University of Pennsylvania

Algebraic Number Theory: MATH 620, 621, 702, 703, 720, 721

Professor: Ted Chinburg
Notes By: Caleb McWhorter

2009 – 2011

Last Updated: September 10, 2019

Contents

0 MATH 620

0.1 Algebraic Numbers & Integers

Definition (Algebraic Number/Integer)**.** $\alpha \in \mathbb{C}$ is an algebraic number (respectively, algebraic integer) if α is the root of an equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

for some $n \geq 1$ and some $a_i \in \mathbb{Q}$ (respectively, $a_i \in \mathbb{Z}$). If α is not algebraic, we say that α is transcendental.

Example 0.1.

(i) $\sqrt{2}$ is an algebraic integer as it satisfies $x^2 - 2 = 0$.

(ii) $\frac{\sqrt{2}}{2}$ is an algebraic number but not an algebraic integer.

(iii) $\alpha = e^{2\pi i/n}$, the cyclotomic integers, is an algebraic integer: $x^n - 1 = 0$.

• The number of algebraic numbers is countable (the countable union of countable sets is countable). So 'most' numbers are transcendental. However, how can you tell if a particular number is algebraic or transcendental?

Theorem 0.1 (Liouville)**.** *Suppose $\alpha \in \mathbb{R}$ is algebraic of degree $n > 1$ so that*

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

for some $a_i \in \mathbb{Q}$. Then for all constants $C > 0$ and $\epsilon > 0$, there are only finitely many rationals p/q with $p, q \in \mathbb{Z}$ so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{C}{q^{nt+\epsilon}}$$

• Moral: Algebraic numbers are hard to approximate using rationals. If α does have infinitely many 'good' rational approximations, then it is transcendental.

• This theorem is great at producing transcendental numbers and is the moral behind most transcendence proofs.

Example 0.2. The Liouville number: $\alpha = \sum 10^{-n!}$. Look at $p_i/q_i = \frac{\sum_{n=1}^{i} 10^{i!-n!}}{10^{i!}}$.

$$|\alpha - p_i/q_i| = \sum_{n>i}^{\infty} \frac{1}{10^{n!}}$$

Generally, take an integer $b \geq 2$ and sequence $(a_1, a_2, \ldots)$ with $a_k \in \{0, \ldots, b-1\}$ with infinitely many nonzero and then $x = \sum_{k=1}^{\infty} a_k/b^{k!}$. The above is the special case of $b = 10$ and $a_k = 1$. Generally, letting $q_n = b^{n!}$ and $p_n = q_n \sum_{k=1}^{n} a_k/b^{k!}$

$$0 < \left|x - \frac{p_n}{q_n}\right| = \sum_{k=n+1}^{\infty} \frac{a_k}{b^{k!}} \leq \sum_{k=n+1}^{\infty} \frac{b-1}{b^{k!}} < \sum_{k=(n+1)!}^{\infty} \frac{b-1}{b^k} = \frac{b-1}{b^{(n+1)!}} \sum_{k=0}^{\infty} \frac{1}{b^k} \leq \frac{b-1}{b^{(n+1)!}} \cdot \frac{b}{b-1} = \frac{b}{b^{(n+1)!}} \leq \frac{b^{n!}}{b^{(n+1)!}} =$$

where we have used $n \cdot n! = n \cdot n! + n! - n! = (n+1)! - n!$. In particular, all these numbers are irrational and transcendental. Generally, a Liouville number is an irrational number α with the property that for each positive integer n, there are p, q, with $q > 1$ such that $0 < |x - p/q| < 1/q^n$.

Theorem 0.2 (Hermite, 1878)**.** *e is transcendental.*

Theorem 0.3 (Lindemann, 1882)**.** *π is transcendental.*

A good reference for these proofs is Hardy and Wright "Theory of Numbers".

Theorem 0.4 (Roth's Theorem, 1952)**.** *If α is algebraic of degree > 1 and if $\epsilon > 0$,*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}$$

has finitely many solutions in integer p, q.

• This was first conjectured by Siegel from work by Thue. The proof is ineffective in that it gives no bounds on p, q. Roth won the fields medal because of this work. Roth was supposed to pass his qualifying exams but was a nervous person. So he was told to take a practice test (which turned out to be the real test). He also got into many arguments with Serge Lang and once wrote a terrible book review for him.

Theorem 0.5 (Gelfond-Schneider, 1934)**.** *If α, β are algebraic with $\alpha \notin \{0, 1\}$ and β is not rational, then α^β is transcendental.*

• We need that a, b be algebraic as $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$. In fact, $2^{\sqrt{2}}$ is called the Gelfond-Schneider constant. Gelfond's constant is e^π as well as i^i. Take $(-1)^i = (e^{\pi i})^i = e^\pi$.

Theorem 0.6 (Baker)**.** *If $\beta_1, \beta_2, \alpha_1, \alpha_2$ are algebraic, then either $\beta_1! \log \alpha_1 + \beta_2 \log \alpha_2 = 0$ or there is a compatible lower bound for $|\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2|$ in terms of the sizes of the coefficients in the equation for the α_i and β_j.*

• Baker also won the Fields Medal. This result later was used to prove the class number 1 problem. Stark later gave another solution to the class number 1 problem. But both later learned that an Electrical Engineer named Heeger first solved it but no one believed the proof (it was written oddly).

Theorem 0.7 (Apéry)**.** *$\zeta(3)$ is irrational.*

• $\zeta(3)$ is Apéry's constant. $\zeta(3) \approx 1.202$. This is conjectured to be transcendental. For even integers, $\zeta(n)$ is known to be a rational multiple of a power of π.
• Integrality generalizes the notion of an algebraic number.

Definition (Integral)**.** If $A \subseteq R$ are commutative rings (which are always assumed to have identity), then $x \in R$ is said to be integral over A if it satisfies a monic polynomial with coefficients in A.

Example 0.3.

(i) $A = \mathbb{Q}$ and $R = \mathbb{C}$: α is integral over $\mathbb{Q}$ if and only if α is an algebraic number.

(ii) $A = \mathbb{Z}$ and $R = \mathbb{C}$: α is integral over $\mathbb{Q}$ if and only if α is an algebraic integer.

(iii) $A = F[k]$ and $R = F[u, v]/F[u, v]f$, where $f = v^n + a_{n-1}v^{n-1} + \cdots a_0$ with $a_i \in A$. Then R is the affine ring of the plane curve defined by setting $f = f(u, v) = 0$. Then $x = v$ is integral over A.

Theorem 0.8. *Suppose $A \subseteq R$ commutative rings and $x \in R$. The following are equivalent:*

(i) *x is integral over A*

(ii) *the subring $\langle A, x\rangle$ of R is finitely generated A-module.*

(iii) *There is a subring $B \subseteq R$ such that $A \subseteq B$, $x \in B$, and B is a finitely generated A-module.*

Proof.

$1 \to 2$ If $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. Then $\langle A, x\rangle$ is generated as an A-module by $1, x, \ldots, x^{n-1}$. [Need identity].

$2 \to 3$ Obvious, $B = \langle A, x\rangle$.

$3 \to 1$ Suppose B as given in the theorem statement. Suppose B is generated by $w_1, \ldots, w_n$ as an A–submodule of R, i.e. $B = Aw_1 + \cdots + Aw_n \subseteq R$. Now $xB \subseteq B$. Therefore,

$$\begin{aligned} xw_1 &= a_{1,1}w_1 + \cdots + a_{1,n}w_n \\ xw_2 &= a_{2,1}w_1 + \cdots + a_{2,n}w_n \\ \vdots &= \vdots \\ xw_n &= a_{n,1}w_1 + \cdots + a_{n,n}w_n \end{aligned}$$

Writing this in matrix form, we have $M = xI_n - (a_{ij})$ and $Mm_j = 0$, where m_j is the vector with 0's everywhere except the jth spot. Therefore, we have $\operatorname{cof}(M)^T M = \det M I_n$ kills B: wow $\det M \in R$ and $\det M \cdot w_j = 0$. But $1 \in B$! Then $\det M = 0$ so that x satisfies the polynomial equation given by the determinant. This resulting polynomial is degree n and is monic. □

• This final criterion is very useful as the proof gives an algorithm for finding the equation the element x satisfies. Note then any finitely generated commutative ring containing the given commutative ring is integral over the ring.
• Above, we only need commutative, not even integral domains. The rings could have zero divisors or nilpotents. What happens if R is not commutative? What happens in the above cases? What if R is not commutative but $A \subseteq Z(R)$?

Corollary 0.1. *If $A \subseteq R$ are commutative rings, the set A' of $x \in R$ which are integral over A is a subring of R. The subring A' is called the integral closure of A in R.*

Proof. Say $x, y \in A'$ and $B_x = \langle A, x\rangle$, $B_y = \langle A, y\rangle$. Say the polynomial equation x, y satisfy are of degree n, m, respectively. Then $\{x^i y^j\}_{1 \le i,j \le \max\{n,m\}}$ certainly generates everything in $\langle A, x, y\rangle$. But then taking this to be B, we see $A \subseteq B \subseteq R$ and B is finitely generated so that $x \pm y$ and xy, rx are all in A'. Then A' is a subring. □

• We say that R/A is integral if every element of R is integral over A.

0.2 Norms/Traces, Integral Closures, Prime Ideals

• Think about the analogy $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ and $k[1/x] \subseteq k(x) = k(x^{-1}) \subseteq k((x))$. How far does this analogy go? These lead to the Vojta Conjectures.

Proposition 0.1. *Suppose $A \subseteq R \subseteq C$ with R/A integral and C/R integral. Then C/A is integral.*

Proof. Take $\alpha \in C$. Then $\alpha^n + r_{n-1}\alpha^{n-1} + \cdots + r_0$ for some $r_i \in R$. Each r_i is integral and $A\langle r_i \rangle = A + Ar_i + Ar_i^2 + \cdots + Ar_i^{\deg r_i}$ is a subring of R. To show C is integral over A, we only need find a subring $B \subseteq C$, finitely generated as an A–module so $\alpha \in B \supseteq A$. Taking $B = A\langle \{r_i\}_i, \alpha \rangle$ completes the proof. □

• Suppose A is a commutative noetherian ring and A is integrally closed in $F = \operatorname{Frac} A$. Let L/F be a finite extension of fields. Let A' denote the integral closure of A in L.

$$\begin{array}{ccc} A' & \subseteq & L \\ \cup & & | \\ A & \subseteq & F = \operatorname{Frac} A \end{array}$$

When is A' finitely generated as an A–module? If L/F is in separable, A' need not be finitely generated. The case we will be interested in is when L is a number field ($A = \mathbb{Z}$, $F = \operatorname{Frac} A = \mathbb{Q}$, and then L is a number field). The proof will give a method of writing down the ring of integers in an arbitrary number field.

Theorem 0.9. *In the notation above, A' is finitely generated if L/F is separable (every $\beta \in L$ is the root of a polynomial in $F[x]$ without multiple roots).*

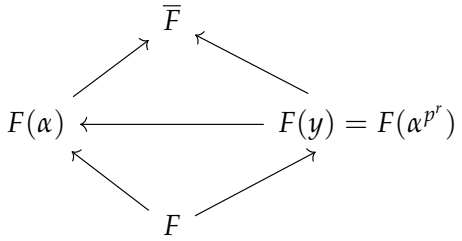
Corollary 0.2. *In the notation above, if the characteristic of F is 0, A' is always finitely generated as an A–module.*

We will need to make use of norms and traces. Take L/F a finite extension of fields. Since L is finitely generated, L is algebraic over F. Let $\{b_i\}_{i=1}^n$ be a basis for L over F. Then the embedding multiplication by $\alpha \in L$ to L gives an action of F-algebras. Then we get a matrix representation for this action, $\psi_L(\alpha)$. Note that the determinant and trace will be well defined as these are invariant of choice of basis: $\operatorname{tr}(AMA^{-1}) = \operatorname{tr} M$ and $\det(AMA^{-1}) = \det M$. Define $\operatorname{tr}_{L/F}(\alpha) = \operatorname{tr}(\psi_L(\alpha)) \in F$ and $\operatorname{Nm}_{L/F} = \det(\psi_L(x)) \in F$ and $\operatorname{char poly}(\psi_L(\alpha)) = \det(xI_n - \psi_L(\alpha)) \in F[x]$.

Definition (Conjugates)**.** The conjugates of α in L are the images $\alpha_i = \sigma_i(x)$ of the embeddings $\sigma_i : L \to \overline{F}$ for some fixed algebraic closure of F.

Now given the irreducible polynomial for α over F. Either this polynomial is separable (which is always the case for characteristic 0) or is inseparable. In the case of char p, then this polynomial is of the form $f(x^{p^r})$ for some separable polynomial f. Let $y = \alpha^{p^r}$. Then the irreducible polynomial for y over F is f. Now $f(x) = \prod_{\sigma_i : F(\alpha) \to \overline{F}} (x - \sigma_i(y)) = \prod_i (x - \sigma_i(\alpha)^{p^r})$. Now as an extension $F(y) = F(\alpha^{p^r})/F$, if you look at the number of embeddings of this field into an algebraic closure, its the degree of the extension as this is a separable extension. Whereas you extend these to $F(\alpha)$, each of these can be extended uniquely to an algebraic closure because $F(\alpha)/F(\alpha^{p^r})$ is a purely inseparable extension: so when you look at an extension of $F(\alpha^{p^r})$ to $F(\alpha)$, there is a unique way to

extend this to $\overline{F}$. [There is only one p^rth root of α in p^r as any other root would differ by a p^rth root of unity and the field has characteristic p.]



Then the number of embeddings of $F(\alpha) \to \overline{F}$ over F is $[F(\alpha) : F]_{\text{sep}} = [F(\alpha^{p^r} : F] = d$. [Recall the separable degree is the number of different embeddings of a field into an algebraic closure.]

Theorem 0.10. *Let L/F be a finite extension.*

(a) $Nm_{L/F}(x) = \left(\prod_{i=1}^{d} \sigma_i\right)^{p^r[L:F(\alpha)]}$

(b) $Tr_{L/F}(\alpha) = p^r\,[L : F(\alpha)] \cdot \sum_{i=1}^{d} \sigma_i(\alpha)$

(c) $\text{char poly}_F(\alpha) = f(x^{p^r})^{[L:F(\alpha)]}$

Remark. $\text{Tr}_{L/F}$ is identically 0 if L/F is not separable: either $F(\alpha)$ is inseparable over F in which case p^r is a positive power of p or else $F(\alpha)$ is separable but then a p is produced from $[L : F(\alpha)]$. It is possible to have a degree p separable extension in fields of characteristic p. Note that above (c) implies (a) and (b) since $f(x) = \prod_{i=1}^{d}(x - \sigma_i(\alpha))$. Remember, we can get these values by looking at the constant term of the minimal polynomial and the coefficient of $x^{[L:F]-1}$.

