MATH 205A Notes

Jiantong Liu

October 12, 2022

1 Lecture 1, September 23, 2022

1.1 Motivation of the Subject

Example 1.1 (Motivating Example).

- Fermat's Last Theorem. For any $n \geq 3$, the equation $x^n + y^n = z^n$ has no integer solutions. This was stated by Fermat in 1637, who solved the case for $n = 4$, and was eventually proven by Wiles in 1995.

  Kummer (approximately 1850) proved the case for prime $n = p \geq 3$, and $\gcd(x, y, z) = 1$, where $p \nmid xyz$. This is called the first case of Fermat's Last Theorem. Take $\xi_p = e^{\frac{2\pi i}{p}}$, we then study $\mathbb{Z}[\xi_p] = \{\sum_{i=0}^{p-1} a_i\xi_p^i \mid a_i \in \mathbb{Z}\}$. Suppose $\mathbb{Z}[\xi_p]$ is a UFD ($p \leq 19$). Note that $x^p + y^p = \prod_{i=0}^{p-1}(x + \xi_p^i y)$. By our assumption, the $x + \xi_p^i y$ are all relatively prime. Their product is z^p, so each $x + \xi_p^i y$ is a pth power times a unit. They are also all congruent modulo $(1 - \xi_p)$, the unique prime of $\mathbb{Z}[\xi_p]$ over (p). One obtains a contradiction using

  1. the structure of $\mathbb{Z}[\xi_p]^\times$,
  2. properties of pth powers in $\mathbb{Z}[\xi_p]$ modulo (p).

  Note that for any p, $\mathbb{Z}[\xi_p]$ has unique factorization of nonzero ideals into prime ideals: Dedekind domain. It is in fact enough that no non-principal ideal has principal pth power. We say p is regular. This includes all $p < 100$ except $37, 59, 67$. Also, Kummer did not require $p \nmid xyz$.

- Power residue. When is 2 a cube modulo p? (c.f. reciprocity) If $p = 3$ or $p \equiv 2 \pmod 3$, the answer is always. If $p \equiv 1 \pmod 3$, then 2 is a cube modulo p if and only if $p = a^2 + 27b^2$ with $a, b \in \mathbb{Z}$. Note that 2 is a cube modulo p if and only if 2 is a cube modulo π.[1] The cubic reciprocity result by Eisenstein says that 2 is a cube modulo π if and only if π is a cube modulo 2. But when is π a cube modulo 2? Note $(\mathbb{Z}[\xi_3]/(2))^\times \cong \mathbb{F}_2[\xi_3]^\times = \mathbb{F}_4^\times$. So π is a cube modulo 2 if and only if $\pi \equiv 1 \pmod 2$. We can choose $\pi \equiv 1 \pmod 3$, so this is when $\pi \equiv 1 \pmod 6$, and with $\xi_3^2 + \xi_3 + 1 = 0$, this is true if and only if $\pi = a + 6b\xi_3$ with $a \equiv 1 \pmod 3$ and $b \in \mathbb{Z}$, if and only if $p = \pi\bar{\pi} = a^2 - 6ab + 36b^2 = (a - 3b)^2 + 27b^2$.

[1] When we say modulo π, we consider $p = \pi\bar{\pi}$ in $\mathbb{Z}[\xi_3]$ for π irreducible.

1.2 Integrality

Definition 1.2 (Number Field). A number field is a finite extension of $\mathbb{Q}$. Being a number field implies it is algebraic. An algebraic number is algebraic over $\mathbb{Q}$, but inside $\mathbb{C}$, i.e. $\bar{\mathbb{Q}} \subseteq \mathbb{C}$. We like to think of $\bar{\mathbb{Q}}$ as an algebraic closure itself.[2]

Definition 1.3 (Ring of Integers). The ring of integers $\mathcal{O}_F$ of a number field F is the set of all roots of monic polynomials in $\mathbb{Z}[x]$ in F. We will see later that this is indeed a ring because it is the integral closure of F.[3]

Let B/A be an extension of commutative rings.

Definition 1.4 (Integral Element). An element of B is integral over A if it is the root of some monic $f \in A[x]$.

Proposition 1.5. Let $\beta \in B$. The following are equivalent:

(i) β is integral over A.

(ii) There exists $n \geq 0$ such that $A[\beta] = \bigoplus_{i=0}^{n} A \cdot \beta^i$, i.e. $\{1, \beta, \cdots, \beta^n\}$ generates $A[\beta]$ as an A-module.

(iii) $A[\beta]$ is finitely-generated as an A-module.

(iv) There exists a finitely-generated A-submodule M of B such that $\beta M \subseteq M$ and M is faithful as an $A[\beta]$-module.

Proof. The proof from (i) to (ii) to (iii) to (iv) is fairly simple. We now prove (iv) implies (i). Suppose $M = \sum_{i=1}^{n} A \cdot \gamma_i \subseteq B$ has the properties in (iv), then $\beta\gamma_i = \sum_{j=1}^{n} a_{ij}\gamma_j$, where (a_{ij}) is defining $T : A^n \to A^n$, which is B-linear. Now the characteristic polynomial $c_T(x) = \det(x \cdot \mathbf{id} - T)$, so $c_T(\beta) \cdot M = 0$, and so $c_T(\beta) = 0$ as M is faithful over $A[\beta]$. □

Definition 1.6 (Integral Extension). An extension B/A is integral if every $\beta \in B$ is integral over A.

Proposition 1.7. Suppose $B = A[\beta_1, \cdots, \beta_k]$ is finitely-generated over A. The following are equivalent:

(i) B/A is integral.

(ii) Each β_i is integral over A.

(iii) B is finitely-generated as an A-module.

[2] In the notes, we defined the ring of algebraic integers to be the integral closure $\bar{\mathbb{Z}}$ of $\mathbb{Z}$ inside $\mathbb{C}$, and an algebraic integer is an element of $\bar{\mathbb{Z}}$

[3] We can define the ring of integers of a number field to be the integral closure of $\mathbb{Z}$ over F.

Proof. Easy if one assumes that we proved "if C/B is an extension and C is a finitely-generated B-module and B is a finitely-generated A-module, then C is a finitely-generated A-module". $\square$

Corollary 1.8. If C/B and B/A are integral extensions, then so is C/A.

Proof. Suppose $\gamma \in C$. It is the root of some monic polynomial $f \in B[x]$. Let B' be an A-algebra (subring) generated by the coefficients of f. Then γ is integral over B' and B' is integral over A, and so $B'[\gamma]$ is integral over A, and so γ is integral over A. $\square$

Definition 1.9 (Integral Closure)**.** The integral closure of A in B is the set of elements of B integral over A.

Proposition 1.10. The integral closure of A in B is a ring.

Proof. Suppose α, β are in the integral closure of A in B. Consider the ring $A[\alpha, \beta]$, then it is integral over A, but it also contains $-\alpha, \alpha + \beta, \alpha \cdot \beta$, and so we have closure. $\square$

Corollary 1.11. If F is a number field, then $\mathcal{O}_F$ is a ring.

Note that we can define $\bar{\mathbb{Z}}$ to be the ring of algebraic integers, i.e. the integral closure of $\mathbb{Z}$ in $\mathbb{Q} \subseteq \mathbb{C}$.

Definition 1.12 (Integrally Closed)**.** We say A is integrally closed in B if the integral closure of A in B is A.

Definition 1.13 (Integrally Closed/Normal)**.** We say a domain A is integrally closed if it is integrally closed in its quotient field $Q(A)$. We use normal and integrally closed interchangably.

This gives an absolute notion of closure.

Example 1.14. $\mathbb{Z}$ is not integrally closed. For example, suppose $\frac{c}{d} \in \mathbb{Q}$ is a reduced fraction, then $\mathbb{Z}[\frac{c}{d}]$ is not finitely generated over $\mathbb{Z}$ if $d > 1$.

Proposition 1.15. Suppose A is integrally closed domain, and $K = Q(A)$, and L/K is a field extension. If $\beta \in L$ is integral over A with minimal polynomial $f \in K[x]$, then $f \in A[x]$.

Proof. See notes. $\square$

Corollary 1.16. Suppose B is an integrally closed domain, then the integral closure of A in B is integrally closed.

2 Lecture 2, September 26, 2022

Recall the following proposition from last time.

Proposition 2.1. Suppose A is integrally closed domain, and $K = Q(A)$, and L/K is a field extension. If $\beta \in L$ is integral over A with minimal polynomial $f \in K[x]$, then $f \in A[x]$.

Proof. There exists a monic polynomial $g \in A[x]$ such that $g(\beta) = 0$. Now f as a minimal polynomial divides g in $K[x]$. However, all roots of g are integral over A, so all roots of f are. But f being a monic polynomial has the form $f = \prod_{i=1}^{n}(x - \alpha_i)$, where α_i's are integral over A, so sums and products of α_i's are also integral over A, and so all coefficients of f are integral over A, and therefore in K, so it is in A as A is normal. □

Proposition 2.2. UFDs are normal, i.e. integrally closed.

Proof. See notes. □

Proposition 2.3. Let B/A be an integral extension of domains. Then B is a field if and only if A is a field.

Proposition 2.4. Suppose B/A is a normal domain. Then the integral closure of A in B is normal.

Proof. Let $\bar{A}$ be the integral closure of A in B, let $\beta \in Q(\bar{A})$ be integral over $\bar{A}$, then $\bar{A}[\beta]$ is integral over $\bar{A}$ and $\bar{A}$ is integral over A, so $\bar{A}[\beta]$ is integral over A, then β is integral over A. Therefore, $\beta \in \bar{A}$. □

Corollary 2.5. If F is a number field, then $\mathcal{O}_F$ is normal.

Proposition 2.6. Let A be normal and $K = Q(A)$, let L/K be an algebraic extension, and B be the integral closure of A in L, then $Q(B) = L$, and in fact, any $\beta \in L$ has the form $\frac{b}{d}$ where $b \in B$ and $d \in A \backslash \{0\}$.

Proof. Let $\beta \in L$ be the root of some monic $f = \sum_{i=0}^{n} a_i x^i \in K[x]$. There exists $d \in A\backslash\{0\}$ such that $df \in A[x]$. Now $d^n f(d^{-1}x) = \sum_{i=0}^{n} a_i d^{n-i} x^i \in A[x]$ monic, and it has $d\beta$ as a root. Now $d\beta \in B$ since it is the root of a monic polynomial in $A[x]$. □

Corollary 2.7. $Q(\mathcal{O}_F) = F$.

We now give a different interpretation of the proposition we just proved.

Remark 2.8. The proposition tells us that $B \otimes_A K \twoheadrightarrow L$ is a surjection given by $b \otimes \frac{1}{d} \mapsto \frac{b}{d}$. In fact, this is an isomorphism. (Left as an exercise.) Then the rank of B over A is just $\dim_K(B \otimes_A K) = [L : K]$.

In general, it is not obvious that this implies that B is a finitely-generated A-module, but we do get $\mathcal{O}_F$ as a finitely-generated Abelian group.

