(R)$ for some n, the sequence $\lambda(c)$ must be periodic with period n. Informally, $\lambda(c)$ has the frequency spectrum c.

Let $R_{(n)}$ be the set of sequences of period n with entries from $R(\zeta_n)$. Then, $\Lambda_\infty(R)$ is contained in $\bigcup_n R_{(n)}$. In analogy with $\mathbf{circ}_n$, we shall call $\bigcup_n R_{(n)}$ the **supercirculant eigenspace**. That is, we view $\bigcup_n R_{(n)}$ as the range (but it is not the image) of the λ map acting on $\mathbf{circ}_\infty(R)$. Just as all elements must finite sums in group rings so all sequences are periodic in the supercirculant eigenspace.

4.4 The Inverse Transform, λ^{-1}

One can easily prove that λ is a monomorphism. For instance, suppose $\lambda(x) = 0$. W.l.o.g., $x \in \mathbf{circ}_n(R)$. Then, taking a subsequence consisting of one whole period of n terms from $\lambda(x)$ we obtain the vector $\lambda^{(n)}(x)$. Whence $x = 0$.

Therefore, λ must have an inverse on its image. A formula for the inverse should specify the coefficient of u for every $\mathrm{u} \in U_\infty$. (Of course, almost all should turn out to be zero.) It is convenient to use the notation $a_{r/n}$ for the coefficient of u_n^r.

4.4.1 Proposition

Let $\mu = (\mu_0, \mu_1, \ldots) \in \bigcup_n R_{(n)}$, and for definiteness, suppose $\mu \in R_{(m)}$. Define $a = \sum_{0 \le r/n < 1} \{a_{r/n} \mathrm{u}_n^r\}$ where $a_{r/n}$ are defined by

$$a_{r/n} \;:=\; \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} \mu_i \zeta_n^{-ir} \tag{3}$$

Then,

(i) $a \in \mathbf{circ}_M(Q)$ where Q is the ring of quotients of R, and

(ii) $\lambda(a) = \mu$.

Proof.

(i) Fix a typical term $a_{r/n}$, and w.l.o.g., suppose $r < n$ are coprime. The trick to evaluating formula (3) is to group terms within periods of $\mu_i \zeta_n^{-ir}$ which in this case has a period of nm/d where $d = \gcd(n, m)$. Assume for the moment that the series in (3) has a whole number of periods of $\mu_i \zeta_n$, i.e., that $N = Lnm/d$ for some integer L. Then,

$$a_{r/n} \quad = \quad \lim_{L\to\infty} \frac{d}{Lmn} \sum_{l=0}^{L-1} \sum_{i=0}^{mn/d-1} \mu_i \zeta_n^{-ir}$$

The second summation is independent of l. So, the outside factor of $1/L$ cancels with the L repetitions of the second sum. Inside the second sum, the coefficients $\mu_i, \mu_{i+m}, \mu_{i+2m}, \ldots$ are all equal. Group together all such terms. (This is a finite derangement of the series.) We obtain inner sums of the form

$$\begin{aligned}
&\mu_i \zeta_n^{-ir} \;+\; \mu_{i+m} \zeta_n^{-ir-mr} \;+\; \mu_{i+2m} \zeta_n^{-ir-2mr} \;+\; \ldots \;+\; \mu_{i+(n/d-1)m} \zeta_n^{-ir-(n/d-1)mr} \\
&\qquad = \quad \mu_i \zeta_n^{-ir} \left(1 \;+\; \zeta_n^{-mr} \;+\; \zeta_n^{-2mr} \;+\; \ldots \;+\; \zeta_n^{-(n/d-1)mr}\right) \\
&\qquad = \quad \mu_i \zeta_n^{-ir} \left(1 \;+\; \zeta_{n/d}^{-s} \;+\; \zeta_{n/d}^{-2s} \;+\; \ldots \;+\; \zeta_{n/d}^{-(n-d)s}\right) \qquad \text{where } s = rm/d \\
&\qquad = \quad \begin{cases} 1 & \text{if } n/d = 1 \\ 0 & \text{otherwise} \end{cases}
\end{aligned}$$

The final choice of values is comes from the fact that both r and m/d are coprime to n/d. The upshot is that $a_{r/n}$ is zero unless $n \,|\, m$.

Finally, we have to consider the remainder term. This will be the sum over some fractional part of the period of $\mu_i \zeta_n^{-ir}$. Because we have already considered any number of whole periods in the series, we can assume that the remainder contains less terms than a complete period. Therefore, the remainder cannot exceed R in absolute value where

$$R \;=\; \frac{1}{N} \frac{mn}{d} \max\{\mu_i \vdash 0 \le i < m\}$$

and this tends to zero as $N \to \infty$. QED *(i)*

Continuing the above formula, but now assuming $n \,|\, m$. We see that

$$a_{r/n} \;=\; \frac{1}{m}\sum_{i=0}^{m-1} \mu_i \zeta_n^{-ir}$$

which we can rewrite by setting $d = m/n$ as

$$a_{rd/m} \;=\; \frac{1}{m}\sum_{i=0}^{m-1} \mu_i \zeta_m^{-ird}$$

This is the regular formula for $\lambda^{-(m)}$. Since a single period of $\lambda|\mathbf{circ}_m(R)$ agrees with $\lambda^{(m)}$ on $\mathbf{circ}_m(R)$, we have that $\lambda(a) = \mu$. $\square$