ALGEBRAIC NUMBER THEORY
LECTURE 34

NOTES BY NATHAN VANDERWERF

Let $S \subset C$, Recall that $\mathcal{O}_S = \mathcal{O}_{K(C),S} = \{f \in K(C) | \text{all poles of } f \subset S\}$.
Proposition 1
(1) $\mathcal{O}_\phi = K$
(2) If $S \neq \phi$ then$\mathcal{O}_S - K \neq \phi$.
Proof
(1) Pick $f \in \mathcal{O}_\phi$, $f : C \to \mathbb{P}^1$. f has no pole so f is not surjective. Hence $f \in K$ is constant.
(2) Later, follows from Riemann Roch.
Proposition 2
(3) $\text{Frac}(\mathcal{O}_S) = K(C)$
Proof:
(3) Pick $f \in \mathcal{O}_\phi$ $K \to K(C)/K(a)$ finite extension. It is separable iff $a \in K(C^{(p)})$. If $a \notin K(C^{(1)})$, then by a primitive element theorem, $K(C) = K(a)(b)$ for some b. We claim you can always write $K(C) = K(a)K(b)$ where $a, b \in \mathcal{O}_S$. Suppose $a \in K(C^{(p)})$. Pick $P \notin S$, $\mathfrak{t}_p =$ uniformizer. $\mathfrak{t}_p \in K(C^{(p)})$. Label poles of t_p outside of S, $p_1, \cdots p_r$ with orders $n_1, \cdots, n_r$. since $p_i \notin S \to a(p_i) \neq \infty \in \bar{K}$, so algebraic over K. There exists $Q_i \in K[x]$ such that $Q_i(a(p_i) = 0$, $c_i = Q_i \circ a$. Then
1. $c_i(p_i) = 0$
2. $c_i \in K(C^{(p)})$ b/c a does. Set $a' = \mathfrak{t} \cap c_i^{n_i} a'(P_i)$ well defined $\mathfrak{t}$ pole order n_i. c_i zero order ≥ 1 at P_i. So $\mathfrak{t} \cap c_i^{n_i}$ has no pole at P_i. a'(Q) well defined for $Q \notin S \cup \{P_i\}$, $a'(Q) \in \bar{K}$. $\implies$ $t'(Q) \in \bar{K}$ so $a' \in \mathcal{O}_S$ and also $a' \notin K(C^{(p)})$. We get an element of $\mathcal{O}_S - K(C^{(p)})$, either a or a'. Thus $K(C) = K(a, b)$ where $a \in \mathcal{O}_S$ and $b \in K(C)$. Take $b' = b \cap d_j^{m_j}$. If $b \notin \mathcal{O}_S$, then it has poles $Q_1, c \ldots Q_s \in S$ with orders $m_1, \cdots, m_s$. $a(Q_i) \in \bar{K}$, so $d_j =$ min poly of $a(Q_i)$ evaluated at a. $b' = b \cap d_j^{m_j} \in \mathcal{O}_S$ with the $d_j^{m_j} \in \mathcal{O}_S$. So $K(a, b) = K(a, b')$. So $K(C) = K(a, b)$ where $a, b \in \mathcal{O}_S$. $K(C) \supset \text{Frak}(\mathcal{O}_S) \supset K[a, b] \supset K(a, b) - K(C)$. $\square$
Proposition 3
(4) Let $S \neq \phi$. If $\mathfrak{p} \subset \mathcal{O}_s$ prime ideal, then $\mathcal{O}_S/\mathfrak{p}$ is algebraic/K.
(5) Every prime ideal of $\mathfrak{p}$ of $\mathcal{O}_S$ is of the form $\mathfrak{p} = \mathcal{O}_S \cap \mathfrak{m}_P$, (which is maximal), $P \in C(\bar{k})$.
Proof:
Pick $a \in \mathfrak{p} - K$, where $\mathfrak{p}$ is a nontrivial ideal and $K(C)/K(a)$ is finite. Let $b \in \mathcal{O}_S \subset K(C)$ be algebraic over $K(a)$. $\sum \frac{P_i(a)}{Q_i(a)} b^i = 0$. Clearing denominator, owe get that b is algebraic over $K[a]$., Therefore, $b \pmod{\mathfrak{p}}$ is algebraic over $K[a]/(\mathfrak{p} \cap K[a] = K$. $a \in \mathfrak{p}$ so $b \pmod{\mathfrak{p}}$ is algebraic over K.
(5). (Sketch of a proof) Let $\mathfrak{p} \subset \mathcal{O}_S$ be a prime ideal. $\mathcal{O}_S/\mathfrak{p}$ is algebraic over K. so $\phi : \mathcal{O}_S/\mathfrak{p} \to \bar{K}$. We can write $K(c) = K(a, b)$ for $a, b \in \mathcal{O}_S$. Then $0 \to \mathfrak{P} \to \mathcal{O}_s \to \bar{K} \to 0$. For $a, b \in \mathcal{O}_S$, the map $K(X, Y) \to K(a, b) = K(c)$ is surjective. Can

