Krull-Schmidt-Remak Theorem, direct-sum decompositions, and G-groups

Alberto Facchini
Università di Padova

Porto, 24 March 2017

Factorization

Factorization, in its broadest sense.

Factorization

Factorization, in its broadest sense.

Uniqueness of factorization.

Factorization

Factorization, in its broadest sense.

Uniqueness of factorization.

In $\mathbb{N} := \{1, 2, 3, \dots\}$, every number a is a product of $n \geq 0$ primes, not necessarily distinct. Moreover, such a factorization is essentially unique: if

$$a = p_1 p_2 \cdots p_r \qquad \text{and} \qquad a = q_1 q_2 \cdots q_s$$

are two factorizations of a with $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ prime numbers, then $r = s$ and, relabelling if necessary, $p_i = q_i$ for $i = 1, 2, \dots, r$.

Finite (abelian) groups

Ferdinand Georg Frobenius (Berlin, 1849-1917)

Finite (abelian) groups

Ferdinand Georg Frobenius (Berlin, 1849-1917)

Frobenius and Stickelberger, "Über Gruppen von vertauschbaren Elementen", J. reine angew. Math. 86 (1879), 217–262:

Finite (abelian) groups

Ferdinand Georg Frobenius (Berlin, 1849-1917)

Frobenius and Stickelberger, "Über Gruppen von vertauschbaren Elementen", J. reine angew. Math. 86 (1879), 217–262:

any finite abelian group is a direct product of cyclic groups whose orders are powers of primes, and this powers of primes are uniquely determined by the group.

Finite (abelian) groups

Ferdinand Georg Frobenius (Berlin, 1849-1917)
Frobenius and Stickelberger, "Über Gruppen von vertauschbaren Elementen", J. reine angew. Math. 86 (1879), 217–262:
any finite abelian group is a direct product of cyclic groups whose orders are powers of primes, and this powers of primes are uniquely determined by the group.

Joseph Henry Maclagan Wedderburn (Angus, Scotland 1882 - Princeton 1948 – a Scottish mathematician, who taught at Princeton University for most of his career.)

Finite (abelian) groups

Ferdinand Georg Frobenius (Berlin, 1849-1917)
Frobenius and Stickelberger, "Über Gruppen von vertauschbaren Elementen", J. reine angew. Math. 86 (1879), 217–262:
any finite abelian group is a direct product of cyclic groups whose orders are powers of primes, and this powers of primes are uniquely determined by the group.

Joseph Henry Maclagan Wedderburn (Angus, Scotland 1882 - Princeton 1948 – a Scottish mathematician, who taught at Princeton University for most of his career.)
"On the Direct Product in the Theory of Finite Groups", Ann. of Math. 10 (1909), 173–176; Wedderburn mentions some credit is due to G. A. Miller):

Finite (abelian) groups

Ferdinand Georg Frobenius (Berlin, 1849-1917)
Frobenius and Stickelberger, "Über Gruppen von vertauschbaren Elementen", J. reine angew. Math. 86 (1879), 217–262:
any finite abelian group is a direct product of cyclic groups whose orders are powers of primes, and this powers of primes are uniquely determined by the group.

Joseph Henry Maclagan Wedderburn (Angus, Scotland 1882 - Princeton 1948 – a Scottish mathematician, who taught at Princeton University for most of his career.)
"On the Direct Product in the Theory of Finite Groups", Ann. of Math. 10 (1909), 173–176; Wedderburn mentions some credit is due to G. A. Miller): if a finite group G has two direct-product decompositions $G = G_1 \times G_2 \times \cdots \times G_t = H_1 \times H_2 \times \cdots \times H_s$ into indecomposables, then $t = s$ and there is an automorphism φ of G such that $\varphi(G_i) = H_{\sigma(i)}$ for all i's for some permutation σ of $1, 2, \ldots, n$.

Finite (abelian) groups

Ferdinand Georg Frobenius (Berlin, 1849-1917)
Frobenius and Stickelberger, "Über Gruppen von vertauschbaren Elementen", J. reine angew. Math. 86 (1879), 217–262:
any finite abelian group is a direct product of cyclic groups whose orders are powers of primes, and this powers of primes are uniquely determined by the group.

Joseph Henry Maclagan Wedderburn (Angus, Scotland 1882 - Princeton 1948 – a Scottish mathematician, who taught at Princeton University for most of his career.)
"On the Direct Product in the Theory of Finite Groups", Ann. of Math. 10 (1909), 173–176; Wedderburn mentions some credit is due to G. A. Miller): if a finite group G has two direct-product decompositions $G = G_1 \times G_2 \times \cdots \times G_t = H_1 \times H_2 \times \cdots \times H_s$ into indecomposables, then $t = s$ and there is an automorphism φ of G such that $\varphi(G_i) = H_{\sigma(i)}$ for all i's for some permutation σ of $1, 2, \ldots, n$.
The proof was not complete.

Krull-Schmidt-Remak Theorem

Robert Erich Remak (Berlin 1888 - Auschwitz 1943), German mathematician, of Jewish ancestry.

Krull-Schmidt-Remak Theorem

Robert Erich Remak (Berlin 1888 - Auschwitz 1943), German mathematician, of Jewish ancestry.

His dissertation, "Über die Zerlegung der endlichen Gruppen in indirekte unzerlegbare Faktoren" ("On the decomposition of finite groups into indirect indecomposable factors", 1911) contained a complete proof and established that if a finite group G has two direct-product decompositions into indecomposables $G = G_1 \times G_2 \times \cdots \times G_t = H_1 \times H_2 \times \cdots \times H_s$, then $t = s$ and there is a *central* automorphism φ of G such that $\varphi(G_i) = H_{\sigma(i)}$ for all i's for some permutation σ of $1, 2, \ldots, n$.

Krull-Schmidt-Remak Theorem

Robert Erich Remak (Berlin 1888 - Auschwitz 1943), German mathematician, of Jewish ancestry.

His dissertation, "Über die Zerlegung der endlichen Gruppen in indirekte unzerlegbare Faktoren" ("On the decomposition of finite groups into indirect indecomposable factors", 1911) contained a complete proof and established that if a finite group G has two direct-product decompositions into indecomposables $G = G_1 \times G_2 \times \cdots \times G_t = H_1 \times H_2 \times \cdots \times H_s$, then $t = s$ and there is a *central* automorphism φ of G such that $\varphi(G_i) = H_{\sigma(i)}$ for all i's for some permutation σ of $1, 2, \ldots, n$.

central automorphism of G = automorphism of G that induces the identity $G/\zeta(G) \to G/\zeta(G)$. Here $\zeta(G)$ denotes the center of G.

Krull-Schmidt-Remak Theorem

Otto Yulyevich Schmidt (Отто Юльевич Шмидт, Mogilëv, Russian Empire (now Belarus) 1891 - Moscow 1956).

Krull-Schmidt-Remak Theorem

Otto Yulyevich Schmidt (Отто Юльевич Шмидт, Mogilëv, Russian Empire (now Belarus) 1891 - Moscow 1956).
His father was a descendant of German settlers in Latvia, while his mother was a Latvian.

Krull-Schmidt-Remak Theorem

Otto Yulyevich Schmidt (Отто Юльевич Шмидт, Mogilëv, Russian Empire (now Belarus) 1891 - Moscow 1956).
His father was a descendant of German settlers in Latvia, while his mother was a Latvian.
Soviet mathematician, astronomer, geophysicist, statesman, academician, celebrated explorer of the Arctic, Hero of the USSR (1937), member of the Communist Party.