Proof. We only need show (c). L is a F and $F(\alpha)$ vector space. As a $F(\alpha)$-vector space, L decomposes as $L = F(\alpha)r_1 \oplus \cdots \oplus F(\alpha)r_s$, where $s = [L : F(\alpha)]$. Left multiplication by α over L preserves the summands. The action of α on $F(\alpha)$ is determined solely based on its action on $f(\alpha)$. So the matrix representation of the multiplication is a block matrix along the diagonal with each block is the action of α on each $F(\alpha)$ relative to some basis. Then $\text{char poly}_F(\alpha \text{ acting on } L) = \text{char poly}_F(\alpha \text{ on } F(\alpha))^s$ but $s = [L : F(\alpha)]$. Now we have reduced to the case $L = F(\alpha)$. Now write $L = F(\alpha)$ has F basis $1, \alpha, \alpha^2, \ldots, \alpha^{p^r-1}, \alpha^{p^r} = y, \alpha y, \alpha^2 y, \ldots, \alpha^{p^r-1}y, y^2, \ldots, \alpha^{p^r-1}y^{d-1}$, where $d = \deg_F(y) = \deg f(x)$ – the separable degree, $= [F(\alpha^{p^r}) : F] = [F(y) : F]$. Now $f(x) = \prod_{i=1}^{d}(x - \sigma_i(\alpha)) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$. The matrix of multiplication by α with this basis is

$$M = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & \vdots \\ & \ddots & & & \vdots & 0 \\ & & \ddots & & 0 & -c_1 \\ & & & & \ddots & \vdots \end{pmatrix}$$

Now we want $\det(xI - M) = F(x^{p^r})$; we assumed $L = F(\alpha)$. Now simply expand this matrix by cofactors along the last column – begin careful of the book keeping. □

0.3 Norms/Traces, Integral Closures, Dual Bases

Recall the situation: A is a noetherian integral domain and A is integrally closed in $F = \operatorname{Frac} A$. Let L/F be a finite separable extension of fields. Let A' denote the integral closure of A in L.

$$\begin{array}{ccc} A' & \subseteq & L \\ \cup & & | \\ A & \subseteq & F = \operatorname{Frac} A \end{array}$$

We want to…

(a) Show that A' is finitely generated as an A-module.

(b) Find a generator for A' as an A-module.

(c) Look at the ring theoretic properties of A'.

Taking $A = \mathbb{Z}$, $F = \mathbb{Q}$, and L a number field, we want to understand $A' = \mathcal{O}_L$, the ring of integers in L. We do know that this is the unique maximal subring of L that is a finitely generated abelian group. Take $\zeta_p = e^{2i\pi/p} \in \mathbb{C}$ a pth root of unity, where p is prime. Consider $L = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Clearly, L/Q is an extension. It turns out $\mathcal{O}_L = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. For any number field L, the class number h_L is the number of isomorphism classes of nonzero $\mathcal{O}_L$-ideals. Now if the class number is 1, all the ideals are isomorphic. But the ring itself is finitely generated, in fact generated by a single element. Therefore, $h_L = 1$ if and only if $\mathcal{O}_L$ is a PID. Now if L is as given, the (Kummer-)Vandiver Conjecture states that $p \nmid h_L$. This implies Fermat's Last Theorem for the prime p. To see also why we would care about integral closures, we look to Algebraic Geometry. Suppose k is a field and $F = k(x)$, the field of rational functions of a single variable. Take a finite separable extension L/F and examine rings inside F, say $A = k[x^{-1}]$. Subrings have an integral closure in L. From Algebraic Geometry, L is the function field of a projective curve C/k. Now $k(x)$ is the function field of $\mathbb{P}^1_k$. Now $\mathbb{P}^1_k$ has two open sets, $A_0 = \operatorname{Spec} k[x]$ and $A_1 = \operatorname{Spec} k[x^{-1}]$, which are glued together. Then $C = \operatorname{Spec}(A_1') \cup \operatorname{Spec}(A_0')$. Then one reason to care about integral closures is that they give a way of understanding projective curves which have a given function field.

We return to traces and norms: take L/F a finite extension.

(a) $\operatorname{Tr}_{L/F} : L \to F$

(b) $\operatorname{Nm}_{L/F} : L \to F$

(c) char poly$_F : L \to F[x]$ obtained considering an embedding $L \to M_n(F)$, where $n = [L : F]$ and α maps to the characteristic polynomial of its matrix multiplication representative.

Corollary 0.3. *If the minimal polynomial for α over F to be $x^d + a_{d-1} + x^{d-1} + \cdots + a_1 x + a_0$, then*

$$Tr_{F(\alpha)/F}(\alpha) = -a_{d-1}, \quad Nm_{F(\alpha)/F}(\alpha) = (-1)^d a_0$$

or more generally,

$$Tr_{L/F}(\alpha) = -\frac{n}{d} a_{d-1}, \quad Nm_{L/F}(\alpha) = (-1)^n a_0^{n/d}$$

Corollary 0.4. *Traces and Norms respect towers of fields: $F \subseteq L \subseteq N$ is a tower of fields, then $Tr_{N/F} = Tr_{L/F} \circ Tr_{N/L}$ and $Nm_{N/F} = Nm_{L/F} \circ Nm_{N/L}$.*

Theorem 0.11. *If L/F is a finite Galois extension with Galois group G and $\alpha \in L$, then*

$$Tr_{L/F}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha), \quad Nm_{L/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$$

Theorem 0.12 (Dedekind)**.** *For all finite extensions L/F of fields, the set $\{\sigma_i\}$ of embeddings of L into an algebraic closure $\overline{F}$ is linearly independent over $\overline{F}$.*

Therefore, if for some $a_i \in \overline{F}$, one has $\sum^d a_i \sigma_i(\beta)$ for all $\beta \in L$, then $a_i = 0$ for all i. This degree is the separable degree: $d = [L : F]_{\text{sep}}$, the number of possible embeddings.

Proof. Take a minimal nonzero relation (meaning t minimal):

$$a_1\sigma_1 + \cdots + a_d\sigma_t \equiv 0$$

with each $a_i \neq 0$. We must have $t > 1$ as otherwise every element of the field is zero. There then exists at least two distinct embedding of L into $\overline{F}$. But then there is a $\gamma \in L$ such that, assuming without loss of generality $\sigma_1 \not\equiv \sigma_2$, $\sigma_1(\gamma) \neq \sigma_2(\gamma)$. We have $\sigma_i(\gamma\beta) = \sigma_i(\gamma)\sigma_i(\beta)$ for all $\beta \in L$. Now we have

$$a_1\sigma_1(\beta) + a_2\sigma_2(\beta) + \cdots + a_t\sigma_t(\beta) = 0 \tag{0.1}$$

Now instead substitute $\gamma\beta$ for β and using $\sigma_i(\gamma\beta) = \sigma_i(\gamma)\sigma_i(\beta)$, we have

$$a_1\sigma_1(\gamma)\sigma_1(\beta) + a_2\sigma_2(\gamma)\sigma_2(\beta) + \cdots + a_t\sigma_t(\gamma)\sigma_t(\beta) = 0 \tag{0.2}$$

But then taking the 'linear combination' Equation (0.2)$-\sigma_t(\gamma)$ Equation(0.1), we have a relation in $t-1$ terms. But this contradicts the minimality of t as this combination is nontrivial. □

Corollary 0.5. *L/F is separable if and only if there exists a $\beta \in L$ such that $Tr_{L/F}(\beta) \neq 0$.*

Corollary 0.6. *L/F is separable if and only if $Tr_{L/F}$ defines a non-degenerate F-bilinear form.*

As a vector space over F, L is isomorphic to d copies of F. When L/F is separable, there is additional structure. Figuring out the isomorphism class of L/F as a vector space is trivial. However, trying to figure out the isometry class ($(L, \text{Tr}_{L/F})$ is isometric to $(V, \langle -, - \rangle)$ if there is a morphism taking one pair to the other) of the field along with the bilinear trace pairing is a nontrivial question.

Corollary 0.7. *There is an F-vector space isomorphism $L \to \text{Hom}_F(L, F) = F$ vector space homomorphisms: $\alpha \mapsto Tr_{L/F}(\alpha\beta)$.*

Proof. Injective as the trace is non-degenerate. The dimensions are the same. Therefore, they must be isomorphic via this map. □

Note that this is the same as giving a non-degenerate pairing: a non-degenerate pairing from a vector space cross itself is the same as giving an isomorphism from the vector space to the linear dual.
Notation: If $\{u_i\}_{i=1}^d$ is an F-basis for a separable extension L of F, the dual basis $\{w_j\}_{j=1}^d$ satisfies

$$\text{Tr}_{L/F}(w_i w_j^*) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

That is, $\text{Tr}_{L/F}(w_i w_j^*) = \delta_{i,j}$, the Kronecker delta function.

Theorem 0.13. *Suppose A is an integral domain and A is integrally closed in $F = \operatorname{Frac} A$. Let L/F be a finite separable extension of fields. Let A' denote the integral closure of A in L.*

$$\begin{array}{ccc} A' & \subseteq & L \\ \cup\!| & & | \\ A & \subseteq & F = \operatorname{Frac} A \end{array}$$

Then there is a basis $\{w_i\}_{i=1}^d$ in A' for L/F. For all such bases, $A' \subseteq \oplus_{j=1}^d A w_i^*$, where $\{w_i^*\}_{i=1}^d$ is the dual basis. So if A is noetherian, then A' is finitely generated.

Proof. Suppose $0 \neq \alpha \in L$, we know α is algebraic over F:

$$\alpha^d + \frac{p_{n-1}}{q_{n-1}}\alpha^{n-1} + \cdots + \frac{p_0}{q_0} = 0$$

for some $p_i, q_i \in A$. Clearing denominators gives

$$(r\alpha)^d + b_{n-1}(r\alpha)^{d-1} + \cdots + b_0 = 0$$

for some $r \in A$ and $b_i \in A$. So there is a basis $\{w_i\}$ contained in A' for L over F. Take any $\{w_i\}$ with this property and $\beta \in A'$. Now $\beta = \sum_{j=1}^d a_i w_i^*$ for some $a_i \in F$. We need show $a_i \in A$. We look at $\operatorname{Tr}_{L/F}(w_i\beta)$ in two ways. Now $\beta \in A'$ and $w_i \in A'$. Therefore, $w_i\beta \in A'$. We know the trace of something in A' is some multiple of the sum of the various conjugates. But if something is integral over A, every conjugate is integral over A (by applying σ_i). Then $\operatorname{Tr}_{L/F}(w_i\beta)$ is a sum of elements of L which are integral over A. But then the sum must be integral over A and be in F (since the trace is to F). Therefore, this sum is in A as A is integrally closed. On the other hand, $\operatorname{Tr}_{L/F}(w_i\beta) = \sum_{j=1}^d a_j \operatorname{Tr}_{L/F}(w_i w_j^*) = a_i$ (due to the formula above). □

This leads to two natural questions: how do you find an integral basis and how do you identify A' in this free module generated by the dual basis? The first is really linear algebra while the second leads to discriminants.

Theorem 0.14. *Suppose L/F is a finite separable extension generated by one element, $L = F(\alpha)$ (though the Primitive Element Theorem says this always can be done). Say $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$, where $a_i \in F$ and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$. Then*

$$\frac{f(x)}{x - \alpha} = b_{n-1}x^{n-1} + \cdots + b_0 \in L[x]$$

The dual basis to $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is $\frac{b_0}{f'(\alpha)}$, $\frac{b_1}{f'(\alpha)}$, …, $\frac{b_{n-1}}{f'(\alpha)}$. Then if α is integral over A is integrally closed in $F = \operatorname{Frac} A$ and A' is the integral closure of A in L, then A' is the integral closure and is contained in the direct sum of the dual basis.

Proof. Take $\{\sigma_i\}_{i=1}^n$ the embeddings of L into $\overline{F}$ over F and $\alpha_i = \sigma_i(\alpha)$. We claim

$$\sum_{i=1}^n \left(\frac{f(x)}{x - \alpha_i}\right) \frac{\alpha_i^r}{f'(\alpha_i)} = x^r$$

for $0 \leq r \leq n-1$. The two sides agree on $\alpha_1, \ldots, \alpha_n$. This uses the fact that α_i is a root of f and separability. Moreover, the α_i are distinct and then the difference of the two sides is a polynomial

of at most degree $n-1$ which vanishes at each of these values. Then the difference must be zero. If $0 \leq l \leq n-1$, the coefficient of x^l in $\sum_{i=1}^n \frac{f(x)}{x-\alpha_i} \frac{\alpha_i^r}{f'(\alpha_i)} = \sum_{i=1}^n \sigma_i(b_0 + b_1 x + \cdots + b_{n-1}x^n) \frac{\sigma_i(\alpha^r)}{\sigma_i(f'(\alpha_i))}$ is 0 if $l \neq r$ and 1 if $l = r$. But then is just exactly $\sum_{i=1}^n \frac{\sigma_i(b_l)}{\sigma_i(f'(\alpha))} \sigma_i(\alpha^r) = \mathrm{Tr}_{L/F}(?)$? □

Example 0.4. Take $F = \mathbb{Q}$, $A = \mathbb{Z}$, $L = F(\alpha)$, where α is a root of $x^3 - x - 1$. So A' is the ring of integers in L. Certainly, $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$. We want to find the dual basis to $\{1, \alpha, \alpha^2\}$. Now $f(x) = x^3 - x - 1$ and its formal derivative is $f'(x) = 3x^2 - 1$. Now divide $f(x)$ by $x - \alpha$. The quotient is $x^2 + \alpha x + (\alpha^2 - 1)$, the remainder is 0 as $\alpha^3 - \alpha - 1 = 0$. Now $x^2 + \alpha x + (\alpha^2 - 1) = b_2 x^2 + b_1 x + b_0$. So the dual basis to $\{1, \alpha, \alpha^2\}$ is $\frac{\alpha^2-1}{3\alpha^2-1}$, $\frac{\alpha}{3\alpha^2-1}$, $\frac{1}{3\alpha^2-1}$. Then the ring of integers, $\mathcal{O}_L$, lies inside the $\mathbb{Z}$ span of these. Then this is $\frac{1}{3\alpha^2-1} h(\alpha)$, where h is a polynomial with integer coefficients [to see this, take a look at the numerators]. Call this space H. Then $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L \subseteq H$. So we have an upper bound for the integral closure, A'. Now $\mathrm{Nm}_{L/F}(3\alpha^2 - 1)$ is what? We know $1 \mapsto 3\alpha^2 - 1$ and $\alpha \mapsto 3\alpha^3 - \alpha = 3(\alpha + 1) - \alpha = 2\alpha + 3$ and $\alpha^2 \mapsto 2\alpha^2 + 3\alpha$. This gives matrix

$$\begin{pmatrix} -1 & 3 & 0 \\ 0 & 2 & 3 \\ 3 & 0 & 2 \end{pmatrix}$$

The determinant of this matrix is 23. Then the matrix for $\frac{1}{3\alpha^2-1}$ has determinant $\frac{1}{23}$. So $\mathbb{Z}[\alpha]$ has index 23. Then $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

0.4 Discriminants

1 ANT I, Lecture 4: Discriminants

Let A be an integral domain and A is integrally closed in $F = \operatorname{Frac} A$. Let L/F be a finite separable extension of fields. Let A' denote the integral closure of A in L. Take a basis $\{w_i\}_{i=1}^d$ for L/F.

Definition (Discriminant)**.** $\operatorname{Disc}(\{w_i\}_{i=1}^d) = \det(\operatorname{Tr}_{L/F}(w_i w_j))$. This is in F.

Lemma 1.1. *Suppose $\{\sigma_l\}_{l=1}^d$ are the embeddings of L into $\overline{F}$ over F. Then* $\operatorname{Disc}(\{w_i\}_1^d) = \det((\sigma_l(w_i))_{i,l})^2$.

