Quals Notes, I guess. We'll see...

Niven Achenjang

April 24, 2022

This is basically a collection of an assortment of facts/results/exercises/etc. knowledge of which will hopefully help me pass quals. Not everything here will be directly related to my quals topics, and not everything I need to know for quals will be here, but everything here will be contained in a document ostensibly about my quals.

The organization is freeform, to put it kindly. Also, I'm not overly concerned with making sure everything is 'correct'; moreso, I hope to have the main ideas of stuff.

Update: I passed my quals. Also, even after taking them, I still sometimes come back and add things to these notes, because it's nice to have some useful facts collected in one place.

Contents

List of Key Examples

Introduction

KeyEx 1. Test

TODO: Get key examples list thing working

Example. Something here.

KeyEx 2. double test

1 Miscellaneous Facts I Didn't Feel Like Putting Under One Subject

1.1 Some flatness stuff

Lemma 1.1. *Let $A \xrightarrow{\varphi} A'$ be a faithfully flat ring map, and let M be an A-module. Then, $M \neq 0 \iff M' := M \otimes_A A' \neq 0$.*

Proof. One direction is easy, so assume that $M \neq 0$, fix some nonzero $m \in M$, and let $\mathfrak{p} \supset \operatorname{Ann}(m) \neq A$ be a prime. Fix some $\mathfrak{p}' \in \operatorname{spec} A'$ such that $\varphi^{-1}(\mathfrak{p}') = \mathfrak{p}$. Note that $\operatorname{Ann}(m)A' \subset \mathfrak{p}A' \subset \mathfrak{p}' \subsetneq A'$. Multiplication by m gives an injection $A/\operatorname{Ann}(m) \hookrightarrow M$, and so after tensoring we get an injection

$$A'/\operatorname{Ann}(m)A' \simeq A/\operatorname{Ann}(m) \otimes_A A' \hookrightarrow M \otimes_A A',$$

but $A' \neq 0$ since $\operatorname{Ann}(m)A' \neq A'$, so $M \otimes_A A'$ is nonzero. Thus, that's a wrap. ■

Lemma 1.2. *Let $\varphi : A \to B$ be a flat ring map such that, for any A-module M,*

$$M \neq 0 \iff M \otimes_A B \neq 0.$$

Then, φ is faithfully flat.

Proof. We need to show that $f = \operatorname{spec} \varphi : \operatorname{spec} B \to \operatorname{spec} A$ is surjective, so pick some $\mathfrak{p} \in \operatorname{spec} A$. We can replace A with $A_{\mathfrak{p}}$ and B with $B_{\mathfrak{p}} := (\varphi(A) \setminus \varphi(\mathfrak{p}))^{-1} B$ in order to assume that $\mathfrak{p} \in \operatorname{spec} A$ is maximal (i.e. a closed point) and that, for every $\mathfrak{q} \in B$, $\varphi^{-1}(\mathfrak{q}) \subset \mathfrak{p}$ (i.e. $\mathfrak{p}$ is in the closure of $f(\mathfrak{q})$). Now, note that $A/\mathfrak{p} \neq 0$, so $B/\varphi(\mathfrak{p})B = A/\mathfrak{p} \otimes_A B \neq 0$ as well. Let $\mathfrak{m} \in \operatorname{spec} B/\varphi(\mathfrak{p})$ be a maximal ideal, so $\mathfrak{m}$ is equivalently a (maximal) ideal of B containing $\varphi(\mathfrak{p})$. By assumption, $\varphi^{-1}(\mathfrak{m}) \subset \mathfrak{p}$ but also $\mathfrak{m} \supset \varphi(\mathfrak{p})$, so $\varphi^{-1}(\mathfrak{m}) \supset \mathfrak{p}$. Thus, $f(\mathfrak{m}) = \varphi^{-1}(\mathfrak{m}) = \mathfrak{p}$ which shows that $\mathfrak{p} \in \operatorname{im} f$, and so we win. ■

Lemma 1.3. *Let A, B be local rings, and let $\varphi : A \to B$ be a flat local map. Then, it is faithfully flat.*

Proof. It suffices to show that $B \otimes_A -$ preserves nonzeroness, i.e. that if M is a nonzero A-module, then $B \otimes_A M$ is a nonzero B-module. Fix some nonzero $m \in M$, and let $\mathfrak{p} \subset A$ be a prime containing the annihilator $\operatorname{Ann}(m)$. Since φ is local, we have

$$\varphi(\operatorname{Ann}(m))B \subset \varphi(\mathfrak{p})B \subset \varphi(\mathfrak{m}_A)B \subset \mathfrak{m}_B \subsetneq B.$$

Now, note that $A/\operatorname{Ann}(m) \hookrightarrow M$ via multiplication by m. After tensoring with B, we get an injection

$$B/\varphi(\operatorname{Ann}(m))B = B \otimes_A A/\operatorname{Ann}(m) \hookrightarrow B \otimes_A M,$$

which shows that $B \otimes_A M \neq 0$ as $\varphi(\operatorname{Ann}(m))B \subsetneq B$. ■