Krull-Schmidt-Remak Theorem

Otto Yulyevich Schmidt (Отто Юльевич Шмидт, Mogilëv, Russian Empire (now Belarus) 1891 - Moscow 1956).
His father was a descendant of German settlers in Latvia, while his mother was a Latvian.
Soviet mathematician, astronomer, geophysicist, statesman, academician, celebrated explorer of the Arctic, Hero of the USSR (1937), member of the Communist Party.

"Sur les produits directs", Bull. Soc. Math. France 41 (1913), 161–164: a simplified proof of Remak's main results.

History of the Krull-Schmidt-Remak Theorem

Wolfgang Krull (Baden-Baden 1899, Bonn 1971)

History of the Krull-Schmidt-Remak Theorem

Wolfgang Krull (Baden-Baden 1899, Bonn 1971)
"Über verallgemeinerte endliche Abelsche Gruppen", Math. Zeitschrift 23 (1925), 161–196:

History of the Krull-Schmidt-Remak Theorem

Wolfgang Krull (Baden-Baden 1899, Bonn 1971)
"Über verallgemeinerte endliche Abelsche Gruppen", Math. Zeitschrift 23 (1925), 161–196:

Abelian operator groups with ascending and descending chain conditions (operator groups = Ω-groups. Here Ω is a set and an Ω-*group* is a pair (H, φ), where H is a group and $\varphi \colon \Omega \to \mathrm{End}(H)$ is a mapping).

History of the Krull-Schmidt-Remak Theorem

Wolfgang Krull (Baden-Baden 1899, Bonn 1971)
"Über verallgemeinerte endliche Abelsche Gruppen", Math. Zeitschrift 23 (1925), 161–196:

Abelian operator groups with ascending and descending chain conditions (operator groups = Ω-groups. Here Ω is a set and an Ω-*group* is a pair (H, φ), where H is a group and $\varphi \colon \Omega \to \mathrm{End}(H)$ is a mapping).

Groups that satisfy ACC and DCC on normal subgroups ($= G$ group,

History of the Krull-Schmidt-Remak Theorem

Wolfgang Krull (Baden-Baden 1899, Bonn 1971)
"Über verallgemeinerte endliche Abelsche Gruppen", Math. Zeitschrift 23 (1925), 161–196:

Abelian operator groups with ascending and descending chain conditions (operator groups = Ω-groups. Here Ω is a set and an Ω-*group* is a pair (H, φ), where H is a group and $\varphi \colon \Omega \to \mathrm{End}(H)$ is a mapping).

Groups that satisfy ACC and DCC on normal subgroups ($=$ G group, $\mathcal{N}(G)$, partially ordered by $\subseteq$, turns out to be a modular lattice.

History of the Krull-Schmidt-Remak Theorem

Wolfgang Krull (Baden-Baden 1899, Bonn 1971)
"Über verallgemeinerte endliche Abelsche Gruppen", Math. Zeitschrift 23 (1925), 161–196:

Abelian operator groups with ascending and descending chain conditions (operator groups = Ω-groups. Here Ω is a set and an Ω-*group* is a pair (H, φ), where H is a group and $\varphi \colon \Omega \to \mathrm{End}(H)$ is a mapping).

Groups that satisfy ACC and DCC on normal subgroups ($=$ G group, $\mathcal{N}(G)$, partially ordered by $\subseteq$, turns out to be a modular lattice. If $\mathcal{N}(G)$ is a partially ordered set that satisfies the ACC and the DCC, then K-S holds for G).

History of the Krull-Schmidt-Remak Theorem

Øystein Ore (Oslo, 1899-1968)

History of the Krull-Schmidt-Remak Theorem

Øystein Ore (Oslo, 1899-1968) unified the proofs from various categories: groups, abelian operator groups, rings and algebras, the theorem of Wedderburn holds for modular lattices with descending and ascending chain conditions.

History of the Krull-Schmidt-Remak Theorem

Øystein Ore (Oslo, 1899-1968) unified the proofs from various categories: groups, abelian operator groups, rings and algebras, the theorem of Wedderburn holds for modular lattices with descending and ascending chain conditions.

Goro Azumaya (Yokohama 1920 - Bloomington, Indiana, 2010).

History of the Krull-Schmidt-Remak Theorem

Øystein Ore (Oslo, 1899-1968) unified the proofs from various categories: groups, abelian operator groups, rings and algebras, the theorem of Wedderburn holds for modular lattices with descending and ascending chain conditions.

Goro Azumaya (Yokohama 1920 - Bloomington, Indiana, 2010). "Corrections and supplementaries to my paper concerning Krull-Remak-Schmidt's theorem", Nagoya Math. J. 1 (1950), 117–124:

History of the Krull-Schmidt-Remak Theorem

Øystein Ore (Oslo, 1899-1968) unified the proofs from various categories: groups, abelian operator groups, rings and algebras, the theorem of Wedderburn holds for modular lattices with descending and ascending chain conditions.

Goro Azumaya (Yokohama 1920 - Bloomington, Indiana, 2010). "Corrections and supplementaries to my paper concerning Krull-Remak-Schmidt's theorem", Nagoya Math. J. 1 (1950), 117–124:
Let R be a ring, M_i $(i \in I)$ be a right R-module, $\mathrm{End}_R(M_i)$ a *local* ring, $M = \bigoplus_{i \in I} M_i$. Then any two direct sum decompositions of M into indecomposable direct summands are isomorphic.

An example that follows a different pattern

R any ring, M_R any right R-module.

An example that follows a different pattern

R any ring, M_R any right R-module.
M_R is *uniserial* if its lattice of submodules is linearly ordered

An example that follows a different pattern

R any ring, M_R any right R-module.
M_R is *uniserial* if its lattice of submodules is linearly ordered, that is, if for any submodules A, B of M_R either $A \subseteq B$ or $B \subseteq A$.

An example that follows a different pattern

R any ring, M_R any right R-module.
M_R is *uniserial* if its lattice of submodules is linearly ordered, that is, if for any submodules A, B of M_R either $A \subseteq B$ or $B \subseteq A$.

The endomorphism ring of a uniserial module has at most two maximal right (left) ideals:

Non-zero uniserial modules and their endomorphism rings

Theorem

[F., T.A.M.S. 1996] *Let* U_R *be a non-zero uniserial module over a ring* R*,*

Non-zero uniserial modules and their endomorphism rings

Theorem

[F., T.A.M.S. 1996] *Let U_R be a non-zero uniserial module over a ring R, $E := \mathrm{End}(U_R)$ its endomorphism ring,*

Non-zero uniserial modules and their endomorphism rings

Theorem

[F., T.A.M.S. 1996] *Let* U_R *be a non-zero uniserial module over a ring* R, $E := \mathrm{End}(U_R)$ *its endomorphism ring,* $I := \{ f \in E \mid f$ *is not injective*$\}$

Non-zero uniserial modules and their endomorphism rings

Theorem

[F., T.A.M.S. 1996] *Let* U_R *be a non-zero uniserial module over a ring* R*,* $E := \mathrm{End}(U_R)$ *its endomorphism ring,* $I := \{\, f \in E \mid f$ *is not injective* $\}$ *and* $K := \{\, f \in E \mid f$ *is not surjective* $\}$.