Proof. Define $M = (\sigma_l(w_i))_{i,l}$.

$$M = \begin{pmatrix} \sigma_1(w_1) & \sigma_2(w_1) & \cdots & \sigma_d(w_1) \\ \sigma_1(w_2) & \sigma_2(w_2) & \cdots & \sigma_d(w_2) \\ \vdots & & \ddots & \vdots \\ \sigma_1(w_d) & \sigma_2(w_d) & \cdots & \sigma_d(w_d) \end{pmatrix}$$

The transpose of this is

$$M^T = \begin{pmatrix} \sigma_1(w_1) & \sigma_1(w_2) & \cdots & \sigma_1(w_d) \\ \sigma_2(w_1) & \sigma_2(w_2) & \cdots & \sigma_2(w_d) \\ \vdots & & \ddots & \vdots \\ \sigma_d(w_1) & \sigma_d(w_2) & \cdots & \sigma_d(w_d) \end{pmatrix}$$

Then $MM^T = (\operatorname{Tr}_(w_i w_j))_{i,j}$. Then $\det M^2 = \det(MM^T) = \operatorname{Disc}(\{w_i\})$. □

Example 1.1. Suppose $\{w_i\}_{i=1}^d = \{\alpha^{i-1}\}_{i=1}^d$, the power basis. Call $\alpha_l = \sigma_l(\alpha)$. Then $M = (\sigma_l(w_i))_{i,l}$ and $w_i = \alpha_{i-1}$. Then

$$M = (\sigma_l(w_i))_{i,l} = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) & \cdots & \sigma_d(1) \\ \sigma_1(\alpha) & \sigma_2(\alpha) & \cdots & \sigma_d(\alpha) \\ \vdots & & \ddots & \vdots \\ \sigma_1(\alpha^{d-1}) & \cdots & & \sigma_d(\alpha^{d-1}) \end{pmatrix} =$$

Of course, this is just the Vandermonde determinant: $\det M = \prod_{1 \le i < j \le d}(\alpha_j - \alpha_i)$. Then we have

$$\begin{aligned} \operatorname{Disc}(\{\alpha_i\}_{i=1}^d) &= \det((\sigma_l(\alpha_i)_{i,l})^2 \\ &= (\prod_{1 \le i < j \le d} (\alpha_j - \alpha_i)^2 \\ &= (-1)^{d(d-1)/2} \prod_{i \ne j} (\alpha_i - \alpha_j) \\ &= (-1)^{d(d-1)/2} \operatorname{Nm}_{L/F}(f'(\alpha)) \\ &= (-1)^{d(d-1)/2} f'(\alpha_1) f'(\alpha_2) \cdots f'(\alpha_n) \end{aligned}$$

where f is the irreducible polynomial for α. This follows since $f = \prod_i (x - \alpha_i)$ and $f' = \prod_{i \ne j}(x - \alpha_i)$ so that $f'(\alpha_i) = \prod_{i \ne j}(\alpha_i - \alpha_j)$. Then

$$\operatorname{Disc}(\{\alpha^i\}_{i=0}^d) = (-1)^{d(d-1)/2} \operatorname{Nm}_{L/F}(f'(\alpha))$$

Corollary 1.1. $\mathrm{Disc}(\{w_i\}_1^d) = \det((\sigma_l(w_i))_{i,l})^2$ *implies that this is nonzero if and only if* $\{\sigma(w_i)\}$ *is a basis and if there is a change of basis to* $\{w_i'\}$ *with chance of basis matrix* T*, then* $\mathrm{Disc}(\{w_i'\}) = \det(T)^2 \mathrm{Disc}(\{w_i\})$.

Corollary 1.2. *(a) If* $T \in \mathrm{GL}_d(A)$*, where* $A \subseteq F = \mathrm{Frac}(A)$*, then*

$$\mathrm{Disc}(\{w_i'\}) \in (U(A))^2 \mathrm{Disc}(\{w_i\}_i)$$

where $U(A)$ *denotes the units of* A*.*

(b) Suppose $\{w_i\}$ *is a basis for* L/F *(so* $\mathrm{Disc}(\{w_i\}_i) \neq 0$*), then if* $w_i' = T(w_i)$ *for* $T \in \mathrm{GL}_d(F)$

$$\bigoplus Aw_i' = \bigoplus Aw_i \iff T \in \mathrm{GL}_d(A) \iff \det T = u \in U(A) \iff \det(T)^2 \in U(A)^2 \iff \frac{\mathrm{Disc}(\{w_i'\})}{\mathrm{Disc}(\{w_i\})} \in U(A)$$

When A *is integrally closed, this happens if and only if* $\frac{\mathrm{Disc}(\{w_i'\})}{\mathrm{Disc}(\{w_i\})} \in U(A)$.

(c) Say A *is integrally closed in* F*,* A' *the integral closure of* A *in* L*, then if* $\{w_i\}$ *is a basis contained in* A'*,* $\mathrm{Disc}(\{w_i\}) \in A$.

(d) Suppose A *PID, then* A' *is a finitely generated* A*-module. But finitely generated* A*-modules are free (since there is no torsion as its sitting inside the field* L *and* A *is a PID). Then* A' *has a basis over* A*. Then for all bases* $\{w_i'\}$ *contained in* A'*,* $\mathrm{Disc}(\{w_i'\}) \in A$.

Definition. Let A be an integral domain and A is integrally closed in $F = \mathrm{Frac}\, A$. Let L/F be a finite separable extension of fields. Let A' denote the integral closure of A in L. Let $D(A'/A)$ be the A-ideal generated by discriminants associated to bases inside A'. Note that if A is a PID, then ideal is principal and any generator of this ideal is given by the discriminant of an A-basis $\{w_i\}$ of A'.

Definition (Unramified)**.** We say that A'/A is unramified if $D(A'/A) = A$.

Note that this does not guarantee the existence of a basis $\{w_i\}$ inside A' with discriminant a unit. It merely says that varying your choice of basis, you can generate all of A.

Localizations: Say S is a multiplicatively closed subset of A. We define $S^{-1}A$ to be the localization. Observe that

$$\begin{array}{c} S^{-1}A' \\ | \\ S^{-1}A \end{array}$$

Now localizations behave well under discriminants: $D(S^{-1}S'/S^{-1}A) = S^{-1}D(A'/A)$.

$$\begin{array}{ccccc} A' & \supseteq & A[x] & \subseteq & L = F(\alpha) \\ & & \cup\!| & & | \\ & & A & \subseteq & F = \mathrm{Frac}\, A \end{array}$$

$$\mathrm{Disc}(\{\alpha^i\}_{i=1}^d) = (-1)^{d(d-1)/2}\mathrm{Nm}_{L/F}(f'(\alpha)) \in (A)\wedge \neq 0$$

Now consider localization. Specifically, localize at α: $S = \{\alpha^i\}$. So we are inverting the norm, i.e. this discriminant. Sometimes in this case we denote $S^{-1}A = A[1/\alpha]$. Now $A[1/\alpha] \subseteq A'[1/\alpha]$. Now if we let $y = f'(\alpha)$, then $A[\alpha][1/y]$ is the integral closure of $A[1/y]$ in L and is unramified over $A[1/y]$. Also, the branch locus of $\mathrm{Spec}\, A' \to \mathrm{Spec}\, A$ is contained inside $\mathrm{Spec}(A/Ay) \subseteq_{\mathrm{closed}} \mathrm{Spec}\, A$.

Definition (Principal Discriminant)**.** Suppose A is an integral domain and A is integrally closed in $F = \operatorname{Frac} A$. Let L/F be a finite separable extension of fields. Let A' denote the integral closure of A in L.

$$\begin{array}{ccc} A' & \subseteq & L \\ \cup\!| & & | \\ A & \subseteq & F = \operatorname{Frac} A \end{array}$$

Now $D(A'/A)$ is the A–ideal generated by all $\operatorname{Disc}(\{w_i\}_i)$ of $\{w_i\}_{i=1}^d \subseteq A'$. However, we could define $D_{\text{prin}}(A'/A)$ the A–ideal generated by the power basis associated to elements of A, i.e. $\operatorname{Disc}(\{\alpha^{i-1}\}_{i=1}^d)$ for $\alpha \in A'$. This is not always the same as the discriminant, even if you look at all ideal generated by all discriminants of power bases and you allow the power basis to change. In general, $D_{\text{prin}}(A'/A) \subseteq D(A'/A)$.

We know that if A is a PID, there exists a basis $\{w_i\} \subseteq A'$ such that $D(A'/A)$ is the ideal generated by the powers of the w_i. (A' is free as an A-module on some basis, take that basis, and look at its discriminant and that will generate the discriminant ideal). In this case, is there always an $\alpha \in A'$ so that $D_{\text{prin}}(A'/A)$ is generated by that basis? This seems to be an open question, even in the case $A = \mathbb{Z}$.

Remark. You should try all of this lecture for the case of a quadratic extensions of $\mathbb{Q}$.

A useful fact is that suppose $A = \mathbb{Z} \subseteq F = \mathbb{Q}$, $L/\mathbb{Q}$ is a number field and $A' = \mathcal{O}_L \supseteq \{w_i\}_{i=1}^d\}$ with $|\operatorname{Disc}(\{w_i\})|$ is minimal among all $|\operatorname{Disc}(\{w_i'\})| \neq 0$ associated to $\{w_i'\} \subseteq \mathcal{O}_L$, then $\mathcal{O}_L = \oplus_{i=1}^d \mathbb{Z} w_i$. This is so if $|\operatorname{Disc}(\{w_i'\})|$ is a square-free integer. [If you find a lot of elements which are integral over L so that the discriminant is square free, then if that weren't a basis there would be another basis so that the found discriminant would be the determinant of a determinant of a matrix in $\mathbb{Z}$ squared times the discriminant of the found basis. So the given discriminant would have a square factor.] This is a nice condition but it is only sufficient and not necessarily necessary. Note that if L is quadratic and d is a square-free integer, then $\operatorname{Disc}(L/\mathbb{Z})$ is either d, if $d \equiv 1 \mod 4$ or $4d$ otherwise.

1.1 Cyclotomic Integers, Kronecker-Weber, Drinfeld Modules, Dedekind Rings

Now we shall see some more examples of integral closures:

Theorem 1.1. *Suppose p is a prime and $n \geq 1$. Consider the p^nth cyclotomic polynomial, $\Phi_{p^n}(x) = \frac{x^{p^n}-1}{x^{p^{n-1}}-1} = 1 + x^{p^{n-1}} + x^{2p^{n-1}} + \cdots + x^{(p-1)p^{n-1}}$, then $\Phi_{p^n}(x)$ is irreducible of degree $\phi(p^n) = \#(\mathbb{Z}/p^n)$ in $\mathbb{Q}[x]$. Let $\zeta = \zeta_p$ be a root in some $\overline{\mathbb{Q}}$. Then $L = Q(\zeta)$ has degree $\phi(p^n)$ and integers $\mathcal{O}_L = \mathbb{Z}[\zeta]$.*

Proof. If ζ has order exactly p^n in $\overline{\mathbb{Q}}$, for $i, j \in \mathbb{Z}$ prime to p, we can find $k \in \mathbb{Z}$ so that $i \equiv jk \mod p^n$ so $\frac{1-\zeta^i}{1-\zeta^j} = \frac{1-\zeta^{jk}}{1-\zeta^j} = 1 + \zeta^j + \cdots + \zeta^{j(k-1)} \in \mathbb{Z}[\zeta] \subseteq \mathcal{O}_L$. Similarly, $\frac{1-\zeta^j}{1-\zeta^i} \in \mathbb{Z}[\zeta]$ so that $\frac{1-\zeta^i}{1-\zeta^j} \in \mathbb{Z}[\zeta]^* \subseteq \mathcal{O}_L^*$ is a unit. Finite subgroups of $\mathbb{Q}^*$ are cyclic and observe

$$\Phi_{p^n}(x) = \prod_{\substack{(i,p)=1 \\ 1 \leq i \leq \phi(p^n) = p^n - 1}} (x - \zeta^i)$$

So we look at $\Phi(1)$ two ways, using the initial formula and the product formula bove. This gives us

$$1 + 1 + \cdots + 1 = p = \Phi_{p^n}(1) = \prod_{\substack{(i,p)=1 \\ 1 \leq i \leq \phi(p^n) = p^n - 1}} (1 - \zeta^i)$$

But each element in the product is equivalent to a unit times $1 - \zeta$ so that the product is $u(1-\zeta)^{\phi(p^n)}$ for some unit $u \in \mathbb{Z}[\zeta]^* \subseteq \mathcal{O}_L^*$. Now $p\mathbb{Z}[\zeta]$ we do not know the rank of over $\mathbb{Z}$ but it is a finitely generated abelian group and $p\mathbb{Z}[\zeta] = (1-\zeta)^{\phi(p^n)}\mathbb{Z}[\zeta]$. But then we have

$$p\mathbb{Z}[\zeta] = (1-\zeta)^{\phi(p^n)}\mathbb{Z}[\zeta] \subseteq (1-\zeta)^{\phi(p^n)-1}\mathbb{Z}[\zeta] \subseteq \cdots \subseteq (1-\zeta)\mathbb{Z}[\zeta] \subseteq \mathbb{Z}[\zeta]$$

Here $(1-\zeta)^{i+1}\mathbb{Z}[\zeta] \neq (1-\zeta)^i\mathbb{Z}[\zeta]$ since if we had equality, $(1-\zeta)\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta]$ for then $1 - \zeta \in \mathbb{Z}[\zeta]^*$, a contradiction.

$$(1-\zeta)^{\phi(p^n)}\mathbb{Z}[\zeta] = p\mathbb{Z}[\zeta] \neq \mathbb{Z}[\zeta]$$

But then (noting $\mathbb{Z}[\zeta]$ is a finitely generated abelian group so it has some rank–it's a direct sum of copies of $\mathbb{Z}$ so taking quotients obtains a sum of copies of $\dim_{\mathbb{Z}/p} \mathbb{Z}[\zeta]/(p\mathbb{Z}[\zeta]) = \operatorname{rank}_{\mathbb{Z}} \mathbb{Z}[\zeta]$) from the above chain, we have at least one factor of p coming in as one goes up the chain showing $\phi(p^n) \leq \dim_{\mathbb{Z}/p} \mathbb{Z}[\zeta]/(p\mathbb{Z}[\zeta]) = \operatorname{rank}_{\mathbb{Z}} \mathbb{Z}[\zeta]$. But then $\phi(p^n) \leq \dim_{\mathbb{Z}/p} \mathbb{Z}[\zeta]/(p\mathbb{Z}[\zeta]) = \operatorname{rank}_{\mathbb{Z}} \mathbb{Z}[\zeta] \leq \operatorname{rank}_{\mathbb{Z}} \mathcal{O}_L = \dim_{\mathbb{Q}} L$, where the last equality follows from the fact that there is a basis for $\mathcal{O}_L$ that consists of a basis for the field elements over $\mathbb{Q}$. Now $\dim_{\mathbb{Q}} L = \dim_{\mathbb{Q}} \mathbb{Q}(\zeta)$ since ζ is a generator. But this the degree of the minimal polynomial which is at most the degree of Φ. Therefore, we have shown

$$\phi(p^n) \leq \dim_{\mathbb{Z}/p} \mathbb{Z}[\zeta]/(p\mathbb{Z}[\zeta]) = \operatorname{rank}_{\mathbb{Z}} \mathbb{Z}[\zeta] \leq \operatorname{rank}_{\mathbb{Z}} \mathcal{O}_L = \dim_{\mathbb{Q}} L = \dim_{\mathbb{Q}} \mathbb{Q}(\zeta) \leq \deg \Phi_{p^n}(x) = \phi(p^n)$$

This shows $[L : \mathbb{Q}] = \dim_{\mathbb{Q}} L = \phi(p^n)$ and $\phi_{p^n}(x)$ is irreducible in $\mathbb{Q}[x]$.