Lemma 1.4. *Let $\varphi : A \to B$ be a faithfully flat ring map. Then, φ is injective.*

Proof. Pick any $x \in \ker \varphi$, and consider the map $A \to A/(x)$. After tensoring with B, we get an isomorphism

$$B = B \otimes_A A \xrightarrow{\sim} B \otimes_A A/(x) = B/\varphi(x)B = B.$$

Since B is faithfully flat over A, this must mean that the original map $A \to A/(x)$ was an isomorphism, so $x = 0$. ■

Definition 1.5. $A \to B$ **satisfies going down** if for any chain $\mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \cdots \supset \mathfrak{p}_n$ of primes in A with first part lying below $\mathfrak{q}_1 \supset \mathfrak{q}_2 \supset \cdots \supset \mathfrak{q}_m$ $(m < n)$ in B, this latter chain can be completed to $\mathfrak{q}_1 \supset \mathfrak{q}_2 \supset \cdots \supset \mathfrak{q}_n$ lying above the entire chain in A.

Lemma 1.6. *If $A \to B$ is a flat map of commutative rings, then it satisfies going down.*

Proof. Let $\mathfrak{p}_1 \subset \mathfrak{p}_2$ be primes of A, and let $\mathfrak{q}_2$ be a prime of B above A. We want a prime $\mathfrak{q}_1 \subset \mathfrak{q}_2$ above $\mathfrak{p}_1$. Since $A \to B$ is flat, the same is true for $A_{\mathfrak{p}_2} \to B_{\mathfrak{q}_2}$, and this latter map is moreover faithfully flat since it's a flat map of local rings. Thus, $\operatorname{spec} B_{\mathfrak{q}_2} \to \operatorname{spec} A_{\mathfrak{p}_2}$ is surjective, so there is a prime $\mathfrak{q}_1$ of $B_{\mathfrak{q}_2}$ lying above $\mathfrak{p}_1 A_{\mathfrak{p}_2}$. Hence, $\mathfrak{q}_1 \cap B$ is our desired prime. ■

Corollary 1.7. *Let $A \to B$ be flat map of local rings. Then,* $\dim A \leq \dim B$.

Proof. Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{m}_A$ be a maximal chain of primes in A. Let $\mathfrak{q}_n := \mathfrak{m}_B$, so $\mathfrak{m}_B \cap A = \mathfrak{m}_A$ by assumption. Since $A \to B$ is flat, it satisfies going down, so this extends to a chain $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ of primes in B. Thus, $\dim A = n \leq \dim B$. ■

Corollary 1.8. *Flat maps of schemes are open.*

Proof. Let $f : X \to Y$ be a flat map of schemes. Since f restricted to any open in X is flat, it suffices to show that f has open image. Since openness can be checked on any open cover, it suffices to assume we're in the affine situation $f : \operatorname{spec} B \to \operatorname{spec} A$. Since $\operatorname{im} f$ is constructible, it's open iff it is closed under generalizations, so fix some $\mathfrak{p} = f(\mathfrak{q}) \in \operatorname{spec} A$. Let $\mathfrak{P} \rightsquigarrow \mathfrak{p}$, i.e. $\mathfrak{p} \in \overline{\{\mathfrak{P}\}}$, i.e. $\mathfrak{p} \supset \mathfrak{P}$. By going down, there's some prime $\mathfrak{Q} \subset \mathfrak{q}$ of B so that $f(\mathfrak{Q}) = \mathfrak{P}$, so we win. ■

2 Algebraic Geometry

2.1 Some Lemmas

Lemma 2.1. *Let* $f = \operatorname{spec}\varphi : \operatorname{spec} B \to \operatorname{spec} A$. *Then, the scheme-theoretic image of* f *is* $V(\ker\varphi) = \operatorname{spec}(A/\ker\varphi)$.

Proof. Let $\psi : A/\ker\varphi \to B$ so that φ factors as $A \twoheadrightarrow A/\ker\varphi \overset{\psi}{\hookrightarrow} B$, and let $g = \operatorname{spec}\psi : \operatorname{spec} B \to \operatorname{spec}(A/\ker\varphi)$. Suppose $Y \subset \operatorname{spec} A$ is a closed subscheme such that f factors through $Y \hookrightarrow A$, i.e. we have $\operatorname{spec} B \xrightarrow{h} Y \hookrightarrow A$. Write $Y = \operatorname{spec} A/I$. Then $\varphi : A \to B$ factors through A/I, so $I \subset \ker\varphi$, so we have a further factorization

$$A \to A/I \to A/\ker\varphi \to B$$

which is to say $B \to Y$ factors through $\operatorname{spec}(A/\ker\varphi)$, so it satisfies the universal property of the scheme-theoretic image. Furthermore, note that, as sets, $\overline{\operatorname{im}(f)} = V(I)$ where

$$I := \bigcap_{\mathfrak{q}\in\operatorname{im}(f)} \mathfrak{q} = \bigcap_{\mathfrak{p}\in\operatorname{spec} B} f(\mathfrak{p}) = \bigcap_{\mathfrak{p}\in\operatorname{spec} B} \varphi^{-1}(\mathfrak{p}) = \varphi^{-1}\left(\bigcap_{\mathfrak{p}\in\operatorname{spec} B} \mathfrak{p}\right) = \varphi^{-1}\left(\sqrt{(0)_B}\right) = \sqrt{\ker\varphi}.$$

