Number Theory Note

Nayeong Kim

Fall 2023

Lecture 1

Introduction

This note is from the Number Theory class held at UC Berkeley in Fall 2023 by Professor Paul Vojta. The prerequisites for this course is Math 250 A, in particular, the following:

- integrality of an element of a ring over a subring;
- integral ring extensions;
- separable and purely inseparable (algebraic) field extensions;
- Galois theory;
- noetherian rings and modules;
- localization (inverting a multiplicative subset of a ring).

In this course, we will cover the following chapters of *Algebraic Number Theory* of Neukirch.

- Ch 1: Algebraic integers (all the sections but 12, 13, 14)
- Ch 2: Valuations (all the sections but 6, parts of 7, 9, 10)

- Ch 3: Primes, different, discriminant (1, 2, and parts of 3)
- Ch 7: Zeta functions and L-series (a thin subset)
- Ch 6: Class field theory (Section 12, a few other parts)

Overview

The following is the overview of the courses. Let us define a number field.

Definition 1. A number field is a finite (field) extension of $\mathbb{Q}$.

For example, $\mathbb{Q}(\sqrt{2})$ is a number field. We often work with one of the following situations:

$$\begin{array}{ccccccc} A & \subseteq & K & \qquad & B & \subseteq & L \\ | & & | & & | & & | \\ \mathbb{Z} & \subseteq & \mathbb{Q} & & A & \subseteq & K \end{array}$$

where K, L are number fields. Here is an example to be proved later. If $K = \mathbb{Q}(\sqrt{2})$, in the left-hand diagram, then $A = \mathbb{Z}[\sqrt{2}]$.

In Chapter 1 Algebraic integers, we will consider a question. Which properties of $\mathbb{Z}$ remain true in A?

$\mathbb{Z}$	A
PID	Usually not PID but non-principality is determined by a finite group

Lecture 2

Friday, August 25, 2023.

Contents

- Reading for today: §1.1
- Rings / Gauss's Lemma / Integrality

1. Algebraic Integers

§2. Integrality

Definition 2. A ring is *entire* if it has 1 ($\Leftrightarrow$ ring is not trivial) and no zero divisors (and is commutative). Equivalently,

- it is a subring of a field; or
- it is an *integral domain.*

Definition 3. A ring is *factorial* if it is entire and all nonzero elements have unique factorization into irreducible elements up to associates. Two elements x, y are *associates* if $x = uy$ for some unit u. An element x is irreducible if $x = ab$ implies that a or b is a unit.

Definition 4. A ring is *principal* if it is nontrivial and every ideal in it is principal. A ring is a *principal ideal domain* (also called *PID*) if it is entire and principal.

Definition 5. A polynomial in one variable is monic if it has leading coefficient 1. So it looks like $x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ where $a_0, a_1, \cdots, a_{n-1}$ are in the ring of constants.

We note that if a polynomial is monic, then it is nonzero.

Lemma 1 (Gauss's Lemma)**.** Let A be a factorial ring (UFD), and let K be its field of fractions. Let $f \in A[x]$ be a non-zero polynomials. If f factors as $f = gh$ with $g, h \in K[x]$, then there exists some $c \in K^*$ such that cg and $c^{-1}h$ have coefficients in A. Furthermore if f, g, h are all monic, then this is true with $c = 1$.

Proof. (Exercise) We assume that all the coefficients are in the form that the denominator and the numerator are relatively prime. Let $a, b \in A$ be gcd of numerators of coefficients of g, h respectively. Let $\alpha, \beta \in A$ be lcms of denominators of coefficients of g, h respectively. Then we claim that β divides a. **TO DO** $\square$

Definition 6.

(a) Let $A \subseteq B$ be rings. Let b in B. Then b is integral over A if there exists a monic $f \in A[x]$ such that $f(b) = 0$.

(b) We say that B is integral over A if b is integral over A for $\forall b \in B$.

(c) The integral closure of A in B is $\overline{A} = \{b \in B \ : \ b \text{ is integral over } A\}$.

(d) Assume that A is entire. Then the integral closure of A is its integral closure in its field of fractions.

Proposition 1. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}(\sqrt{2})$.