Non-zero uniserial modules and their endomorphism rings

Theorem

[F., T.A.M.S. 1996] *Let* U_R *be a non-zero uniserial module over a ring* R, $E := \mathrm{End}(U_R)$ *its endomorphism ring,* $I := \{ f \in E \mid f$ *is not injective*$\}$ *and* $K := \{ f \in E \mid f$ *is not surjective*$\}$. *Then* I *and* K *are two two-sided completely prime ideals of* E,

Non-zero uniserial modules and their endomorphism rings

Theorem

[F., T.A.M.S. 1996] *Let* U_R *be a non-zero uniserial module over a ring* R, $E := \mathrm{End}(U_R)$ *its endomorphism ring,* $I := \{ f \in E \mid f$ *is not injective*$\}$ *and* $K := \{ f \in E \mid f$ *is not surjective*$\}$. *Then* I *and* K *are two two-sided completely prime ideals of* E, *and every proper right ideal of* E *and every proper left ideal of* E *is contained either in* I *or in* K.

Non-zero uniserial modules and their endomorphism rings

Theorem

[F., T.A.M.S. 1996] *Let U_R be a non-zero uniserial module over a ring R, $E := \mathrm{End}(U_R)$ its endomorphism ring, $I := \{ f \in E \mid f$ is not injective$\}$ and $K := \{ f \in E \mid f$ is not surjective$\}$. Then I and K are two two-sided completely prime ideals of E, and every proper right ideal of E and every proper left ideal of E is contained either in I or in K. Moreover,*

(a) *either E is a local ring with maximal ideal $I \cup K$, or*

Non-zero uniserial modules and their endomorphism rings

Theorem

[F., T.A.M.S. 1996] *Let U_R be a non-zero uniserial module over a ring R, $E := \mathrm{End}(U_R)$ its endomorphism ring, $I := \{ f \in E \mid f$ is not injective$\}$ and $K := \{ f \in E \mid f$ is not surjective$\}$. Then I and K are two two-sided completely prime ideals of E, and every proper right ideal of E and every proper left ideal of E is contained either in I or in K. Moreover,*

(a) *either E is a local ring with maximal ideal $I \cup K$, or*

(b) *E/I and E/K are division rings, and $E/J(E) \cong E/I \times E/K$.*

Monogeny class, epigeny class

Two modules U and V are said to have

1. *the same monogeny class*, denoted $[U]_m = [V]_m$, if there exist a monomorphism $U \to V$ and a monomorphism $V \to U$;

Monogeny class, epigeny class

Two modules U and V are said to have

1. *the same monogeny class*, denoted $[U]_m = [V]_m$, if there exist a monomorphism $U \to V$ and a monomorphism $V \to U$;
2. *the same epigeny class*, denoted $[U]_e = [V]_e$, if there exist an epimorphism $U \to V$ and an epimorphism $V \to U$.

Weak Krull-Schmidt Theorem

Theorem

[F., T.A.M.S. 1996] *Let* $U_1, \dots, U_n$, $V_1, \dots, V_t$ *be* $n+t$ *non-zero uniserial right modules over a ring* R*. Then the direct sums* $U_1 \oplus \cdots \oplus U_n$ *and* $V_1 \oplus \cdots \oplus V_t$ *are isomorphic* R*-modules if and only if* $n = t$ *and there exist two permutations* σ *and* τ *of* $\{1, 2, \dots, n\}$ *such that* $[U_i]_m = [V_{\sigma(i)}]_m$ *and* $[U_i]_e = [V_{\tau(i)}]_e$ *for every* $i = 1, 2, \dots, n$*.*

Cyclically presented modules over local rings

The behavior of uniserial modules is enjoyed by other classes of modules.

Cyclically presented modules over local rings

The behavior of uniserial modules is enjoyed by other classes of modules.

First example [B. Amini, A. Amini and A. Facchini, J. Algebra 2008].

Cyclically presented modules over local rings

The behavior of uniserial modules is enjoyed by other classes of modules.

First example [B. Amini, A. Amini and A. Facchini, J. Algebra 2008].

A right module over a ring R is *cyclically presented* if it is isomorphic to R/aR for some element $a \in R$.

Cyclically presented modules over local rings

The behavior of uniserial modules is enjoyed by other classes of modules.

First example [B. Amini, A. Amini and A. Facchini, J. Algebra 2008].

A right module over a ring R is *cyclically presented* if it is isomorphic to R/aR for some element $a \in R$. For any ring R, we will denote with $U(R)$ the group of all invertible elements of R.

Cyclically presented modules over local rings

If R/aR and R/bR are cyclically presented modules over a local ring R, we say that R/aR and R/bR *have the same lower part*, and write $[R/aR]_l = [R/bR]_l$, if there exist $u, v \in U(R)$ and $r, s \in R$ with $au = rb$ and $bv = sa$.

Cyclically presented modules over local rings

If R/aR and R/bR are cyclically presented modules over a local ring R, we say that R/aR and R/bR *have the same lower part*, and write $[R/aR]_l = [R/bR]_l$, if there exist $u, v \in U(R)$ and $r, s \in R$ with $au = rb$ and $bv = sa$.

(Two cyclically presented modules over a local ring have the same lower part if and only if their Auslander-Bridger transposes have the same epigeny class.)

Cyclically presented modules and idealizer

The endomorphism ring $\mathrm{End}_R(R/aR)$ of a non-zero cyclically presented module R/aR is isomorphic to E/aR, where $E := \{\, r \in R \mid ra \in aR \,\}$ is the *idealizer* of aR.

Cyclically presented modules over local rings

$E := \{ r \in R \mid ra \in aR \}$ is the *idealizer* of aR.

Cyclically presented modules over local rings

$E := \{ r \in R \mid ra \in aR \}$ is the *idealizer* of aR.

Theorem

Let a be a non-zero non-invertible element of an arbitrary local ring R, let E be the idealizer of aR, and let E/aR be the endomorphism ring of the cyclically presented right R-module R/aR.

Cyclically presented modules over local rings

$E := \{ r \in R \mid ra \in aR \}$ is the *idealizer* of aR.

Theorem

Let a be a non-zero non-invertible element of an arbitrary local ring R, let E be the idealizer of aR, and let E/aR be the endomorphism ring of the cyclically presented right R-module R/aR. Set $I := \{ r \in R \mid ra \in aJ(R) \}$ and $K := J(R) \cap E$. Then I and K are two two-sided completely prime ideals of E containing aR, the union $(I/aR) \cup (K/aR)$ is the set of all non-invertible elements of E/aR, and every proper right ideal of E/aR and every proper left ideal of E/aR is contained either in I/aR or in K/aR.

Cyclically presented modules over local rings

$E := \{ r \in R \mid ra \in aR \}$ is the *idealizer* of aR.