Definition 2.9 (Square-free Integer)**.** A square-free integer is an integer which is divisible by no square number other than 1. That is, its prime factorization has exactly one factor for each prime that appears in it.

Theorem 2.10. Let d be a square-free integer that is not 1. Then we know $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}], & d \equiv 2,3 \pmod 4 \end{cases}$.

Proof. Note $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. If $\alpha = a + b\sqrt{d}$ with $a \in \mathbb{Q}$ and $b \in \mathbb{Q}^\times$ that are integral over $\mathbb{Z}$, then $f = x^2 - 2ax + a^2 - b^2 d$ is its minimal polynomial in $\mathbb{Z}[x]$, then $a \in \frac{1}{2}\mathbb{Z}$. If $a \in \mathbb{Z}$, then $b^2 d \in \mathbb{Z}$ and d is square-free, so $b \in \mathbb{Z}$. If $a \notin \mathbb{Z}$, $a' = 2a \in \mathbb{Z}$ and $b' = 2b \in \mathbb{Z}$ are odd. And $(a')^2 \equiv (b')^2 d \pmod 4$. Since $(a')^2, (b')^2 \equiv 1 \pmod 4$, $d \equiv 1 \pmod 4$. Since all elements $\frac{a'+b'\sqrt{d}}{2} \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, we are done. $\square$

2.1 Dedekind Domains

Definition 2.11 (Dedekind Domain)**.** A Dedekind domain is a Noetherian, normal domain of Krull dimension at most 1.

Remark 2.12. Krull dimension at most 1 means all nonzero prime ideals are maximal.

Example 2.13.

- Fields.
- PIDs. A PID is Noetherian, and it is a UFD, so it is integrally closed. Its nonzero prime ideals are maximal, generated by its irreducible elements.

Lemma 2.14. Suppose B/A is integral. If $\mathfrak{b} \in B$ is an ideal containing a nonzero element that is not a zero divisor, then $\mathfrak{b} \cap A \neq (0)$.

Proof. Let $\beta \in B \backslash \{0\}$ not be a zero divisor. Let $f \in A[x]$ be a minimal polynomial of β, so $f(0) \neq 0$. Suppose $\beta \in \mathfrak{b}$, then $f(\beta) - f(0) \in \mathfrak{b}$, but $f(\beta) = 0$, then $f(0) \in \mathfrak{b}$, and so $f(0) \in \mathfrak{b} \cap A$. $\square$

Proposition 2.15. If $\dim(A) \leq 1$, and B/A is an integral extension of domains, then $\dim(B) \leq 1$.

Proof. Let P be a nonzero prime ideal of B and $\mathfrak{p} = P \cap A$ prime. Then $\mathfrak{p} \neq 0$ by the lemma, and so $F = A/\mathfrak{p}$ is a field since $\dim(A) = 1$. For $\beta \in B$, let $f \in A[x]$ be monic with $f(\beta) = 0$. Let $\bar{f} \in F[x]$ be its image under the reduction modulo $\mathfrak{p}$ map, $\bar{\beta} \in B/P$ be the image of β, then $\bar{f}(\bar{\beta}) = 0$. Then $\bar{\beta}$ is algebraic over F, so $B/P = F[\bar{\beta} \mid \bar{\beta} \in B]$ is a field since all of them are algebraic elements. Therefore, P is maximal. $\square$

We want to show the following theorem.

Theorem. Let A be a Dedekind domain, $K = Q(A)$, L/K is a finite extension, B is the integral closure of A in L, then B is a Dedekind domain.

This will help us prove the corollary.

Corollary. $\mathcal{O}_F$ is a Dedekind domain.

2.2 Norm and Trace

Definition 2.16 (Trace Map, Norm Map)**.** Let L/K be a finite extension of fields. For $\alpha \in L$, let $m_\alpha : L \to L$ denote the linear transformation of K-vector spaces defined by left multiplication by α. Then

- The trace map $Tr_{L/K}$ is defined by sending $\alpha \in L$ to the trace of m_α.
- The norm map $N_{L/K}$ is defined by sending $\alpha \in L$ to the determinant of m_α.

Proposition 2.17. Let L/K be a finite extension of fields, and let $\alpha \in L$. Let $f \in K[x]$ be the minimal polynomial of α over K, let $d = [K(\alpha) : K]$ and $s = [L : K(\alpha)]$. Suppose f factors in $\bar{K}[x]$ as $f = \prod_{i=1}^{d}(x - \alpha_i)$ for some $\alpha_1, \cdots, \alpha_d \in \bar{K}$. Then the characteristic polynomial of m_α is f^s, and we have

$$N_{L/K}(\alpha) = \prod_{i=1}^{d} \alpha_i^s$$

and

$$Tr_{L/K}(\alpha) = s \sum_{i=1}^{d} \alpha_i.$$

Proof. See notes. □

Proposition 2.18. Let L/K be a finite extension of fields, and let $m = [L : K]_i$ be its degree of inseparability. Let $\mathfrak{S}$ denote the set of embeddings of L fixing K in a given algebraic closure of K, i.e. $K \hookrightarrow L$. Then, for $\alpha \in L$, we have

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathfrak{S}} \sigma\alpha^m$$

and

$$Tr_{L/K}(\alpha) = m \sum_{\sigma \in \mathfrak{S}} \sigma\alpha.$$

Remark 2.19. Note that the distinct conjugates of α in a fixed algebraic closure $\bar{K}$ of K are exactly the $\tau\alpha$ for τ in the set of distinct embeddings of $K(\alpha)$ in K, and these $\tau\alpha$'s are the distinct roots of the minimal polynomial of α over K.

Proof. See notes. □

Corollary 2.20. Let L/K be a finite separable extension of fields. Let S denote the set of embeddings of L fixing K in a given algebraic closure of K. Then, for $\alpha \in L$, we have

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathfrak{S}} \sigma\alpha$$

and

$$Tr_{L/K}(\alpha) = \sum_{\sigma \in \mathfrak{S}} \sigma\alpha.$$

Proposition 2.21. Let M/K be a finite field extension and L be an intermediate field in the extension. Then we have

$$N_{M/K} = N_{L/K} \circ N_{M/L}$$

and

$$Tr_{M/K} = Tr_{L/K} \circ Tr_{M/L}.$$

2.3 Discriminant

Definition 2.22 (Symmetric Bilinear Form)**.** Let V be a K-vector space. A symmetric bilinear form is a bilinear form $\psi : V \times V \to K$ which is K-linear in each variable, with symmetric if $\psi(w, v) = \psi(v, w)$ for all $v, w \in V$.

Example 2.23. $V = K^n$, $Q \in M_n(F)$, $\psi(v, w) = v^T Q w$ bilinear. It is symmetric if and only if Q is.

Another example of symmetric bilinear form is the trace form.

Example 2.24. If L/K is a finite extension of fields, then $\psi : L \times L \to K$ defined by $\psi(\alpha, \beta) = Tr_{L/K}(\alpha\beta)$ for $\alpha, \beta \in L$ is a symmetric K-bilinear form on L.

Definition 2.25. The discriminant of $\psi : V \times V \to K$ with respect to (ordered) basis $(v_1, \cdots, v_n)$ of V/K is $\det(\psi(v_i, v_j))_{i,j}$.

Lemma 2.26. If $T : V \to V$ is K-linear, then $\det(\psi(Tv_i, Tv_j)) = \det(T)^2 \det(\psi(v_i, v_j))$.

Proof. See notes. □

Definition 2.27. The discriminant of a finite field extension L/K related to a basis of L as a K-vector space is the discriminant of the trace form related to that basis $\beta_1, \cdots, \beta_n \in L$: $D(\beta_1, \cdots, \beta_n) = \det(Tr_{L/K}(\beta_i\beta_j)_{i,j})$.

Remark 2.28. This depends on the basis you choose.

3 Lecture 3, September 28, 2022

Exercise 3.1. If L/K is inseparable, then $D(\beta_1, \cdots, \beta_n) = 0$.

Suppose L/K is separable and let $\sigma_1, \cdots, \sigma_n : L \hookrightarrow \bar{K}$ be the distinct embeddings of L in an algebraic closure of K that fix K.

Proposition 3.2. Then $D(\beta_1, \cdots, \beta_n) = \det((\sigma_i(\beta_j))_{i,j})^2$.

Proof. Note $Tr_{L/K}((\beta_i\beta_j)_{i,j}) = \sum_{k=1}^{n} \sigma_k(\beta_i)\sigma_k(\beta_j)$, and so $(Tr_{L/K}(\beta_i\beta_j))_{i,j} = Q^T Q$, where $Q = (\sigma_i(\beta_j))_{i,j}$. □

Definition 3.3. Let $\alpha_1, \cdots, \alpha_n \in L$. The Vandermonde matrix $Q(\alpha_1, \cdots, \alpha_n)$ with respect to those coefficients is

$$(\alpha_i^{j-1})_{i,j} = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \ddots & \ddots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

Lemma 3.4. $\det(Q(\alpha_1, \cdots, \alpha_n)) = \prod_{1 \le i < j < n} (\alpha_j - \alpha_i)$.

Proof. Prove by induction. See notes. □

Proposition 3.5. Suppose $L = K(\alpha)$, then $D(1, \alpha, \cdots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)^2 \neq 0$.

Proof. Let $\alpha_i = \sigma_i(\alpha)$ for all i. Then $D(1, \alpha, \cdots, \alpha^{n-1}) = \det((\alpha_i^{j-1})_{i,j}) = \prod_{i<j} (\alpha_i - \alpha_i)^2$ by the lemma. □

Example 3.6. Suppose d is square-free and not 1, and consider $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Now $D(1, \sqrt{d}) = (\sqrt{d} - (-\sqrt{d}))^2 = 4d$.

Corollary 3.7. Suppose f is a minimal polynomial of α, then the discriminant can be expressed as $D(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha))$, where f' is the derivative of f.

Proof. Left as an exercise using $f'(\alpha_j) = \prod_{i \neq j} (\alpha_j - \alpha_i)$. □

Corollary 3.8. $D(\beta_1, \cdots, \beta_n) \neq 0$ for any ordered basis $(\beta_1, \cdots, \beta_n)$ of L/K.

Now let A be a normal domain and suppose B/A is integral.

Definition 3.9. Suppose B is free of rank n over A, i.e, $B \cong A^n$ as an A-module. Let $(\beta_1, \cdots, \beta_n) \in B^n$ be an ordered basis of B over A. The discriminant of B/A relative to $(\beta_1, \cdots, \beta_n)$ is $D(\beta_1, \cdots, \beta_n)$.

Remark 3.10. This discriminant is well-defined up to multiplication up to an element of $(A^\times)^2$, i.e. square of a unit. Therefore, if $A = \mathbb{Z}$, the discriminant is well-defined, i.e. independence of choice.

In particular, we can define:

Definition 3.11. The discriminant $disc(K)$ of a number field K is the discriminant of $\mathcal{O}_k/\mathbb{Z}$ relative to some basis (but does not matter what choice we make).