Proof. We claim that $\mathbb{Z}(\sqrt{2})$ is integral over $\mathbb{Z}$. For any $\alpha = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$, α is integral over $\mathbb{Z}$ because it is a root of

$$x^2 - 2ax + (a^2 - 2b^2) = (x - a - b\sqrt{2})(x - a + b\sqrt{2}).$$

For the backward direction, assume that some $\alpha \in \mathbb{Q}(\sqrt{2})$ is integral over $\mathbb{Z}$. Then there exists a monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. Let g be the irreducible polynomial of α over $\mathbb{Q}$. Since g divides f and both f, g are monic, g is in $\mathbb{Z}[x]$ by Gauss's lemma.

If α is in $\mathbb{Q}$, g has degree 1 hence $g(x) = x - \alpha$; hence α is in $\mathbb{Z}$; hence α is in $\mathbb{Z}[\sqrt{2}]$. Otherwise, g is in the form $g(x) = x^2 - 2ax + (a^2 - 2b^2)$ where $\alpha = a + b\sqrt{2}$

and $a, b \in \mathbb{Q}$; hence $2a, a^2-2b^2$ are integers. So $(2a)^2-4(a^2-2b^2) = 8b^2$ is an integer; so $2b$ is an integer. If $2a$ is an odd integer, then $4(a^2 - 2b^2) = (2a)^2 + 2(2b)^2$ is an odd integer which contradicts to that $a^2 - 2b^2$ is an integer. Hence a is an integer; hence $2b^2$ is an integer; hence b is an integer. Therefore $\alpha = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. $\square$

Note that this is not a general case. For example, the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{5})$ is not $\mathbb{Z}[\sqrt{5}]$ because $\alpha = (1+\sqrt{5})/2$ is a root of $x^2 - x - 1$.

Definition 7.

(a) An algebraic number is an element of $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$.

(b) An algebraic integer is an algebraic number which is integral over $\mathbb{Z}$.

(c) A rational integer is an element of $\mathbb{Z}$ (to distinguish it from an algebraic integer).

Definition 8. Let $A \subseteq B$ be rings. We say that B is finite over A, or that B is a finite ring extension of A if B is finitely generated as a module over A.

Example 1. The polynomial ring $\mathbb{Q}[t]$ is finitely generated over $\mathbb{Q}$ but not finite over $\mathbb{Q}$.

Lecture 3

Monday, August 28, 2023.

Contents

- Reading for today: §1.2
- Integral ring extensions

Proposition 2. Let $A \subseteq B$ be rings and let $b \in B$. Then TFAE:

(i) b is integral over A;

(ii) $A[b]$ is finite over A;

(iii) There is a faithful module M over $A[b]$ which is finitely generated as an A-module. A faithful module M over R is an R-module such that $\alpha M \neq 0$ for all nonzero $\alpha \in R$.

Proof. For (i) $\Rightarrow$ (ii), assume that b is integral over A. Let $f(b) = 0$ be an integral equation for b over A where $f(x)$ is a monic polynomial of degree n. Then $A[b]$ is generated as A-module by $1, b^2, \cdots, b^{n-1}$. For (ii) $\Rightarrow$ (iii), take $M = A[b]$.

For (iii) $\Rightarrow$ (i), let M be a faithful module over A which is generated by $m_1, \cdots, m_n$. We can write

$$bm_i = c_{i1}m_1, \cdots, c_{in}m_n$$

for all i and define a matrix $C = (c_{ij})$ with the coefficients c_{ij} in A. Let $f(x) = \det(xI_n - C)$ and $D = bI_n - C$. We realize that f is a monic polynomial with coefficients in A.

Let $\mathbf{m}$ be a column vector having m_i as its ith row. Recall that $D^*D = DD^* = (\det D)I_n$ where D^* is the adjoint matrix of D. Hence we have $D\mathbf{m} = b\mathbf{m} - b\mathbf{m} = 0$; hence $D^*D\mathbf{m} = 0$; hence $(\det D)\mathbf{m} = 0$; hence $(\det D)m_i = 0$ for all m_i. Since M is faithful, we notice $f(b) = \det D = 0$. Therefore b is integral over A. $\square$

Lemma 2. Let $A \subseteq B \subseteq C$ be rings. If C is finite over B and B is finite over A, then C is finite over A.