Hence, the underlying space of the scheme-theoretic image is the closure of the topological image. ∎

Remark 2.2. Similarly, if $f : X \to Y$ is quasi-compact, it's scheme theoretic image is the defined by the (quasi-coherent!) sheaf of ideals $\ker(\mathscr{O}_Y \to f_*\mathscr{O}_X) \subset \mathscr{O}_Y$. To see that this is quasi-coherent, can assume Y is affine, and then use that $X = \bigcup_{i=1}^n \operatorname{spec} B_i$ has a finite affine cover, and consider

$$\operatorname{spec} B := \bigsqcup_{i=1}^n \operatorname{spec} B_i \overset{g}{\twoheadrightarrow} X \xrightarrow{f} Y.$$

One has that $\mathscr{O}_X \to g_*\mathscr{O}_B$ is an isomorphism (check on stalks), so $f_*\mathscr{O}_X \to (f\circ g)_*\mathscr{O}_B$ is an injection (pushforward is left-exact). Thus,

$$\ker(\mathscr{O}_Y \to f_*\mathscr{O}_X) = \ker(\mathscr{O}_Y \to (f\circ g)_*\mathscr{O}_B)$$

is quasi-coherent (recall Y affine).

Lemma 2.3. *Let* $f : X \to Y$ *be a continuous map, and let* $Z \subset X$ *be irreducible. Then,* $f(Z) \subset Y$ *is irreducible as well.*

Proof. To avoid issues of being closed in Y v.s. being closed in $f(Z)$ and whatnot, restrict f to a map $Z \to f(Z)$. Write $f(Z) = E_1 \cup E_2$ as a union of closed sets. Then, $f^{-1}(f(Z)) = f^{-1}(E_1) \cup f^{-1}(E_2)$, so, after relabeling if necessary, $Z = f^{-1}(E_1)$. As such, $f(Z) = f(f^{-1}(E_1)) \subset E_1 \implies f(Z) = E_1$. ∎

2.2 Useful Results

2.2.1 Misc/algebra

Theorem 2.4 (**Cancellation Theorem for Properties of Morphisms**). *Let P be a class of morphisms preserved by composition and base change. Suppose*

$$\begin{tikzcd} X \arrow[rr, "\pi"] \arrow[dr, "\tau"'] & & Y \arrow[dl, "\rho"] \\ & Z & \end{tikzcd}$$

is a commuting diagram of schemes. Suppose that the diagonal $\delta_\rho : Y \to Y \times_Z Y$ is in P, and that $\tau : X \to Z$ is in P. Then, $\pi : X \to Y$ is in P. In summary,

$$\begin{tikzcd} X \arrow[rr, "\therefore \in P"] \arrow[dr, "\in P"'] & & Y \arrow[dl, "\delta \in P"] \\ & Z & \end{tikzcd}$$

Proof. This is simply an application of the magic (graph) diagram

$$\begin{tikzcd} X \arrow[r, "\Gamma_\pi"] \arrow[d] & X \times_Z Y \arrow[d] \\ Y \arrow[r, "\Delta"] & Y \times_Z Y \end{tikzcd}$$

which shows that $\Gamma_\pi \in P$ (since Δ is). Furthermore, the Cartesian diagram

$$\begin{tikzcd} X \times_Z Y \arrow[r, "\mathrm{pr}_2"] \arrow[d] & Y \arrow[d] \\ X \arrow[r, "\tau"] & Z \end{tikzcd}$$

shows that $\mathrm{pr}_2 : X \times_Z Y \to Y$ is in P (since τ is). Thus, the composition

$$\begin{tikzcd} X \arrow[r, "\Gamma_\pi"'] \arrow[rr, bend left, "f"] & X \times_Z Y \arrow[r, "\mathrm{pr}_2"'] & Y \end{tikzcd}$$

is in P as well, as desired. ∎

Theorem 2.5. *If $I \subset A$ is generated by a regular sequence $a_1, \ldots, a_d$, then the natural map*

$$\mathrm{Sym}^n_A(I/I^2) \to I^n/I^{n+1}$$

is an isomorphism.

Question: Can you prove something similar where instead of starting with a regular sequence, you require A to be graded and I to be a homogeneous ideal?

