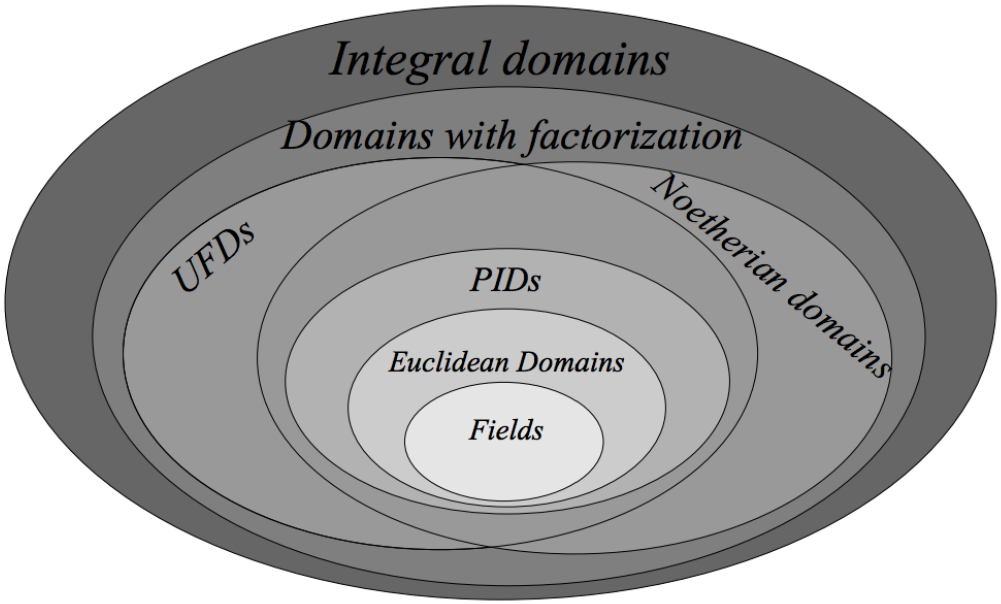
Commutative Rings



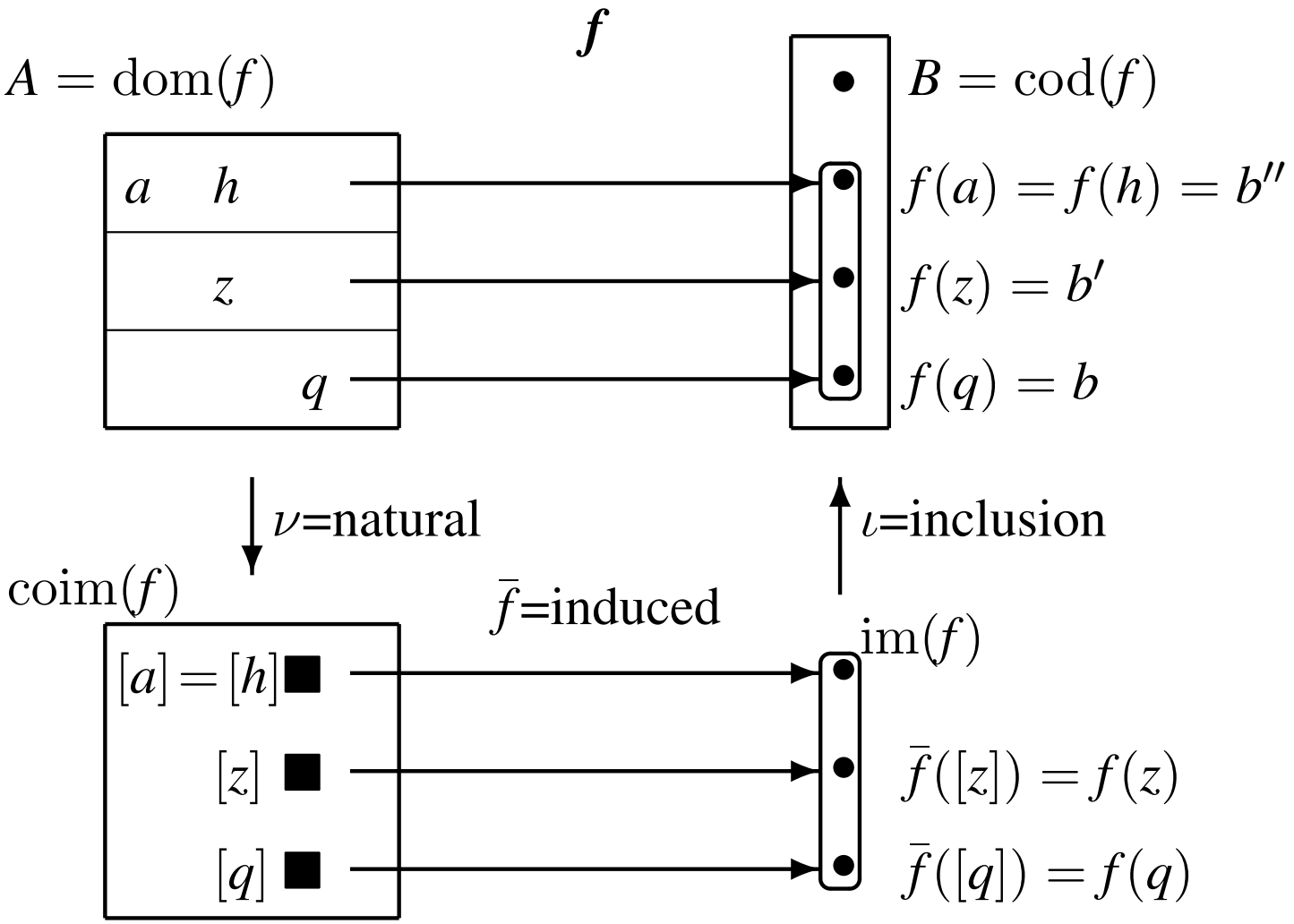
Language + laws

$\mathbf{R} = \langle R; \cdot, +, -, 0, 1 \rangle \ (= R)$

1. $\langle R; +, -, 0 \rangle$ is an abelian group.
   1. $(\forall x)(\forall y)(\forall z)(x + (y + z) = (x + y) + z)$
   2. $(\forall x)(x + 0 = x = 0 + x)$
   3. $(\forall x)(x + (-x) = 0 = (-x) + x)$
2. $\langle R; \cdot, 1 \rangle$ is a commutative monoid.
   1. $(\forall x)(\forall y)(\forall z)(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
   2. $(\forall x)(\forall y)(x \cdot y = y \cdot x)$
   3. $(\forall x)(x \cdot 1 = x = 1 \cdot x)$
3. distributive laws hold.
   1. $(\forall x)(\forall y)(\forall z)(x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
   2. $(\forall x)(\forall y)(\forall z)((x + y) \cdot z = (x \cdot z) + (y \cdot z))$

(Choose language so that the formulas, substructures, and morphisms are what you want them to be.)

Comparisons of sets/structures



Comparisons of sets/structures

1. The *image* of f is $\operatorname{im}(f) = f[A] = \{b \in B \ : \ \exists a \in A(f(a) = b)\}$. The image of a subset $U \subseteq A$ is $f[U] = \{b \in B \ : \ \exists u \in U(f(u) = b)\}$.
2. The *preimage* or *inverse image* of a subset $V \subseteq B$ is $f^{-1}[V] = \{a \in A \ : \ f(a) \in V\}$.
3. The preimage of a singleton $\{b\}$ is written $f^{-1}(b)$ and sometimes called the *fiber* of f *over* b. The fiber containing the element a is sometimes written $[a]$.
4. The *coimage* of f is the set $\operatorname{coim}(f) = \{f^{-1}(b) \ : \ b \in \operatorname{im}(f)\}$ of all nonempty fibers.