Theorem

Let a be a non-zero non-invertible element of an arbitrary local ring R, let E be the idealizer of aR, and let E/aR be the endomorphism ring of the cyclically presented right R-module R/aR. Set $I := \{ r \in R \mid ra \in aJ(R) \}$ and $K := J(R) \cap E$. Then I and K are two two-sided completely prime ideals of E containing aR, the union $(I/aR) \cup (K/aR)$ is the set of all non-invertible elements of E/aR, and every proper right ideal of E/aR and every proper left ideal of E/aR is contained either in I/aR or in K/aR. Moreover, exactly one of the following two conditions holds:
(a) *Either I and K are comparable (that is, $I \subseteq K$ or $K \subseteq I$), in which case E/aR is a local ring, or*
(b) *I and K are not comparable, and in this case E/I and E/K are division rings, $J(E/aR) = (I \cap K)/aR$, and $(E/aR)/J(E/aR)$ is canonically isomorphic to the direct product $E/I \times E/K$.*

Weak Krull-Schmidt Theorem for cyclically presented modules over local rings

Theorem

(Weak Krull-Schmidt Theorem) *Let $a_1, \dots, a_n, b_1, \dots, b_t$ be $n+t$ non-invertible elements of a local ring R. Then the direct sums $R/a_1R \oplus \cdots \oplus R/a_nR$ and $R/b_1R \oplus \cdots \oplus R/b_tR$ are isomorphic right R-modules if and only if $n = t$ and there exist two permutations σ, τ of $\{1, 2, \dots, n\}$ such that $[R/a_iR]_l = [R/b_{\sigma(i)}R]_l$ and $[R/a_iR]_e = [R/b_{\tau(i)}R]_e$ for every $i = 1, 2, \dots, n$.*

Equivalence of matrices

The Weak Krull-Schmidt Theorem for cyclically presented modules has an immediate consequence as far as equivalence of matrices is concerned. Recall that two $m \times n$ matrices A and B with entries in a ring R are said to be *equivalent* matrices, denoted $A \sim B$, if there exist an $m \times m$ invertible matrix P and an $n \times n$ invertible matrix Q with entries in R (that is, matrices invertible in the rings $M_m(R)$ and $M_n(R)$, respectively) such that $B = PAQ$.

Equivalence of matrices

The Weak Krull-Schmidt Theorem for cyclically presented modules has an immediate consequence as far as equivalence of matrices is concerned. Recall that two $m \times n$ matrices A and B with entries in a ring R are said to be *equivalent* matrices, denoted $A \sim B$, if there exist an $m \times m$ invertible matrix P and an $n \times n$ invertible matrix Q with entries in R (that is, matrices invertible in the rings $M_m(R)$ and $M_n(R)$, respectively) such that $B = PAQ$. We denote by $\mathrm{diag}(a_1, \dots, a_n)$ the $n \times n$ diagonal matrix whose (i, i) entry is a_i and whose other entries are zero.

Equivalence of matrices

If R is a *commutative* local ring and $a_1, \ldots, a_n, b_1, \ldots, b_n$ are elements of R, then $\mathrm{diag}(a_1, \ldots, a_n) \sim \mathrm{diag}(b_1, \ldots, b_n)$ if and only if there exists a permutation σ of $\{1, 2, \ldots, n\}$ with a_i and $b_{\sigma(i)}$ associates for every $i = 1, 2, \ldots, n$. Here $a, b \in R$ are *associates* if they generate the same principal ideal of R.

Equivalence of matrices

If R is a *commutative* local ring and $a_1, \dots, a_n, b_1, \dots, b_n$ are elements of R, then $\mathrm{diag}(a_1, \dots, a_n) \sim \mathrm{diag}(b_1, \dots, b_n)$ if and only if there exists a permutation σ of $\{1, 2, \dots, n\}$ with a_i and $b_{\sigma(i)}$ associates for every $i = 1, 2, \dots, n$. Here $a, b \in R$ are *associates* if they generate the same principal ideal of R.
If the ring R is local, but non-necessarily commutative, we have the following result:

Proposition

Let $a_1, \dots, a_n, b_1, \dots, b_n$ be elements of a local ring R. Then $\mathrm{diag}(a_1, \dots, a_n) \sim \mathrm{diag}(b_1, \dots, b_n)$ if and only if there exist two permutations σ, τ of $\{1, 2, \dots, n\}$ with

$$[R/a_iR]_l = [R/b_{\sigma(i)}R]_l \quad \text{and} \quad [R/a_iR]_e = [R/b_{\tau(i)}R]_e$$

for every $i = 1, 2, \dots, n$.

Several other classes of modules have the same behaviour:

Several other classes of modules have the same behaviour:

Biuniform modules.

Several other classes of modules have the same behaviour:

Biuniform modules.
Kernels of morphisms between indecomposable injective modules (Ecevit, F., Koşan).

Several other classes of modules have the same behaviour:

Biuniform modules.
Kernels of morphisms between indecomposable injective modules (Ecevit, F., Koşan).
Couniformly presented modules (F., Girardi).

Several other classes of modules have the same behaviour:

Biuniform modules.
Kernels of morphisms between indecomposable injective modules (Ecevit, F., Koşan).
Couniformly presented modules (F., Girardi).
Auslander-Bridger modules (F., Girardi).

Several other classes of modules have the same behaviour:

Biuniform modules.
Kernels of morphisms between indecomposable injective modules (Ecevit, F., Koşan).
Couniformly presented modules (F., Girardi).
Auslander-Bridger modules (F., Girardi).
Also for direct products (Alahmadi, F., J. Algebra 2015).

Other algebraic structures?

Other algebraic structures, not only modules, could have the same behavior.

Groups, Lie algebras, G-groups,...

Algebras

K a commutative ring with identity

Algebras

K a commutative ring with identity

M a K-module

Algebras

K a commutative ring with identity

M a K-module with a K-bilinear mapping $M \times M \to M$ is a K-*algebra* (not necessarily associative).

Algebras

K a commutative ring with identity

M a K-module with a K-bilinear mapping $M \times M \to M$ is a K*-algebra* (not necessarily associative).

If M is a K-algebra and we endow M with the multiplication $M \times M \to M$, $(x, y) \mapsto yx$, we get another algebra, called its *opposite algebra*, denoted by M^{op}.

Rings

Rings are the *associative* K-algebras (for $K = \mathbb{Z}$).

Rings

Rings are the *associative* K-algebras (for $K = \mathbb{Z}$).

(a) The main example of ring is the endomorphism ring of any abelian group (or the endomorphism ring of any K-module).

Rings

Rings are the *associative* K-algebras (for $K = \mathbb{Z}$).

(a) The main example of ring is the endomorphism ring of any abelian group (or the endomorphism ring of any K-module).

(b) More generally, for any ring R and any $a \in R$, left multiplication by a is an abelian group endomorphism $\lambda_a \colon R \to R$.

Rings

Rings are the *associative* K-algebras (for $K = \mathbb{Z}$).

(a) The main example of ring is the endomorphism ring of any abelian group (or the endomorphism ring of any K-module).

(b) More generally, for any ring R and any $a \in R$, left multiplication by a is an abelian group endomorphism $\lambda_a \colon R \to R$.

(c) There is a canonical ring morphism $\lambda \colon R \to \mathrm{End}_{\mathrm{Ab}}(R)$, $\lambda \colon a \mapsto \lambda_a$.

R-modules

Correspondingly, we have:

R-modules

Correspondingly, we have:

(d) *Left R-modules* $=$ abelian groups G with a ring homomorphism $\lambda\colon R \to \mathrm{End}_{\mathrm{Ab}}(G)$.

R-modules

Correspondingly, we have:

(d)	*Left R-modules*	$=$	abelian groups G with a ring homomorphism $\lambda\colon R \to \mathrm{End}_{\mathrm{Ab}}(G)$.
(e)	*Right R-modules*	$=$	abelian groups G with a ring antihomomorphism $\rho\colon R \to \mathrm{End}_{\mathrm{Ab}}(G)$

R-modules

Correspondingly, we have:

(d)	*Left R-modules*	$=$	abelian groups G with a ring homomorphism $\lambda\colon R \to \mathrm{End}_{\mathrm{Ab}}(G)$.
(e)	*Right R-modules*	$=$	abelian groups G with a ring antihomomorphism $\rho\colon R \to \mathrm{End}_{\mathrm{Ab}}(G)$, or equivalently
		$=$	abelian groups G with a ring homomorphism $\rho\colon R^{\mathrm{op}} \to \mathrm{End}_{\mathrm{Ab}}(G)$.