It remains to prove the claim of what the ring of integers is.

$$\operatorname{Disc}(\mathbb{Z}[\zeta]/\mathbb{Z}) = \pm \operatorname{Nm}_{L/\mathbb{Q}}(\Phi'_{p^n}(\zeta))$$

Now using the quotient rule,

$$\Phi'_{p^n}(x) = \frac{p^n x^{p^n-1}(x^{p^{n-1}}-1) - (x^{p^n}-1)p^{n-1}x^{p^{n-1}-1}}{(x^{p^{n-1}}-1)^2}$$

But then we have

$$\Phi'_{p^n}(\zeta) = \frac{p^n \zeta^{p^n-1}(\zeta^{p^{n-1}}-1) - 0 \cdot p^{n-1}\zeta^{p^{n-1}-1}}{(\zeta^{p^{n-1}}-1)^2} = \frac{p^n \zeta^{p^n-1}}{(\zeta^{p^{n-1}}-1)}$$

The denominator is an integer so the norm of the denominator is an integer. The norm of the numerator is a power of p times a power ± 1 (as the norm of ζ is ± 1). Therefore, we have shown $\mathrm{Nm}_{L/\mathbb{Q}}\Phi_{p^n}(\zeta)$ is a power of p. Then $\mathrm{Disc}(\mathbb{Z}[\zeta]/\mathbb{Z})$ is a power of p so when you look at the dual basis, the index of $\mathbb{Z}[\zeta]$ in the $\mathbb{Z}$-module generated by the dual basis are also a power of p. The $\mathbb{Z}$-module generated by the dual basis contains $\mathcal{O}_L$: $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_L \subseteq Z$, the $\mathbb{Z}$-module generated by the dual basis of $\{1, \ldots, \zeta^{\phi(p^n)-1}\}$ and the index of $\mathbb{Z}[\zeta]$ in Z is a power of p. So if the integers are not $\mathbb{Z}[\zeta]$, the contain $\mathbb{Z}[\zeta]$ with an index a power of p. To show $\mathcal{O}_L = \mathbb{Z}[\zeta]$, it is enough to show that there is no element of $\mathbb{Z}[\zeta]$ that is not p times an element that's actually in $\mathcal{O}_L$. Meaning, it is enough to show $\frac{1}{p}\sum_{i=0}^{\phi(p)-1} b_i\zeta^i$ is not in $\mathcal{O}_L$ if all $b_i \in \mathbb{Z}$ but some $b_i \notin p\mathbb{Z}$. [If $\mathcal{O}_L \neq \mathbb{Z}[\zeta]$, then $[\mathcal{O}_L : \mathbb{Z}[\zeta]]$ is a power of p. Then there is at least some element of $\mathbb{Z}[\zeta]$ which is p times an integer (that is something in $\mathcal{O}_L$) but not p times something in the subring $\mathbb{Z}[\zeta]$.]

The $\mathbb{Z}$-module generated by $1, (1-\zeta), (1-\zeta)^2, \ldots, (1-\zeta)^{\phi(p^n)-1}$ is the same as $\mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$.

$$\frac{1}{p}\sum_{i=0}^{\phi(p^n)-1} b_i\zeta^i = \frac{1}{p}\sum_{i=0}^{\phi(p^n)-1} c_i(1-\zeta)^i$$

We are asking if this is in $\mathcal{O}_L$, where some of the c_i are in $\mathbb{Z}$ but not in $p\mathbb{Z}$. Let i_0 be the smallest i with $c_{i_0} \notin p\mathbb{Z}$. Then we have

$$\frac{1}{p}c_{i_0}(1-\zeta)^{i_0} + \frac{1}{p}\sum_{i>i_0} c_i(1-\zeta)^i \in \mathcal{O}_L$$

We can multiply by powers of $1-\zeta$ and stay in $\mathcal{O}_L$. Multiply by $(1-\zeta)^{\phi(p^n)-1-i_0}$.

$$\frac{1}{p}c_{i_0}(1-\zeta)^{\phi(p^n)-1} + \frac{1}{p}\sum_{i>i_0} c_i(1-\zeta)^{\phi(p^n)-1+(i-i_0)} \in \mathcal{O}_L$$

The exponents $\phi(p^n) - 1 + (i - i_0)$ are all at least $\phi(p^n)$ and $(1-\zeta)^{\phi(p^n)}\mathbb{Z}[\zeta] = p\mathbb{Z}[\zeta]$. Therefore, the term on the right is in $\mathcal{O}_L$ (note that the sum is clearly in $p\mathbb{Z}[\zeta]$ and the $\frac{1}{p}$ cancels the p). Then the term on the left must be in $\mathcal{O}_L$. But $p \nmid c_{i_0}$. Now if this left term was an integer, its trace and norm have to be a rational integer. We calculate the norm of $\delta := \frac{1}{p}c_{i_0}(1-\zeta)^{\phi(p^n)-1}$.

$$\mathrm{Nm}_{L/\mathbb{Q}}(\delta) = \left(\frac{c_{i_0}}{p}\right)^{\phi(p^n)} \mathrm{Nm}_{L/\mathbb{Q}}(1-\zeta)^{\phi(p^n)-1}$$

Now $\mathrm{Nm}_{L/\mathbb{Q}}(1-\zeta) = \prod_{\sigma:L\hookrightarrow\overline{\mathbb{Q}}}(1-\sigma(\zeta))$ (since we have a finite separable extension) but as $\Phi_{p^n} = \prod_{\sigma:L\hookrightarrow\overline{\mathbb{Q}}}(x-\sigma(\zeta))$, since $\Phi_{p^n}(x)$ is irreducible, we must have

$$\mathrm{Nm}_{L/\mathbb{Q}}(1-\zeta) = \prod_{\sigma:L\hookrightarrow\overline{\mathbb{Q}}}(1-\sigma(\zeta)) = \Phi_{p^n}(1) = p$$

But then looking at the powers of p in δ, we have $\delta \notin \mathbb{Z}$. □

This is a general strategy: if you have a submodule of some finitely generated abelian group and you wish to prove that it is the whole group, prove that if you look at the whole group mod your subgroup you have no torsion. Now we shall say a bit more on the results on cyclotomic ring of integers:

Proposition 1.1. *For all $n \geq 0$, the nth cyclotomic polynomial*

$$\Phi_m(x) = \prod_{\substack{\zeta \in \overline{\mathbb{Q}} \\ \zeta^m = 1, \\ \zeta^l \neq 1 \text{ for } l < m}} (x - \zeta)$$

is irreducible in $\mathbb{Q}[x]$. If $\zeta = \zeta_n$ is any root, then

(a) $[\mathbb{Q}[\zeta] : \mathbb{Q}] = \phi(m)$

(b) $\mathcal{O}_{\mathbb{Q}[\zeta]} = \mathbb{Z}[\zeta]$

(c) There is an isomorphism of groups $(\mathbb{Z}/m)^* \to \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ given by $a \mapsto \sigma_a$, where $\sigma_a(\zeta) = \zeta^a$. So in particular, $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ is abelian.

(d) $\mathcal{O}_L = \mathbb{Z}[\zeta]$ has discriminant $D(\mathcal{O}_L/\mathbb{Z}) = d_{L/\mathbb{Q}}$ which only involves powers dividing m. In otherwise, $\mathcal{O}_L/\mathbb{Z}$ is unramified outside m.

Theorem 1.2 (Kronecker-Weber)**.** *If $L/\mathbb{Q}$ is a finite abelian extension then $L \subseteq \mathbb{Q}(\zeta_m)$ for some m.*

This is all related to Hilbert's 12th Problem: give a similar construction, via explicit elements, of all abelian (respectively, all) extensions of a given number field F. The 'good' answers known are for $F = \mathbb{Q}$ (Kronecker-Weber), $F = \mathbb{Q}(\sqrt{d})$ for $0 < d \in \mathbb{Z}$ square-free (Weber, Weierstrass, et al.) using torsion points on elliptic curves, and F number field so that F is a quadratic extension of a field F^+ and all embeddings $\sigma : F^+ \to \mathbb{C}$ have $\sigma(F^+) \subseteq \mathbb{R}$ and all $\tau : F \to$ have $\tau(F^+) \not\subseteq \mathbb{R}$ (complex multiplication theory due to Shimura et al.). This is related also to Stark's conjecture.

There is a characteristic p-analog of cyclotomic fields called Drinfeld modules. Anytime you prove something about number fields, you should try to prove something about function fields of transcendence degree 1 over a finite field as these are very similar. Let $\zeta = \zeta_m$ a root of $\Phi_m(x)$. Consider the set $\mathcal{M}_m = \{\zeta^i : i \in \mathbb{Z}\}$. This is $\ker\{\phi_m : \overline{\mathbb{Q}}^* \to \overline{\mathbb{Q}}^*, \alpha \mapsto \alpha^m\}$. If you look at the field adjoining ζ, it is the same as the field obtained by joining all the kernel elements of these homomorphisms: $\mathbb{Q} \subseteq \mathbb{Q}(\zeta) = \mathbb{Q}(\mathcal{M}_m) \subseteq \overline{\mathbb{Q}}$.

Now let L be a field with characteristic $p > 0$. Let τ be an indeterminate. Define $L\{\tau\}$ to be the (noncommutative) ring of all twisted polynomials: $a_0 + a_1\tau + a_2\tau^2 + \cdots + a_n\tau^n$ with $a_i \in L$ and $\tau a = a^p \tau$ if $a \in L$. Take A to be a commutative ring.

Definition (Drinfeld Module)**.** A Drinfeld module is a homomorphism of rings $\psi : A \to L\{\tau\}$.

Note that if $\overline{L}$ is an algebraic closure of L, then τ gives a Frobenius automorphism of the additive group L^+ via $\tau : \overline{L}^+ \to \overline{L}^+$ given by $\beta \mapsto \beta^p = \tau(\beta)$: $\tau(\beta + \gamma) = (\beta + \gamma)^p = \beta^p + \gamma^p = \tau(\beta) + \tau(\gamma)$. Each element λ of $F\{\tau\}$ gives an endomorphism $L^+ \to L^+$.

Definition (Carlitz Module)**.** Take $L = \mathbb{F}_p(T)$, $A = \mathbb{F}_p[T] \xrightarrow{\psi} L\{\tau\}$ a ring homomorphism determined completely by $\psi(T)$ and choose $T \mapsto T + \tau$. This gives an action of A on L. The resulting module is called the Carlitz Module. Note we require $\psi(A) \not\subseteq L$.

Definition (Division Points)**.** Suppose $\pi(t)$ is any nonzero polynomial in $A = \mathbb{F}_p[T]$. Let $\mu_{\pi(T)} = \{\beta \in \overline{L}^+ : \psi(\pi(T))(\beta) = 0\}$. That is, $\mu_{\pi(T)}$ is the $\pi(T)$ division points on $\overline{L}^+$ with respect to the $\mathbb{F}_p[T]$ A module structure of $\overline{L}^+$ coming from the Carlitz module.

Theorem 1.3 (Carlitz)**.**

(a) $L(\mu_{\pi(T)})$ *is an abelian extension of* $L = \mathbb{F}_p(T)$.

(b) $\mathrm{Gal}(L(\mu_{\pi(T)})/L) \xleftarrow{\sim} (A/\pi(T)A)^*$.

For (b), we know that $\sigma \in \mathrm{Gal}$ is determined by its action on $\mu_{\pi(T)}$. On the other hand, take $a \in A$ and let it act on the division points $\mu_{\pi(T)}$. Taking this element and modifying it by $\pi(T)A$, $\pi(T)$ sends all division points to 0 so it does not move them around at all. This is a great counterpart to the analogy for $\mathbb{Q}(\mu_m)$: $\mathbb{Q}(\mu_m)/\mathbb{Q}$, $\mu_m = \ker(\overline{\mathbb{Q}}^* \to \overline{\mathbb{Q}}^*)$ given by $\alpha \mapsto \alpha^m$, where m plays the role of $\pi(T)$ [$\psi(\pi(T)) : \overline{L}^+ \to \overline{L}^+$]. Then μ_m is the 'stuff' mapped to the identity and $\pi(T)$ is the 'stuff' mapped to the identity in the Carlitz case. [Note here $\mathbb{Z} \sim A$.]

Example 1.2. Take $\pi(T) = T$. Now $\psi(\pi(T)) = T + \tau \in L\{\tau\}$, where $L = \mathbb{F}_q(T)$. This acts on $\overline{L}^+$ via $\beta \mapsto \psi(\pi(T))(\beta) = (T + \tau)(\beta) = T\beta + \beta^p$, where $\beta \in \overline{L}^+$. Now

$$\mu_T = \{\beta \in \overline{L}^+ : \psi(T)(\beta) = \beta T + \beta^p = 0\} = \{0\} \cup \{\beta \in \overline{L}^+ : \beta^{p-1} = T\}$$

Furthermore, we have $L(\mu_T) = \mathbb{F}_p(T^{1/(p-1)})$—all the other roots differ by a $(p-1)$-st root of unity. The $(p-1)$-st roots of unity are in the right side so that $L(\mu_T)$ is a Kummer extension.

$$\begin{array}{ccc} \mathrm{Gal}(L(\mu_T)/L) & \xrightarrow{\quad\psi\quad} & L\{\tau\} \\ \downarrow\wr & & \\ \mathbb{F}_p^* = (\mathbb{F}_p[T]/T\mathbb{F}_p[T])^* & \longrightarrow & T + \tau \end{array}$$

Now

$$\begin{array}{c} L(\mu_T) = \mathbb{F}_p(T^{1/(p-1)}) \\ \Big| \\ \mathbb{F}_p[T] \subseteq L = \mathbb{F}_p(T) \end{array}$$

For more on this, see Rosen *Number Theory in Function Fields*.

Definition. A Dedekind ring is an integral domain A such that A is noetherian, integrally closed, and every nonzero prime ideal is a maximal ideal, and there is at least one non-zero prime ideal.

Note that requiring one non-zero prime is to exclude fields (forcing dimension 1). Many texts such as Lang, Samuel, Jansz, etc. exclude this condition (so that fields are Dedekind). Note that Hartshorne requires this last condition.

Definition (Fractional Ideal)**.** A fractional ideal of A is a nonzero finitely generated A-submodule of F.

We can multiply such ideals, say I, J, by taking the A-submodule generated by all products $\alpha\beta$ with $\alpha \in I$ and $\beta \in J$.

Theorem 1.4. *Every fractional ideal I in a Dedekind ring can be written uniquely as a product of integral powers of primes: $P_1^{b_1} P_2^{b_2} \cdots P_n^{b_n}$, where P_i are distinct primes and $Pi^{-1} = \{\beta \in F \colon \beta P_i \subseteq A\}$. The fractional ideals form a commutating group, $\mathrm{I}(A)$, with subgroup of principal fractional ideals $\mathrm{Prin}(A) = \{A\beta \colon 0 \neq \beta \in F^\times\}$.*

We will be interested in $\mathrm{Cl}(A) = \mathrm{I}(A) / \mathrm{Prin}(A)$.

1.2 Fractional Ideals, Dedekind Rings, Ideal Class Groups

Let A be a Dedekind domain (that is, A is a noetherian integral domain integrally closed in $F = \mathrm{Frac}(A)$ with all nonzero prime ideals maximal and at least one nonzero prime ideal). Recall also that J is a fractional ideal of A if $J = x^{-1}I \subseteq H$ for some $0 \neq x \in F$ and some A-ideal I. We define $J_1 \cdot J_2$ to be the A-module generated by all products of elements of J_1 with elements of J_2.