Proof. **TO DO** $\square$

Lemma 3. Let $A \subseteq B$ be rings, and let $b_1, b_2 \in B$. If b_1 and b_2 are integral over A, then so is $b_1 \pm b_2$ and $b_1 b_2$.

Proof. Since b_2 is integral over A, it's integral over $A[b_1]$. So $A[b_1, b_2]$ is finite over $A[b_1]$; so $A[b_1, b_2]$ is finite over A. Therefore $b_1 \pm b_2$ and $b_1 b_2$ are integral over A by Proposition 2. $\square$

Corollary 1. Let $A \subseteq B$ be rings. Then the integral closure of A in B is a subring of B and contains A.

Lecture 4

Wednesday, August 30

Lecture 5

Friday, September 1

Lecture 6

Wednesday, September 6

Lecture 7

Friday, September 8.

Lecture 8

Monday, September 11.

Lecture 9

Wednesday, September 13.

Contents

- Lattice
- Minkowski Theory

§4. Lattices

We will use this to prove that $|cl_K| < \infty$ for all number fields K. Throughout today's class, V is a vector space over $\mathbb{R}$ with $0 < \dim V < \infty$ and $n = \dim V$.

Definition 9. A *lattice* in V is an additive subgroup of V of the form

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

where $v_1, \cdots, v_m \in V$. A lattice is *complete* or *full* if $m = n$ (it is equivalent to that Γ spans V).

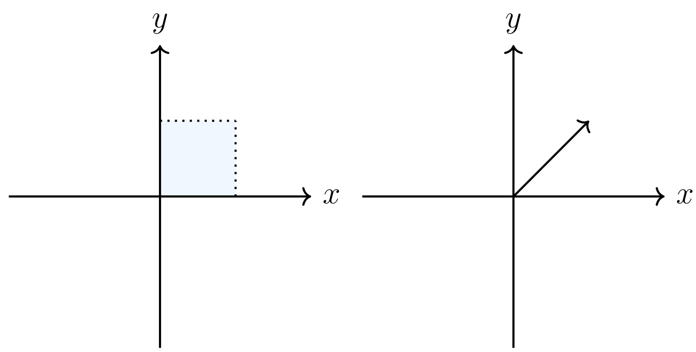
Equivalently, we can define that a lattice in V is a discrete additive subgroup of V (Proposition 4.2).

Definition 10. A *fundamental mesh* for Γ is a set

$$\sum_{i=1}^{m} x_i v_i \ : \ 0 \leq x_i < 1 \ \forall i\}$$

for some basis $v_1, \cdots, v_m$ of Γ. This is a particular type of the set of coset representatives of Γ in $\mathrm{span}(\Gamma)$.

Here are examples of fundemental mesh.



Fix an additive (nonzero) Haar measure *vol* on V. This is a positive multiple of the standard Lebesgue measure on $\mathbb{R}^n$. Or we can say that the cube spanned by an orthonormal basis has *vol* 1 given a symmetric positive definite bilinear $\langle \cdot, \cdot \rangle$ on V.

Definition 11. Let Γ be a full lattice in V. Then the *covolume* of Γ, denoted $covol(\Gamma)$, is the volume of a fundamental mesh for Γ.

We notice that this is independent of the choice of fundamental mesh. Also, $covol(\Gamma) = |\det A|$ where A is the change of basis matrix from an orthonormal basis of V to a basis of Γ. Also note that $\Gamma' \subsetneq \Gamma$ implies that $covol(\Gamma') > covol(\Gamma)$.

Definition 12. A subset X of V is

(a) *symmetric* if $-x \in X \quad \forall x \in X$; and

(b) *convex* if X contains all the line segments $AB \quad \forall A, B \in X$.

Theorem 1 (Minkowski)**.** Let Γ be a full lattice in V_1 and let X be a convex, centrally symmetric subset of V. Assume also that

(a) $vol(X) > 2^n covol(\Gamma)$; or

(b) X is compact and $vol(X) \geq 2^n covol(\Gamma)$.

Then X contains a nonzero lattice point of Γ.