Lie algebras

They are the K-algebras with $[x, x] = 0$ and the Jacobi identity.

Lie algebras

They are the K-algebras with $[x, x] = 0$ and the Jacobi identity. The first example is, for any K-module M, the algebra $\mathfrak{gl}(M)$ of all K-module endomorphisms of M with multiplication
$[f, g] = fg - gf$.

Lie algebras

They are the K-algebras with $[x, x] = 0$ and the Jacobi identity.
The first example is, for any K-module M, the algebra $\mathfrak{gl}(M)$ of all K-module endomorphisms of M with multiplication
$[f, g] = fg - gf$. But:
(a) The main example of Lie algebra is the algebra of derivations $\mathrm{Der}_K(M)$ of any K-algebra M.

Lie algebras

They are the K-algebras with $[x, x] = 0$ and the Jacobi identity. The first example is, for any K-module M, the algebra $\mathfrak{gl}(M)$ of all K-module endomorphisms of M with multiplication $[f, g] = fg - gf$. But:

(a) The main example of Lie algebra is the algebra of derivations $\mathrm{Der}_K(M)$ of any K-algebra M.

A *derivation* of a K-algebra M is a mapping $D\colon M \to M$ that is K-linear and is such that $D(xy) = (Dx)y + x(Dx)$ for every $x, y \in M$.

Lie algebras

They are the K-algebras with $[x, x] = 0$ and the Jacobi identity.
The first example is, for any K-module M, the algebra $\mathfrak{gl}(M)$ of all K-module endomorphisms of M with multiplication
$[f, g] = fg - gf$. But:
(a) The main example of Lie algebra is the algebra of derivations $\mathrm{Der}_K(M)$ of any K-algebra M.
A *derivation* of a K-algebra M is a mapping $D \colon M \to M$ that is K-linear and is such that $D(xy) = (Dx)y + x(Dx)$ for every
$x, y \in M$.
If D_1, D_2 are derivations of an algebra M, then $D_1 D_2 - D_2 D_1$ is a derivation of M.

Lie algebras

They are the K-algebras with $[x, x] = 0$ and the Jacobi identity. The first example is, for any K-module M, the algebra $\mathfrak{gl}(M)$ of all K-module endomorphisms of M with multiplication $[f, g] = fg - gf$. But:

(a) The main example of Lie algebra is the algebra of derivations $\mathrm{Der}_K(M)$ of any K-algebra M.

A *derivation* of a K-algebra M is a mapping $D\colon M \to M$ that is K-linear and is such that $D(xy) = (Dx)y + x(Dx)$ for every $x, y \in M$.

If D_1, D_2 are derivations of an algebra M, then $D_1 D_2 - D_2 D_1$ is a derivation of M.

(b) If L is any Lie algebra, the mapping $\mathrm{ad}\, x := [x, -]\colon L \to L,\ y \mapsto [x, y]$, is a derivation of L for every $x \in L$.

Lie algebras

They are the K-algebras with $[x, x] = 0$ and the Jacobi identity.
The first example is, for any K-module M, the algebra $\mathfrak{gl}(M)$ of all K-module endomorphisms of M with multiplication
$[f, g] = fg - gf$. But:
(a) The main example of Lie algebra is the algebra of derivations $\mathrm{Der}_K(M)$ of any K-algebra M.
A *derivation* of a K-algebra M is a mapping $D\colon M \to M$ that is K-linear and is such that $D(xy) = (Dx)y + x(Dx)$ for every $x, y \in M$.
If D_1, D_2 are derivations of an algebra M, then $D_1D_2 - D_2D_1$ is a derivation of M.
(b) If L is any Lie algebra, the mapping
$\operatorname{ad} x := [x, -]\colon L \to L,\ y \mapsto [x, y]$, is a derivation of L for every $x \in L$.
(c) There is a canonical Lie algebra morphism $L \to \mathrm{Der}_K(L)$, $x \mapsto \operatorname{ad} x$.

L-modules, L a Lie algebra

Correspondingly, we have:

L-modules, L a Lie algebra

Correspondingly, we have:

(d) *Left L-modules* $=$ K-modules M with a Lie algebra homomorphism $L \to \mathfrak{gl}(M)$.

L-modules, L a Lie algebra

Correspondingly, we have:

(d)	*Left L-modules*	$=$	K-modules M with a Lie algebra homomorphism $L \to \mathfrak{gl}(M)$.
(e)	*Right L-modules*	$=$	K-modules M with a Lie algebra antihomomorphism $L \to \mathfrak{gl}(M)$

L-modules, L a Lie algebra

Correspondingly, we have:

(d)	*Left L-modules*	=	K-modules M with a Lie algebra homomorphism $L \to \mathfrak{gl}(M)$.
(e)	*Right L-modules*	=	K-modules M with a Lie algebra antihomomorphism $L \to \mathfrak{gl}(M)$, or equivalently
		=	K-modules M with a Lie algebra homomorphism $L^{\mathrm{op}} \to \mathfrak{gl}(M)$.

L-modules, L a Lie algebra

Correspondingly, we have:

(d) *Left L-modules* $=$ K-modules M with a Lie algebra homomorphism $L \to \mathfrak{gl}(M)$.

(e) *Right L-modules* $=$ K-modules M with a Lie algebra antihomomorphism $L \to \mathfrak{gl}(M)$, or equivalently

$=$ K-modules M with a Lie algebra homomorphism $L^{\text{op}} \to \mathfrak{gl}(M)$. But:

(1) the opposite of any Lie algebra L is a Lie algebra L^{op};

L-modules, L a Lie algebra

Correspondingly, we have:

(d) *Left L-modules* = K-modules M with a Lie algebra homomorphism $L \to \mathfrak{gl}(M)$.

(e) *Right L-modules* = K-modules M with a Lie algebra antihomomorphism $L \to \mathfrak{gl}(M)$, or equivalently
= K-modules M with a Lie algebra homomorphism $L^{\mathrm{op}} \to \mathfrak{gl}(M)$. But:

(1) the opposite of any Lie algebra L is a Lie algebra L^{op};
(2) the mapping $L \to L^{\mathrm{op}}$, defined by $x \in L \mapsto -x$, is an isomorphism of L onto L^{op}. So there is no need to introduce/distinguish left modules or right modules, they form isomorphic categories.

Groups

(a) The main example is the automorphism group $\mathrm{Aut}(A)$ of any algebraic structure A.

Groups

(a) The main example is the automorphism group Aut(A) of any algebraic structure A.
(b) If G is any group, the mapping $\alpha_g \colon G \to G, \ \alpha_g \colon h \mapsto ghg^{-1}$, is an automorphism of G (the *inner automorphism*) for every $g \in G$.

Groups

(a) The main example is the automorphism group $\mathrm{Aut}(A)$ of any algebraic structure A.
(b) If G is any group, the mapping $\alpha_g \colon G \to G,\ \alpha_g \colon h \mapsto ghg^{-1}$, is an automorphism of G (the *inner automorphism*) for every $g \in G$.
(c) There is a canonical group morphism $G \to \mathrm{Aut}(G)$, $g \mapsto \alpha_g$.

G-groups

Correspondingly, we have:

G-groups

Correspondingly, we have:

(d) *Left G-groups* $=$ groups H with a group homomorphism $G \to \mathrm{Aut}(H)$.