Example 3.12. Suppose d is square-free and not 1 and $K = \mathbb{Q}(\sqrt{d})$, then $disc(K) = \begin{cases} d, & d \equiv 1 \pmod 4 \\ 4d, & d \equiv 2, 3 \pmod 4 \end{cases}$.

Suppose $K = Q(A)$ and L/K is finite separable, and let B be the integral closure of A in L, with $n = [L : K]$.

Lemma 3.13. Let $(\alpha_1, \cdots, \alpha_n) \in B^n$ be an ordered basis of L as a K-vector space. (Note that it exists.) Let $\beta \in L$ be such that $Tr_{L/K}(\alpha\beta) \in A$ for all $\alpha \in B$, then $disc(\alpha_1, \cdots, \alpha_n)\beta \in \sum\limits_{i=1}^{n} A \cdot \alpha_i$.

Proof. We write $\beta = \sum\limits_{i=1}^{n} a_i\alpha_i$ for some $a_i \in K$. Then $Tr_{L/K}(\alpha_i\beta) = \sum\limits_{j=1}^{n} a_i Tr_{L/K}(\alpha_i\alpha_j) =: c_i$. Now let $Q = (Tr_{L/K}(\alpha_i\alpha_j))_{i,j}$, so $Q \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \in A^n$. If we left multiply it by Q^*, the adjoint of Q, then $Q^*Q = dI_n$ for some $d \in A$. Note that by our definition we have $d = D(\alpha_1, \cdots, \alpha_n)$. Therefore, $A^n \ni Q^*Q \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = d \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$, and so $da_i \in A$ for all i, which means $d\beta \in B$. $\square$

Corollary 3.14. Let $(\alpha_1, \cdots, \alpha_n) \in B^n$ be an ordered basis of L as a K-vector space. Then $\sum\limits_{i=1}^{n} A\alpha_i \subseteq B \subseteq \sum\limits_{i=1}^{n} Ad^{-1}\alpha_i$, with $d = D(\alpha_1, \cdots, \alpha_n)$.

Remark 3.15. We squeeze B between two free A-modules of rank n.

Definition 3.16. The rank of a module M over a domain A is $rank_A(M) = \dim_K(K \otimes_A M)$.

Corollary 3.17. Suppose in addition that A is Noetherian. Then B is a finitely-generated torsion-free A-module of rank $[L : K]$.

Proof. B is now a submodule of a free A-module, so it is finitely-generated. $\square$

3.1 Fractional Ideal

Definition 3.18 (Fractional Ideal)**.** A fractional ideal of a Noetherian domain R is a non-zero finitely-generated R-submodule of $Q(R)$.

Proposition 3.19. Suppose in addition that A is Neotherian. Any fractional ideal of B is a finitely-generated A-module of rank n.

Proof. Suppose $\mathfrak{A} \subseteq Q(B)$ is a fractional ideal of B. If $\beta \in L^\times$, then $\beta : B \xrightarrow{\sim} B \cdot \beta$ that sends $x \mapsto \beta x$, so $B\beta$ has A-rank n. Take $\beta \in \mathfrak{A}$, then the rank of $\mathfrak{A}$ over A is bounded below by the rank of B over A, which is n. By assumption, $\mathfrak{A}$ is B-finitely generated in L, so there exists $\alpha \in A$ such that $\alpha\mathfrak{A} \subseteq B$. Now $\alpha : \mathfrak{A} \xrightarrow{\sim} \alpha\mathfrak{A} \subseteq B$, so the rank of $\mathfrak{A}$ over A is bounded above by the rank of B over A, which is n. $\square$

Corollary 3.20. In a number field F, any fractional ideal of $\mathcal{O}_F$ is $\mathbb{Z}$-free of rank $[F : \mathbb{Q}]$.

Theorem 3.21. Suppose A is a Dedekind domain, and B is the integral closure of A in a finite separable extension of $Q(A)$. Then B is a Dedekind domain.

Proof. By corollary, B is a finitely-generated A-module, so any ideal $\mathfrak{b} \subseteq B$ is finitely-generated. Therefore, B is Noetherian as A is. Recall that $\dim(A) \leq 1$ indicates $\dim(B) \leq 1$, and we already know that A normal implies B normal, so we are done. $\square$

Corollary 3.22. $\mathcal{O}_F$ is a Dedekind domain for any number field F.

Definition 3.23. A fractional ideal $\mathfrak{A}$ of a domain R is a non-zero R-submodule of $Q(R)$ such that there exists $d \in R\backslash\{0\}$ with $d\mathfrak{A} \subseteq R$.

Lemma 3.24. If R is a Noetherian domain, then a R-submodule $\mathfrak{A} \subseteq Q(R)$ is a fractional ideal if and only if it is R-finitely-generated.

Proof. Left as an exercise. $\square$

Definition 3.25. $\mathfrak{A}^{-1} = \{b \in Q(R) \mid ab \in R \ \ \forall a \in \mathfrak{A}\}$.

Exercise 3.26. This is a fractional ideal if $\mathfrak{A}$ is.

Now for $b \in Q(R)$, we denote $(b) = Rb$ to be the principal fractional ideal. Then $(b)^{-1} = (b^{-1})$. Moreover, $\mathfrak{A}\mathfrak{B} = R \cdot (ab \mid a \in \mathfrak{A}, b \in \mathfrak{B})$ is also a fractional ideal. The intersection of two fractional ideals is also a fractional ideal. But in general, $\mathfrak{A} \cdot \mathfrak{A}^{-1} \neq R$.

Example 3.27. Note $(x, y) \subsetneq \mathbb{Q}[x, y]$, with $(x, y)^{-1} = \mathbb{Q}[x, y]$. But $(x, y) \cdot (x, y)^{-1} = (x, y) \neq \mathbb{Q}[x, y]$.

4 Lecture 4, September 30, 2022

Lemma 4.1. Let A be a Noetherian domain and $\mathfrak{A} \subseteq A$ is a nonzero ideal. Then

(a) There exists $k \geq 0$ and nonzero prime ideals $\mathfrak{P}_1, \cdots, \mathfrak{P}_k$ of A such that $\mathfrak{P}_1 \cdots \mathfrak{P}_k \subseteq \mathfrak{A}$.

(b) Suppose $\dim(A) \leq 1$. If $\mathfrak{P}_1, \cdots, \mathfrak{P}_k$ are as in (a) and $\mathfrak{P}$ is prime with $\mathfrak{A} \subseteq \mathfrak{P}$, then $\mathfrak{P} = \mathfrak{P}_i$ for some i.

Proof. (a) Let X be the set of non zero ideals $\mathfrak{B}$ of A such that there does not exist primes $\mathfrak{P}'_1, \cdots, \mathfrak{P}'_l$ with $\mathfrak{P}'_1 \cdots \mathfrak{P}'_l \subseteq \mathfrak{B}$. Suppose $X \neq \varnothing$. Order X by the partial relation $\subseteq$. Any chain in X has a maximal element since A is Noetherian. Therefore, X has a maximal element $\mathfrak{A}$ by Zorn's Lemma. In particular, $\mathfrak{A}$ is not a prime ideal. Therefore, there exists $a, b \in A \backslash \mathfrak{A}$ such that $ab \in \mathfrak{A}$. Consider $\mathfrak{A} + (a)$ and $\mathfrak{A} + (b)$ which contain $\mathfrak{A}$. So both ideals are not in X, which means there exists $\mathfrak{P}_1, \cdots, \mathfrak{P}_m$ and $\mathfrak{Q}_1, \cdots, \mathfrak{Q}_n$ such that $\mathfrak{P}_1 \cdots \mathfrak{P}_m \subseteq \mathfrak{A} + (a)$ and $\mathfrak{Q}_1 \cdots \mathfrak{Q}_n \subseteq \mathfrak{A} + (b)$. Then $\mathfrak{P}_1 \cdots \mathfrak{P}_m \mathfrak{Q}_1 \cdots \mathfrak{Q}_n \subseteq (\mathfrak{A} + (a))(\mathfrak{A} + (b)) \subseteq \mathfrak{A}$, contradiction.

(b) Consider $\mathfrak{P}_1 \cdots \mathfrak{P}_k \subseteq \mathfrak{A} \subseteq \mathfrak{P}$. If $\mathfrak{P} \neq \mathfrak{P}_i$, since $\mathfrak{P}_i$ is maximal, then there exists $b_i \in \mathfrak{P}_i$ with $b_i \notin \mathfrak{P}$. If $\mathfrak{P} \neq \mathfrak{P}_i$ for all i, then $b_1 \cdots b_k \notin \mathfrak{P}$ as $\mathfrak{P}$ is prime. But $b_1 \cdots b_k \in \mathfrak{P}_1 \cdots \mathfrak{P}_k \subseteq \mathfrak{P}$, contradiction.

□

Lemma 4.2. Let A be a Dedekind domain and $\mathfrak{P} \subseteq A$ be a nonzero prime ideal. Then $\mathfrak{P} \cdot \mathfrak{P}^{-1} = A$.

Proof. Let $a \in \mathfrak{P} \backslash \{0\}$. By Lemma 4.1, we take $k \geq 1$ minimal such that $\mathfrak{P}_1 \cdots \mathfrak{P}_k \subseteq (a)$, and without loss of generality we take $\mathfrak{P}_k = \mathfrak{P}$. Let $b \in \mathfrak{P}_1 \cdots \mathfrak{P}_{k-1}$, $b \notin (a)$. Then $a^{-1}b \notin A$. But $a^{-1}b\mathfrak{P} \subseteq a^{-1}\mathfrak{P}_1 \cdots \mathfrak{P}_k \subseteq A$, so $a^{-1}b \in \mathfrak{P}^{-1}$. If $\mathfrak{P}^{-1}\mathfrak{P} = \mathfrak{P}$, then $a^{-1}b\mathfrak{P} \subseteq \mathfrak{P}$. Since $\mathfrak{P}$ is a finitely-generated faithful A-module, then $a^{-1}b$ is integral over A. But A is integrally closed, so $a^{-1}b \in A$, contradiction, so $\mathfrak{P}^{-1}\mathfrak{P} \neq \mathfrak{P}$. Now this is an ideal bigger than $\mathfrak{P}$, so it has to be the whole ring since $\mathfrak{P}$ is maximal, i.e. $\mathfrak{P}^{-1}\mathfrak{P} = A$. □

Theorem 4.3. Let A be a Dedekind domain and $\mathfrak{A}$ is a fractional ideal of A. Then there exists $k \geq 0$ and nonzero prime ideals $\mathfrak{P}_1, \cdots, \mathfrak{P}_k$, and integers $r_1, \cdots, r_k \neq 0$ such that $\mathfrak{A} = \mathfrak{P}_1^{r_1} \cdots \mathfrak{P}_k^{r_k}$. Moreover, this factorization is unique up to reordering. If $\mathfrak{A} \subseteq \mathfrak{A}$ as an ideal, then $r_i \geq 1$ for all i.

