21-237: Math Studies Algebra I	November 9, 2022

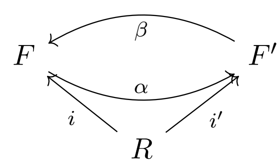
Lecture 27 : Factorization

Lecturer: James Cummings

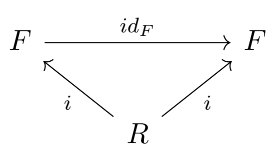
Scribe: Rajeev Godse

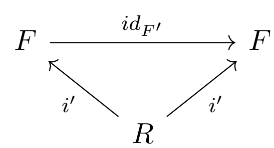
1 Uniqueness up to unique isomorphism

Let R be an integral domain. Our construction of the field of fractions from last time is universal, and thus unique in a powerful way. Let F, F' both satisfy the condition of our construction. We have the commutative diagram below, where α, β are unique:



However, we also have that the below commutative diagrams have the identity as their unique morphism:





So $\alpha\beta = id_{F'}$ and $\beta\alpha = id_F$, so α is the **unique** isomorphism between F and F'.

2 Factorization

For a ring R, elements $a, b \in R$ are **associates** if there is unit u such that $ua = b$.

In an integral domain R,

(1) We say an element $a \in R$ is **irreducible** if $a \neq 0$, a is not a unit, and for all $b, c \in R$, $a = bc$ implies that one of b, c is a unit (and consequently, the other is an associate of a).

(2) We say an element $a \in R$ is **prime** if $a \neq 0$, a is not a unit, and for all $b, c \in R$, $a \mid bc$ implies that $a \mid b$ or $a \mid c$.

Fact: If R is an integral domain, and $a \in R$ is prime, then a is irreducible.

Proof: Let $a = bc$, so $a \mid bc$. Since a is prime, $a \mid b$ or $a \mid c$. WLOG, suppose $a \mid b$, say $b = xa$. Now $a = bc = axc$, so $a(1 - xc) = 0$. $a \neq 0$, and R is ID, so $1 - xc = 0$, $1 = xc$, and c is a unit. □

Easy fact: Let R be ID. Let $a, b \in R$ be associates. Then, a is irreducible iff b is irreducible. Also, a is prime iff b is prime.

We say a **unique factorization domain** (UFD) is a ring R such that

(1) R is an ID.

(2) For all $a \in R$ such that a is nonzero nonunit, a is a finite product of irreducible elements.

(3) If $a \in R$, a is non-zero non-unit and $a = r_1 \ldots r_m = s_1 \ldots s_n$, r_i, s_j irreducibles, then $m = n$ and there is a permutation $\pi \in S_m$ such that r_i is an associate of $s_{\pi(i)}$ for all i.

Fact: If R is a UFD, concepts of "prime" and "irreducible" coincide.

Proof: Suppose p is irreducible and $p \mid ab$ for $a, b \in R$, so $ab = px$ for $x \in R$. So if $a = r_1 \dots r_m$ and $b = s_1 \dots s_n$ for r_i, s_j irreducible, then $ab = r_1 \dots r_m s_1 \dots s_m = px$. x itself can also be factored into irreducibles, so because factorization into irreducibles is unique up to associates and permutation, we know that p is an associate of some r_i or s_j. In the former case, $p \mid a$, and in the latter, $p \mid b$. $\square$

Coming soon: PID implies UFD.

3 More on modules

For R a ring, M is a R-module, we M is **finitely generated** if there exist $m_1, \dots, m_n \in M$ such that $M = \{\sum_{i=1}^{n} r_i m_i : r_i \in R\}$.

Let M, N be R-modules. We say M is a **submodule** of N (and write $M \leq N$) if $M \leq (N, +)$ and M is closed under scalar multiplication, i.e. $rm \in M$ for $r \in R$, $m \in M$.

We say an R-module N is **Noetherian** if all submodules of N are finitely generated.

We say a ring R is **Noetherian** if R is Noetherian when viewed as an R-module, that is, all ideals of R are finitely generated.