think of C as a curve in $\mathbb{P}^2$ with vars X, Y. Take $P = \psi(a), \psi(b)$ as a point in $C(\bar{K})$. If $f \in K(C)$ in the X, Y parameters, then $f(P) = f(\psi(a), \psi(b)) = \psi(f(a,b))$, and $\mathfrak{m}_P = \{f | f(P) = 0\}\{f | \psi(f(a,b)) = 0\} = \ker\, \psi = \mathfrak{p}.\square$

Recall that R is a Dedakind domain if (a), all $\mathfrak{p}$ are maximal (b) Noetherian, and (c) integrally closed.

Theorem 4 Let $S \neq \phi$.
(1) $\forall \mathfrak{p}$ prime, $\exists \mathfrak{p}^{-1} = \mathcal{O}_S$-submodule of $K(C)$ such that $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_S$.
(2) Every $I \subset \mathcal{O}_S$ factors uniquely into prime ideals.
(3) $\mathcal{O}_S$ is Noetherian.
(4) $\mathcal{O}_S$ is Integrally closed.
(5) $\implies \mathcal{O}_S$ is Dedakind (e.g. $\phi(\mathcal{O}_S) =$ class group.
Proof
(1) $\mathfrak{p} = \mathfrak{m}_p$ for some $p \in C(\bar{K})$
$\mathfrak{p}^{-1} := \{f \in K(C) | f \text{has no pole at} p \text{or simple pole}\}$
$\mathfrak{p}\mathfrak{p}^{-1} = \{fg | f(p) = 0,\, g(p) \text{ pole order } \leq 1\} \subset \mathcal{O}_S$ So $\mathcal{O}_S \subset \mathfrak{p}\mathfrak{p}^{-1}$. $\mathfrak{t} =$ uniformizer at $\mathfrak{p}$ so $\mathfrak{p}K(C)_p = (\mathfrak{t})$. $\frac{1}{t}$ pole order 1 at p. $\forall f \in \mathcal{O}_S$, $f = f\mathfrak{t}\mathfrak{t}^{-1} \in \mathfrak{p}\mathfrak{p}^{-1}$
(2) Existence Remarks: $\cap_{k \geq 1} \mathfrak{p}^k = 0 \; \forall \mathfrak{p}$, $\cap_{\text{all } \mathfrak{p}_i \text{ distinct}} \mathfrak{p}_i = 0$
This is true because $f \in K(C)$ has finitely many poles. $I_1 = I =$ ideal. $\subset \mathfrak{p}_1$ if equal $I = \mathfrak{p}_1$ If not, $I_2 = I_1\mathfrak{p}_1^{-1} = \mathfrak{p}_2$ Either $I = \mathfrak{p}_1\mathfrak{p}_2$ or not. If not, set $I_3 = I_2\mathfrak{p}_2^{-1} \subset \mathfrak{p}_3$. If not does not terminate, then $I \subset \mathfrak{p}_1 \cdots \mathfrak{p}_k$ as $k \to \infty$ but $\cap_{i \to \infty} \mathfrak{p}_i \cdots \mathfrak{p}_k = 0$ so must terminate, and therefore $I = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ for primes $\mathfrak{p}_i$. For uniqueness, note that if $\prod \mathfrak{p}_n = \prod \mathfrak{q}_m$, then it must be that $\mathfrak{p}_i = q_j$ for some $i \leq n, j \leq m$. Multiply by $\mathfrak{p}_i^{-1}$ and repeat.