Definition (Class Group)**.** If A is a Dedekind ring, then $\mathrm{Cl}(A) := \mathrm{I}_F(A)/\mathrm{Prin}(A)$ is the class group of A.

Our goal is to prove the following theorem:

Theorem 1.5. *The set $\mathrm{I}_F(A)$ of all fractional ideals of A forms a multiplicative group with subgroup $\mathrm{Prin}(A) = \{Ax : 0 \neq x \in F\}$. Moreover, every fractional ideal of A can be written uniquely as a product of prime ideals.*

Proof.

Step 1: Every maximal ideal $\mathfrak{m}$ of A is invertible. [That is, nonzero prime ideals are invertible.]

$$\mathfrak{m}' := \{x \in F = \mathrm{Frac}(A) : x\mathfrak{m} \subseteq A\}$$

Now certainly $A \subseteq \mathfrak{m}$. Now if $0 \neq \beta \in \mathfrak{m}$, then $\mathfrak{m}' \subseteq \frac{1}{\beta}A$. But $\frac{1}{\beta}A$ is a nonzero noetherian A-submodule of F (it is isomorphic to A itself). Therefore, $\mathfrak{m}'$ is a nonzero noetherian A-submodule of F and is then a fractional ideal. We want to show that $\mathfrak{m}\mathfrak{m}' = A$. We know $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}' \subseteq A$. But $\mathfrak{m}$ is a maximal ideal of A so there are only two possibilities: $\mathfrak{m}\mathfrak{m}' = A$ or $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$. Suppose $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$. Choose $x \in \mathfrak{m}'$. Now $x\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}' = \mathfrak{m}$. But then $x^2\mathfrak{m} \subseteq x\mathfrak{m} \subseteq \mathfrak{m}$ and so $x^d\mathfrak{m} \subseteq \mathfrak{m}$. So if $0 \neq d \in \mathfrak{m}$, $x^n d = p_n \in \mathfrak{m}$ for some $p_n \in \mathfrak{m}$. This shows that the ring $A[x]$ is generated by A and x and is contained in $\frac{1}{d}A$. But $\frac{1}{d}A$ is a finitely generated A-module. This forces $A[x]$ is a finitely generated A-module so that x is integral over A. But A is Dedekind so that $x \in A$. Thus, if $x \in \mathfrak{m}'$ then $x \in A$. So $\mathfrak{m}' = A$.

Now if $0 \neq a \in \mathfrak{m}$, then Aa contains a finite product product $P_1P_2P_n$ of prime ideals. [Any noetherian integral domain has this property.] To see this, let Φ be the set of all nonzero ideals I of A which do not contain such a product. Suppose Φ is nonempty. Since A is noetherian, there is an element J of Φ which is maximal in the inclusion order on Φ. Now $J \neq A$ as A is a empty product of prime ideals. Moreover, J cannot be a maximal ideal as then it would be prime and hence contain a prime ideal (itself). Then J is a proper non-maximal ideal. Now clearly J cannot be prime, so there exist $x, y \in A \setminus J$ with $xy \in J$. Now $J \subsetneq (J, x)$ so by maximality, (J, x) contains a product of prime ideals as $(J, x) \notin \Phi$. Similarly, (J, y) contains a product of primes. Suppose $(J, x) \supseteq P_1P_2 \cdots P_n$ and $(J, y) \supseteq Q_1Q_2 \cdots Q_m$, all nonzero prime ideals. Then $P_1P_2 \cdots P_nQ_1Q_2 \cdots Q_m \subseteq (J, x)(J, y) = J + Jx + Jy + Axy \subseteq J$, a contradiction.

We were trying to show $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$ is impossible. Take $0 \neq a \in \mathfrak{m}$. Certainly, $\mathfrak{m} \supseteq Aa \supseteq P_1 \cdots P_n$ for some primes P_i and n minimal. If $P_i \not\subseteq \mathfrak{m}$ for all i, then there is a $\gamma_i \in P_i \setminus \mathfrak{m}$. Look at $\gamma := \gamma_1 \cdots \gamma_n$. Now $\gamma \in P_1 \cdots P_n \subseteq \mathfrak{m}$. Now $\gamma \notin \mathfrak{m}$ as $\mathfrak{m}$ is prime. Then $P_i \subseteq \mathfrak{m}$ for some i, a contradiction. But P_i is maximal as A is Dedekind and then $\mathfrak{m} = P_i$ for some i. Without loss of generality, $\mathfrak{m} = P_1$. Look at $B = P_2 \cdots P_n$. We know that $Aa \not\supseteq B$ as we chose n minimal. But $Aa \supseteq \mathfrak{m}B = P_1P_2 \cdots P_n$. Choose $\beta \in B$ with $\beta \notin Aa$. Now $\mathfrak{m}\beta \subseteq \mathfrak{m}B = P_1 \cdots P_n \subseteq Aa = aA$. Therefore, $\mathfrak{m}\beta a^{-1} \subseteq A$. Hence, $\beta a^{-1} \in \mathfrak{m} = \{\alpha \in F : \alpha\mathfrak{m} \subseteq A\}$. Now $\beta \subseteq \mathfrak{m}'a$ but we supposed $\mathfrak{m}' = A$. Then $\mathfrak{m}'a = Aa$, a contradiction since $\beta \notin Aa$.

Step 2: We finish the proof that fractional ideals form a group: every fractional ideal can be written uniquely as a product of powers of distinct prime ideals, i.e. $I = P_1^{e_1} P_2^{e_2} \cdots P_n^{e_n}$. Since we can invert prime ideals (they are maximal) then we will have the desired group structure.

Suppose J is a fractional ideal. Clearing denominators, J is a finitely generated A-submodule of F. That is, $J = (dJ)(Ad)^{-1}$ for some $0 \neq d \in A$ with $dJ \subseteq A$. So to show existence of a factorization, we can reduce to the case where J is an ideal of A. Say Ψ is the set of nonzero A-ideals which are *not* products of a finite number of prime ideals. Suppose this is nonempty. Since A is noetherian, there is a maximal element in the partial order on Ψ in inclusion, call this maximal element $I \in \Psi$. Now $I \neq A$, which is the empty product. Then I is contained in some maximal ideal, say $\mathfrak{m}$. Now $I\mathfrak{m}' \subseteq \mathfrak{m}\mathfrak{m}' = A$, where $\mathfrak{m}'$ is the inverse of $\mathfrak{m}$. We know $A \subseteq \mathfrak{m}' = \{\alpha \in F : \alpha\mathfrak{m} \subseteq A\}$. Then $I = IA \subseteq I\mathfrak{m}' \subseteq \mathfrak{m}\mathfrak{m}' = A$. If $I\mathfrak{m}'$ is a product of primes, as $\mathfrak{m}'$ is a product of primes, then by multiplication by inverses, we obtain I as a product of primes. So we need only show $I \subsetneq I\mathfrak{m}'$. Suppose $I = I\mathfrak{m}'$. For all $x \in \mathfrak{m}'$, using the same argument as before, we have $x^n I \subseteq I$. For any $0 \neq d \in I$, $x^n d \in I$ so that $x^n \in \frac{1}{d} I$. Now $A[x] \subseteq A + \frac{1}{d} I$ is a finitely generated A-module. Then x is integral over A so that by Dedekind-ness, $x \in A$. But then $\mathfrak{m}' \subseteq A$, a contradiction. So $I \not\subseteq I\mathfrak{m}'$ is not in Ψ. Then $I\mathfrak{m}'$ is a product of primes and hence after multiplication by $\mathfrak{m}$, we obtain I as a product of primes, so $I \notin \Psi$, a contradiction.

Step 3: We need to show uniqueness of this prime decomposition.

Suppose $I = P_1^{a_1} \cdots P_n^{a_n} = Q_1^{b_1} \cdots Q_m^{b_m}$, where P_i, Q_i are prime and $a_i, b_j > 0$. Now $P_1 \supseteq P_1^{a_1} \cdots P_n^{a_n} = Q_1^{b_1} \cdots Q_m^{b_m}$ so that $P_1 \supseteq Q_j$ for some j. By maximality, $P_1 = Q_j$ for some j. Multiply by $P_1^{-1} = Q_j^{-1}$ and continue inductively. □

Example 1.3.

(i) We first prove a way of constructing many examples of Dedekind rings.

Theorem 1.6. *Suppose we have*

$$\begin{array}{ccc} A' & \subseteq & L \\ \Big| & & \Big|{\scriptstyle \text{fin. sep.}} \\ A & \subseteq & F = \mathrm{Frac}(A) \end{array}$$

where A is Dedekind and A' is the integral closure of A in L. Then A' is Dedekind.

Proof. Certainly A' is an integral domain and is integrally closed as $\mathrm{Frac}(A') = L$. Now A' is a finite A-module (since L/F is finite separable) so A' is a noetherian ring. It remains to show that all primes P' of A' are maximal and A' is not a field. If P' is nonzero, then $P := P' \cap A \subseteq A$ is a prime ideal of A. Choose $0 \neq x \in P'$. Look at the polynomial of minimal degree with x satisfies: $x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0$ with $a_i \in A$. Then $a_0 \neq 0$ as $a_0 = -(x^m + a_{m-1}x^{m-1} + \cdots + a_1 x) \in P'$ since $x \in P'$. Then $0 \neq a_0 \in P = P' \cap A$ is a nonzero prime ideal. Now A'/P' is an integral domain and a finitely generated module for the field A/P. But then A'/P' is a field so that P' is a nonzero maximal ideal. [The Going-down theorem would do this quickly.] Now A' is a finitely generated A-module. Suppose $0 \neq Q \subseteq A$ is a prime ideal. If $QA' = A'$, then $A' = Q^{-1}A$. This implies that each $x \in Q^{-1}$ is integral

over A. But then $Q^{-1} \subseteq A$, a contradiction. Now A'/QA' is nonzero finitely generated A/Q-module; that is, a finitely generated commutative algebra over the field A/Q. Then pull back a maximal ideal to get a maximal nonzero ideal P' of A'. □

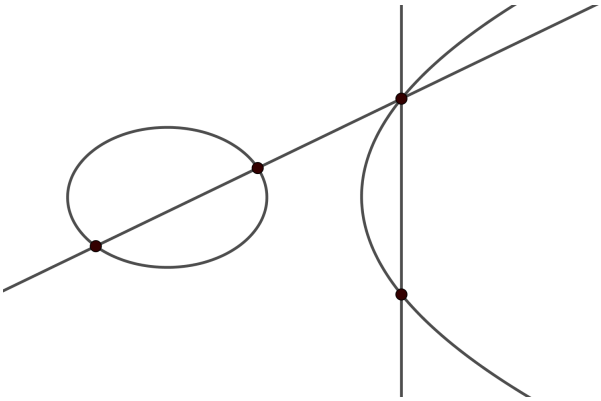
(ii) The most common example we will deal with follows from the above theorem: $\mathbb{Z} = A$, $F = \mathrm{Frac}(A) = \mathbb{Q}$, L a number field, and $A' = \mathcal{O}_L$.

(iii) Let k be an algebraically closed field, e.g. $\mathbb{C}$. Consider $A = k[t] \subseteq F = k(t)$. Consider $y^2 = h(t) := t^3 + a_2t^2 + a_1t + a_0$, a cubic in $k[t]$ with no multiple roots. Assume char $k \neq 2$ and let $L = F(y)$. Now L is a separable quadratic extension since we have adjoined a square root of a cubic polynomial. It turns out A', the integral closure of A in L, is $A \oplus Ay$. This is an affine ring of the elliptic curve defined by $y^2 = h(t)$.

Anytime we have a diagram as above, i.e. the integral closure in a finite separable extension, if P is a nonzero prime ideal of A, then $PA' = p_1^{e_1} \cdots p_s^{e_s}$ as fractional ideals A'-ideals with the p_i distinct primes of A'. Now let $e_i = e(P_i/P)$ is the ramification degree and f_i is the residue field extension degree, which is $[A'/p_i : A/P]$. Next time we shall see $\sum_{i=1}^{s} e_i f_i = [L : F]$.

Returning to the affine ring $A' = A + Ay$, $E : y^2 = h(t)$ and $A = k[t]$. We claim the prime ideals of A' are of the form $p(t_0, y_0) := A(t - t_0) + A'(y - y_0)$ as $(t_0, y_0) \in k \times k$ ranges over all solutions of the equation $y_0^2 = h(t_0)$. To prove this, note if $p \subseteq A'$ is a prime, $p \cap A \subseteq A = k[t]$ is a nonzero prime ideal (so it must be 'linear'). But k is algebraically closed so that $p \cap A$ must be of the form $k[t](t - t_0)$. What are the primes over this? Now $A'/(t - t_0)A' = k[y]/(y^2 - h(t_0))$. If $h(t_0) \neq 0$, there are two distinct solutions (we are not in characteristic 2) and if $h(t_0) \neq 0$ then this is not a field and has a unique maximal ideal. Then the prime ideals of $A'/(t - t_0)A'$ give the prime ideals of A': $p(t_0, y_0)$ and $p(t_0, -y_0)$ over $(t - t_0)k[t]$.

What about $\mathrm{Cl}(A') := \mathrm{Frac}(A')/\mathrm{Prin}(A')$? We claim this corresponds to the group law of the elliptic curve, i.e. $\mathrm{Cl}(A') \cong \{\infty\} \cup E(k)$ with the usual group law (the sum of 3 points on a line is the additive identity ∞). The isomorphism being $p(t_0, y_0) \mapsto$ the point (t_0, y_0) and A' maps to ∞. We need to prove every fractional ideal has the same class in the class group as either A or a unique prime ideal $p(t_0, y_0)$.



The idea is this: suppose you start with two primes that correspond to two points on the elliptic curve (say the two on the 'ellipse'), you want to say that the product of those two primes is linearly equivalent (adjusted by a principal ideal) to a singleton. Take the two primes and look at the equation of the line. This gives a function and look at the ideal generated by

that function, its the product of the primes lying along the time (the three points). Then you have one function that generates a principal ideal whose product is the product of those three primes. Then the product of the first two primes (on the 'ellipse') is linearly equivalent to the inverse of the third point on the line (along the 'curve'). Consider the vertical line through the third point (hitting the 'curve' at a fourth point). The product of these two ideals is the ideal generated by the function $t - t_0$ (the vertical line). Thus, the product of those two primes is a principal ideal. Therefore, the class of the third point is the inverse of the class of the fourth point. Hence, we have duplicated the group law: the product of the ideals associated to the first two points is linearly equivalent to the inverse of the prime ideal associated to the third point which is linearly equivalent to the ideal associated to the fourth point. Therefore, the product of the first two primes is linearly equivalent to the ideal associated to the fourth point.

1.3 Applications of Dedekind Rings & Decomposition of Primes

We now shall give some context and background for Dedekind rings. First, we begin with Fermat's last theorem. Let $p > 2$ be prime. Suppose $x^p + y^p = z^p$ has a solution in relatively prime integers $x, y, z \in \mathbb{Z} \setminus \{0\}$ and $p \nmid xyz$. Now $z^p = \prod_{k=0}^{p-1}(x + \zeta^k y)$, where ζ is a primitive pth root of unity using the fact that $w^p - 1 = \prod_{k=0}^{p-1}(w - \zeta^k)$. That is, if there were a solution, we would have a factorization in $\mathbb{Z}[\zeta]$, where ζ is a primitive pth roof of unity. This works if $\mathbb{Z}[\zeta]$ were a UFD.