5. The *kernel* of f is $\ker(f) = \{(a, a') \in A^2 \ : \ f(a) = f(a')\}$.
6. The *natural map* is $\nu : A \to \operatorname{coim}(f) : a \mapsto [a]$.
7. The *inclusion map* is $\iota : \operatorname{im}(f) \to B : b \mapsto b$.
8. The *induced map* is $\bar{f} : \operatorname{coim}(f) \to \operatorname{im}(f) : [a] \mapsto f(a)$.
9. The *canonical factorization of* f is $f = \iota \circ \bar{f} \circ \nu$.

coimage, kernel, Kernel

The amount of "collapsing" associated with a homomorphism is coded in the coimage (a partition) or the kernel (the associated equivalence relation). If our algebra has underlying group structure, the information is coded in the cell/equivalence class containing the group identity element 0:

$$\mathrm{Ker}(f) = \{a \in \mathrm{dom}(f) \mid f(a)\ (= f(0))\ = 0\}$$

For rings these sets are called *ideals*.

Computational check: (A theorem)
A subseteq $I \subseteq R$ is an ideal exactly when

1. I is closed under $+$, and
2. $rI, Ir \subseteq R$ for all $r \in R$.

The ideal lattice

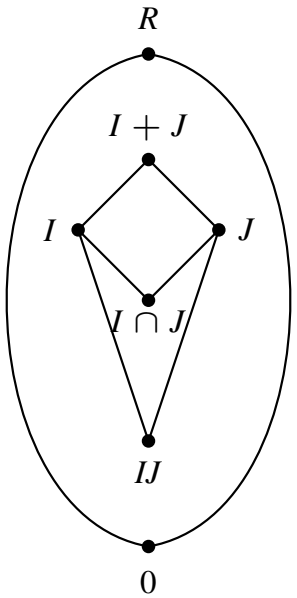
The set of all ideals of R, ordered by inclusion, form a (complete) lattice:

$$\bigwedge I_k = \bigcap I_k$$

$$\bigvee I_k = \sum I_k = \langle \bigcup I_k \rangle_{\text{abelian group}}$$

This lattice is equipped with a product:

$$IJ = \langle \{ij | i \in I, j \in J\} \rangle_{\text{ideal}} = \langle \{ij | i \in I, j \in J\} \rangle_{\text{abelian group}}$$



For $I \lhd \mathbb{Z}$, $I = (n)$ for some (nonnegative) n.