Proof. It suffices to show the graded surjection

$$\begin{array}{rccc} \alpha: & (A/I)[X_1,\dots,X_d] & \longrightarrow & \displaystyle\bigoplus_{n=0}^{\infty} I^n/I^{n+1} \\ & X_i & \longmapsto & a_i \end{array}$$

is really an isomorphism, so suppose $F \in \ker\alpha$. Since α is graded, we may assume that F is homogeneous, say of degree n. Lift α to

$$\alpha' : A[X_1,\dots,X_d] \to \bigoplus_{n=0}^{\infty} I^n/I^{n+1},$$

and lift F to $A[X_1,\dots,X_d]$ as well, so $F \in \ker\alpha'$. We want to show that $F \in IA[X_1,\dots,X_d]$. We know $F(a_1,\dots,a_d) = 0 \in I^n/I^{n+1}$, so write $F(a_1,\dots,a_d) = x \in I^{n+1}$. Note that $x = G(a_1,\dots,a_d)$ is given by some degree n homogeneous polynomial G *with coefficients in* I, so we may replace $F \rightsquigarrow F - G$ to assume $x = 0$. That is, we have $F \in A[X_1,\dots,X_d]$ homogeneous of degree n satisfying $F(a_1,\dots,a_d) = 0$, and we want to show that $F \in IA[X_1,\dots,X_n]$ (i.e. it's coefficients lie in I). Now, note that this means

$$F(1, a_2/a_1, \dots, a_d/a_1) = 0 \in A\left[\frac{a_2}{a_1},\dots,\frac{a_d}{a_1}\right]$$

where we think of $A\left[\frac{a_2}{a_1},\dots,\frac{a_d}{a_1}\right]$ as a subring of $A_{a_1} = A[1/a_1]$ (recall a_1 is not a zero divisor since we started with a regular sequence). In essence, we're reduced to understanding the kernel of the natural map

$$\begin{array}{rccc} \beta: & A[T_2,\dots,T_d] & \longrightarrow & A\left[\dfrac{a_2}{a_1},\dots,\dfrac{a_d}{a_1}\right] \\ & T_i & \longmapsto & \dfrac{a_i}{a_1} \end{array}$$

(in particular, it would be super great is this kernel was generated by polynomials with coefficients in I). Let $L_i := a_1T_i - a_i \in \ker\beta$. We claim $\ker\beta = (L_2,\dots,L_d)$ which suffices to win by the above discussion. Since we have a regular sequence floating around, I guess the most natural approach to proving something is induction (on d), so that's what we'll do.

($d = 2$) First suppose we have $F(T_2) \in \ker\beta$ so $F(a_2/a_1) = 0$. We divide $a_1^{\deg F}F(T_2)$ by $a_1T_2 - a_2$ to write

$$a_1^{\deg F}F(T_2) = Q(T_2)(a_1T_2 - a_2) + R$$

where $G(T_2) \in A[T_2]$ and $R \in A$ (must have degree less than $\deg(a_1T_2 - a_2) = 1$). Since $A \hookrightarrow A[a_2/a_1]$ is injective (a_1 not a zero divisor), we can evaluate at $T_2 = a_2/a_1$ to see that $0 = R$, i.e. $(a_1T_2 - a_2)G(T_2) \equiv 0 \pmod{a_1^{\deg F}}$. Since a_1, a_2 is regular, we conclude (using Problem 2.6) that the coefficients of $G(T_2)$ must all be divisible by $a_1^{\deg F}$. Since a_1 is not a zero divisor, we conclude that $F(T_2)$ is divisible by $a_1T_2 - a_2$ and so win.

($d > 2$) Let $A' = A[a_2/a_1]$, so $a_1, a_3, a_4, \dots, a_d$ is regular in A' (note that $A'/(a_1) = A[T_2]/(a_1T_2 - a_2, a_1) = A[T_2]/(a_1, a_2)$). Now, consider the composition

$$A[T_2,\dots,T_d] \to A'[T_3,\dots,T_d] \to A'[a_3/a_1,\dots,a_d/a_1] = A[a_2/a_1,\dots,a_d/a_1].$$

By the $d = 2$ case, the kernel of the first map is $L_2 = a_1 T_2 - a_2$. By induction, the kernel of the second map is $(L_3, \dots, L_d)$. We win.

■

2.2.2 Divisors

Proposition 2.6. *If X is an integral scheme, then the homomorphism $\operatorname{CaCl} X \to \operatorname{Pic} X$ is an isomorphism.*

Remark 2.7. In general, there's an injection $\operatorname{CaCl} X \hookrightarrow \operatorname{Pic} X$ which image consisting of those line bundles which appear as a subsheaf of $\mathscr{K}$.

Proposition 2.8. *If X is an integral, separated,* ***locally factorial*** *(all its local rings are UFDs) noetherian scheme, then Weil divisors and Cartier divisors coincide.*

Remark 2.9. Regular local rings are UFDs, so this applies to regular integral separated noetherian schemes.

Proposition 2.10. *Let X be a noetherian scheme with invertible divisors $\mathscr{L}, \mathscr{M}$. Then,*

(a) *$\mathscr{L}$ ample, $\mathscr{M}$ globally generated $\implies \mathscr{L} \otimes \mathscr{M}$ ample*

(b) *$\mathscr{L}$ ample $\implies \mathscr{L}^n \otimes \mathscr{M}$ ample for $n \gg 0$*

(c) *$\mathscr{L}, \mathscr{M}$ both ample $\implies \mathscr{L} \otimes \mathscr{M}$ ample*

For the last two, also assume X of finite type over a noetherian ring A.