G-groups

Correspondingly, we have:

(d)	*Left G-groups*	$=$	groups H with a group homomorphism $G \to \mathrm{Aut}(H)$.
(e)	*Right G-groups*	$=$	groups H with a group antihomomorphism $G \to \mathrm{Aut}(H)$,

G-groups

Correspondingly, we have:

(d) *Left G-groups* = groups H with a group homomorphism $G \to \mathrm{Aut}(H)$.

(e) *Right G-groups* = groups H with a group antihomomorphism $G \to \mathrm{Aut}(H)$, or equivalently
= groups H with a group homomorphism $G^{\mathrm{op}} \to \mathrm{Aut}(H)$.

G-groups

Correspondingly, we have:

(d)	*Left G-groups*	$=$	groups H with a group homomorphism $G \to \mathrm{Aut}(H)$.
(e)	*Right G-groups*	$=$	groups H with a group antihomomorphism $G \to \mathrm{Aut}(H)$, or equivalently
		$=$	groups H with a group homomorphism $G^{\mathrm{op}} \to \mathrm{Aut}(H)$.

Now the opposite of any group G is a group G^{op} and the mapping $G \to G^{\mathrm{op}}$, defined by $g \in G \mapsto g^{-1}$, is an isomorphism of G onto G^{op}. So there is no need to distinguish left G-groups from right G-groups, they form isomorphic categories.

G-groups

Correspondingly, we have:

(d) *Left G-groups* = groups H with a group homomorphism $G \to \mathrm{Aut}(H)$.

(e) *Right G-groups* = groups H with a group antihomomorphism $G \to \mathrm{Aut}(H)$, or equivalently = groups H with a group homomorphism $G^{\mathrm{op}} \to \mathrm{Aut}(H)$.

Now the opposite of any group G is a group G^{op} and the mapping $G \to G^{\mathrm{op}}$, defined by $g \in G \mapsto g^{-1}$, is an isomorphism of G onto G^{op}. So there is no need to distinguish left G-groups from right G-groups, they form isomorphic categories.

The notion of G-group is classical

G-groups

Correspondingly, we have:

(d) *Left G-groups* = groups H with a group homomorphism $G \to \mathrm{Aut}(H)$.

(e) *Right G-groups* = groups H with a group antihomomorphism $G \to \mathrm{Aut}(H)$, or equivalently = groups H with a group homomorphism $G^{\mathrm{op}} \to \mathrm{Aut}(H)$.

Now the opposite of any group G is a group G^{op} and the mapping $G \to G^{\mathrm{op}}$, defined by $g \in G \mapsto g^{-1}$, is an isomorphism of G onto G^{op}. So there is no need to distinguish left G-groups from right G-groups, they form isomorphic categories.

The notion of G-group is classical, and sometimes G is called an *operator group* on H [Suzuki, Group Theory I, 1982, Definition 8.1].

G-groups

Let G be a group. A *(left) G-group* is a pair (H, φ), where H is a group and $\varphi\colon G \to \mathrm{Aut}(H)$ is a group homomorphism.

G-groups

Let G be a group. A *(left)* G*-group* is a pair (H, φ), where H is a group and $\varphi\colon G \to \mathrm{Aut}(H)$ is a group homomorphism.
Equivalently, a G-group is a group H endowed with a mapping $\cdot\colon G \times H \to H$, $(g, h) \mapsto gh$, called *left scalar multiplication*, such that
(a) $g(hh') = (gh)(gh')$
(b) $(gg')h = g(g'h)$
(c) $1_G h = h$
for every $g, g' \in G$ and every $h, h' \in H$.

The category G-**Grp**

Objects of G-**Grp**: all pairs (H, φ), where H is any group and $\varphi \colon G \to \mathrm{Aut}(H)$ is a group homomorphism.

The category G-**Grp**

Objects of G-**Grp**: all pairs (H, φ), where H is any group and $\varphi\colon G \to \mathrm{Aut}(H)$ is a group homomorphism.

Strict analogy with left modules over a ring R:
Objects of R-Mod: all pairs (H, φ), where H is any abelian group and $\varphi\colon R \to \mathrm{End}(H)$ is a ring homomorphism.

The category G-**Grp**

A special object of G-**Grp** is the *regular G-group* (G, α). Here $\alpha\colon G \to \mathrm{Aut}(G)$, $g \mapsto \alpha_g$, where $\alpha_g(x) = gxg^{-1}$ for every $g, x \in G$.

The category G-**Grp**

A special object of G-**Grp** is the *regular* G*-group* (G, α). Here $\alpha\colon G \to \mathrm{Aut}(G)$, $g \mapsto \alpha_g$, where $\alpha_g(x) = gxg^{-1}$ for every $g, x \in G$.

The regular G-group (G, α) plays, in the category G-**Grp**, a role pretty similar to the role of the regular module ${}_R R$ in the category R-Mod.

The category G-**Grp**

Subobjects of the regular G-group G = normal subgroups of G

The category G-**Grp**

Subobjects of the regular G-group G = normal subgroups of G
(Subobjects of the regular R-module ${}_R R$ = left ideals of R)

The category G-**Grp**

Subobjects of the regular G-group G = normal subgroups of G
(Subobjects of the regular R-module ${}_R R$ = left ideals of R)

Quotient objects of the regular G-group G = factor groups G/M

The category G-**Grp**

Subobjects of the regular G-group G = normal subgroups of G
(Subobjects of the regular R-module ${}_RR$ = left ideals of R)

Quotient objects of the regular G-group G = factor groups G/M
(Quotient objects of the regular R-module ${}_RR$ = cyclic right R-modules)

The category G-**Grp**

Subobjects of the regular G-group G = normal subgroups of G
(Subobjects of the regular R-module ${}_RR$ = left ideals of R)

Quotient objects of the regular G-group G = factor groups G/M
(Quotient objects of the regular R-module ${}_RR$ = cyclic right R-modules)

Normal homomorphisms $f\colon H \to H'$, $f(gh) = gf(h)$, are morphisms in the category G-**Grp**

The category G-**Grp**

G-**Grp** is a semi-abelian category in the sense of Janelidze, Márki and Tholen.

The category G-**Grp**

G-**Grp** is a semi-abelian category in the sense of Janelidze, Márki and Tholen.

We determine free G-groups and show that the injective objects in the category G-**Grp** are only the trivial groups, like in the case of the category **Grp** of groups.

The category G-**Grp**

G-**Grp** is a semi-abelian category in the sense of Janelidze, Márki and Tholen.

We determine free G-groups and show that the injective objects in the category G-**Grp** are only the trivial groups, like in the case of the category **Grp** of groups.

The category G-**Set** of G-sets is a Boolean topos (which does not satisfy the Axiom of Choice), and the category of G-groups is the category of groups of that topos (Janelidze).

Modules vs groups

module M_R, $E := \mathrm{End}(M_R)$	group H
idempotents in E $\updownarrow$ $\{ (A, B) \mid A, B \leq M_R, M_R = A \oplus B \}$	idempotents in $\mathrm{End}(H)$ $\updownarrow$ $\{ (A, B) \mid A, B \leq H, H = A \rtimes B \}$
	normal idempotents in $\mathrm{End}(H)$ $\updownarrow$ $\{ (A, B) \mid A, B \leq H, H = A \times B \}$

Modules vs groups

Ω-groups G-sets

\   /

G-groups

$E\text{-}\mathrm{Mod}$ ${}_E E$ regular module

${}_G G$ regular G-group

$E\text{-}\mathrm{Mod}$ is the category
in which it is natural to study
direct-sum decompositions
of ${}_E E$
$=$ direct-sum decompositions
of M_R

G-**Grp** is the category
in which it is natural to study
direct-product decompositions
of G

$\mathrm{End}_{G\text{-}\mathbf{Grp}}(G) =$
$=\{$*normal* endomorphisms of $G\}$
$\mathrm{Aut}_{G\text{-}\mathbf{Grp}}(G) =$
$=\{$*central* automorphisms of $G\}$

Factorisation of polynomials

A different application: uniqueness of factorisation of polynomials into irreducible polynomials.