Proof. Assuming (a), note that

$$vol(\frac{1}{2}X) = \frac{1}{2^n}vol(X) > covol(\Gamma). \tag{1}$$

Let D be a fundamental mesh for Γ. Note that

$$\bigcup_{\gamma\in\Gamma}(D+\gamma) = V.$$

Therefore

$$\bigcup_{\gamma\in\Gamma}((D+\gamma)\cap\frac{1}{2}X) = \frac{1}{2}X$$

and we have

$$\sum_{\gamma\in\Gamma} vol((D+\gamma)\cap\frac{1}{2}X) \geq vol(\frac{1}{2}X). \tag{2}$$

But also we have that

$$\bigcup_{\gamma\in Gamma}((\frac{1}{2}X-\gamma)\cap D) \subseteq D$$

because those are subsets of D, so either they overlap or

$$\sum_{\gamma\in\Gamma} vol((\frac{1}{2}X-\gamma)\cap D) \leq vol(D). \tag{3}$$

However, translating by γ gives

$$vol((\frac{1}{2}X-\gamma)\cap D) = vol((D+\gamma)\cap\frac{1}{2}X)$$

for all $\gamma\in\Gamma$. So (2) contradicts to (3) by (1); so there exists some distinct γ_1,γ_2 such that

$$((\frac{1}{2}X-\gamma_1)\cap D)\cap((\frac{1}{2}X-\gamma_2)\cap D)\neq\emptyset.$$

Pick some v in this set. Then $v+\gamma_1$ and $v+\gamma_2$ are contained in $\frac{1}{2}X$. So is $-v-\gamma_2$ by the symmetry. Hence the middle point $(\gamma_1-\gamma_2)/2$ of $v+\gamma_1$ and $-v-\gamma_2$ is in $\frac{1}{2}X$ since X is convex. Hence $\gamma_1-\gamma_2$ is a nonzero element in $\Gamma\cap X$.

The proof of (b) is the next homework. $\square$

§5. Minkowski Theory

This is also called as "Geometry of Numbers". Let K be a number field and let $n = [K : \mathbb{Q}]$. Let $\mathbf{a}$ be a fractional ideal of K. Since $\mathbf{a}$ has a basis over $\mathbb{Z}$ (and is full), its addtive group is isomorphic to $\mathbb{Z}^n$ thinking of $\mathbf{a}$ as a $\mathbb{Z}$-submodule of K. Also, we notice that $K \cong \mathbb{Q}^n$ as a vector space of $\mathbb{Q}$, so it's tempting to let $V = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^n$ and show that the map $K \hookrightarrow V$ takes $\mathbf{a}$ to a full lattice in V. This is true but we will need more.

Instead, we have n distinct embeddings of K into $\mathbb{C}$ over $\mathbb{Q}$ where $n = [K : \mathbb{Q}]_s = [K : \mathbb{Q}]$. Call them $\tau_1, \cdots \tau_n$. So we get a map $(\tau_1, \cdots, \tau_n) : K \hookrightarrow \mathbb{C}^n$. Note that $\mathbb{C}^n$ is a vector space over $\mathbb{R}$ of dimension $2n$. Let $\rho_1, \cdots, \rho_r$ be those τ_i with $\tau(K) \subset \mathbb{R}$. For the remaining τ_j, we realize that the conjugate of each τ_j is also among the τ_js (other than ρ_i) and $\tau_j \neq \overline{\tau_j}$. So $\{\tau_i\} \setminus \{\rho_i\}$ consists of pairwise disjoint complex conjugate pairs of embeddings $K \hookrightarrow \mathbb{C}$. Let s be the number of such pairs. Then clearly $r + 2s = n$. Let $\sigma_1, \cdots, \sigma_s$ be a chose of one element from each pair.

Now we have $\rho_1, \cdots \rho_r, \sigma_1, \overline{\sigma_1}, \cdots, \sigma_s, \overline{\sigma_s}$ instead of $\tau_1, \cdots, \tau_n$. We have a map $j := (\rho_1, \cdots, \rho_r, \sigma_1, \cdots, \sigma_s) : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$.

Lecture 10

Friday, September 15.

Contents

- (Additive) Minkowski Theory

Lecture 11

Monday, September 18.

Lecture 12

Lecture 13

Friday, September 22.

Lecture 14

Monday, September 25.

Contents

- Reading for today: : §1.11
- Localization

§11 Localization

We can consider localization as a generalization of the construction of the fraction field of an entire ring to allow fewer denominators; or to handle non-entire rings.