(d) *$\mathscr{L}$ very ample, $\mathscr{M}$ globally generated $\implies \mathscr{L} \otimes \mathscr{M}$ very ample*

(e) *$\mathscr{L}$ ample $\implies \exists n_0 > 0$ s.t. $\mathscr{L}^n$ is very ample for all $n \geq n_0$*

2.2.3 Projective stuff

Theorem 2.11. *Let X be separated and fin. type over a noetherian ring A. Then, a line bundle $\mathscr{L} \in \operatorname{Pic} X$ is ample iff a power of it is very ample.*

Proof. $(\rightarrow)$ ■

Lemma 2.12 (Stack Exchange)**.** *Let $S = A[x_0, \dots, x_n]$, let $I \subset S$ be a homogeneous ideal, and let $T = S/I$. Let $\mathfrak{p} \in \operatorname{Proj} S = \mathbb{P}^n_A$ be a homogeneous ideal not containing $S_+ = (x_0, \dots, x_n)$, and let $X = \operatorname{Proj}(S/I) \hookrightarrow \mathbb{P}^n_A$. Consider the sheaf*

$$\mathscr{S} := \bigoplus_{n \geq 0} \mathscr{O}_X(n).$$

Finally, choose some degree one $x \in S_1$ not contained in $\mathfrak{p}$. Then,

$$\mathscr{S}_\mathfrak{p} \simeq \mathscr{O}_{X,\mathfrak{p}}[x] = S_{(\mathfrak{p})}[x].$$

Proof. Since $\mathfrak{p} \in D_+(x)$, we have $\mathscr{O}_X(n)_\mathfrak{p} = \left(\mathscr{O}_X(n)|_{D_+(x)}\right)_\mathfrak{p}$. Note that $\mathscr{O}_X|_{D_+(x)} \cong \widetilde{S_{(x)}}$ from which we see that $\mathscr{O}_X(n)|_{D_+(x)} \cong \widetilde{x^n S_{(x)}}$. This identification sends the prime $\mathfrak{p}$ to the prime $\mathfrak{p}' := \mathfrak{p}_{(x)}$ of $S_{(x)}$. Hence,

$$\mathscr{O}_X(n)_\mathfrak{p} = \left(\mathscr{O}_X(n)|_{D_+(x)}\right)_\mathfrak{p} = (x^n S_{(x)})_{\mathfrak{p}'} = x^n S_{(\mathfrak{p})}.$$

As a consequence

$$\mathscr{P}_\mathfrak{p} = \bigoplus_{n\geq 0} \mathscr{O}_X(n)_\mathfrak{p} \simeq \bigoplus_{n \geq 0} x^n S_{(\mathfrak{p})} = S_{(\mathfrak{p})}[x].$$

■

Theorem 2.13 (**Bertini's Theorem**). *Let $X \hookrightarrow \mathbb{P}^n_k$ ($k = \overline{k}$) be a nonsingular closed subvariety. Then there exists a hyperplane $H \subset \mathbb{P}^n_k$ not containing X, and such that the scheme $H \cap X$ is regular at every point (and secretly irreducible, so a nonsingular variety, if $\dim X \geq 2$). Furthermore, the set of hyperplanes with this property forms a dense open subset of the linear system $|H| \cong \mathbb{P}\Gamma(\mathbb{P}^n, \mathscr{O}(H))$, considered as a projective space.*

Proof. Let's try and prove something stronger. Fix some integer $d \geq 1$. We want to prove the theorem with H replaced by some hypersurface V of degree $\deg V = d$.

For a closed point $x \in X$, consider the set $B_x = \{$degree d hypersurfaces $S : S \supset X$ or $S \not\supset X$ but $x \in S \cap X$, and x is not a regular point of $H \cap X\}$. These are the bad hypersurfaces with respect to the point x. Any hypersurface is determined by a nonzero global section $f \in V := \Gamma(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(d))$. Fix some nonzero $f_0 \in V$ with $x \notin S_0 = \{f_0 = 0\}$. We now define a map of k-vector spaces

$$\varphi_x : V \to \mathscr{O}_{X,x}/\mathfrak{m}_x^2$$

as follows: given $f \in V$, f/f_0 is a regular function on $\mathbb{P}^n \setminus S_0$ so induces a regular function on $X \setminus (X \cap S_0)$. We set $\varphi_x(f)$ to be the image of f/f_0 in the local ring $\mathscr{O}_{X,x}$ modulo $\mathfrak{m}_x^2$. Letting $S = \{f = 0\}$, the scheme $S \cap X$ is defined at x by the ideal generated by f/f_0 in $\mathscr{O}_{X,x}$ (note f_0 is a unit here), so $x \in S \cap X$ iff $\varphi_x(f) \in \mathfrak{m}_x/\mathfrak{m}_x^2$, and x is nonregular on $H \cap X$ iff $\varphi_x(f) \in \mathfrak{m}_x^2$ (in this case, the local ring $\mathscr{O}_{X\cap H,x} = \mathscr{O}_{X,x}/(\varphi(f))$ will not be regular. It's not even a domain). Thus, the hypersurfaces $S \in B_x$ correspond exactly to those $f \in \ker \varphi_x$ (note that $f/f_0 = 0 \in \mathscr{O}_{X,x} \iff S \supset X$).

