Cyclic numbers

The spectrum of a class of structures

The spectrum of a class of structures

The spectrum of a class $\mathcal{K}$ of structures is the function $\mathrm{Spec}_{\mathcal{K}}(\kappa)$ = number of isotypes of structures in $\mathcal{K}$ of size κ.

The spectrum of a class of structures

The spectrum of a class $\mathcal{K}$ of structures is the function $\mathrm{Spec}_{\mathcal{K}}(\kappa)$ = number of isotypes of structures in $\mathcal{K}$ of size κ.

If $\mathcal{A}$ is the class of abelian groups, then $\mathrm{Spec}_{\mathcal{A}}(\kappa) = 2^{\kappa}$ for infinite κ, which is "the largest it could be".

The spectrum of a class of structures

The spectrum of a class $\mathcal{K}$ of structures is the function $\text{Spec}_{\mathcal{K}}(\kappa)$ = number of isotypes of structures in $\mathcal{K}$ of size κ.

If $\mathcal{A}$ is the class of abelian groups, then $\text{Spec}_{\mathcal{A}}(\kappa) = 2^\kappa$ for infinite κ, which is “the largest it could be”. For finite k, we can compute $\text{Spec}_{\mathcal{A}}(k)$ using the structure theorem for finite abelian groups.

The spectrum of a class of structures

The spectrum of a class $\mathcal{K}$ of structures is the function $\mathrm{Spec}_{\mathcal{K}}(\kappa)$ = number of isotypes of structures in $\mathcal{K}$ of size κ.

If $\mathcal{A}$ is the class of abelian groups, then $\mathrm{Spec}_{\mathcal{A}}(\kappa) = 2^{\kappa}$ for infinite κ, which is “the largest it could be”. For finite k, we can compute $\mathrm{Spec}_{\mathcal{A}}(k)$ using the structure theorem for finite abelian groups. If $k = p_1^{e_1} \cdots p_r^{e_r}$, then $\mathrm{Spec}_{\mathcal{A}}(k) = p(e_1) \cdots p(e_r)$ where $p(x)$ is the partition function of number theory.

The spectrum of a class $\mathcal{K}$ of structures is the function $\mathrm{Spec}_{\mathcal{K}}(\kappa)$ = number of isotypes of structures in $\mathcal{K}$ of size κ.

If $\mathcal{A}$ is the class of abelian groups, then $\mathrm{Spec}_{\mathcal{A}}(\kappa) = 2^{\kappa}$ for infinite κ, which is "the largest it could be". For finite k, we can compute $\mathrm{Spec}_{\mathcal{A}}(k)$ using the structure theorem for finite abelian groups. If $k = p_1^{e_1} \cdots p_r^{e_r}$, then $\mathrm{Spec}_{\mathcal{A}}(k) = p(e_1) \cdots p(e_r)$ where $p(x)$ is the partition function of number theory.
Observe that the smallest value of the function $\mathrm{Spec}_{\mathcal{A}}(k)$ is $\mathrm{Spec}_{\mathcal{A}}(k) = 1$, and this happens iff $p(e_1) = \cdots = p(e_r) = 1$

The spectrum of a class of structures

The spectrum of a class $\mathcal{K}$ of structures is the function $\text{Spec}_{\mathcal{K}}(\kappa)$ = number of isotypes of structures in $\mathcal{K}$ of size κ.

If $\mathcal{A}$ is the class of abelian groups, then $\text{Spec}_{\mathcal{A}}(\kappa) = 2^{\kappa}$ for infinite κ, which is "the largest it could be". For finite k, we can compute $\text{Spec}_{\mathcal{A}}(k)$ using the structure theorem for finite abelian groups. If $k = p_1^{e_1} \cdots p_r^{e_r}$, then $\text{Spec}_{\mathcal{A}}(k) = p(e_1) \cdots p(e_r)$ where $p(x)$ is the partition function of number theory.
Observe that the smallest value of the function $\text{Spec}_{\mathcal{A}}(k)$ is $\text{Spec}_{\mathcal{A}}(k) = 1$, and this happens iff $p(e_1) = \cdots = p(e_r) = 1$ iff $e_1 = \cdots e_r = 1$

The spectrum of a class of structures

The spectrum of a class $\mathcal{K}$ of structures is the function $\text{Spec}_{\mathcal{K}}(\kappa)$ = number of isotypes of structures in $\mathcal{K}$ of size κ.