Proof. Suppose $\mathfrak{A} \subseteq A$ is a nonzero ideal. If $\mathfrak{A} \neq A$ ($m \neq 0$), there exists $m \geq 1$ such that there exists nonzero ideals $\mathfrak{Q}_1, \cdots, \mathfrak{Q}_m$ of A with $\mathfrak{Q}_1 \cdots \mathfrak{Q}_m \subseteq \mathfrak{A}$, according to Lemma 4.1. Without loss of generality, $\mathfrak{Q}_m \supseteq \mathfrak{A}$. Then $\mathfrak{Q}_1 \cdots \mathfrak{Q}_{m-1} = \mathfrak{Q}_1 \cdots \mathfrak{Q}_m \mathfrak{Q}_m^{-1} \subseteq \mathfrak{A}\mathfrak{Q}_m^{-1} \subseteq A$. By induction on m, there exists primes $\mathfrak{Q}'_1, \cdots, \mathfrak{Q}'_l$ of A such that $\mathfrak{Q}'_1 \cdots \mathfrak{Q}'_l = \mathfrak{A} = \mathfrak{Q}_m^{-1}$. So $\mathfrak{A}$ has a factorization into primes.

In general, suppose $\mathfrak{A}$ is a fractional ideal. Let $d \in A \backslash \{0\}$ such that $d\mathfrak{A} \subseteq A$. Then $d\mathfrak{A} = \mathfrak{P}_1 \mathfrak{P}_k$ with some primes $\mathfrak{P}_i$ and $(d) = \mathfrak{P}'_1 \cdots \mathfrak{P}'_l$, so $\mathfrak{A} = \mathfrak{P}_1 \cdots \mathfrak{P}_k (\mathfrak{P}'_1)^{-1} \cdots (\mathfrak{P}'_l)^{-1}$. For uniqueness, if $\mathfrak{P}_1^{r_1} \cdots \mathfrak{P}_k^{r_k} = \mathfrak{Q}_1^{s_1} \cdots \mathfrak{Q}_l^{s_l}$ with $r_i, s_j \geq 1$ for all i, j, then the right-hand-side contains $\mathfrak{P}_k$, so there exists $\mathfrak{Q}_i$ (say $i = l$ without loss of generality) such that $\mathfrak{P}_k = \mathfrak{Q}_i$ by Lemma 4.1. Then $\mathfrak{P}_1^{r_1} \cdots \mathfrak{P}_{k-1}^{r_{k-1}} \mathfrak{P}_k^{r_k - 1} = \mathfrak{Q}_1^{s_1} \cdots \mathfrak{Q}_{l-1}^{s_{l-1}} \mathfrak{Q}_l^{s_l - 1}$,. By induction on the sum of r_i's ($\sum_{i=1}^{r} s_i$), there are the same factorizations up to the reordering of primes. □

Definition 4.4 (Divides)**.** A nonzero ideal $\mathfrak{b}$ of a commutative ring divides an ideal $\mathfrak{a}$ if there exists an ideal $\mathfrak{c}$ such that $\mathfrak{b}\mathfrak{c} = \mathfrak{a}$.

Let A be a Dedekind domain.

Corollary 4.5. Suppose $\mathfrak{A}, \mathfrak{B}$ are nonzero ideals of A.

(a) $\mathfrak{A}$ and $\mathfrak{B}$ have no common divisors if and only if $\mathfrak{A} + \mathfrak{B} = A$, i.e. $\gcd(\mathfrak{A}, \mathfrak{B}) = A$.

(b) $\mathfrak{A} \subseteq \mathfrak{B}$ if and only if $\mathfrak{B} \mid \mathfrak{A}$.

Definition 4.6 (Ideal Group)**.** The ideal group $I(A)$ of A is the group of fractional ideals of A under $\cdot$.

By the theorem, $I(A)$ is a free Abelian group on the nonzero prime ideals of A.

Definition 4.7 (Principal Ideal Group, Ideal Class Group)**.** The principal ideal group $P(A)$ is the subgroup of $I(A)$ of principal fractional ideals.

The class group $Cl(A)$ of A is $I(A)/P(A)$.

Exercise 4.8. The class group is trivial if and only only if A is a PID.

Proposition 4.9. A Dedekind domain A is a PID if and only if it is a UFD.

Proof. Let A be a Dedekind UFD. Let $P \in I(A)$ be prime. If $a \in P\backslash\{0\}$, there exists irreducible element π in A such that $\pi \mid a$ and $\pi \in P$ since P is prime. But (π) is maximal as $\dim(A) \leq 1$, so $P = (\pi)$. Then the unqiue factorization of ideals implies A is a PID. $\square$

Definition 4.10 (Class Group)**.** The class group Cl_F of a number field F is $Cl(\mathcal{O}_F)$. (Set $I_F = I(\mathcal{O}_F), P_F = P(\mathcal{O}_F)$). Then there is a map from $\mathfrak{A} \in I(A)$ to $[\mathfrak{A}] \in Cl(A)$.

Example 4.11. $F = \mathbb{Q}(\sqrt{-5})$ and $\mathcal{O}_F = \mathbb{Z}[\sqrt{-5}]$. Then $Cl_{\mathbb{Q}(\sqrt{-5})} \neq 0$. In fact, $[\mathfrak{A}] \neq 0$ for $\mathfrak{A} = (2, 1 + \sqrt{-5})$.

Here $N_{F/\mathbb{Q}}(2) = 4$ and $N_{F/\mathbb{Q}}(1 + \sqrt{-5}) = 6$, so if $\mathfrak{A} = (x)$, then $N_{F/\mathbb{Q}}(x) \in \{\pm 1, \pm 2\}$. But $N_{F/\mathbb{Q}}(a + b\sqrt{-5}) = a^2 + 5b^2$ forces $x = \pm 1$. Therefore, A is the whole ring. This is a contradiction, because

$$\mathbb{Z}[\sqrt{-5}]/(2, 1 + \sqrt{-5}) \cong \mathbb{Z}[x]/(x^2 + 5, 2, 1 + x) \cong \mathbb{Z}[x]/(2, 1 + x) \cong \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2 \neq 0.$$

Hence, $x \neq \pm 1$, and so $(2, 1 + \sqrt{-5})$ is not principal.

Exercise 4.12. In a Dedekind domain, every ideal can be generated by two elements.

5 Lecture 5, October 3, 2022

5.1 Discrete Valuation Ring

Proposition 5.1. Any localization of a Dedekind domain is Dedekind.

Definition 5.2 (Discrete Valuation Ring)**.** A discrete valuation ring (DVR) is a PID with exactly on non-zero prime ideal. The prime ideal therefore has a generator. A generator of this ideal is therefore called a uniformizer.

Proposition 5.3. Let A be a domain, then A is a DVR if and only if it is a local Dedekind domain which is not a field.

Proof. ($\Rightarrow$): PID implies Dedekind.

($\Leftarrow$): Let $\mathfrak{p} \neq 0$ be the unique prime ideal of A. Choose $\pi \in \mathfrak{p} - \mathfrak{p}^2$, then $(\pi) = \mathfrak{p}^n$ for some n, so $n = 1$, then $\mathfrak{p}^n = (\pi^n)$, so A is a PID. $\square$

Theorem 5.4. A Noetherian domain is Dedekind if and only if its localization at every nonzero prime ideal is a DVR.

Proof. ($\Rightarrow$): By the proposition, it is trivial.

($\Leftarrow$): Consider A where $A_\mathfrak{p}$ is a DVR for all $\mathfrak{p} \neq 0$. Let B be the intersection of $A_\mathfrak{p}$ for nonzero prime $\mathfrak{p}$. Let $\frac{c}{d} \in B$, $c \in A$ and $d \in A \backslash \{0\}$. Set $\mathfrak{A} = \{a \in A \mid ac \in (d)\}$. We have $\frac{c}{d} = \frac{r}{s}$ with $r \in A$ and $s \in A \backslash \mathfrak{p}$. Therefore, $sc = rd \in (d)$, then by definition $s \in \mathfrak{A}$. Then $\mathfrak{A} \not\subseteq \mathfrak{p}$ for all $\mathfrak{p}$, so $\mathfrak{A} = A$. But that means $1 \in \mathfrak{A}$, so $c \in (d)$, and $\frac{c}{d} \in A$. Therefore, $B = A$. Now each $A_\mathfrak{p}$ is normal, so $B = A$ is normal. Suppose $\mathfrak{q} \neq 0$ is a prime ideal in A. Let $\mathfrak{m} \supseteq \mathfrak{q}$ be a maximal ideal. Then $\mathfrak{q}A_\mathfrak{m}$ is a nonzero prime ideal of the DVR $A_\mathfrak{m}$, but then $\mathfrak{q}A_\mathfrak{m} = \mathfrak{m}A_\mathfrak{m}$. Note $\mathfrak{q} = A \cap \mathfrak{q}A_\mathfrak{m}$ (exercise) as $\mathfrak{q} \subseteq \mathfrak{m}$. So $\mathfrak{q} = A \cap \mathfrak{q}A_m = A \cap \mathfrak{m}A_\mathfrak{m} = \mathfrak{m}$. Therefore, $\dim(A) \leq 1$. $\square$

Definition 5.5 (Discrete Valuation)**.** A discrete valuation v on a field K is a surjective function $v : K \to \mathbb{Z} \cup \{\infty\}$ such that

1. $v(a) = \infty$ if and only if $a = 0$, and
2. $v(ab) = v(a) + v(b)$, and
3. $v(a + b) \geq \min(v(a), v(b))$ for all $a, b \in K$.

We call $v(a)$ the valuation of a. (K, v) is called a discrete valuation field.

Remark 5.6. $v(a + b) = \min(v(a), v(b))$ if $v(a) \neq v(b)$.

$v(1) = 0$.

$v(-a) = v(a)$.

Definition 5.7 (Valuation Ring)**.** The valuation ring of v is $\mathcal{O}_v = \{a \in K \mid v(a) \geq 0\}$.

Lemma 5.8. $\mathcal{O}_v$ is a DVR with maximal ideal $\mathfrak{m}_v = \{a \in K \mid v(a) \geq 1\}$.

Proof. Take $\pi \in \mathcal{O}_v$ with $v(\pi) = 1$. Any $a \in \mathcal{O}_v$ with $v(a) = n$ has $v(a\pi^{-n}) = 0$. So $u = a\pi^{-n} \in \mathcal{O}_v$ and this is a unit. Then $a = u\pi^n$. Thus, $\mathcal{O}_v$ is a DVR with uniformizer π. □

Definition 5.9 (p-adic Valuation)**.** Let A be Dedekind with $Q(A) = K$ and p is a prime in A. The p-adic valuation of A is $v_p : K \to \mathbb{Z} \cup \{\infty\}$ given by $(a) = p^{v_p(a)}\mathfrak{b}\mathfrak{c}^{-1}$ where $p \nmid \mathfrak{b}\mathfrak{c}$, for $a \in K^\times$.