Since x is a closed point and k is algebraically closed, $\mathfrak{m}_x$ is generated by linear forms in the coordinates, so we see that φ_x is surjective (by Nakyama). If $\dim X = r$, then $\dim_k \mathscr{O}_x/\mathfrak{m}_x^2 = \dim_k \mathscr{O}_x/\mathfrak{m}_x + \dim_k \mathfrak{m}_x/\mathfrak{m}_x^2 = 1 + r$. At the same time, $\dim V = \binom{n+d}{d}$, so $\dim \ker \varphi_x = \binom{n+d}{d} - (r+1)$. Thus, B_x is a linear system of hyperplanes of dimension $\binom{n+d}{d} - r - 2$ (as a projective space).

Now we're basically done. Consider the complete linear system $|S|$ as a projective space, and consider the subset $B \subset X \times |S|$ consisting of pairs (x, S) s.t. $x \in X$ is a closed point and $S \in B_x$. Then B is the set of closed points of a closed subset of $X \times |S|$, which we still denote by B and give the reduced scheme structure. Consider the two projections

$$\begin{tikzcd} & B \arrow[dl, "p_1"'] \arrow[dr, "p_2"] & \\ X & & {|S|}. \end{tikzcd}$$

We have just seen that $p_1 : B \to X$ is surjective with fiber $B_x \cong \mathbb{P}^{\binom{n+d}{d}-r-2}$. Thus, B is irreducible of dimension

$$\dim B = \left(\binom{n+d}{d} - r - 2\right) + r = \binom{n+d}{d} - 2.$$

Now consider the second projection $p_2 : B \to |S|$. We see that $\dim p_2(B) \leq \binom{n+d}{d} - 2 < \binom{n+d}{d} - 1 = \dim |S|$. Thus, is $S \in |S| \setminus p_2(B)$, then $S \not\supset X$ and every point of $S \cap X$ is regular, so S satisfies the requirements of the theorem. Finally, since X is projective, $p_2 : X \times |S| \to |S|$ is a proper morphism, so $p_2(B) \overset{\text{closed}}{\subset} |S|$ which means that $|S| \setminus p_2(B)$ is an open dense subset of $|S|$, proving the theorem. ∎

I guess one also needs to know that the subspace of $|S|$ corresponding to nonsingular hypersurfaces is open and dense. But this is easy since it's simply when the derivatives of f are non-vanishing, so an intersection of $n+1$ open sets.

Remark 2.14. Alternatively, one can prove Bertini only when $d = 1$ as in Hartshorne, and then use the d-uple embedding $\mathbb{P}^n \hookrightarrow \mathbb{P}^{\binom{n+d}{d}-1}$,

$$[x_0 : \cdots : x_n] \mapsto [x_0^d, x_0^{d-1}x_1 : \cdots : x_n^d]$$

to reduce Bertini for general d to the case $d = 1$.

2.2.4 Differentials

Theorem 2.15. *Let A be a ring, $Y = \operatorname{spec} A$ and $X = \mathbb{P}^n_A$. Then, there is an exact sequence*

$$0 \longrightarrow \Omega_{X/Y} \longrightarrow \mathscr{O}_X(-1)^{\oplus(n+1)} \longrightarrow \mathscr{O}_X \longrightarrow 0$$

of sheaves on X.

Proof. Let $S = A[x_0, \ldots, x_n]$ be the homogeneous coordinate ring of X, and let $E = S(-1)^{\oplus(n+1)}$ with basis $e_0, \ldots, e_n$ in degree 1. Consider the map $E \to S$ given by sending $e_i \mapsto x_i$. This is visibly surjective in degrees ≥ 1 (E vanishes in degree 0), so induces a surjection of sheaves $\mathscr{O}_X(-1)^{\oplus(n+1)} \twoheadrightarrow \mathscr{O}_X$. We need to show the kernel K is $\Omega_{X/Y}$.

If we localize at x_i, then $E_{x_i} \to S_{x_i}$ is a surjection of graded S_{x_i}-modules, so K_{x_i} is free of rank $(n+1) - 1 = n$, generated by $e_j - \frac{x_j}{x_i} e_i$ ($j \neq i$). Thus, if $U_i = D_+(x_i)$, we see that $K|_{D_+(x_i)}$ is a free $\mathscr{O}_{U_i}$-module generated by the global sections

$$\frac{1}{x_i} e_j - \frac{x_j}{x_i^2} e_i \text{ for } j \neq i.$$

Now we can define $\varphi : \Omega_{X/Y} \to K$ by defining it on the opens U_i and checking it agrees on overlaps. On $U_i \cong \operatorname{spec} A\left[\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\right]$, $\Omega_{X/Y}|_{U_i}$ is a free $\mathscr{O}_{U_i}$-module generated by $\mathrm{d}(x_0/x_i), \ldots, \mathrm{d}(x_n/x_i)$, so we set

$$\varphi\left(\mathrm{d}\left(\frac{x_j}{x_i}\right)\right) := \frac{e_j x_i - x_j e_i}{x_i^2}.$$

This is our isomorphism. ∎

Corollary 2.16. *The canonical bundle on $X = \mathbb{P}^n_A$ is $\Omega_X = \mathscr{O}_X(-(n+1))$.*

2.2.5 Riemann-Hurwitz

Definition 2.17. A (generically) finite morphism between integral schemes $X \to Y$ is **(generically) separable** if it is dominant, and the induced extension of function fields $K(X)/K(Y)$ is separable.