Definition 13. A multiplicative subset of a ring A is a subset $S \subseteq A$ such that

(a) S contains the multiplicative identity 1;

(b) S is closed under multiplication i.e. $s_1 s_2 \in S \quad \forall s_1, s_2 \in S$.

In other words, S is a submonoid of the multiplicative monoid of A.

Throughout today, A is a commutative ring and $S \subseteq A$ is a multiplicative subset.

Proposition 3. Define a relation $\sim$ on $S \times A$ by

$$(s_1, a_1) \sim (s_2, a_2) \Leftrightarrow \exists s' \in S \; s' s_1 a_2 = s' s_1 a_2.$$

The intuition of $\sim$ is

$$(s_1, a_1) \sim (s_2, a_2) \Leftrightarrow \frac{a_1}{s_1} = \frac{a_2}{s_2}.$$

Then

(a) $\sim$ is an equivalence relation; and

(b) $\sim$ is the smallest equivalence relation satisfying $(s, a) \sim (s's, s'a)$ for all $s, s' \in S$ and all $a \in A$.

Proof. For (a), we will show that $\sim$ is reflexive, symmetric, and transitive. Since a multiplicative subset has 1, the reflexivity is straightforward. Due to the symmetry of the equation $s's_1a_2 = s's_2a_1$, the symmetry is clear. Suppose that $(s_1, a_1) \sim (s_2, a_2)$ and $(s_2, a_2) \sim (s_3, a_3)$. Then we have $s's_1a_2 = s's_2a_1$ and $s''s_2a_3 = s''s_3a_2$ for some $s', s'' \in S$. Hence $(s's''a_2)s_1a_3 = s's''a_1s_2a_3 = (s's''a_2)a_1s_3$; hence we have $(s_1, a_1) \sim (s_3, a_3)$.

Let $\approx$ be the smallest equivalence relation satisfying the given condition in (b). We may consider relations $\approx, \sim$ as subsets of $(S \times A) \times (S \times A)$. It is clear that $\sim$ satisfies the given condition hence $\sim \subseteq \approx$. Take any $(s_1, a_1) \sim (s_2, a_2)$. Then

$$
\begin{aligned}
&(s_1, a_1) \sim (s_2, a_2) \\
\Rightarrow\ &\exists s' \in S\ (s_1, a_1) \approx (s's_2s_1, s's_2a_1) \wedge (s's_1s_2, s's_1a_2) \approx (s_2, a_2) \\
\Rightarrow\ &(s_1, a_1) \approx (s_2, a_2).
\end{aligned}
$$

So $\sim \subseteq \approx$ and we obtained the desired result. $\square$

Definition 14. The localization $S^{-1}A$ (or $A[S^{-1}]$) is the set of $\sim$-equivalence classes of $S \times A$. The equivalence class of (s, a) is denoted as $s^{-1}a$ or a/s.

Corollary 2 (From Proposition 3)**.** Let B, C be sets, and let $f : S \times A \times B \to C$ be a function. If $f(s, a, b) = f(s's, s'a, b)$ for all $s, s' \in S, a \in A$ and $b \in B$, then there is a unique well-defined function $\tilde{f} : S^{-1}A \times B \to C$ such that $\tilde{f}(a/s, b) = f(s, a, b)$ for all s, a, b.

Proposition 4. The usual formulas for addition and multiplication of fractions

$$
\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1s_2 + a_2s_1}{s_1s_2}, \quad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1a_2}{s_1s_2}
$$

give $S^{-1}A$ a well-defined structure of a (commutative) ring, such that the map $\varphi : a \mapsto a/1$ is a ring homomorphism $A \to S^{-1}A$. Moreover, this homomorphism satisfies the following universal property: every ring homomorphism $\psi : A \to B$ in which $\psi(S) \subset B^*$ factors uniquely through the canonical map $A \to S^{-1}A$. In other words, the following diagram commutes via $\theta(a/s) = \psi(a)\psi(s)^{-1}$.

$$\begin{tikzcd} A \arrow[r, "\psi"] \arrow[dr, "\varphi"'] & B \\ & S^{-1}A \arrow[u, dashed, "\exists!\theta"'] \end{tikzcd}$$

Example 2.