Remark 5.10 (Why is this a valuation?)**.** It suffices to check the last property. Note that for $a, b \in K^\times$, $(a+b) = p^{v_p(a+b)} \subseteq (a) + (b) = p^{v_p(a)}\frac{\mathfrak{b}}{\mathfrak{c}} + p^{v_p(b)}\frac{\mathfrak{b}'}{\mathfrak{c}'} = p^{\min(v_p(a), v_p(b))}\frac{\mathfrak{b}''}{\mathfrak{c}''}$. Therefore, $v_p(a+b) \geq \min(v_p(a), v_p(b))$.

Remark 5.11. Valuation ring of v_p is A_p.

Example 5.12. Let p be a prime. Then $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ with $v_p = v_{(p)}$ is a p-adic valuation. Now $\mathcal{P}_{v_p} = \mathbb{Z}_{(p)} = \{\frac{c}{d} \mid c, d \in \mathbb{Z}, p \nmid d\}$.

Example 5.13. Let K be a field. $v_\infty : K(t) \to \mathbb{Z} \cup \{\infty\}$ is given by $v_\infty(\frac{f}{g}) = \deg(g) - \deg(f)$ for $f.g \in K[t]$ and $g \neq 0$.[4] Now consider $A = K[t^{-1}]$, then $v_\infty = v_{(t^{-1})}$. In particular, $\mathcal{O}_v = A_{(t^{-1})} = K[t^{-1}]_{(t^{-1})}$.

5.2 Orders

Definition 5.14 (Order)**.** An order R in a normal domain $A \subseteq Q(R)$ is a Noetherian subring of Krull dimension at most 1 with integral closure A.

Lemma 5.15. An integral extension B of an order R that is a domain and finitely-generated as an R-algebra is also an order.

Theorem 5.16 (Krull-Akizuki)**.** Let A be a Noetherian domain with $\dim(A) \leq 1$ and $K = Q(A)$. Let L/K be a finite extension and B is any subring of L containing A. Then B is Noetherian and $\dim(B) \leq 1$.

Corollary 5.17. Let A be an order and $K = Q(A)$ and L/K is a finite extension and B is the integral closure of A in L. Then B is a Dedekind domain.

In particular, for a number field F, we know that any subring of F is finitely-generated over $\mathbb{Z}$ if and only if it is contained in $\mathcal{O}_F$. So an order in $\mathcal{O}_F$ is exactly a subring that is finitely-generated over $\mathbb{Z}$ and has rank $[F : \mathbb{Q}]$.

Example 5.18. Let F be a number field and $F = \mathbb{Q}(\alpha)$ where $\alpha \in \mathcal{O}_F$. Then $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_F$ is an order.

Definition 5.19 (Discriminant)**.** The discriminant $disc(R)$ of an order R in $\mathcal{O}_F$ is its discriminant relative to a $\mathbb{Z}$-basis.

Remark 5.20. $disc(R) = [\mathcal{O}_F : R]^2 disc(\mathcal{O}_F)$. So if $disc(R)$ is square-free, then $R = \mathcal{O}_F$.

[4] Here we assume $\deg(0) = -\infty$.

Definition 5.21 (Conductor)**.** Let R be an order with integral closure A. The conductor f_R of R is $f_R = \{a \in A \mid aA \subseteq R\}$.

Remark 5.22. f_R is the largest ideal of A contained in R, so it is also an ideal of R.

Lemma 5.23. $f_R \neq 0$ if and only if A is a finitely-generated R-module.

Proof. ($\Leftarrow$): Let A be finitely-generated as an R-module, so $A = \sum_{i=1}^{m} Ra_i$, then there exists $r_i \in R \backslash \{0\}$ such that $r_i a_i \in R$ (as $A \subseteq Q(R)$). Now $r_1 \cdots r_m \in f_R$, which is nonzero, and we are done.

($\Rightarrow$): Consider $r \in f_R \backslash \{0\}$ and $r : AA \hookrightarrow R$ is the map $x \mapsto rx$ and $rA \cong A$ (as R-modules), so R is Notherian implies rA is finitely generated over R (since it is an ideal of R). $\square$

6 Lecture 6, October 5, 2022

Example 6.1. Suppose $d \neq 1$ is square-free, then $f_{\mathbb{Z}[\sqrt{d}]} = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \equiv 2,3 \pmod 4 \\ 2\mathbb{Z}[\sqrt{d}], & d \equiv 1 \pmod 4 \end{cases}$.

Lemma 6.2. Let A be Dedekind and $K = Q(A)$, and L/K is a finite extension and B is the integral closure of A in L. Suppose $L = K(\alpha)$ with $\alpha \in B$, then $D(1, \alpha, \cdots, \alpha^{n-1}) \in f_{A[\alpha]}$.

Proposition 6.3. Let R be an order and $\mathfrak{p} \subseteq R$ is a nonzero prime ideal and A is the integral closure of R in $Q(R)$. Suppose $f_R \neq 0$, then $\mathfrak{p} \not\supseteq f_R$ if and only if $R_\mathfrak{p}$ is a DVR.

Example 6.4. Consider $\mathbb{Z}[\sqrt{5}]$ with $\mathfrak{p} = (2, 1-\sqrt{5})$. Then

$$\mathbb{Z}[\sqrt{5}]/\mathfrak{p} \cong \mathbb{Z}[x]/(x^2-5, 2, 1-x) \cong \mathbb{F}_2[x]/(x-1) \cong \mathbb{F}_2,$$

so $\mathfrak{p}$ is prime. Now $\mathfrak{p} \supset (2) = f_{\mathbb{Z}[\sqrt{5}]}$, and $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, and the ideal $\mathfrak{p}A = (2)$ is prime:

$$\mathbb{Z}[\frac{\sqrt{5}-1}{2}]/(2) \cong \mathbb{Z}[x]/(x^2+x-1, 2) \cong \mathbb{F}_2[x]/(x^2+x+1) \cong \mathbb{F}_4[x].$$

Therefore, we have an embedding $\mathbb{Z}[\sqrt{5}]/\mathfrak{p} \hookrightarrow A_{\mathfrak{p}A}/\mathfrak{p}A$, but their isomorphism fields give $\mathbb{F}_2 \hookrightarrow \mathbb{F}_4$ is not an isomorphism, and so $\mathbb{Z}[\sqrt{5}]/\mathfrak{p} \ncong A_{\mathfrak{p}A}$ with $A = \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. Hence, $\mathfrak{p}\mathbb{Z}[\sqrt{5}]_\mathfrak{p}$ is not principal: for $v_{(2)} : \mathbb{Q}(\sqrt{5}) \to \mathbb{Z} \cup \{\infty\}$, we have $v_{(2)}(2) = 1$ and $v_{(2)}(\sqrt{5}-1) = 1$. So if $2a + (\sqrt{5}-1)b$ generates $p\mathbb{Z}[\sqrt{5}]_\mathfrak{p}$, it has 2-adic valuation 1, and then it is associated to 2 (say $b \notin \mathfrak{p}\mathbb{Z}[\sqrt{5}]_\mathfrak{p}$), for example

$$\frac{2a + b(\sqrt{5}-1)}{2} \in \mathbb{Z}[\sqrt{5}]_\mathfrak{p}^\times$$

which means $b\frac{\sqrt{5}-1}{2} \in \mathbb{Z}[\sqrt{5}]_\mathfrak{p}$, contradiction.

This shows that the order is not a DVR, and therefore the proposition fails.

Proof. Suppose $f_R \not\subseteq \mathfrak{p}$. Let $x \in f_R$ and $x \notin \mathfrak{p}$. Then $xA \subseteq R$ and $x \in R_\mathfrak{p}^\times$. Thus, $A \subseteq R_\mathfrak{p}$. Let $\mathfrak{q} = A \cap \mathfrak{p}R_\mathfrak{p}$ be a prime ideal of A. containing $\mathfrak{p}$. As $\mathfrak{q} \cap R$ is prime in R, $\mathfrak{p} = \mathfrak{q} \cap R$ as $\dim(R) \leq 1$. Note $R_\mathfrak{p} \subseteq A_\mathfrak{q}$. If $\frac{a}{s} \in A_\mathfrak{q}$ with $a \in A$ and $s \in A \backslash \mathfrak{q}$, then $xa \in R$ and $xs \in R \backslash \mathfrak{p}$, and so $\frac{a}{s} = \frac{xa}{xs} \in R_\mathfrak{p}$. Therefore, $R_\mathfrak{p} = A_\mathfrak{q}$.

Claim 6.5. $\mathfrak{q} = \mathfrak{p}A$.

Subproof. Note $\mathfrak{q} \mid \mathfrak{p}A$ by definition. If $\mathfrak{q}'$ prime with $\mathfrak{q}' \mid \mathfrak{p}A$, then $A_{\mathfrak{q}'} \supseteq R_\mathfrak{p} = A_\mathfrak{q}$. Since $\mathfrak{q}'$ is maximal, then $A_{\mathfrak{q}'} = A_\mathfrak{q}$, and so $\mathfrak{q}' = \mathfrak{q}$. Thus, $\mathfrak{p}A = \mathfrak{q}^e$ for some $e \geq 1$. Therefore, $\mathfrak{p}R_\mathfrak{p} = \mathfrak{p}A_\mathfrak{q} = \mathfrak{q}^e A_\mathfrak{q}$, which is maximal in $R_\mathfrak{p} = A_\mathfrak{q}$, so $e = 1$. Thus, $\mathfrak{p}A = \mathfrak{q}$. ■

Conversely, suppose $R_\mathfrak{p}$ is a DVR. Then $R_\mathfrak{p}$ is normal. Since A is integrally closed in R, then $A \subseteq R_\mathfrak{p}$, then $\mathfrak{p} = R \cap \mathfrak{p}R_\mathfrak{p} \supseteq R \cap \mathfrak{p}A$, so $\mathfrak{p} = R \cap \mathfrak{p}A$. Write $A = \sum_{i=1}^n Ra_i$, where $a_i \in A$ for $1 \leq i \leq n$ (since $f_R \neq 0$). Then $a_i = \frac{y_i}{s_i}$ for $y_i \in R$ and $s_i \in R \backslash \mathfrak{p}$. Take $s = s_1 \cdots s_n$, now $sa_i \in R$ for all i, and so $s \in f_R$, and $s \notin \mathfrak{p}$. So $\mathfrak{p} \not\supseteq f_R$. □

Lemma 6.6. Let F be a number field and $R \subseteq \mathcal{O}_F$ be an order. The prime numbers dividing $[\mathcal{O}_F : R]$ are exactly those dividing a generator of $f_R \cap \mathbb{Z}$.

Proof. $f_R \cap \mathbb{Z} = (f)$. Now $f\mathcal{O}_F \subseteq R$, so f is a multiple of exponent of $\mathcal{O}_{F/R}$. If $p \mid f$ but not $[\mathcal{O}_F : R]$, there exists prime $\mathfrak{p}$ of $\mathcal{O}_F$ with $\mathfrak{p} \cap \mathbb{Z} = (p)$ and dividing f_R. Set $\mathfrak{g} = \mathfrak{p}^{-1} f_R$ as an ideal of $\mathcal{O}_F$.