Proposition 2.18. *If $\pi : X \to Y$ is a generically separable morphism of irreducible smooth varieties of the same dimension n, then the* ***relative cotangent sequence*** *is exact on the left as well, i.e.*

$$0 \longrightarrow \pi^*\Omega_{Y/k} \xrightarrow{\varphi} \Omega_{X/k} \longrightarrow \Omega_{X/Y} \longrightarrow 0.$$

Proof. We need φ to be injective. We know $\Omega_{Y/k}$ is a rank n locally free sheaf on Y (by smoothness). A locally free sheaf on an integral scheme (e.g. $\pi^*\Omega_{Y/k}$) is torsion-free (any section over any open set is nonzero at the generic point), so any nonzero subsheaf will be nonzero at the generic point. Thus, it suffices to show that φ is an inclusion at the generic point (which will force $\ker \varphi_\eta = 0$). We thus tensor with $\mathscr{O}_\eta$, an exact functor. Note that $\mathscr{O}_\eta \otimes \Omega_{X/Y} = 0$ precisely since $K(X)/K(Y)$ is separable. Similarly, $\mathscr{O}_\eta \otimes \pi^*\Omega_{Y/k}$ and $\mathscr{O}_\eta \otimes \Omega_{X/k}$ are both n-dimensional $\mathscr{O}_\eta$-vector spaces. Thus, the map $\mathscr{O}_\eta \otimes \pi^*\Omega_{Y/k} \to \mathscr{O}_\eta \otimes \Omega_{X/k}$ (with trivial cokernel) is surjective and so an isomorphism. ∎

Say $f : X \to Y$ is a finite, separable morphism of smooth curves.

Notation 2.19. For a point $P \in X$, we write $Q = f(P)$, we let t be a local parameter at Q (uniformizer of $\mathscr{O}_{Y,Q}$), and let u be a local parameter at P. Then, $\mathrm{d}t$ generates the free $\mathscr{O}_Q$-module $\Omega_{Y/Q}$, and $\mathrm{d}u$ generates the free $\mathscr{O}_P$-module $\Omega_{X/P}$. In particular, there is a unique element $g \in \mathscr{O}_P$ such that $f^*\mathrm{d}t = g\mathrm{d}u$, and we write $\mathrm{d}t/\mathrm{d}u := g$.

Proposition 2.20.

(a) *$\Omega_{X/Y}$ is a torsion sheaf on X, with support equal to the set of ramification points of f. In particular, f is ramified at only finitely many points.*

(b) *For each $P \in X$, the stalk $(\Omega_{X/Y})_P$ is a principal $\mathscr{O}_P$-module of finite length $v_P(\mathrm{d}t/\mathrm{d}u)$.*

(c)

$$\mathrm{length}(\Omega_{X/Y})_P \geq e_p - 1.$$

with equality iff f is tamely ramified at P.

Proof. **(a)** This comes from the exact sequence

$$0 \longrightarrow \pi^*\Omega_{Y/k} \xrightarrow{\varphi} \Omega_{X/k} \longrightarrow \Omega_{X/Y} \longrightarrow 0.$$

(b) The exact sequence shows that $(\Omega_{X/Y})_P \cong \Omega_{X,P}/f^*\Omega_{Y,Q}$ which is isomorphism to $\mathscr{O}_P/(\mathrm{d}t/\mathrm{d}u)$.

(c) If f has ramifiecation index $e = e_p$, i.e. $t = au^e$ for some $a \in \mathscr{O}_P^\times$, then

$$\mathrm{d}t = aeu^{e-1}\mathrm{d}u + u^e\mathrm{d}a.$$

If the ramification is tame, then $e \neq 0 \in k$ so $v_p(\mathrm{d}t/\mathrm{d}u) = e - 1$. Otherwise, $v_p(\mathrm{d}t/\mathrm{d}u) \geq e$. ∎

Definition 2.21. The **ramification divisor** of f is

$$R := \sum_{P \in X} \operatorname{length}(\Omega_{X/Y})_P \cdot P.$$

Proposition 2.22. *Let K_X, K_Y be canonical divisors for X, Y. Then,*

$$K_X \sim f^* K_Y + R.$$

Proof. Consider R as a closed subscheme of X. By definition, its structure sheaf is $\Omega_{X/Y}$. Tensoring our favorite exact sequence with Ω_X^{-1} then gives

$$0 \longrightarrow f^*\Omega_Y \otimes \Omega_X^{-1} \longrightarrow \mathscr{O}_X \longrightarrow \mathscr{O}_R \longrightarrow 0$$