Suppose $\mathbb{Z}[\zeta]$ is a UFD ('almost never' true, i.e. for finitely many p, fails first for $p = 23$). Consider the irreducible factorizations of the $x + \zeta^k y$.

(i) $\{x + \zeta^k y\}_{k=0}^{p-1}$ are pairwise relatively prime: $(x + \zeta^k y) - (x + \zeta^l y) = (\zeta^k - \zeta^l)y$. Since $\zeta^k - \zeta^l$ has norm $\pm p$, the only factors on the right are multiples of p or divisors of y. But y is relatively prime to p. Then if they were not relatively prime, a divisor would divide either the difference or y. Then one can routinely show that x and y are not relatively prime.

(ii) Now if we are in a UFD and these are relatively prime, the product $\prod_{k=0}^{p-1}(x + \zeta^k y)$ would have to be a p-power. Then all the factors in the product are p-powers times a unit. That is for all k, $x + \zeta^k y = \epsilon_k \alpha_k^p$ for some unit $\epsilon_k \in \mathbb{Z}[\zeta]^\times$ and some $\alpha_k \in \mathbb{Z}[\zeta]$.

(iii) Now one must show that $\mathbb{Z}[\zeta]^\times = \mathbb{Z}[\zeta + \zeta^{-1}]^\times \cdot \langle \zeta \rangle$. Morally what one is saying is that taking the field generated by a primitive pth root of unity, there is a totally real subfield such that almost all the units come from this subfield. So the units coming up in the above equations are coming up from small subrings.

$$\begin{array}{ccc} \mathbb{Q}(\zeta) & \supseteq & \mathbb{Z}[\zeta] \\ | & & | \\ \mathbb{Q}(\zeta + \zeta^{-1}) & \supseteq & \mathbb{Z}[\zeta + \zeta^{-1}] \\ | & & | \\ \mathbb{Q} & \supseteq & \mathbb{Z} \end{array}$$

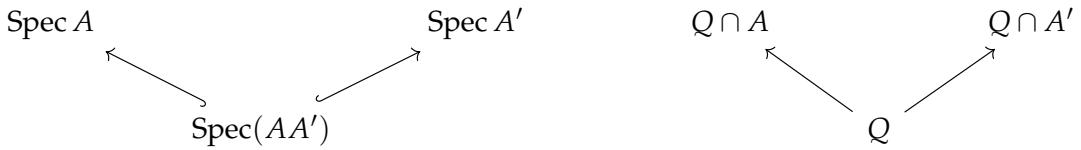
(iv) Looking at x^p in $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$, we have $x^p = (a_0 + a_1\zeta_1 + \cdots + a_{p-1}\zeta^{p-1})^p \mod p$ is $a_0^p + a_1^p\zeta^p + \cdots + a_{p-2}\zeta^p \in \mathbb{Z}$.

(v) $(x + \zeta^k y) = \epsilon_k \alpha_k^p \mod p$ so that $(x + \zeta^k y) \mod p$ is in the image of $\{1, \ldots, \zeta^{p-1}\}\mathbb{Z}[\zeta + \zeta^{-1}]$ in $\mathbb{Z}[\zeta]/p = (\mathbb{Z}/p) \oplus (\mathbb{Z}/p)\zeta \oplus \cdots \oplus (\mathbb{Z}/p)\zeta^{p-2}$. Vary the k and show this does not happen.

However, $\mathbb{Z}[\zeta]$ is not generally a UFD! The question is how bad is the factorization then? This is exactly where fractional ideals came into play. You do not have factorization with elements but you do with ideals. This leads to the study of class groups.

As a second context for Dedekind rings, we look at curves over a field k. Say F is a field of transcendence degree 1 (a finite (algebraic) extension of $k(t)$ for any $t \in F \setminus k$). For example, take $F = k(t)$. Note that Weil showed one can always find t with F separable, finite (algebraic) over $k(t)$. Then F defines a unique regular projective C_F over k. The affine rings of C_F are Dedekind k-algebras $A \subseteq F$ with A-finitely generated over k and fraction field F. For example, if $F = k(t)$ then $A = k[t]$ or $A = k[t^{-1}]$ or $A = k[t, t^{-1}]$. Now $\operatorname{Spec} A = \{p \subseteq A \colon p \text{ prime}\} = \{(0)\} \cup \{p \text{ maximal}\}$. For example, $\operatorname{Spec} k[t] = \{(0)\} \cup \{k[t]\pi(t) \colon \pi \text{ irred, monic}\}$. Now to glue, if A, A' are affine rings of F,

then $A \cdot A'$ is also an affine ring. Then we have a diagram



where the inclusion is taking a prime ideal of $A \cdot A'$, say Q, and identify this with the prime $Q \cap A$, $Q \cap A'$, respectively. [Note, $A \cdot A'$ is finitely generated over k as an algebra.] It turns out that these inclusions have finite complement, i.e. there are only finitely many primes missed by the inclusion. We wish to identify these 'points', i.e. these primes. The points of C_F are the 'union' of all these spectra glued over diagrams of the form above; that is, $C_F = \varinjlim_{\text{A affine ring}} \operatorname{Spec} A$. If you glue $\operatorname{Spec}(k[t]) \cong \mathbb{A}_k$ and $\operatorname{Spec}(k[t^{-1}]) \cong \mathbb{A}_k$ over $\operatorname{Spec}(k[t, t^{-1}] \cong \mathbb{A}_k \setminus \{tk[1]\}$, one obtains $C_{k(t)} = \mathbb{P}^1_k$.

Now define $\operatorname{Div}(C_F)$ to be the free abelian group on $[P]$ as P ranges over all maximal ideals of affine rings A of F, identified with one another via diagrams of the form above. Certainly, this 'includes' the fractional ideals of A, $I_F(A)$: choosing an affine ring, one looks at the fractional ideal which factors as $P_1^{a_1} \cdots P_s^{a_s}$ and map it to $\sum_i a_i[P_i]$. Hence inside $\operatorname{Div}(C_F)$, we have the group of fractional ideals of every Dedekind subring (every affine piece). Generally, $\operatorname{Div}(C_F)$ is bigger since not every P coming from some affine ring necessarily comes from the affine ring $I_F(A)$. Furthermore inside $\operatorname{Div}(C_F)$, one has $\operatorname{Prin}(C_F) := \{\operatorname{div}(f) \colon f \in F\}$, where $\operatorname{div} f = \sum_{P \text{ max}} n_P P$ and n_P is such that for A Dedekind with $f \in A$ and $F = \operatorname{Frac}(A)$ (one can take integral closures for this) so that $fA = P^{n_P}$ (product of integral powers of primes of A different from P). We can define a map $\operatorname{Pic}(C_F) := \operatorname{Div}(C_F)/\operatorname{Prin}(C_F) \to \operatorname{Cl}(A) = \operatorname{IF}(A)/\operatorname{Prin}(A)$ via mapping $C_F \in [Q]$ (for some Q a maximal ideal in an affine ring) to 0 if Q does not come from A and $[Q]$ otherwise. In fact, this mapping is surjective: $\operatorname{Cl}(A)$ is the quotient of $\operatorname{Pic}(C_F)$ by the subgroup generated by the 'subgroups that do not come from A.' So an interesting fact coming from this is that if k is algebraically closed, we obtain the following theorem:

Theorem 1.7 (Jacobi, Weil, ...)**.** *There is an abelian variety* $\operatorname{Jac}(C)/k$ *(projective, regular, group variety) such that* $\operatorname{Jac}(C)(k) = \operatorname{Div}(C_F)/\operatorname{Prin}(C_F)$.

As an example, take $F = k(t)(y)$, where $y^2 = h(t) \in k[t]$ is a cubic without multiple roots (assuming $k = \bar{k}$ and $\operatorname{char} k = 0$ to avoid worrying about inseparability).

$$\begin{array}{ccc} A = k[t] + k[t]y & \subseteq & F \\ | & & \\ k[t] & & \end{array}$$

Now F is an affine ring of C_F and $E : y^2 = h(t)$ defines an affine curve. If one looks at the 'projectivization' of the curve in $\mathbb{P}^2$, instead of (t, y), we have $(t/x, y/x)$ so that in projective space we have projective curve $\operatorname{Jac}(C_F) \subseteq \mathbb{P}^2_k = \{(x : t : y) \colon x, t, y \in k \text{ not all } 0\}$, assuming the normal identifications of these triples. A good calculation is to compute $\operatorname{Pic}(\operatorname{Jac}(C_F))$. One shows the divisor group of $\operatorname{Jac}(C_F)$ is generated by the prime ideals of the affine ring together with one more point—the point at infinity.

$$\begin{array}{ccc} & & \operatorname{Div}(\operatorname{Jac}(C_F))/\operatorname{Prin}(C_F) = \operatorname{Pic}(C_F) \\ & \overset{\sim}{\swarrow} & \downarrow \\ \operatorname{Pic}^0(C_F) = \operatorname{Div}^0(\operatorname{Jac}(C_F))/\operatorname{Prin}(\operatorname{Jac}(C_F)) & \xrightarrow[\sim]{} & E(k) \end{array}$$

So the theorem generalizes the discussion at the end of the previous lecture. In summation, Dedekind rings are a way to understand curves.

Returning to Dedekind rings, we want to prove the statement made about decomposition of prime ideals in finite separable extension fields. We have the usual situation when A is Dedekind and L/F is a finite separable extension (A' being the integral closure of A in L):

$$\begin{array}{ccc} A' & \subseteq & L \\ | & & | \\ A & \subseteq & F = \mathrm{Frac}(A) \end{array}$$

The ideal generated by P, PA', has a decomposition $PA' = P_1^{e_1} \cdots P_s^{e_s}$, where $e_i > 0$ and distinct primes P_i of A. The numbers $e_i = e(P_i/P)$ are the ramification degree, $f_i = f(P_i/P) = [(A'/P_i) \colon (A/P)]$ is the residue field degree over F, and norm $\mathrm{Nm}_{L/F}(P_i) := P^{f_i}$. The main theorem we want to prove is the following:

Theorem 1.8. *If A is a Dedekind ring, $F = \mathrm{Frac}(A)$, L/F is a finite separable extension, A' is the integral closure of A in L, and $P = P_1^{e_1} \cdots P_s^{e_s} \in \operatorname{Spec} A$, then*

$$\sum_{i=1}^{s} e_i f_i = [L : F] = \dim_{A/P}(A'/PA')$$

We shall prove this (rather finish the proof) in the next lecture. But consider a special case as an example. In the case $\mathbb{Z} \subseteq \mathbb{Q}$, consider quadratic extensions, i.e. $[L : F] = 2$. There are only a few possibilities. First, $PA' = Q^2$, i.e. P ramifies. Second, $PA' = Q_1 Q_2$, where $f_1 = f_2 = 1$, i.e. P splits. Lastly, $PA' = Q$ in which case we say P is inert ($f(Q/P) = 2$). We say that P splits in A' if all the P_i and f_1 are 1; that is, $P = P_1 \cdots P_{[L:F]}$. Later when the Chebotarev Density Theorem is covered, we shall see that in the case where L and F are number fields, there are infinitely many such P in A.

1.4 Decomposition of Primes in Galois Extensions & DVRs

Lemma 1.2. *Let A be a Dedekind ring. For all multiplicatively closed sets S of A, $S^{-1}A$ is either a field or a Dedekind ring. In all cases, there is a bijection between* $\operatorname{Spec}(S^{-1}A)$ *and* $\{P \in \operatorname{Spec} A \colon S \cap P = \emptyset\}$.

Proof. For all ideals J of $S^{-1}A$, $J = S^{-1}(J \cap A)$ since each element of J has the form j/s for some $j \in J \cap A$, $s \in S$. Now $S^{-1}A$ is noetherian, since if J is an ideal of $S^{-1}A$, $J \cap A$ is a finitely generated A ideal as A is noetherian. To show $S^{-1}A$ is algebraically closed in $F = \operatorname{Frac}(S^{-1}A) = \operatorname{Frac}(A)$. If $\alpha \in F$ is integral over $S^{-1}A$, we have $\alpha^m + \frac{b_{m-1}}{s_{m-1}}\alpha^{n-1} + \cdots + \frac{b_0}{s_0} = 0$ for some $b_i \in A$, $s_i \in S$. Then $(\prod_{i=1}^n s_i)\alpha$ is integral over A by clearing denominators. But then this is in A so that $\alpha \in S^{-1}A$ is integrally closed. Finally, we need to see all nonzero primes are maximal. Let Q be a nonzero prime ideal of $S^{-1}A$. Then $Q = S^{-1}(Q \cap A)$. Now $Q \cap A$ is an ideal of A but it must be proper since $Q \neq S^{-1}A$. Therefore, $Q \cap A$ is a prime ideal as Q is prime. Since $0 \neq Q$, we know $Q \cap A \neq 0$. But then $Q \cap A$ is a nonzero prime ideal and hence $Q \cap A$ must be maximal. Then $S \cap (Q \cap A) = \emptyset$ as $s \in S \cap S \cap (Q \cap A)$ implies $1 = \frac{s}{s} \in S^{-1}(Q \cap A) = Q$.

Look at the field $L = A/(Q \cap A)$. We have

$$\lambda : L = A/(Q \cap A) \longrightarrow \frac{S^{-1}A}{S^{-1}(Q \cap A)}$$

Now L is a quotient of A and we have a diagram

$$\begin{array}{ccccccc} & & S & \subseteq & A & & \\ & & \downarrow & & \downarrow & & \\ L^* = L \setminus \{0\} & \supseteq & \overline{S} & \subseteq & L = A/(Q \cap A) & \longrightarrow & \dfrac{S^{-1}A}{S^{-1}(Q \cap A)} \end{array}$$

so that S maps to the invertible elements in the residue field. Then the map λ is surjective since every element of S is invertible in the field $A/(Q \cap A)$. But then this is a surjection of a field into a nonzero ring, hence λ is an isomorphism. Therefore, $S^{-1}(Q \cap A)$ is maximal. Lastly, we must show that $S^{-1}A$ has a nonzero prime. If $S^{-1}A$ is not a field, then there is a nonzero maximal ideal so that $S^{-1}A$ is Dedekind.

We now need to show the bijection portion of the Lemma. Take the map $P \mapsto S^{-1}P$ from $\{P \in \operatorname{Spec} A \colon S \cap P = \emptyset\}$ to $\operatorname{Spec}(S^{-1}A)$. This map is clearly surjective since for $Q \in \operatorname{Spec}(S^{-1}A)$, we know $P = A \cap Q$ is in $\{P \in \operatorname{Spec} A \colon S \cap P = \emptyset\}$ and $S^{-1}(A \cap Q) = Q$. For injectivity, if $S^{-1}P = S^{-1}P'$, where $P, P' \in \{P \in \operatorname{Spec} A \colon S \cap P = \emptyset\}$, then $P \subseteq A \cap S^{-1}P$. Define $Q = S^{-1}P$. If P is nonzero, then it is maximal so $P = A \cap Q$. If $P = \{0\}$, then $Q = S^{-1}P = \{0\}$. If $P = \{0\}$ or $P' = \{0\}$, we have $Q = \{0\}$. Otherwise, $P = A \cap Q = P'$. Hence, we have a bijection. □

This gives that the localization at prime ideals are DVRs (by definition, local PIDs). [All DVRs are Dedekind.]