Now there is $p : \mathcal{O}_F/R \xrightarrow{\sim} \mathcal{O}_F/R$, so $\mathfrak{g}\mathcal{O}_F/R = \mathfrak{p}\mathfrak{g}\mathcal{O}_F/R \subseteq f_R\mathcal{O}_F/R = 0$. Therefore, $\mathfrak{g}$ is contained in the conductor, but it is not by definition, contradiction. □

6.1 Ramification

Let A be Dedekind and $K = Q(A)$ and L/K is a finite extension and B is integral closure of A in L.

Because $\mathfrak{p}$ is prime in A, then $\mathfrak{p}B = \prod_{i=1}^{g} P_i^{e_i}$ where P_i's are distinct primes and $e_i \geq 1$ for all i, and for some $g \geq 1$.

Definition 6.7. (a) $\mathfrak{p}$ ramifies in B/A (or L/K) if $e_i \geq 2$ for some i. We then say P_i is ramified in B/A.

(b) $\mathfrak{p}$ is inert in B/A if $\mathfrak{p}B$ remains prime.

(c) $\mathfrak{p}$ splits in B/A if $g \geq 2$.

Example 6.8. Let $A = \mathbb{Z}$, and $L = \mathbb{Q}(\sqrt{-5})$ and $\mathcal{O}_L = \mathbb{Z}[\sqrt{-5}]$. Now (2) ramifies $(2, 1 - \sqrt{-5})^2 = (2)$, and (5) ramifies $(\sqrt{-5})^2 = (5)$. (3) splits: $\mathbb{Z}[x]/(3, x^2+5) \cong \mathbb{F}_3[x]/(x^2-1) \cong \mathbb{F}_3 \times \mathbb{F}_3$, and $(3) = (3, \sqrt{-5} - 1)(3, \sqrt{5} + 1)$.

(7) also splits, and (11) is inert: $-5 \notin \mathbb{F}_{11}^{\times 2}$, $\mathbb{Z}[\sqrt{-5}]/(11) \cong \mathbb{F}_{121}$.

Definition 6.9 (Residue Field)**.** The residue field of $\mathfrak{p}$ is $A/\mathfrak{p}$.

Remark 6.10. If $P \mid \mathfrak{p}$, then $(B/P)/(A/\mathfrak{p})$ becomes a field extension, an extension of residue field.[5]

Definition 6.11. $e_{P/\mathfrak{p}}$, called the ramification index, is the largest e such that $P^e \mid \mathfrak{p}$.

$f_{R/\mathfrak{p}}$, called the residue degree, is $[B/P : A/\mathfrak{p}]$.

Definition 6.12 (Lying Over, Lying Under)**.** If $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals of A and B, respectively, such that $\mathfrak{q} \cap A = \mathfrak{p}$, (note that $\mathfrak{q} \cap A$ is automatically a prime ideal of A,) then we say that $\mathfrak{p}$ lies under $\mathfrak{q}$ and that $\mathfrak{q}$ lies over $\mathfrak{p}$.

A ring extension $A \subseteq B$ of commutative rings is said to satisfy the lying over property if every prime ideal $\mathfrak{p}$ of A lies under some prime ideal $\mathfrak{q}$ of B.

[5] We usually say P is a prime of B lying over $\mathfrak{p}$.

7 Lecture 7, October 7, 2022

As usual, let A be a Dedekind domain, $K = Q(A)$, L/K is a finite extension, and B is the integral closure of A in L.

Theorem 7.1. Write $\mathfrak{p}R = P_1^{e_1} \cdots P_g^{e_g}$ with P_i distinct and $e_i \geq 1$, then $e_i = e_{P_i}/\mathfrak{p}$ and set $f_i = f_{P_i}/\mathfrak{p}$, then $\sum_{i=1}^{g} e_i f_i = [L : K]$.

We will use the folloing lemma to prove the theorem.

Lemma 7.2. Suppose $S \subseteq A$ is a multiplicatively closed set. Let P be a set of primes of A such that $S \cap \mathfrak{q} = \varnothing$ for all $\mathfrak{q} \in P$. Let $\mathfrak{a}$ be a nonzero ideal of A is divisible only by primes in P, then

$$A/\mathfrak{a} \xrightarrow{\sim} S^{-1}A/S^{-1}\mathfrak{a}.$$

Proof. Injective: Let $b \in S^{-1}\mathfrak{a} \cap A$, then $b = \frac{a}{s}$ for $a \in \mathfrak{a}$ and $s \in S$. Therefore, $(s) + \mathfrak{a} = A$. Then $b \in \mathfrak{a}$ by the unique factorization into primes.

Surjective: For $c \in A$ and $t \in S$, we have $(t) + \mathfrak{a} = A$, so there exists $u \in A$ such that $ut - 1 \in A$. Then we have $cu + \mathfrak{a} \mapsto \frac{c}{t} + S^{-1}\mathfrak{a}$. □

Proof of Theorem. When considering them as $A/\mathfrak{p}$-algebras, we have

$$B/\mathfrak{p}B = \prod_{i=1}^{g} B/P_i^{e_i}$$

by the Chinese Remainder Theorem. Now $\dim_{A/\mathfrak{p}A} B/\mathfrak{p}B = \sum_{i=1}^{g} \sum_{j=r}^{e_i - 1} \dim_{A/P_i}(P_i^j/P_i^{j+1})$. This equals to $\sum_{i=1}^{g} e_i f_i$ because

$$P_i^j/P_i^{j+1} \cong P_i^j B_{P_i}/P_i^{j+1} B_{P_i}$$

is one-dimensional over $B_{P_i}/P_i \cong B/P_i$. Consider $S_\mathfrak{p} = A \backslash \mathfrak{p}$, then $S_\mathfrak{p}^{-1}B$ is the integral closure of A_p in L, so $S_\mathfrak{p}^{-1}B$ is free of rank $[L : K]$ over $A_\mathfrak{p}$. Then $B/\mathfrak{p}B$ is isomorphic to $S_\mathfrak{p}^{-1}B/\mathfrak{p}S_\mathfrak{p}^{-1}B$ by lemma, and so it is $[L : K]$-dimensional over $A/\mathfrak{p}$, i.e. $\dim_{A/\mathfrak{p}}(B/\mathfrak{p}B) = [L : K]$. □

Example 7.3. Let $[L : K] = 2$. Now $\mathfrak{p}B = P_1 P_2$ splits where P_1 and P_2 have residue degree 1, and $\mathfrak{p} = P_1^2$ ramified has residue degree 1, and $\mathfrak{p} = P_1$ inert has residue degree 2.

Let $[L : K] = 3$. Now $\mathfrak{p}B = P_1 P_2 P_3$ is completely split and each P_i has residue degree 1. The possibilities are $P_1^2 P_2$, where each has residue degree 1, and $P_1 P_2$, where P_1 has degree 2 and P_2 has degree 1, and P_1^3 which is totally ramified with degree 1, and P_1 which is inert with degree 3.

Theorem 7.4 (Kummer-Dedekind)**.** Let $h \in A[x]$ be the minimal polynomial of α, and $\bar{h} \in A/\mathfrak{p}[x]$ is its reduction modulo $\mathfrak{p}$. Suppose $\mathfrak{p}B + f_{A[\alpha]} + B$. Write $\bar{h} = \bar{h}_1^{e_1} \cdots \bar{h}_g^{e_g}$, with $\bar{h}_i$ distinct irreducible with $e_i \geq 1$. Let $h_i \in A[x]$ be a lift of $\bar{h}_i$. Set $P_i = \mathfrak{p}B + (h_i(\alpha))$. Then P_i's are distinct primes over $\mathfrak{p}$, and $\mathfrak{p}B = \prod_{i=1^g} P_i^{e_i}$, and $f_{P_i/\mathfrak{p}} = \deg(\bar{h}_i)$.

Proof. Set $F = A/\mathfrak{p}$, then

$$\begin{aligned} A[\alpha]/\mathfrak{p}A[\alpha] &\cong A[x]/(\mathfrak{p}A[x] + (h)) \\ &\cong F[x]/(\bar{h}) \\ &\cong \prod_{i=1}^{g} F[x]/(\bar{h}_i^{e_i}). \end{aligned}$$

Let $Q_i = \mathfrak{p}A[\alpha] + (h_i(\alpha)) \subseteq A[\alpha]$ and let $\varphi_i : A[\alpha] \twoheadrightarrow F[x]/(\bar{h}_i^{e_i})$.

Claim 7.5. $\ker(\varphi_i) = Q_i^{e_i}$.

Subproof. Since the $\bar{h}_i$'s are relatively prime, so are the Q_i's, and $A[\alpha]/Q_i \cong F[x]/(\bar{h}_i)$ so Q_i's are prime. Therefore, $[A[\alpha]/Q_i : F] = f_i := \deg(\bar{h}_i)$. Then $A[\alpha]/Q^{e_i} \cong A[\alpha]_{Q_i}/Q_i^{e_i}A[\alpha]_{Q_i}$. Since $Q_i = P_i \cap A[\alpha]$, $f_{A[\alpha}$'s are prime, and the ring $A[\alpha]_{Q_i}$ is a DVR, so only ideals of $A[x]/Q_i^{e_i}$ are $Q_i^j/Q_i^{e_i}$ for $0 \le j \le e_i$. Therefore,

$$\ker(A[\alpha]/Q_i^{e_i} \twoheadrightarrow F[x]/(\bar{h}_i^{e_i})) = 0,$$

which means $\ker(\varphi_i) = Q_i^{e_i}$. ■

Now we know

$$\prod_{i=1}^{g} A[\alpha]/Q_i^{e_i} \cong \prod_{i=1}^{g} F[x]/(\bar{h}_i^{e_i})$$

and so $\mathfrak{p}A[\alpha] = \prod_{i=1}^{g} Q_i^{e_i}$, and so $\mathfrak{p}B = \prod_{i=1}^{g} P_i^{e_i}$.

Now $P_i = Q_iB$ is prime and the residue fields $B_{P_i} \cong A[alpha]_{Q_i}$, so P_i are distinct and $f_{P_i/\mathfrak{p}} = \deg(\bar{h}_i)$. □

Example 7.6. Let $h(x) = x^3 + x + 1$, then it is irreducible in $\mathbb{Q}[x]$. Let $L = Q(\alpha)$ and $h(\alpha) = 0$. Exercise: the discriminant of $\mathbb{Z}[\alpha] = -31$. Therefore, the discriminant is square-free, so $\mathcal{O}_L = \mathbb{Z}[\alpha]$. Now $h(x)$ is irreducible modulo 2, so (2) is inert in L. Also, $h(x) = (x-1)(x^2+x-1)$ modulo 3, so $3\mathbb{Z}[\alpha] = P_1P_2$ with residue degree 1 and 2 respectively, where $P_1 = (3, \alpha - 1)$ and $P_2 = (3, \alpha^2 + \alpha - 1)$.