Factorisation of polynomials

A different application: uniqueness of factorisation of polynomials into irreducible polynomials.
Uniqueness of factorisation: UFD.

Factorisation of polynomials

A different application: uniqueness of factorisation of polynomials into irreducible polynomials.

Uniqueness of factorisation: UFD. The standard definition is:

Factorisation of polynomials

A different application: uniqueness of factorisation of polynomials into irreducible polynomials.

Uniqueness of factorisation: UFD. The standard definition is:

A *unique factorisation domain* R (UFD) is a commutative integral domain R in which:

(i) every element $a \in R$, $a \neq 0$ and a non-invertible, is a product of finitely many irreducible elements of R;

(ii) if $p_1, \ldots, p_n, q_1, \ldots, q_m$ are irreducible elements of R and $p_1 \ldots p_n = q_1 \ldots q_m$, then $n = m$ and there exists a permutation σ of $\{1, 2, \ldots, n\}$ such that p_i and $q_{\sigma(i)}$ are associates for every $i = 1, 2, \ldots, n$.

Primes and irreducible elements

In an integral domain R, every prime element is irreducible.

Primes and irreducible elements

In an integral domain R, every prime element is irreducible. If R is a UFD, the converse holds. More precisely:
An integral domain R is a UFD if and only if every irreducible is prime and R satisfies ascending chain condition on principal ideals, if and only if every irreducible is prime and R is atomic (every element $a \in R$, $a \neq 0$ and a non-invertible, is a product of finitely many irreducible elements of R.)

Associated elements

Proposition

The following conditions are equivalent for two prime elements a, b of a commutative integral domain R:

(i) $a = bu$ *for some invertible element* $u \in R$.

(ii) $aR = bR$.

(iii) $R/aR \cong R/bR$.

(iv) $[R/aR]_m = [R/bR]_m$.

(v) $[R/aR]_e = [R/bR]_e$.

(vi) $[R/aR]_l = [R/bR]_l$.

Commutative polynomials, non-commutative polynomials

The ring $\mathbb{Z}[x_1, \ldots, x_n]$.

Commutative polynomials, non-commutative polynomials

The ring $\mathbb{Z}[x_1, \ldots, x_n]$. Coefficients in the ring of integers $\mathbb{Z}$.
n commuting indeterminates $x_1, \ldots, x_n$.

Commutative polynomials, non-commutative polynomials

The ring $\mathbb{Z}[x_1, \ldots, x_n]$. Coefficients in the ring of integers $\mathbb{Z}$.
n commuting indeterminates $x_1, \ldots, x_n$.

It is a UFD.

Non-commutative polynomials

The ring $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$.

Non-commutative polynomials

The ring $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$. Coefficients in the ring of integers $\mathbb{Z}$.
n non-commuting indeterminates $x_1, \ldots, x_n$.

Non-commutative polynomials

The ring $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$. Coefficients in the ring of integers $\mathbb{Z}$. n non-commuting indeterminates $x_1, \ldots, x_n$. $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$ is the free ring on n objects.

Non-commutative polynomials

The ring $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$. Coefficients in the ring of integers $\mathbb{Z}$. n non-commuting indeterminates $x_1, \ldots, x_n$. $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$ is the free ring on n objects.

Do polynomials in $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$ factorise in a unique way as product of irreducible polynomials?

Non-commutative polynomials

The ring $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$. Coefficients in the ring of integers $\mathbb{Z}$. n non-commuting indeterminates $x_1, \ldots, x_n$. $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$ is the free ring on n objects.

Do polynomials in $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$ factorise in a unique way as product of irreducible polynomials?

$\mathbb{Z}\langle x_1, \ldots, x_n \rangle$ is atomic: polynomials do factorise as product of irreducible polynomials. The invertible elements in $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$ are only 1 and -1.

Non-commutative polynomials

Does a polynomial in $\mathbb{Z}\langle x_1, \ldots, x_n\rangle$ factorise as a product of irreducible polynomials in a unique way up to the sign of the irreducible factors?

Non-commutative polynomials

Does a polynomial in $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$ factorise as a product of irreducible polynomials in a unique way up to the sign of the irreducible factors?

No: $x(yx-2) = (xy-2)x$ in the ring $\mathbb{Z}\langle x, y \rangle$.

The Brungs Theorem

Theorem

Every polynomial in $R := \mathbb{Z}\langle x_1, \ldots, x_n \rangle$ *factorises as a product of irreducible polynomials. Moreover, if* $p_1, \ldots, p_n, q_1, \ldots, q_m$ *are irreducible polynomials in* R *and* $p_1 \ldots p_n = q_1 \ldots q_m$*, then* $n = m$ *and there exists a permutation* σ *of* $\{1, 2, \ldots, n\}$ *such that* $[R/p_i R]_m = [R/q_{\sigma(i)} R]_m$. □

The Brungs Theorem

Theorem

Every polynomial in $R := \mathbb{Z}\langle x_1, \ldots, x_n\rangle$ *factorises as a product of irreducible polynomials. Moreover, if* $p_1, \ldots, p_n, q_1, \ldots, q_m$ *are irreducible polynomials in* R *and* $p_1 \ldots p_n = q_1 \ldots q_m$*, then* $n = m$ *and there exists a permutation* σ *of* $\{1, 2, \ldots, n\}$ *such that* $[R/p_iR]_m = [R/q_{\sigma(i)}R]_m$. $\square$

For $x(yx-2) = (xy-2)x$ in the ring $R = \mathbb{Z}\langle x, y\rangle$,
$[R/(xy-2)R]_m = [R/(yx-2)R]_m$,
because $\lambda_y \colon R/(xy-2)R \to R/(yx-2)R$ and
$\lambda_x \colon R/(yx-2)R \to R/(xy-2)R$ are monomorphisms.

Polynomials with non-negative coefficients

Now consider $\mathbb{N}_0[x]$, set of all polynomials in $\mathbb{Z}[x]$ whose coefficients are all ≥ 0.

Polynomials with non-negative coefficients

Now consider $\mathbb{N}_0[x]$, set of all polynomials in $\mathbb{Z}[x]$ whose coefficients are all ≥ 0.
It is not a ring (it is a commutative semiring), it is a semigroup with respect to multiplication. In $\mathbb{N}_0[x]$ every element is a finite product of atoms (= polynomials irreducible in $\mathbb{N}_0[x]$). The unique invertible element is 1. Does a polynomial in $\mathbb{N}_0[x]$ factorise as a product of irreducible polynomials in a unique way?

Polynomials with non-negative coefficients

Now consider $\mathbb{N}_0[x]$, set of all polynomials in $\mathbb{Z}[x]$ whose coefficients are all ≥ 0.
It is not a ring (it is a commutative semiring), it is a semigroup with respect to multiplication. In $\mathbb{N}_0[x]$ every element is a finite product of atoms ($=$ polynomials irreducible in $\mathbb{N}_0[x]$). The unique invertible element is 1. Does a polynomial in $\mathbb{N}_0[x]$ factorise as a product of irreducible polynomials in a unique way?