Corollary 1.3. *If $S = A \setminus P$ for $P \in \operatorname{Spec} A$, then $S^{-1}A = A_P$ is a discrete valuation ring (DVR) that are not fields.*

Proof. The nonzero prime ideals of $S^{-1}A = A_P$ are $\{S^{-1}J \colon 0 \neq J \in \operatorname{Spec} A, J \cap S = \emptyset\}$. Here $S = A \setminus P$ so that $J \cap S = \emptyset$ if and only if $J \subseteq P = A \setminus S$. But A is Dedekind so J must be maximal. Then it must be that $J = P$. Then the unique nonzero prime ideals of $S^{-1}A = A_P$ is $S^{-1}P$. Therefore, A_P is local.

Call the unique maximal ideal $\mathfrak{m}_P$. By unique factorization of fractional ideals in the Dedekind ring A_P, we know $\mathfrak{m}_P \neq \mathfrak{m}_P^2$. Note that $A_P\pi \subseteq \mathfrak{m}_P$ but $A_P\pi \not\subseteq \mathfrak{m}_P^2$. We know that $A_P\pi$ is a product of powers of prime ideals of A_P. Then it must be that $A_P\pi = \mathfrak{m}_P$. Note that all ideals of A_P have the form $A_P\pi^n$ for some n and $A_P^* = A_P \setminus \mathfrak{m}_P$. If $\beta \in A_P$ then we know $\beta A_P = A_P\pi^n$ for some n. But then we can write $\beta = u\pi^n$ for some $u \in A_P^*$. Then A_P is a local PID and not a field. □

We create a definition from a piece of the proof above.

Definition (Uniformizer)**.** Any $\pi \in \mathfrak{m}_P$ with $\pi \notin \mathfrak{m}_P^2$ is called a uniformizer.

Note that we used that a DVR was Dedekind in the proof of the corollary above. We prove this here.

Proposition 1.2. *If B is a DVR, then it is Dedekind.*

Proof. (Sketch) Suppose B is a DVR (that is a local PID) and not a field. We need show that B is noetherian, integrally closed, and nonzero primes are maximal (and there is a nonzero prime ideal). Now B is a PID so it is certainly noetherian. Further, B is integrally closed as it is a UFD (being a PID). It is trivial in a PID that nonzero primes are maximal. The last fact is also routine to verify. □

We can now return to the proof from the last lecture.

Theorem 1.9. *If A is a Dedekind ring, $F = \mathrm{Frac}(A)$, L/F is a finite separable extension, A' is the integral closure of A in L, and $P = P_1^{e_1} \cdots P_s^{e_s} \in \operatorname{Spec} A$, then*

$$\sum_{i=1}^{s} e_i f_i = [L : F] = \dim_{A/P}(A'/PA')$$

Proof. First, we show $\sum_{i=1}^{s} e_i f_i = \dim_{A/P}(A'/PA')$. Let $PA' = P_1^{e_1} \cdots P_s^{e_s}$. We know

$$A' \supseteq P_1 \supseteq P_1^2 \supseteq \cdots \supseteq P_1^{e_1} \supseteq P_1^{e_1}P_2 \supseteq \cdots \supseteq P_1^{e_1} \cdots P_s^{e_s} = PA'$$

This is a filtration. But this gives a filtration of the quotient. Suppose I is a nonzero ideal of A'. We know P is a prime ideal of A'. We claim I/IP is a one-dimensional A'/P-vector space. Now A'/P acts on I/IP since I is an ideal of A' and if you look at the action of something in P, it sends things in I to IP. Now $I \neq IP$ as if $I = IP$, since I is nonzero it must be invertible this would imply $A = I^{-1}I = I^{-1}IP$. We also know $I \supseteq J \supseteq IP$, where J is an ideal, then $A \supset I^{-1}J \supseteq P$ (P maximal) implies $I^{-1}J = A$ or P. Then J/IP is either 0 or I/IP. But then the only A'-submodules of the I/IP are 0 or itself, i.e. a simple module for the field A'/P. Since I/IP is nonzero, I/IP must be one-dimensional. Therefore, $\dim(A'/P)(I/IP) = \dim_{A'/P} A'/P = 1$. If $P = P' \cap A$, where P' is a prime of A, then $\dim_{A/P}(A'/P) = f(P'/P)$. Applying this to the filtration above, $\dim_{A/P}(A'/PA') = \sum_{i=1}^{s} e_i(P_i/P)f_i(P_i/P)$ because each of the stages are one-dimensional over the associated residue field of that prime but the dimension of the residue field of the prime $P_i^{e_i}$ over A/P is the residue field degree of that prime.

The harder part is to show that $[L : F] = \dim_{A/P}(A'/PA')$. The idea will be to show that it is enough to show this after localizing at $S = A \setminus P$. Then we show $S^{-1}A = A_P$ is local and a PID. Since this is not a field, it must a DVR. Replacing A by A_P, then A' is a free A-module of rank $[L : F]$ (since it is finitely generated as an A-module as it is torsion free over a PID). On the other hand, $L = FA'$ so that the result will then follow after a brief observation.

Now by clearing denominators, we know that $S^{-1}A'$ is the integral closure of $S^{-1}A = A_P$ inside L. We showed that $A/P \cong A_P/\mathfrak{m}_P = S^{-1}A/S^{-1}(AP)$, where $\mathfrak{m}_P = S^{-1}P$. We have to show that $\dim_{A/P}(A'/PA') = \dim_{A_P/\mathfrak{m}_P}(S^{-1}A/S^{-1}PA')$. We have an exact sequence

$$0 \longrightarrow PA' \longrightarrow A' \longrightarrow A'/PA' \longrightarrow 0$$

But localization is an exact functor so that we have

$$0 \longrightarrow S^{-1}PA' \longrightarrow S^{-1}A' \longrightarrow S^{-1}(A'/PA') \longrightarrow 0$$

is exact. But every element of S is invertible in A/P so that the map $A'/PA' \to S^{-1}(A'/PA')$ is surjective. Note A'/pA' is a module for A/P. If there were a kernel for this map, it would be in A'/P times something annihilated by some nonzero element of S. However, S does not interest P so that the map must be injective (S and P generate the unit ideal in A). This shows that $\dim_{A/P}(A'/PA') = \dim_{A_P/\mathfrak{m}_P}(S^{-1}A/S^{-1}PA')$. Therefore, we can reduce to the case where $A = A_P$, i.e. A is local and a PID, i.e. a DVR. Then A' is finitely generated over A, a PID, and is torsion free. But then A' is a free A-module. Looking at $L = FA'$, we see $L = F \oplus \cdots \oplus F$, where the number of copies must be $[L : F]$. Finally, $A'/A'P \cong (A/P)^{[L:F]}$ and we get $\dim_{A/P}(A'/A'P) = [L : F]$. □

Now lets look at an example of how to use this theorem and a few examples of DVRs to see why they are worthwhile.

Lemma 1.3. *Suppose L/F is a finite Galois extension and $G = \mathrm{Gal}(L/F)$. Then the prime ideals P of A' over $\underline{P}$ are permuted transitively by G.*

Proof. Suppose this is not the case. We have $\underline{P}A' = Q^e \cdot Q_2^{e_2} \cdots Q_s^{e_s}$ with Q a prime ideal not in $\{\sigma P : \sigma \in G\}$ and $e > 0, e_i > 0$. The Chinese Remainder Theorem gives a $x \in A'$ such that $x \equiv 0 \mod Q$ but $x \equiv 1 \mod \sigma P$ for $\sigma \in G$. Since L/F is a finite Galois extension, the extension is separable and then must be given by $\mathrm{Nm}_{L/F}(x) = \prod_{\sigma \in G} \sigma(x) \in A \cap Q = \underline{P}$. But $\sigma^{-1} \equiv \sigma^{-1}(1) = 1 \mod P$ for all $\sigma \in G$. Then $\mathrm{Nm}_{L/F}(x) = \prod_{\sigma \in G} \sigma^{-1}(x) \equiv 1 \mod P$. Therefore, $\mathrm{Nm}_{L/F} \notin P \cap A = \underline{P}$, a contradiction. □

This gives a formula for the factorization of prime ideals in a Galois extension.

Corollary 1.4. *When L/F is Galois, $\underline{P}A' = (P_1 \cdots P_s)^e$,w here $P_1, \ldots, P_s$ are distinct prime ideals and $f = f(P_i/\underline{P})$ is independent of i and $e \cdot f \cdot s = [L : F]$.*

This is because the examine the factorization of $\underline{P}A'$, the Galois group must permute those primes transitively and preserves $\underline{P}A'$. But we want to compute these decompositions explicitly.

Example 1.4. Suppose $A' = A[\alpha]$. Examine the irreducible polynomial $f(x) = \mathrm{Irred}(x, \alpha, F) \in A[x]$, which is a monic polynomial with degree the degree of L/F, which is the rank of $A[x]$ as a free A-module. Reducing this, $\overline{f}(x) = f(x) \mod \underline{P}$ in $(A/\underline{P})[x]$. But $A/\underline{P}$ is a field so we can write $\overline{f}(x) = \overline{P}_1(x)^{e_1} \cdots \overline{P}_r^{e_r}$ for some monic polynomials $\overline{P}_i$ in $A[x]$, where $\overline{P}_i(x) = P_i(x) \mod \underline{P}$. Assume that $\overline{P}_i(x)$ is irreducible in $(A/\underline{P})[x]$. We want to lift these polynomials to monic polynomials of the same degree. The following theorem allows us to do just that.

Theorem 1.10. *If $P_i = \underline{P}A' + \underline{P}_i(\alpha)A'$ is a prime ideal of A' and $A'\underline{P} = P_1^{e_1} \cdots P_s^{e_s}$ is the prime factorization of $A'\underline{P}$, where $f_i = f(P_i/\underline{P}) = \deg \overline{P}_i(x) = \deg P_i(x)$.*

Proof. Choose a root $\overline{\alpha}$ of $\overline{P}_i(x)$ in $\overline{(A/\underline{P})}$, the algebraic closure of $A/\underline{P}$. We have a surjection $A' \to (A/\underline{P})[\overline{\alpha}]$ given by $\alpha \mapsto \overline{\alpha}$. Now $\overline{P}_i(x)$ was an irreducible polynomial with coefficients in $A/\underline{P}$. So when looking at the ring generated over $A/\underline{P}$ by $\overline{\alpha}$ inside the algebraic closure, it must be a field. On the other hand, we have a maximal ideal of $A[\alpha]$, say $J \subset \underline{P}A' + \underline{P}_i(\alpha)A'$. Putting this together, we have a diagram

$$0 \longrightarrow J \longrightarrow A' = A[\alpha] \longrightarrow (A/\underline{P})[\overline{\alpha}] \longrightarrow 0$$

We want to show $J = \underline{P}A' + \underline{P}_i(\alpha)A'$. Suppose $g(\alpha) \in J$ for some $g(x) \in A[\alpha]$. Looking at the reduction $\overline{g}(x) =\equiv g(x) \mod p$, this must have $\overline{\alpha}$ as a root. Since $\overline{\alpha}$ is a root of the irreducible $\overline{P}_i(x)$ in $\overline{A/\underline{P}}$, we get $\overline{g}(x) = \overline{P}_i(x) \cdot \overline{h}(x)$ for some $h(x) \in A[x]$.

But then $g(\alpha) \in \underline{P}A' + \underline{P}_i(\alpha)A'$. Hence, $g(\alpha) - \underline{P}_i(\alpha)h(\alpha) \in \underline{P}A'$. This shows that $P_i = \underline{P}A' + \underline{P}_i(\alpha)A'$ is a prime ideal of A'. Furthermore, it shows $f(P_i/\underline{P}) = \dim_{A/\underline{P}}(A/\underline{P}(\overline{\alpha}) = \deg \overline{P}_i(x) = \deg \underline{P}_i$. Now $\prod_{i=1}^s P_i^{e_i} = \prod(\underline{P}A' + \underline{P}_i(\alpha)A')^{e_i} \subseteq \underline{P}A'$ since (expanding and noting you always get something in $\underline{P}A'$ except the products of only the 'right-most' terms which is) $\prod_{i=1}^s \underline{P}_i(\alpha)^{e_i} = \overline{f(\alpha)} = 0$ as $f(\alpha) = 0$. But this shows $Q_1^{a_1} \cdots Q_r^{a_r}$ is the factorization of $\underline{P}A'$. We know

$$\deg f(x) = \deg \overline{f}(x) = \sum e_i \deg \overline{P}_i(\alpha) = \sum_{i=1}^{s} e_i f(P_i/\underline{P}) \geq \sum_{j=1}^{r} a_j f(Q_j/\underline{P}) \stackrel{*}{=} [L : F] = \deg f(x)$$

where the starred equality follows by the theorem. But then the inequality must be an equality so that $\prod_{i=1}^s P_i^{e_i} = \underline{P}A'$. □

Example 1.5. If $f(x) = x^3 - x - 1$, we know $A' =_L= \mathbb{Z}[\alpha]$ and $A \subseteq \mathbb{Q} = F \subseteq L = \mathbb{Q}(\alpha)$, where α is a root of $f(x)$. Now $x^3 - x - 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ is irreducible (it has no root). So $s = 1$ and we can take $P_1(x) = f(x)$. What does this say about the decomposition? It must be $A'\underline{P} = P_1 = 2_L + P_i(\alpha)A' = 2_L$ since $P_i(\alpha)A' = 0$.

Definition (Discrete Valuation)**.** A discrete valuation on a field F is a surjective function $\nu : F \setminus \{0\} \to \mathbb{Z}$ such that

(i) $\nu(xy) = \nu(x) + \nu(y)$

(ii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ if $x + y \neq 0$

The valuation ring of ν is $R_\nu = \{0\} \cup \{\beta \in F \colon \nu(\beta) \geq 0\}$.

Some easy facts about discrete valuations:

1. R_ν is a DVR.
2. $R_\nu^* = \{\beta \in R \colon \nu(\beta) = 0\}$
3. π is a uniformizer in R_ν if and only if $\nu(\pi) = 1$

Example 1.6. Choose $F = k(t) \supseteq k[t] = A$. The ν arise as either

(i) $\nu = \operatorname{ord}_{\pi(t)} : F \setminus \{0\} \to \mathbb{Z}$ for some $\pi(t) \in k[t]$ monic irreducible, where $\operatorname{ord}_{\pi(t)}(\beta(t)) = m$ if $\beta(t) \in k[t]$ is $\pi(t)^m \cdot u \cdot \prod f$, where u is a unit and the f's are non-associate irreducibles. Note that have made use of unique factorization in a PID.

(ii) $\nu(\beta(t)) = \deg \beta(t)$ for $\beta \in k[t]$.

In terms of Algebraic Geometry, the discrete valuations correspond to the equivalence classes of prime ideals in a curve defined by the rational function field, the first is the points over the affine line and the second is the point at infinity. It is non-trivial to check that these are all the valuations.

1.5 DVRs, Absolute Values, Completions

Recall that a discrete valuation ring is just a local PID R, which is not a field, such that R is Dedekind. If A is Dedekind and $\mathfrak{p}$ is a nonzero prime ideal, then $(A \setminus \mathfrak{p})^{-1}A = A_{\mathfrak{p}}$, the localization of A at $\mathfrak{p}$, is a DVR. We want to generalize this notion: instead of talking about rings, we talk about their fraction fields and valuations on their fraction fields. So we need to discuss valuations on fields.