Corollary 7.7. Let p be an odd prime and $a \in \mathbb{Z}$ is square-free with $p \nmid a$. Then $a \in \mathbb{F}_p^{\times 2}$ if and only if (p) splits in $\mathbb{Q}(\sqrt{a})$.

Proof. Note $f_{\mathbb{Z}[a]} \mid 2$. We can determine $p\mathcal{O}_{\mathbb{Q}(\sqrt{a})}$ by factoring $x^2 - a$ modulo p. Because $p \nmid a$, then $x^2 - a$ is not a square modulo p. So (p) splits if and only if $x^2 - a$ splits over $\mathbb{F}_p$, if and only if $a \in \mathbb{F}_p^{\times 2}$. □

Proposition 7.8. If $\mathfrak{p}$ ramifies in B, then $\mathfrak{p} \mid D(1, \alpha, \cdots, \alpha^{[L:K]-1}) =: d(\alpha)$.

Proof. Let h be the minimal polynomial of α. Suppose $\mathfrak{p} + f_{A[\alpha]} = (1)$, then by Theorem 7.4, $\mathfrak{p}$ ramifies in B if and only if $\bar{h}$ is divisible by a square, i.e. $\bar{h}$ has a multiple root, and that is true if and only if $d(\alpha) \equiv 0 \pmod{\mathfrak{p}}$.

Note that $f_{A[\alpha]} \mid (d(\alpha))$, and $(d(\alpha))$ is an ideal of A and $f_{A[\alpha]}$ is an ideal of $A[\alpha]$. So if $p + f_{A[\alpha]} \neq (1)$, then $\mathfrak{p} \mid (d(\alpha))$. □

Corollary 7.9. Only finitely-many primes are ramified in L/K.

Lemma 7.10. Let $b \in B$. Every prime of B dividing (b) lies over a prime of A dividing $N_{L/K}A$. Every prime of Adividing $N_{L/K}(b)$ lies below some prime of B dividing (b).

Corollary 7.11. $b \in B^\times$ if and only if $N_{L/K}(b) \in A^\times$.

8 Lecture 8, October 10, 2022

Example 8.1. $\mathbb{Z}[\sqrt{5}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. Notice that 2 is inert in $\mathbb{Q}(\sqrt{5})$, $(2) = f_{\mathbb{Z}[\sqrt{5}]}$, where $x^2 - 5 \equiv (x-1)^2 \pmod 2$. However, $2\mathbb{Z}[\sqrt{5}] \neq (2, \sqrt{5}-1)^2 = (4, 2(\sqrt{5}-1))$.

Exercise 8.2. Let A be a domain, $K = Q(A)$, L/K is separable, and B is integral closure of A in L. Given $\mathfrak{A} \subseteq B$ is a nonzero ideal, there exists $\alpha \in B$ such that $L = K(\alpha)$ and $\mathfrak{A} + f_{A[\alpha]} = B$.

In particular, we can always apply Kummer-Dedekind Theorem to get factorization of pB for p prime of A.

8.1 Decomposition Groups

Suppose we take the notation in the exercise above, but now L/K is a Galois extension, and $G = \mathbf{Gal}(L/K)$. Let $p \subseteq A$ be prime and P be prime of B over p.

Definition 8.3 (Galois Conjugate)**.** For $\sigma \in G$, $\sigma(P)$ is called a Galois conjugate of P. This is essentially an orbit.

Proposition 8.4. All primes of B over p are conjugate, i.e. G acts transitively on the set of primes over p.

Proof. Let Q be a prime that is not $\sigma(P)$ for all $\sigma \in G$. By the Chinese Remainder Theorem, there exists $b \in Q$ such that $b \equiv 1 \pmod{\sigma(P)}$ for all $\sigma \in G$. Then $N/_{L/K}(b) \in Q \cap A$ and $N_{L/K}(b) \equiv 1 \pmod p$, so $Q \cap A \neq p$. ☐

Definition 8.5. The decomposition group G_P of P is the stabilizer of P under the action of G on primes.

By the orbit-stabilizer theorem, there is a bijection from set of cosets G/G_P to the set of primes of B over p (prime of A), given by $\sigma \mapsto \sigma \cdot P$.

Proposition 8.6. $f_{P/p}$ and $e_{P/p}$ are independent of choice of P/p.

Proof. Let S be the set of coset representatives of G/G_P. Now $pB = \prod_{\sigma \in S} (\sigma P)^{e_{\sigma P/p}}$. If $\tau \in G$, then $pB = \tau pB = \prod_{\sigma \in S} (\tau\sigma P)^{e_{\sigma P/p}}$. Therefore, $e_{P/p} = e_{\tau P/p}$ for all τ by uniqueness of factorization. Note that $\tau : B/P \xrightarrow{\sim} B/\tau P$ is an isomorphism of A/p-vector spaces, so they have the same dimension, i.e. $f_{P/p} = f_{\tau P/p}$. ☐

Corollary 8.7. Suppose $\sigma, \cdots, \sigma_g$ are coset representatives of G/G_P, then $pB = \prod_{i=1}^{g} (\sigma_i P)^e$ with $e = e_{P/p}$. Setting $f = f_{P/p}$, we have $efg = [L : K]$.

Remark 8.8. $G_{\sigma(P)} = \sigma G_P \sigma^{-1}$ for $\sigma \in G$.

So, if L/K is Abelian, then $G_{\sigma(P)} = G_P$, so we can speak of "G_p").

Lemma 8.9. Consider the usual L/K extension. Let $E = L^{G_P}$ be the fixed field and C be the integral closure of A in E. Then P is the only prime of E lying over $\mathfrak{P} = P \cap C$, and the ramification index and residue degree $e_{\mathfrak{P}/p} = f_{\mathfrak{P}/p} = 1$. Therefore, p splits completely in E/K and $G_P = \mathbf{Gal}(L/E)_P = \mathbf{Gal}(L/E)$.

Proof. $\mathbf{Gal}(L/E)_P = \mathbf{Gal}(L/E)$, so P is the only prime over $\mathfrak{P}$ by transitivity. Now $e_{P/\mathfrak{P}} f_{P/\mathfrak{P}} = [L : E]$. There are $g = [E : K]$ primes dividing p in L. Therefore, $e_{P/\mathfrak{P}} f_{P/\mathfrak{P}} g = [L : K]$, but $e_{P/p} f_{P/p} g = [L : K]$. Since $e_{P/\mathfrak{P}} \mid e_{P/p}$ and $f_{P/\mathfrak{P}} \mid f_{P/p}$, we have $e_{P/\mathfrak{P}} = e_{P/p}$ and $f_{P/\mathfrak{P}} = f_{P/p}$, so $e_{\mathfrak{P}/p} = f_{\mathfrak{P}/p} = 1$. □

Proposition 8.10. Set $K_P = B/P$ and $K_P = A/P$, the extension K_P/K_p is normal, and $\pi_P : G_P \to \mathbf{Gal}(K_P/K_p)$ given by $\sigma \mapsto (b + P \mapsto \sigma b + P)$ is a surjective homomorphism.

Proof. Let $\alpha \in B$. Let $f \in A[x]$ be its minimal polynomial. Consider $f \mapsto \bar{f} \in A_p[x] = K_p[x]$. Then $\alpha \mapsto \bar{\alpha} \in K_P$ and $\bar{\alpha}$ is a root of $\bar{f}$. Since f splits completely in L, with roots in B, $\bar{f}$ splits completely in the residue field K_P. Therefore, the minimal polynomial of $\bar{\alpha}$ under K_p splits completely as it divides $\bar{f}$. This is saying that the extension is normal.

π_P is obviously a well-defined homomorphism. We now prove surjectivity. Let $\bar{\sigma} \in \mathbf{Gal}(K_P/K_p)$. Let $E = L^{G_P}$ and C be the integral closure of A in E and $\mathfrak{P} = P \cap C$. Let $\bar{\theta} \in K_P$ generate the maximal separable subextension of K_P/K_p (note that $K_p = C/\mathfrak{P}$). Let $\theta \in B$ lift $\bar{\theta}$. Let $g \in C[x]$ be the minimal polynomial of θ over E. Let $\bar{g} \in K_p[x]$ be its residue modulo $\mathfrak{P}$, so $\bar{g}(\bar{\theta}) = 0$. Let $\bar{h} \in K_p[x]$ be the minimal polynomial of $\bar{\theta}$, so $\bar{h} \mid \bar{g}$. Then $\bar{g}(\bar{\sigma}(\bar{\theta})) = 0$ as well, so there exists a root of g, say $\theta' \in B$ such that $\theta' \mapsto \bar{\sigma}(\bar{\theta})$, then there exists $\sigma \in G$ such that $\sigma(\theta) = \theta'$. Then the reduction at $\sigma(\theta)$, $\pi_P(\sigma)(\bar{\theta}) = \bar{\sigma}(\bar{\theta})$. This forces $\pi_P(\sigma) = \bar{\sigma}$, as $\bar{\theta}$ generates a maximal separable subextension of K_P/K_p. This proves the surjectivity. □

Definition 8.11. The inertia group I_P of I over p is $\ker(\pi_P)$.

This gives an exact sequence

$$1 \to I_P \to G_P \xrightarrow{\pi_P} \mathbf{Gal}(K_P/K_p) \to 1$$

If K_P/K_p is separable, then $|\mathbf{Gal}(K_P/K_p))| = f_{P/p}$, so $|I_P| = e_{P/p}$.

Example 8.12. Let $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ over $K = \mathbb{Q}(\zeta_3)$. Now $G = \mathbf{Gal}(L/\mathbb{Q}) \rhd N = \mathbf{Gal}(L/K)$. We know that $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}]$.

Now, (2) is inert in $K/\mathbb{Q}$ as $x^2 + x + 1$ is irreducible modulo 2 and ramifies in L/K since $(2) = (\sqrt[3]{2})^3$, here $f_{(\sqrt[3]{2})/(2)} = 2$ and $I_{(\sqrt[3]{2})} = N$ and $G_{(\sqrt[3]{2})} = G$.

Moreover, (3) is totally ramified: $I_P = G$ and $3\mathcal{O}_L = P^6$.

We also know (5) is inert in K and splits in L/K: $x^3 - 2$ has a single root (3) modulo 5 and splits over $\mathbb{F}_{25}$. So $5\mathcal{O}_L = Q_1Q_2Q_3$, and $G_{Q_i} = \mathbf{Gal}(L/E_i)$ where $E_i = \mathbb{Q}(\zeta_3^{i-1}\sqrt[3]{2})$. Here we have $E_1 = \mathbb{Q}(\sqrt[3]{2})$, $5\mathcal{O}_{E_1} = \mathfrak{q}_1\mathfrak{q}_2$, then $Q_1 \mid \mathfrak{q}_1$ and $Q_2, Q_3 \mid \mathfrak{q}_2$. Here $f_{\mathfrak{q}1|(5)} = (1)$ and $f_{\mathfrak{q}2/(5)} = f_{\mathfrak{q}3/(5)=2}$. Therefore, $I_{Q_i} = 1$ for all i, and GQ_1 permutes Q_2 and Q_3.