For $(m) \subseteq (n)$ iff $n|m$.

For $(m) + (n) = (\gcd(m, n))$

For $(m) \cap (n) = (\text{lcm}(m, n))$

For $(m)(n) = (mn)$

The ideal lattice is modular

Dedekind observed that the ideal lattice of a ring satisfies the following equivalent conditions:

1. $I \cap (J + L) = (I \cap J) + (I \cap L)$ whenever $J \subseteq I$.
2. $I \cap ((I \cap J) + L) = (I \cap J) + (I \cap L)$.
3. No sublattice isomorphic to a pentagon.

(Context.)

(Proof.)

(Isomorphism of perspective intervals.)

(A product of two Noetherian rings is Noetherian.)

The ideal product vs group commutator

If you are familiar with groups, then you might compare:

1. ring $R \leftrightarrow$ group G
2. ideal $I \leftrightarrow$ normal subgroup M
3. ideal product $IJ \leftrightarrow$ commutator of normal subgroups $[M,N]$
4. annihilation $(IJ = 0) \leftrightarrow$ centrality $([M,N] = 1)$
5. commutator words for rings: xy, $yx \leftrightarrow$ commutator word for groups $[x,y] = x^{-1}y^{-1}xy$

For example

1. $I \leq I', J \leq J'$ implies $IJ \leq I'J'$ ($M \leq M', N \leq N'$ implies $[M,N] \leq [M',N']$)
2. $IJ \subseteq I \cap J$ ($[M,N] \subseteq M \cap N$)
3. $I(\sum J_k) = \sum(IJ_k)$ ($[M, \bigvee N_k] = \bigvee [M,N_k]$)
4. $I^2 = 0$ means that the induced structure on I is that of an R-module ($[M,M] = 0$ means that the induced structure on M is that of an G-module)

The ideal product is residuated

If you thought to divide ideals, you would want division to satisfy

$$IJ \subseteq K \iff I \subseteq K/J.$$

There is such a division, but it is written $(K : J)$ instead of K/J, it is called the *ideal quotient* of K by J, and it is defined $(K : J) := \{r \in R \mid rJ \subseteq K\}$.
Some properties:

1. $(K : J) = R$ iff $J \subseteq K$.
2. $K \subseteq (K : J)$.
3. $(K : J)J \subseteq K$.
4. $(\bigcap K_i : J) = \bigcap (K_i : J)$.
5. $(K : \sum J_i) = \bigcap (K : J_i)$. (In particular, $(K : J) = (K : J + K)$.)
6. $(K : IJ) = ((K : I) : J)$.
7. In $\mathbb{Z}$, If $(m) \subseteq (n)$, then $((m) : (n)) = (m/n)$.

Ideals the square to zero, solvability = nilpotence

If $I \lhd R$ satisfies $I^2 = 0$, then the structure induced on I by R is that of an R-module.

That is, if $p(x_1, \ldots, x_n) \in \mathrm{Pol}(R)$ has the property that $p(I, \ldots, I) \subseteq I$, then $p|_I$ agrees with a module polynomial $\sum r_i x_i + c$, $c \in I$. The structure of such ideals can be understood using 'linear algebra'.

If $I \subseteq J$ and $J^2 \subseteq I$, then the structure J/I can be understood using linear algebra. More generally, given a 'solvability chain' $I_0 \subseteq \cdots \subseteq I_n$ with $I_{k+1}^2 \subseteq I_k$ for all k, we can theoretically understand I_n/I_0 using linear algebra.

For associative rings, solvability = nilpotence. $(IJ)(KL) = (I(J(KL)))$, so 2-step solvability $(II)(II) = 0$ implies at most 3-step nilpotence $(I(I(II)))$.

Nilradical

Defn. The *nilradical* of R, possibly written $\mathrm{nil}(R)$ or $\mathfrak{N}$, is the set of nilpotent elements of R: $\mathrm{nil}(R) := \{r \in R \mid \exists n(r^n = 0)\}$.

The *nilradical* of an ideal $I \lhd R$ is the set of elements 'nilpotent over I', or 'nilpotent modulo I':

$$\sqrt{I} := \{r \in R \mid \exists n(r^n \in I)\}.$$

So, $\mathrm{nil}(R) = \sqrt{(0)}$.

Everyone knows:

1. $\sqrt{I}$ is an ideal.
2. The mapping $X \mapsto \sqrt{\langle X \rangle}$ is a closure operator. In particular, this mapping is
   1. (Extensive) $I \subseteq \sqrt{I}$.
   2. (Monotone) $I \subseteq J$ implies $\sqrt{I} \subseteq \sqrt{J}$.
   3. (Idempotent) $\sqrt{\sqrt{I}} = \sqrt{I}$.
3. $\sqrt{I}$ is the intersection of the prime ideals containing I.

In $R = \mathbb{Z}$

In number theory, the *radical* of a positive integer $n = p_1^{e_1} \cdots p_k^{e_k}$ is the square-free number whose factorization contains the same primes: $\mathrm{rad}(n) = p_1 \cdots p_k$.

Exercise. Explain why $\sqrt{(n)} = (\mathrm{rad}(n))$.