No. Example:

Polynomials with non-negative coefficients

Now consider $\mathbb{N}_0[x]$, set of all polynomials in $\mathbb{Z}[x]$ whose coefficients are all ≥ 0.
It is not a ring (it is a commutative semiring), it is a semigroup with respect to multiplication. In $\mathbb{N}_0[x]$ every element is a finite product of atoms ($=$ polynomials irreducible in $\mathbb{N}_0[x]$). The unique invertible element is 1. Does a polynomial in $\mathbb{N}_0[x]$ factorise as a product of irreducible polynomials in a unique way?

No. Example:
From the theory of cyclotomic polynomials we know that the factorization of $x^n - 1$ in the UFD $\mathbb{Q}[x]$ is $x^n - 1 = \prod_{d|n} \Phi_d(x)$, where $\Phi_d(x)$ is the d-th cyclotomic polynomial. Here
$\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$,
$\Phi_4(x) = x^2 + 1$, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$.

Polynomials with non-negative coefficients

Thus $x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) =$

Polynomials with non-negative coefficients

Thus $x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$, so we have a factorization $x^5+x^4+x^3+x^2+x+1 = (x+1)(x^2+x+1)(x^2-x+1)$ into irreducibles in $\mathbb{Q}[x]$. Multiplying the first factor and the last one, we get that $(x+1)(x^2-x+1) = x^3+1 \in \mathbb{N}_0[x]$, and multiplying the last two factors we get that $(x^2+x+1)(x^2-x+1) = x^4+x^2+1 \in \mathbb{N}_0[x]$. Thus we get two essentially different factorizations $(x^3+1)(x^2+x+1) = (x+1)(x^4+x^2+1)$ of $x^5+x^4+x^3+x^2+x+1$ into irreducibles of $\mathbb{N}_0[x]$. Thus factorizations into irreducibles in $\mathbb{N}_0[x]$ are not unique (but every polynomial in $\mathbb{N}_0[x]$ has only finitely many distinct factorizations into irreducibles).

An application to direct-product decompositions of partially ordered set.

The Krull-Schmidt theorem does not hold for finite partially ordered sets (Nakayama and Hashimoto).

An application to direct-product decompositions of partially ordered set.

The Krull-Schmidt theorem does not hold for finite partially ordered sets (Nakayama and Hashimoto). In fact:

An application to direct-product decompositions of partially ordered set.

The Krull-Schmidt theorem does not hold for finite partially ordered sets (Nakayama and Hashimoto). In fact:
(1) The category of partially ordered sets has coproducts (disjoint unions) and products (direct products with the component-wise order).

An application to direct-product decompositions of partially ordered set.

The Krull-Schmidt theorem does not hold for finite partially ordered sets (Nakayama and Hashimoto). In fact:
(1) The category of partially ordered sets has coproducts (disjoint unions) and products (direct products with the component-wise order).
(2) This is a distributive category:
$X \times (Y \dot{\cup} Z) \cong (X \times Y) \dot{\cup} (X \times Z)$.

An application to direct-product decompositions of partially ordered set.

The Krull-Schmidt theorem does not hold for finite partially ordered sets (Nakayama and Hashimoto). In fact:
(1) The category of partially ordered sets has coproducts (disjoint unions) and products (direct products with the component-wise order).
(2) This is a distributive category:
$X \times (Y \dot{\cup} Z) \cong (X \times Y) \dot{\cup} (X \times Z)$.
(3) Let $L = \{0, 1\}$ be the partially ordered set with two elements $0 < 1$.

An application to direct-product decompositions of partially ordered set.

The Krull-Schmidt theorem does not hold for finite partially ordered sets (Nakayama and Hashimoto). In fact:
(1) The category of partially ordered sets has coproducts (disjoint unions) and products (direct products with the component-wise order).
(2) This is a distributive category:
$X \times (Y \dot{\cup} Z) \cong (X \times Y) \dot{\cup} (X \times Z)$.
(3) Let $L = \{0, 1\}$ be the partially ordered set with two elements $0 < 1$.
(4) For every $n \geq 0$, L^n is a connected partially ordered set with 2^n elements and its automorphism group is the symmetric group S_n.

An application to direct-product decompositions of partially ordered set.

The Krull-Schmidt theorem does not hold for finite partially ordered sets (Nakayama and Hashimoto). In fact:
(1) The category of partially ordered sets has coproducts (disjoint unions) and products (direct products with the component-wise order).
(2) This is a distributive category:
$X \times (Y \dot{\cup} Z) \cong (X \times Y) \dot{\cup} (X \times Z)$.
(3) Let $L = \{0, 1\}$ be the partially ordered set with two elements $0 < 1$.
(4) For every $n \geq 0$, L^n is a connected partially ordered set with 2^n elements and its automorphism group is the symmetric group S_n.
(5) Two essentially different direct-product decompositions of the partially ordered set $1 \dot{\cup} L \dot{\cup} L^2 \dot{\cup} L^3 \dot{\cup} L^4 \dot{\cup} L^5$ into indecomposable partially ordered sets are given by
$(L^3 \dot{\cup} 1) \times (L^2 \dot{\cup} L \dot{\cup} 1) \cong (L \dot{\cup} 1) \times (L^4 \dot{\cup} L^2 \dot{\cup} 1)$

Further current directions of investigation

(1) (with Federico Campanini) Description of the behaviour, as far as direct-sum decompositions are concerned, of short exact sequences

$$0 \longrightarrow A_R \xrightarrow{\alpha} B_R \xrightarrow{\beta} C_R \longrightarrow 0, \tag{1}$$

where A_r and C_R are uniserial modules. Their endomorphism ring in the category of all short exact sequences has at most four maximal ideals, and their isomorphism types are described by four invariants $[B]_{m,l}$, $[B]_{e,l}$, $[B]_{m,u}$, $[B]_{e,u}$.

Further current directions of investigation

(1) (with Federico Campanini) Description of the behaviour, as far as direct-sum decompositions are concerned, of short exact sequences

$$0 \longrightarrow A_R \xrightarrow{\alpha} B_R \xrightarrow{\beta} C_R \longrightarrow 0, \qquad (1)$$

where A_r and C_R are uniserial modules. Their endomorphism ring in the category of all short exact sequences has at most four maximal ideals, and their isomorphism types are described by four invariants $[B]_{m,l},\ [B]_{e,l},\ [B]_{m,u},\ [B]_{e,u}$.

(2) (with María José Arroyo Paniagua) Description of the behaviour, as far as direct-sum decompositions are concerned, of abelian ideals in groups.

Further current directions of investigation

(3) (with Zahra Nazemian) Study of the factorizations $A = A_1 \dots A_n$ of a right ideal A of non-necessarily commutative ring R as a product of right ideals $A_1, \dots, A_n$, with $R/A \cong R/A_1 \oplus \cdots \oplus R/A_n$ and the right modules $R/A_1, \dots, R/A_n$ uniserial. The main example is $R =$ a Dedekind domain.

(4) (with Michael Hoefnagel) Krull-Schmidt theorem in distributive categories. Recall that a category $\mathcal{C}$ with finite products $(-) \times (-)$ and coproducts $(-) + (-)$ is called *(finitary) distributive* if, for any objects X, Y, Z of $\mathcal{C}$, the canonical morphism

$$X \times Y + X \times Z \to X \times (Y + Z)$$

is an isomorphism.