1. Let $S = \{1\}$ or $S = A^*$. Then $S^{-1}A \cong A$ via φ.

2. A is an entire ring and $S = A \setminus \{0\}$. Then $S^{-1}A$ is the fraction ring K of A.

3. $S^{-1}A = 0$ iff $0 \in S$.

   Proof.

   $$S^{-1}A = 0 \Leftrightarrow \frac{1}{1} = \frac{0}{1} \Leftrightarrow \exists s \in S \ s(1 \cdot 1 - 1 \cdot 0) = 0 \Leftrightarrow s = 0 \in S.$$

   □

4. If A is entire and $0 \notin S$, then $A \to S^{-1}A$ is injective, and $S^{-1}A$ is isomorphic to a subring of the fraction field K.

5. $A = \mathbb{Z}$ and $S = \{3^k \ : \ k \in \mathbb{Z}_{\geq 0}\}$. Then $S^{-1}A = \mathbb{Z}[1/3]$.

6. If A is any ring, $\mathfrak{p}$ is a prime ideal, and $S = A \setminus \mathfrak{p}$, then S is a multiplicative subset of A and $S^{-1}A$ is called the local ring of A at $\mathfrak{p}$ denoting $A_{\mathfrak{p}}$.

   Proof. Since $\mathfrak{p}$ is prime, 1 is not in $\mathfrak{p}$ hence it is in S. Also, we realize that

   $$\forall x_1, x_2 \ (x_1 \notin \mathfrak{p} \wedge x_2 \notin \mathfrak{p} \Rightarrow \ x_1x_2 \notin \mathfrak{p}) \ \Leftrightarrow \ \forall x_1, x_2 \ (x_1x_2 \in \mathfrak{p} \Rightarrow x_1 \in \mathfrak{p} \vee x_2 \in \mathfrak{p}).$$

   Since $x \notin \mathfrak{p}$ iff $x \in S$, we have $S = A \setminus \mathfrak{p}$ is a multiplicative subset of A. □

   For example, we have $\mathbb{Z}_{(2)} \subset \mathbb{Q}$ has elements of the form q/p where p is odd. This is the opposite of $\mathbb{Z}[1/2]$ in some sense.

When $A = \mathbb{Z}/10\mathbb{Z}$ and $S = \{1, 2, 4, 6, 8\}$, what is $S^{-1}A$? The following proposition is useful in addressing such questions.

Proposition 5. The kernel of φ is $\{a \in A \ : \ \operatorname{ann}(a) \cap S \neq \emptyset\}$ where $\varphi : A \to S^{-1}A$ is given as $\varphi(a) = a/1$.

Proof.

$$a \in \ker \varphi \Leftrightarrow \frac{a}{1} = \frac{0}{1} \Leftrightarrow \exists s \in S \ s(a-1) = 0 \Leftrightarrow \operatorname{ann}(a) \cap S \neq \emptyset$$

□

In $\mathbb{Z}/10\mathbb{Z}$, we observe that

$$\begin{aligned}
&\operatorname{ann}(2) = \operatorname{ann}(4) = \operatorname{ann}(6) = \operatorname{ann}(8) = \{0, 5\}, \\
&\operatorname{ann}(5) = \{0, 2, 4, 6, 8\}, \\
&\operatorname{ann}(1) = \operatorname{ann}(3) = \operatorname{ann}(7) = \operatorname{ann}(9) = \{0\}.
\end{aligned}$$

So the kernel of φ is $\{0, 5\}$ and $S^{-1}A \cong \mathbb{Z}/5\mathbb{Z}$.

We can also localize A-modules. Let M be an A-module. Then we may define an equivalence relation $\sim$ on $S \times M$ and let $S^{-1}M = (S \times M)/\sim$. This is a module over $S^{-1}A$. Also, if $f : M_1 \to M_2$ is a homomorphism of A-modules, then f induces a $S^{-1}A$-module homomorphism $S^{-1}f : S^{-1}M_1 \to S^{-1}M_2$. We get a (covariant) functor $S^{-1} : \mathrm{Mod}_A \to \mathrm{Mod}_{S^{-1}A}$. In addition, it is exact i.e. if $0 \to M' \to M \to M'' \to 0$ is exact, then $0 \to S^{-1}M' \to S^{-1}M \to S^{-1}M'' \to 0$ is exact.

Lecture 15