Definition. A valuation ν on a field F is a function $\nu : F \setminus \{0\} \to G$, where G is a totally ordered (additive) abelian group, such that

(i) $\nu(xy) = \nu(x) + \nu(y)$

(ii) $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$ if $x + y \neq 0$

The valuation ring of ν is $B_\nu = \{0\} \cup \{b \in F \colon \nu(b) \geq 0\}$ (note this is a ring by the properties above) with a unique maximal ideal $\mathfrak{m}_{B_\nu} = \{0\} \cup \{b \in F \colon \nu(b) > 0\}$. [Therefore, B_ν is a local ring with maximal ideal $\mathfrak{m}B_\nu$.] We say that ν is discrete if $G = \mathbb{Z}$ and ν is surjective. Then B_ν is a DVR, i.e. a local PID that is not a field.

We shall see examples where $G \neq \mathbb{Z}$. One question we shall consider is how does one produce all the valuations on a field such that the valuation is discrete. Moreover, what are all the valuations for a given field? How does one produce these valuations? First, we need prove some of the claims in the definition above. It is routine to verify that B_ν is a ring and that $\mathfrak{m}_{B_\nu}$ is an ideal. Let 1 be the identity of B. Then $\nu(1) = \nu(1^2) = \nu(1) + \nu(1)$ so that $\nu(1) = 0$ (by subtraction as we are in an abelian group, assuming we treat the operation as addition). We claim that the units of the ring are exactly the elements with valuation 0, i.e $B^* = \{b \in B \colon \nu(b) = 0\}$. Certainly if $b \in B$ is a unit, then for some $b' \in B$, $bb' = 1$. But $\nu(bb^{-1}) = \nu(1) = 0$ and $\nu(bb') = \nu(b) + \nu(b')$. Then as $b, b' \in B$, $\nu(b), \nu(b') \neq 0$ so that we must have $\nu(b) = 0$. Now if $\beta \in B$ and $\nu(\beta) = 0$, then $\nu(1/\beta) = -\nu(\beta) = 0$ so that $1/\beta \in B$ and then $\beta \in B^*$. Observe that $B^* = B \setminus \mathfrak{m}_{B_\nu}$. Finally if ν is discrete, choose $\pi \in B$ with $\nu(\pi) = 1$ (which exists by surjectivity). Each $0 \neq \beta \in B$ is of the form $u\pi^m$ with $m = \nu(\beta)$, where $u \in B^* = \{b \in F \colon \nu(b) = 0\}$. Then $B\beta = B\pi^m$. Each ideal $0 \neq I$ of B is $B\pi^l$, where $l = \min\{\nu(\beta) \colon 0 \neq \beta \in I\}$.

Proposition 1.3. *If A is a DVR, then A is a valuation ring of $F = \operatorname{Frac} A$.*

Proof. (Sketch) Let $\nu : F \setminus \{0\} \to \mathbb{Z}$ be given by $\nu(\beta) := \operatorname{ord}_{\mathfrak{p}}(A\beta)$, where $A\beta$ is the fractional A-ideal of F which is $\mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(A\beta)}$ times the product of integral powers of other primes of A. □

Notice this gives a way of producing discrete valuation rings. In fact if you take any prime ideal in any Dedekind ring, the same construction gives you a discrete valuation ring. Given a Dedekind ring, we will want to characterize those valuations of the fraction field which come about from prime ideals of the ring. But first, we shall see an example of a non-discrete valuation.

Example 1.7. Let k be a field and let $R = k[x, y]$. Take $G = \mathbb{Z} \times \mathbb{Z} = \{(m, n) \colon m, n \in \mathbb{Z}\}$ with the lexicographic ordering: $(m, n) \leq (m', n')$ if and only if $m < m'$ or $m = m'$ and $n \leq n'$. Define $\nu : R \to G$ via $x^n y^m \mapsto (m, n)$ and extend to R via $\nu(\sum_{m,n \geq 0} x^m y^n) = \min_{a_{m,n} \neq 0}\{(m, n) \in G\}$. Extend to the fraction field $F = \operatorname{Frac} R = k(x, y)$ by $\nu(f/h) = \nu(f) - \nu(h)$.

Now given a field F, how to all the discrete valuations arise? When the field is the fraction field of a Dedekind ring, there is a 'nice' description.

Theorem 1.11. *Suppose that A is a Dedekind ring and $F = \operatorname{Frac} A$. There is a bijection*

$$\left\{\mathfrak{p} : \begin{array}{c}\mathfrak{p} \text{ nonzero prime} \\ \text{ideal of } A\end{array}\right\} \longleftrightarrow \left\{\nu : F^\times \to \mathbb{Z} : \begin{array}{c}\nu \text{ is a discrete valuation,} \\ \nu(A \setminus \{0\}) \subseteq \mathbb{Z}_{\geq 0} \\ \nu(\beta) \geq 0 \text{ for } \beta \in A \setminus \{0\}\end{array}\right\}$$

The correspondence is given by

$$\mathfrak{p} \longmapsto \nu = \nu_\mathfrak{p} \colon \nu_\mathfrak{p}(\beta) = \operatorname{ord}_\mathfrak{p}(A\beta) \text{ for } \beta \in F^\times$$

$$A \cap \mathfrak{m}_{B_\nu} = \mathfrak{p}(v) = \{\beta \in A \colon \nu(\beta) > 0\} \cup \{0\} \longmapsto \nu$$

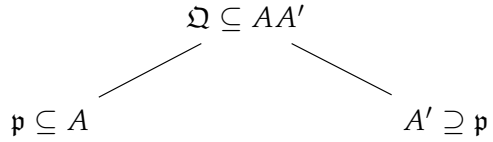
Of course, one could think about $A = \{\beta \in A \colon \nu(\beta) > 0\} \cup \{0\}$ as $A = \mathfrak{p}(\nu) := A \cap \mathfrak{m}_{\beta_\nu}$. By the theorem, the prime ideals of the Dedekind ring can be found via valuations on the fraction field of the form in the theorem. Furthermore given a field F, to find discrete valuations on F one can look at Dedekind subrings for which F is the fraction field.

Example 1.8. Let $A = \mathbb{Z}$ and $F + \mathbb{Q}$. If $\nu : F \setminus \{0\} \to \mathbb{Z}$ is a discrete valuation, then $\nu(1) = 0$. ($2\nu(1) = \nu(1^2) = \nu(1)$). For $0 < \beta \in \mathbb{Z}$, then $\beta = 1 + 1 + \cdots + 1$ so that $\nu(\beta) \geq 0$. We know also $(-1)^2 = 1$ so that $\nu(-1) = 0$. But then $\nu(-\beta) \geq 0$. Therefore, $\nu(\beta) \geq 0$ if $0 \neq \beta \in \mathbb{Z}$. The theorem says that the discrete valuations of $\mathbb{Q}$ all have the form $\operatorname{ord}_{p\mathbb{Z}}$ for some prime p.

Example 1.9. Let k be a field and define $A = k[t] \subseteq F = k(t)$. Suppose ν is a discrete valuation of F and $\nu(\alpha) = 0$ if $\alpha \in k \setminus \{0\}$. If $\nu(t) \geq 0$, then $\nu(\sum_{i=0}^s a_i t^i) \geq 0$. Then $\nu(\beta) \geq 0$ if $0 \neq \beta \in k[t]$. Similarly, if $\nu(t) \leq 0$, then $\nu(\beta) \geq 0$ if $0 \neq \beta \in k[t^{-1}]$. The theorem then says that looking at the valuations that are 0 on the constants, then you can take the ring to be either $k[t]$ or $k[t^{-1}]$ and then the valuation came from a prime ideal of A or A'. Therefore, all the discrete valuations ν of F with $\nu(\alpha) = 0$ if $0 \neq \alpha \in k$ are of the form $\operatorname{ord}_\mathfrak{p}$ or $\operatorname{ord}_{\mathfrak{p}'}$ for a prime $\mathfrak{p}$ of $k[t]$ or a prime $\mathfrak{p}'$ of $k[t^{-1}]$. This leads to a bijection between valuations ν of F with $\nu(k \setminus \{0\}) = 0$ and points $[\mathfrak{p}]$ of the curve C_F associated to F.

$$\left\{\begin{array}{c}\text{discrete valuations } \nu \text{ of} \\ F \text{ with } \nu(k \setminus \{0\}) = 0.\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{points } [\mathfrak{p}] \text{ of } C_F \text{ associated} \\ \text{to } \mathfrak{p}, \text{ a nonzero prime} \\ \text{ideal of Dedekind} \\ A \subseteq F \text{ with } \operatorname{Frac}(A) = F \\ \text{and } A \text{ a } k\text{-algebra.}\end{array}\right\}$$

So we have Dedekind subrings of F which are k-algebras, inside of which we have various prime ideals $\mathfrak{p}$. We identify these ideals if they come about from a prime in the subring generated by the product. Meaning given $\mathfrak{p} \subseteq A$ and $\mathfrak{p}' \subseteq A'$, one looks at the ring they generate AA', which is also Dedekind, and if there is a prime $\mathfrak{Q} \subseteq AA'$ with $\mathfrak{Q} \cap A = \mathfrak{p}$ and $\mathfrak{Q} \cap A' = \mathfrak{p}'$, then we identify $\mathfrak{p}$ and $\mathfrak{p}'$. Then the valuation given by $\mathfrak{Q}$ is the same as the one given by $\mathfrak{p}$ and $\mathfrak{p}'$. Geometrically, we are talking about closed points on the curve C_F. The same ideals give the correspondence above whenever F is a finite of transcendence degree 1 over k.



Remark. Note that $\nu(1) = 0$, always. However, if $b, b' \in A$ and $bb' = 1$, then $0 = \nu(1) = \nu(b) + \nu(b')$. If one does not assume $\nu \geq 0$ on A, then there is no reason to say that the units in A have valuation 0. As an example, take $k = l(x)$ for some field l. We can construct a discrete valuation on k by defining $\nu : k \setminus \{0\} \to 0$ to be ord_x, where $l[x] \cdot x$ is a prime ideal of $l[x]$. Now $l[x]$ is a Dedekind subring of k whose fraction field is k. In particular, one can discuss the valuation on k coming from this prime ideal. Look at $F = k(y)$. Extend ν to $\nu : F \setminus \{0\} \to 0$ by $\nu(y) = 0$. Now ν is a discrete valuation on F that is nontrivial on k. This comes from $F = k(y)(x)$. Then ν is a valuation on F with $\nu(\alpha) = 0$ if $\alpha \in k(y) \setminus \{0\}$ and $\nu(x) = 1$. Note that F has transcendence degree 1 over k.

Example 1.10. Suppose R is any UFD and let $\pi \in R$ be an irreducible. We have a discrete valuation $\nu_\pi : \mathrm{Frac}\, R \setminus \{0\} \to \mathbb{Z}$ given by $\nu_\pi = \mathrm{ord}_\pi(\beta)$ for $\beta \in \mathrm{Frac}\, R$. However, this does not produce all possible discrete valuations on R. This produces a map

$$\left\{ \begin{array}{c} \text{irreducible elements} \\ \pi \in R, \\ \text{up to mult. by unit.} \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{discrete valuations} \\ \text{of } F = \mathrm{Frac}\, R. \end{array} \right\}$$

This map is surjective if $R = \mathbb{Z}$. But even for polynomials in one variable, this map fails to be surjective. Generally, this map is rarely surjective. For example, take $R = k[x, y]$. We have $\mathrm{Frac}(R) = k(x, y)$. Note that $R \subseteq R' := k[x/y, y]$ and $\mathrm{Frac}(R') = k(x, y)$.

1.6 Absolute Values & Completions

1.7 Ostrowski's Theorem

1.8 Ostrowski's Theorem & Approximation Theorems

1.9 Weak/Strong Approximation & Extension Fields

1.10 Extension of Absolute Values & Manin-Batryev Conjecture

1.11 Extensions of Absolute Values, Hensel's Lemma, Selberg's Analogy

1.12 Extensions of Absolute Values & Hensel's Lemma

1.13 Applications of Hensel's Lemma, Dynamical Systems, Morphisms of Varieties

1.14 Hensel's Lemma & Dynamical Systems

1.15 Product Formula, Geometry of Numbers, Finiteness of Class Numbers & Unit Generators

1.16 Geometry of Numbers, Finite Generation of Class Numbers & Unit Groups

1.17 Algorithms for Class Ideal Groups & Quadratic Examples

1.18 Minkowski Bound

1.19 Minkowski Bound & the Function Field Case

1.20 Dirichlet's Unit Theorem in Number Fields & Function Fields

1.21 Small Generators with Fundamental Domains & S-units

1.22 Curves, Codes, Algebraic Integers & Ray Class Groups

1.23 Class Field Theory via Ray Class Groups & Congruence Subgroups

1.24 Frobenius Elements & Class Field Theory

1.25 Class Field Theory

s

2 MATH 621

2.1 Ideles and Adeles

2.2 Idele Class Groups

2.3 ?

2.4 ?

2.5 ?

2.6 ?

2.7 ?

2.8 ?

2.9 ?

2.10 ?

2.11 ?

2.12 ?

2.13 ?

2.14 ?

2.15 ?

2.16 ?

2.17 ?

2.18 ?

2.19 ?

2.20 ?

2.21 ?

2.22 ?

2.23 ?

2.24 ?

2.25 ?

2.26 ?

2.27 ?

2.28 ?

2.29 ?

2.30 ?

2.31 ?

3 MATH 702

3.1 Algebraic Numbers & Integers

3.2 Norms/Traces, Integral Closures, Prime Ideals

3.3 ?

3.4 ?

3.5 ?

3.6 ?

3.7 ?

3.8 ?

3.9 ?

3.10 ?

3.11 ?

3.12 ?

3.13 ?

3.14 ?

3.15 ?

3.16 ?

3.17 ?

3.18 ?

3.19 ?

3.20 ?

3.21 ?

3.22 ?

3.23 ?

3.24 ?

3.25 ?

3.26 ?

3.27 ?

4 MATH 703

4.1 Ideles and Adeles

4.2 Idele Class Groups

4.3 ?

4.4 ?

4.5 ?

4.6 ?

4.7 ?

4.8 ?

4.9 ?

4.10 ?

4.11 ?

4.12 ?

4.13 ?

4.14 ?

4.15 ?

4.16 ?

4.17 ?

4.18 ?

4.19 ?

4.20 ?

4.21 ?

4.22 ?

4.23 ?

4.24 ?

4.25 ?

4.26 ?

4.27 ?

4.28 ?

4.29 ?

4.30 ?

5 MATH 720

5.1 Ideles and Adeles

5.2 Idele Class Groups

5.3 ?

5.4 ?

5.5 ?

5.6 ?

5.7 ?

5.8 ?

5.9 ?

5.10 ?

5.11 ?

5.12 ?

5.13 ?

5.14 ?

5.15 ?

5.16 ?

5.17 ?

5.18 ?

5.19 ?

5.20 ?

5.21 ?

5.22 ?

5.23 ?

5.24 ?

5.25 ?

5.26 ?

5.27 ?

5.28 ?

5.29 ?

5.30 ?

5.31 ?

5.32 ?

5.33 ?

5.34 ?

6 MATH 721

6.1 Ideles and Adeles

6.2 Idele Class Groups

6.3 ?

6.4 ?

6.5 ?

6.6 ?

6.7 ?

6.8 ?

6.9 ?

6.10 ?

6.11 ?

6.12 ?

6.13 ?

6.14 ?

6.15 ?

6.16 ?

6.17 ?

6.18 ?