If $\mathcal{A}$ is the class of abelian groups, then $\text{Spec}_{\mathcal{A}}(\kappa) = 2^{\kappa}$ for infinite κ, which is "the largest it could be". For finite k, we can compute $\text{Spec}_{\mathcal{A}}(k)$ using the structure theorem for finite abelian groups. If $k = p_1^{e_1} \cdots p_r^{e_r}$, then $\text{Spec}_{\mathcal{A}}(k) = p(e_1) \cdots p(e_r)$ where $p(x)$ is the partition function of number theory.
Observe that the smallest value of the function $\text{Spec}_{\mathcal{A}}(k)$ is $\text{Spec}_{\mathcal{A}}(k) = 1$, and this happens iff $p(e_1) = \cdots = p(e_r) = 1$ iff $e_1 = \cdots e_r = 1$ iff k is square free.

The spectrum of a class of structures

The spectrum of a class $\mathcal{K}$ of structures is the function $\text{Spec}_{\mathcal{K}}(\kappa)$ = number of isotypes of structures in $\mathcal{K}$ of size κ.

If $\mathcal{A}$ is the class of abelian groups, then $\text{Spec}_{\mathcal{A}}(\kappa) = 2^{\kappa}$ for infinite κ, which is "the largest it could be". For finite k, we can compute $\text{Spec}_{\mathcal{A}}(k)$ using the structure theorem for finite abelian groups. If $k = p_1^{e_1} \cdots p_r^{e_r}$, then $\text{Spec}_{\mathcal{A}}(k) = p(e_1) \cdots p(e_r)$ where $p(x)$ is the partition function of number theory.
Observe that the smallest value of the function $\text{Spec}_{\mathcal{A}}(k)$ is $\text{Spec}_{\mathcal{A}}(k) = 1$, and this happens iff $p(e_1) = \cdots = p(e_r) = 1$ iff $e_1 = \cdots e_r = 1$ iff k is square free.

$\text{Spec}_{\mathcal{A}}(k) = 1$ exactly when the only isotype of abelian group of cardinality k is the isotype of the cyclic group $\mathbb{Z}_k$.

The spectrum of a class of structures

The spectrum of a class $\mathcal{K}$ of structures is the function $\text{Spec}_{\mathcal{K}}(\kappa)$ = number of isotypes of structures in $\mathcal{K}$ of size κ.

If $\mathcal{A}$ is the class of abelian groups, then $\text{Spec}_{\mathcal{A}}(\kappa) = 2^{\kappa}$ for infinite κ, which is "the largest it could be". For finite k, we can compute $\text{Spec}_{\mathcal{A}}(k)$ using the structure theorem for finite abelian groups. If $k = p_1^{e_1} \cdots p_r^{e_r}$, then $\text{Spec}_{\mathcal{A}}(k) = p(e_1) \cdots p(e_r)$ where $p(x)$ is the partition function of number theory.
Observe that the smallest value of the function $\text{Spec}_{\mathcal{A}}(k)$ is $\text{Spec}_{\mathcal{A}}(k) = 1$, and this happens iff $p(e_1) = \cdots = p(e_r) = 1$ iff $e_1 = \cdots e_r = 1$ iff k is square free.

$\text{Spec}_{\mathcal{A}}(k) = 1$ exactly when the only isotype of abelian group of cardinality k is the isotype of the cyclic group $\mathbb{Z}_k$. This happens iff k is square-free.

Cyclic numbers

Cyclic numbers

Now consider the class $\mathcal{G}$ of all groups. Call k "cyclic" if $\mathrm{Spec}_{\mathcal{G}}(k) = 1$, i.e. if the only isotype of group of cardinality k is the isotype of the cyclic group $\mathbb{Z}_k$.

Cyclic numbers

Now consider the class $\mathcal{G}$ of all groups. Call k "cyclic" if $\mathrm{Spec}_{\mathcal{G}}(k) = 1$, i.e. if the only isotype of group of cardinality k is the isotype of the cyclic group $\mathbb{Z}_k$.

Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free, but square-freeness is not enough (think about $k = 2 \cdot 3$).

Cyclic numbers

Now consider the class $\mathcal{G}$ of all groups. Call k "cyclic" if $\mathrm{Spec}_{\mathcal{G}}(k) = 1$, i.e. if the only isotype of group of cardinality k is the isotype of the cyclic group $\mathbb{Z}_k$.

Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free, but square-freeness is not enough (think about $k = 2 \cdot 3$).

Say that primes p and q are "related" if p divides $q - 1$ or q divides $p - 1$.

Cyclic numbers

Now consider the class $\mathcal{G}$ of all groups. Call k "cyclic" if $\text{Spec}_{\mathcal{G}}(k) = 1$, i.e. if the only isotype of group of cardinality k is the isotype of the cyclic group $\mathbb{Z}_k$.

Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free, but square-freeness is not enough (think about $k = 2 \cdot 3$).

Say that primes p and q are "related" if p divides $q - 1$ or q divides $p - 1$.

Theorem

A number n is cyclic iff $n = p_1 \cdots p_r$ is square free, and no two primes in its factorization are related.

Proof of the theorem

Proof of the theorem

(Only if:)

Proof of the theorem

(Only if:)
Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free.

Proof of the theorem

(Only if:)
Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free. To see the necessity of the "no relations" condition, assume instead that $k = p_1 p_2 \cdots p_r$ and p_1 divides $p_2 - 1$. There will exist a nontrivial action $\alpha\colon \mathbb{Z}_{p_1} \to \mathrm{Aut}(\mathbb{Z}_{p_2})$ by automorphisms of $\mathbb{Z}_{p_1}$ on $\mathbb{Z}_{p_2}$, hence a nonabelian semidirect product $\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}$.

Proof of the theorem

(Only if:)

Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free. To see the necessity of the "no relations" condition, assume instead that $k = p_1 p_2 \cdots p_r$ and p_1 divides $p_2 - 1$. There will exist a nontrivial action $\alpha\colon \mathbb{Z}_{p_1} \to \mathrm{Aut}(\mathbb{Z}_{p_2})$ by automorphisms of $\mathbb{Z}_{p_1}$ on $\mathbb{Z}_{p_2}$, hence a nonabelian semidirect product $\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}$. Hence there is a nonabelian group $(\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}) \times \mathbb{Z}_{p_3 \cdots p_r}$ of cardinality k.

Proof of the theorem

(Only if:)

Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free. To see the necessity of the "no relations" condition, assume instead that $k = p_1 p_2 \cdots p_r$ and p_1 divides $p_2 - 1$. There will exist a nontrivial action $\alpha\colon \mathbb{Z}_{p_1} \to \mathrm{Aut}(\mathbb{Z}_{p_2})$ by automorphisms of $\mathbb{Z}_{p_1}$ on $\mathbb{Z}_{p_2}$, hence a nonabelian semidirect product $\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}$. Hence there is a nonabelian group $(\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}) \times \mathbb{Z}_{p_3 \cdots p_r}$ of cardinality k.

(If:)

(Only if:)
Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free. To see the necessity of the "no relations" condition, assume instead that $k = p_1 p_2 \cdots p_r$ and p_1 divides $p_2 - 1$. There will exist a nontrivial action $\alpha \colon \mathbb{Z}_{p_1} \to \mathrm{Aut}(\mathbb{Z}_{p_2})$ by automorphisms of $\mathbb{Z}_{p_1}$ on $\mathbb{Z}_{p_2}$, hence a nonabelian semidirect product $\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}$. Hence there is a nonabelian group $(\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}) \times \mathbb{Z}_{p_3 \cdots p_r}$ of cardinality k.

(If:)
Suppose that $|G| = p_1 \cdots p_r$, where no two primes are related.

Proof of the theorem

(Only if:)
Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free. To see the necessity of the "no relations" condition, assume instead that $k = p_1 p_2 \cdots p_r$ and p_1 divides $p_2 - 1$. There will exist a nontrivial action $\alpha\colon \mathbb{Z}_{p_1} \to \mathrm{Aut}(\mathbb{Z}_{p_2})$ by automorphisms of $\mathbb{Z}_{p_1}$ on $\mathbb{Z}_{p_2}$, hence a nonabelian semidirect product $\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}$. Hence there is a nonabelian group $(\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}) \times \mathbb{Z}_{p_3 \cdots p_r}$ of cardinality k.

(If:)
Suppose that $|G| = p_1 \cdots p_r$, where no two primes are related.
G must have cyclic Sylow subgroups, so $G \cong \mathbb{Z}_m \rtimes \mathbb{Z}_n$ where $\gcd(m, n) = 1$.