9 Lecture 9, October 12, 2022

Definition 9.1 (Absolute Norm)**.** Let L/K be a Galois extension of number fields, let $G = \mathrm{Gal}(L/K)$. Consider the extension P/p of $P \subseteq \mathcal{O}_L$ and $p \subseteq \mathcal{O}_K$. Then the absolute norm of P is $N(P) = [\mathcal{O}_L : P]$.

Definition 9.2 (Frobenius Element)**.** A Frobenius element at P for L/K is $\varphi_P \in G$ such that $\varphi_P(x) = x^{N_p} \pmod{P}$.

For the map $\pi_P : G_P \twoheadrightarrow \mathrm{Gal}(\mathcal{O}_{L/P}/\mathcal{O}_{K/p})$, we have $\pi_P(\sigma)(y) = y^{N_p}$. Note that the Galois group has a generator.

There are two types of global fields.

1. Number fields.

2. Function fields: finite extension of $\mathbb{F}_p(x)$ for some p in $\mathbb{F}_p(x)$, there are many Dedekind subrings, e.g. $\mathbb{F}_p[x]$.

In both cases, residue fields are finite.

Note that the Galois group is an finite extension, so it makes sense to talk about a Frobenius element.

9.1 Cyclotominc Fields

Let K be a field and $n \geq 1$. We denote $\mu_n(K)$ to the the nth roots of unity of K. Now $\mu_n(\bar{K})$ has order N if and only if $\mathrm{char}(K) \nmid n$.

Definition 9.3 (Cyclotomic Field)**.** The field $\mathbb{Q}(\mu_n)$ is the nth cyclotomic field.

The field $\mathbb{Q}(\mu_n)$ is Galois over $\mathbb{Q}$, as it is the splitting field of $x^n - 1$. All nth roots of unity are powers of any primitive nth root of unity ζ_n, so $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n)$.

Definition 9.4 (Cyclotomic Polynomial)**.** The nth cyclotomic polynomial $\Phi_n \in \mathbb{Z}[x]$ is the polynomial which has as its roots the primitive nth roots of unity. Note that $x^n - 1 = \prod\limits_{d|n} \Phi_d(x)$.

Definition 9.5 (Mobius Function)**.** The Mobius function $\mu : \mathbb{Z}_{\geq 1} \to \mathbb{Z}$ sends an integer n to $(-1)^k$ when $n = p_1 \cdots p_k$ where p_i's are distinct, and 0 otherwise.

Proposition 9.6 (Mobius Inversion Formula)**.** Let $f, G : \mathbb{Z}_{\geq 1} \to A$ where A be an Abelian group, and such that $F(n) = \sum\limits_{d|n} f(A)$, then $f(n) = \sum\limits_{d|n} \mu(\frac{n}{d})F(d)$.

Lemma 9.7. For all $n \geq 1$, we have $\Phi_n = \prod\limits_{d|n}(x^d - 1)^{\mu(\frac{n}{d})}$.

Proof. Use Mobius Inversion Formula. $\square$

Example 9.8. $\Phi_{15} = \frac{(x^{15}-1)(x-1)}{(x^5-1)(x^3-1)} \cdots$.

$\Phi_{p^n} = x^{p^{n-1}(p-1)} + \cdots + x^{p^{n-1}} + 1$.

Lemma 9.9. If $i, j \geq 1$ are relatively prime to n, then $\frac{1-\zeta_n^i}{1-\zeta_n^j} \in \mathbb{Z}[\mu_n]^\times = \mathcal{O}_{\mathbb{Q}(\mu_n)}^\times$.

Proof. Take $k \in \mathbb{Z}$ such that $jk \equiv 1 \pmod{n}$, then $1-\zeta_n^i = 1-\zeta_n^{ijk}$, and as $1-x^j$ divides $1-x^{ijk}$, then $\frac{1-\zeta_n^i}{1-\zeta_n^j} \in \mathbb{Z}[\mu_n]$, so this is a unit. □

Lemma 9.10. Let p be a prime number and $r \geq 1$. Then the absolute value of the discriminant of $\mathbb{Z}[\mu_{p^r}]$ is a power of p, and (p) is the only prime of $\mathbb{Z}$ that ramifies in $\mathbb{Q}(\mu_{p^r})$. It is totally ramified and lies below $(1-\zeta_{p^r})$. Moreover, $[\mathbb{Q}(\mu_{p^r}) : \mathbb{Q}] = p^{r-1}(p-1)$.

Proof. Note that $[\mathbb{Q}(\mu_{p^r}) : \mathbb{Q}] \mid \deg(\Phi_{p^r}) = p^{r-1}(p-1)$. By the lemma, we have

$$\prod_{i=1, p\nmid i}^{p^r-1} (1-\zeta_{p^r}^i) = \Phi_{p^r}(1) = p.$$

Therefore, $p.Z[\mu_{p^r}] = (1-\zeta_{p^r})^{p^{r-1}(p-1)}$, which is the same in $\mathcal{O}_{\mathbb{Q}(\mu_{p^r})}$.

Now $efg = [\mathbb{Q}(\mu_{p^r}) : \mathbb{Q}]$, so all claims about ramifications of p holds because $e = p^{r-1}(p-1)$.

Then $\operatorname{disc}(\mathbb{Z}[\mu_{p^r}] = \prod_{1 \leq i < j \leq p-1} (\zeta_{p^j} - \zeta_{p^i})^2$, but they are primes dividing p, so the result on discriminant holds. □

Proposition 9.11. The nth cyclotomic polynomial is irreducible for all $n \geq 1$. In other words, $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \varphi(n)$, where φ is Euler's phi-function. Moreover, the prime ideals of $\mathbb{Z}$ that ramify in $\mathcal{O}_{Q(\mu_n)}$ are those generated by the odd primes dividing n and, if n is a multiple of 4, the prime 2.

Proof. Note that $\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{2n})$ if n is odd, so we may ask the case when n is odd or $4 \mid n$, let $n = p_1^{r_1} \cdots p_k^{r_k}$. Now $\mathbb{Q}(\mu_n) = \prod_i \mathbb{Q}(\mu_{p_i}^{r_i})$, here p_i's are ramified in $\mathbb{Q}(\mu_{p_i}^{r_i})$, so it is in $\mathbb{Q}(\mu_n)$. Also, if no other primes ramified in any $\mathbb{Q}(\mu_{p_i}^{r_i})$, then it is not in $\mathbb{Q}(\mu_n)$.

Since p_i is totally ramified in $\mathbb{Q}(\mu_{p_i}^{r_i})$ but unramified in $\mathbb{Q}(\mu_{p_i}^{r_i})$, these two fields have intersection $\mathbb{Q}$. So $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \prod_{i=1}^k [\mathbb{Q}(\mu_{p_i}^{r_i} : \mathbb{Q}] = \varphi(n)$ by induction. □

Proposition 9.12. $\mathcal{O}_{\mathbb{Q}(\mu_n)} = \mathbb{Z}[\mu_n]$.

Proof. We first consider $n = p^r$ for prime p. Now $f_{\mathbb{Z}[\mu_p^r]} \mid (D(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{p^{r-1}(p-1)-1}) = (\operatorname{disc}(\mathbb{Z}[\mu_{p^r}])) = (p^m)$ for some $m \geq 1$.

Now let $\lambda_r = 1-\zeta_{p^r}$, which generates the unqiue primes over (p) in $\mathbb{Q}(\mu_{p^r})$. Since (p) is totally ramified in $\mathbb{Q}(\mu_{p^r})/\mathbb{Q}$, we have that $\mathcal{O}_{\mathbb{Q}(\mu_{p^r})}/(\lambda_r) \cong \mathbb{Z}/p\mathbb{Z}$. In particular,

$$\begin{aligned}
\mathcal{O}_{\mathbb{Q}(\mu_{p^r})} &= \mathbb{Z}[\mu_{p^r}] + \lambda_r \mathcal{O}_{\mathbb{Q}(\mu_{p^r})} \\
&= \mathbb{Z}[\mu_{p^r}] + \lambda_r(\mathbb{Z}[\mu_r] + \lambda_r \mathcal{O}_{\mathbb{Q}(\mu_{p^r})}) \\
&= \mathbb{Z}[\mu_{p^r}] + \lambda_r^2 \mathcal{O}_{\mathbb{Q}(\mu_{p^r})} \\
&= \cdots \\
&= \mathbb{Z}[\mu_{p^r}] + p^m \mathcal{O}_{\mathbb{Q}(\mu_{p^r})} = \mathbb{Z}[\mu_p^r].
\end{aligned}$$

In the general case, we write $n = p_1^{r_1} \cdots p_k^{r_k}$. We have a basis $\zeta_{p_1^{r_1}}^{i_1} \cdots \zeta_{p_k^{r_k}}^{i_k}$ with $0 \le i_j \le \varphi(p_j^{r_j}) - 1$ of $\mathbb{Z}[\mu_n]$ over $\mathbb{Z}$.

We need the following useful result (1.4.28):

Proposition 9.13. Let A be a normal domain, $K = Q(A)$, and L and L' are linearly disjoint and are finite separable extensions of K. Suppose B and B' are integral closures of A in L and L', respectively. Suppose B is A-free with basis $\beta_1, \cdots, \beta_n$ and B' is A-free with basis $\gamma_1, \cdots, \gamma_m$. Set $d = D(\beta_1, \cdots, \beta_n)$, $d' = D(\gamma_1, \cdots, \gamma_m)$, then $\{\beta_i\gamma_j\}$ has discriminant $d^m(d')^n$. If C is the integral closure of A in LL' and C' is the A-span of $\{\beta_i\gamma_j\}$, then $(d, d')C \subseteq C'$.

Here take $\mathbb{Z}[\mu_{p_k}^{r_k}]$ and $\mathbb{Z}[\mu_n/p_k^{r_k}]$ by induction on k. The discriminants of these rings, d and d', are relatively prime. Therefore, $(d, d')\mathcal{O}_{\mathbb{Q}(\mu_n)} \subseteq \mathbb{Z}[\mu_n]$ by the proposition. Now (d, d') is the unit ideal (1), and we are done. $\square$

We revise linear disjoint for a bit.

Definition 9.14 (Linear Disjoint)**.** Let $L, L' \subseteq \Omega$ be extensions of K. We say L and L' are linearly disjoint over K if every K-linear independent subset of L is linearly independent over L'. Equivalently, $L \otimes_K L' \hookrightarrow LL'$ sends $x \otimes_y \mapsto xy$. If $\Omega = \bar{K}$, this is equivalent to saying $L \otimes_K L'$. If L and L' are finite over K, then this is equivalent to $[LL' : K] = [L : K][L' : K]$. Finally, if L be finite Galois over K, then this is equivalent to $L \cap L' = K$.

10 Lecture 10, October 14, 2022