(Only if:)
Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free. To see the necessity of the "no relations" condition, assume instead that $k = p_1 p_2 \cdots p_r$ and p_1 divides $p_2 - 1$. There will exist a nontrivial action $\alpha \colon \mathbb{Z}_{p_1} \to \mathrm{Aut}(\mathbb{Z}_{p_2})$ by automorphisms of $\mathbb{Z}_{p_1}$ on $\mathbb{Z}_{p_2}$, hence a nonabelian semidirect product $\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}$. Hence there is a nonabelian group $(\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}) \times \mathbb{Z}_{p_3 \cdots p_r}$ of cardinality k.

(If:)
Suppose that $|G| = p_1 \cdots p_r$, where no two primes are related.
G must have cyclic Sylow subgroups, so $G \cong \mathbb{Z}_m \rtimes \mathbb{Z}_n$ where $\gcd(m, n) = 1$. Order the prime factors of $|G|$ so that $m = p_1 \cdots p_i$ and $n = p_{i+1} \cdots p_r$.

Proof of the theorem

(Only if:)
Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free. To see the necessity of the "no relations" condition, assume instead that $k = p_1 p_2 \cdots p_r$ and p_1 divides $p_2 - 1$. There will exist a nontrivial action $\alpha\colon \mathbb{Z}_{p_1} \to \mathrm{Aut}(\mathbb{Z}_{p_2})$ by automorphisms of $\mathbb{Z}_{p_1}$ on $\mathbb{Z}_{p_2}$, hence a nonabelian semidirect product $\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}$. Hence there is a nonabelian group $(\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}) \times \mathbb{Z}_{p_3 \cdots p_r}$ of cardinality k.

(If:)
Suppose that $|G| = p_1 \cdots p_r$, where no two primes are related.
G must have cyclic Sylow subgroups, so $G \cong \mathbb{Z}_m \rtimes \mathbb{Z}_n$ where $\gcd(m, n) = 1$. Order the prime factors of $|G|$ so that $m = p_1 \cdots p_i$ and $n = p_{i+1} \cdots p_r$. The structure of this semidirect product is determined by a homomorphism

$$\beta\colon \mathbb{Z}_n \to \mathrm{Aut}(\mathbb{Z}_m) \cong \mathbb{Z}_m^\times.$$

The domain of β has cardinality $n = p_{i+1} \cdots p_r$ while the codomain has cardinality $\phi(m) = (p_1 - 1) \cdots (p_i - 1)$.

Proof of the theorem

(Only if:)
Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free. To see the necessity of the "no relations" condition, assume instead that $k = p_1 p_2 \cdots p_r$ and p_1 divides $p_2 - 1$. There will exist a nontrivial action $\alpha \colon \mathbb{Z}_{p_1} \to \mathrm{Aut}(\mathbb{Z}_{p_2})$ by automorphisms of $\mathbb{Z}_{p_1}$ on $\mathbb{Z}_{p_2}$, hence a nonabelian semidirect product $\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}$. Hence there is a nonabelian group $(\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}) \times \mathbb{Z}_{p_3 \cdots p_r}$ of cardinality k.

(If:)
Suppose that $|G| = p_1 \cdots p_r$, where no two primes are related.
G must have cyclic Sylow subgroups, so $G \cong \mathbb{Z}_m \rtimes \mathbb{Z}_n$ where $\gcd(m, n) = 1$. Order the prime factors of $|G|$ so that $m = p_1 \cdots p_i$ and $n = p_{i+1} \cdots p_r$. The structure of this semidirect product is determined by a homomorphism

$$\beta \colon \mathbb{Z}_n \to \mathrm{Aut}(\mathbb{Z}_m) \cong \mathbb{Z}_m^\times .$$

The domain of β has cardinality $n = p_{i+1} \cdots p_r$ while the codomain has cardinality $\phi(m) = (p_1 - 1) \cdots (p_i - 1)$. Since the primes are unrelated,

Proof of the theorem

(Only if:)
Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free. To see the necessity of the "no relations" condition, assume instead that $k = p_1 p_2 \cdots p_r$ and p_1 divides $p_2 - 1$. There will exist a nontrivial action $\alpha\colon \mathbb{Z}_{p_1} \to \mathrm{Aut}(\mathbb{Z}_{p_2})$ by automorphisms of $\mathbb{Z}_{p_1}$ on $\mathbb{Z}_{p_2}$, hence a nonabelian semidirect product $\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}$. Hence there is a nonabelian group $(\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}) \times \mathbb{Z}_{p_3 \cdots p_r}$ of cardinality k.

(If:)
Suppose that $|G| = p_1 \cdots p_r$, where no two primes are related.
G must have cyclic Sylow subgroups, so $G \cong \mathbb{Z}_m \rtimes \mathbb{Z}_n$ where $\gcd(m, n) = 1$. Order the prime factors of $|G|$ so that $m = p_1 \cdots p_i$ and $n = p_{i+1} \cdots p_r$. The structure of this semidirect product is determined by a homomorphism

$$\beta\colon \mathbb{Z}_n \to \mathrm{Aut}(\mathbb{Z}_m) \cong \mathbb{Z}_m^\times.$$

The domain of β has cardinality $n = p_{i+1} \cdots p_r$ while the codomain has cardinality $\phi(m) = (p_1 - 1) \cdots (p_i - 1)$. Since the primes are unrelated, $\gcd(\phi(m), n) = 1$, so Lagrange's Theorem forces β to be constant,

Proof of the theorem

(Only if:)
Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free. To see the necessity of the "no relations" condition, assume instead that $k = p_1 p_2 \cdots p_r$ and p_1 divides $p_2 - 1$. There will exist a nontrivial action $\alpha \colon \mathbb{Z}_{p_1} \to \mathrm{Aut}(\mathbb{Z}_{p_2})$ by automorphisms of $\mathbb{Z}_{p_1}$ on $\mathbb{Z}_{p_2}$, hence a nonabelian semidirect product $\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}$. Hence there is a nonabelian group $(\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}) \times \mathbb{Z}_{p_3 \cdots p_r}$ of cardinality k.

(If:)
Suppose that $|G| = p_1 \cdots p_r$, where no two primes are related.
G must have cyclic Sylow subgroups, so $G \cong \mathbb{Z}_m \rtimes \mathbb{Z}_n$ where $\gcd(m,n) = 1$. Order the prime factors of $|G|$ so that $m = p_1 \cdots p_i$ and $n = p_{i+1} \cdots p_r$. The structure of this semidirect product is determined by a homomorphism

$$\beta \colon \mathbb{Z}_n \to \mathrm{Aut}(\mathbb{Z}_m) \cong \mathbb{Z}_m^\times.$$

The domain of β has cardinality $n = p_{i+1} \cdots p_r$ while the codomain has cardinality $\phi(m) = (p_1 - 1) \cdots (p_i - 1)$. Since the primes are unrelated, $\gcd(\phi(m), n) = 1$, so Lagrange's Theorem forces β to be constant, so $G \cong \mathbb{Z}_m \rtimes \mathbb{Z}_n \cong \mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

Proof of the theorem

(Only if:)
Since $\mathcal{G} \supseteq \mathcal{A}$, any cyclic number is square-free. To see the necessity of the "no relations" condition, assume instead that $k = p_1 p_2 \cdots p_r$ and p_1 divides $p_2 - 1$. There will exist a nontrivial action $\alpha\colon \mathbb{Z}_{p_1} \to \mathrm{Aut}(\mathbb{Z}_{p_2})$ by automorphisms of $\mathbb{Z}_{p_1}$ on $\mathbb{Z}_{p_2}$, hence a nonabelian semidirect product $\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}$. Hence there is a nonabelian group $(\mathbb{Z}_{p_2} \rtimes \mathbb{Z}_{p_1}) \times \mathbb{Z}_{p_3 \cdots p_r}$ of cardinality k.

(If:)
Suppose that $|G| = p_1 \cdots p_r$, where no two primes are related.
G must have cyclic Sylow subgroups, so $G \cong \mathbb{Z}_m \rtimes \mathbb{Z}_n$ where $\gcd(m, n) = 1$. Order the prime factors of $|G|$ so that $m = p_1 \cdots p_i$ and $n = p_{i+1} \cdots p_r$. The structure of this semidirect product is determined by a homomorphism

$$\beta\colon \mathbb{Z}_n \to \mathrm{Aut}(\mathbb{Z}_m) \cong \mathbb{Z}_m^\times.$$

The domain of β has cardinality $n = p_{i+1} \cdots p_r$ while the codomain has cardinality $\phi(m) = (p_1 - 1) \cdots (p_i - 1)$. Since the primes are unrelated, $\gcd(\phi(m), n) = 1$, so Lagrange's Theorem forces β to be constant, so $G \cong \mathbb{Z}_m \rtimes \mathbb{Z}_n \cong \mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. $\square$