(no nontrivial line bundles on R). Thus, $f^*\Omega_Y \otimes \Omega_X^{-1} \cong \mathscr{O}_X(-R)$ so we win. ■

Corollary 2.23. *Let $f : X \to Y$ be a finite separable morphism of curves. Let $n = \deg f$. Then,*

$$2g(X) - 2 = n(2g(Y) - 2) + \deg R.$$

Furthermore, if f only has tame ramification, then

$$\deg R = \sum_{P \in X} (e_p - 1).$$

2.2.6 Classifying Curves of genus ≤ 3

2.2.7 Affine and projective dimension theorems

2.2.8 Associated Points

2.2.9 Some cohomological stuff

Theorem 2.24. *Let X be a noehterian scheme. TFAE*

- ***(i)*** *X is affine*
- ***(ii)*** $\mathrm{H}^i(X, \mathscr{F}) = 0$ *for all $\mathscr{F}$ qcoh and all $i > 0$*
- ***(iii)*** $\mathrm{H}^1(X, \mathscr{I}) = 0$ *for all coh sheaves of ideals $\mathscr{I}$*

Theorem 2.25. *Let A be a notherian ring, and let X be a proper A-scheme. Let $\mathscr{L}$ be an invertible sheaf on X. TFAE*

- ***(i)*** *$\mathscr{L}$ is ample*
- ***(ii)*** *For each coh sheaf $\mathscr{F}$ on X, there is an integer n_0, depending on $\mathscr{F}$, such that for each $i > 0$ and each $n \geq n_0$,* $\mathrm{H}^i(X, \mathscr{F} \otimes \mathscr{L}^n) = 0$.

2.3 Exercises

Problem 2.1 (Hartshorne II.3.15). *Let X be a scheme of finite type over a field.*

(a) TFAE

- **(i)** $X \times_k \overline{k}$ is irreducible.
- **(ii)** $X \times_k k_s$ is irreducible.
- **(iii)** $X \times_k K$ is irreducible for every field extension K/k

Proof. **(iii)** $\implies$ **(i)** $\implies$ **(ii)** is obvious, so we do **(ii)** $\implies$ **(iii)**, by contrapositive. Fix a field K s.t $X \times_k K$ is reducible. Then, there exists an open affine $\operatorname{spec}(A \times_k K) \subset X \times_k K$ which is also reducible.[1], so we may assume $X = \operatorname{spec} A$ is affine (all opens in an irreducible space are irreducible). By assumption, $A \otimes_k K$ has multiple minimal primes, and we want to show that $A \otimes_k k_s$ also has multiple minimal primes. Let $\mathfrak{p}_1, \mathfrak{p}_2$ be two minimal primes of A. Since A is of finite type over a field, it's noetherian, so each $\mathfrak{p}_i$ is finitely generated, so we may assume that K/k is a finitely generated field extension (generated by generators of the $\mathfrak{p}_i$'s). Let R be the f.g. k-algebra (not the field K) generated by these same generators, so $A \otimes_k R$ has multiple minimal primes. Let $\mathfrak{m} \subset R$ be a maximal ideal. Then, $A \otimes_k R/\mathfrak{m} = A \otimes_k L$ for some finite (by weak Nullstellsatz of Zariski's lemma or whatever) extension L/k has multiple minimal primes (this proves **(i)** $\implies$ **(iii)**). I guess to finish one now wants to do some sort of inseparable descent... ■

Question: Does it? Why did I think this?

Problem 2.2 (Hartshorne II.3.22). *Let $f : X \to Y$ be a dominant morphism of integral schemes of finite type over a field k.*

(a) Let Y' be a closed irreducible subset of Y, whose generic point η' is contained in $f(X)$. Let Z be an irreducible component of $f^{-1}(Y')$, such that $\eta' \in f(Z)$. Then, $\operatorname{codim}(Z, X) \leq \operatorname{codim}(Y', Y)$.

Proof. ■

(b) Let $e = \dim X - \dim Y$ be the relative dimension of X over Y. For any point $y \in f(X)$, every irreducible component of the fiber X_y has dimension $\geq e$.

Problem 2.3 (Ravi 1.3.S, The **magic diagram**). *Suppose we are given morphisms $X_1, X_2 \to Y$ and $Y \to Z$. Then, the following diagram is Cartesian*

$$\begin{tikzcd} X_1 \times_Y X_2 \arrow[r] \arrow[d] & X_1 \times_Z X_2 \arrow[d] \\ Y \arrow[r] & Y \times_Z Y. \end{tikzcd}$$

[1] If $X \times_k K$ is disconnected, take a disjoint union of affines on two components. If it is connected, let Z, Z' be two irreducible components. Then, any $z \in Z \cap Z'$ satisfies $\mathscr{O}_{X,z}$ has multiple minimal primes. Hence any basic affine around z will be reducible.

Proof. Check universal properties. Given maps $A \rightrightarrows Y, X_1 \times_Z X_2$ with the same composition $A \to Y \times_Z Y$, the definition of the diagonal morphism $\Delta : Y \to Y \times_Z Y$ tells us that the induced maps $A \rightrightarrows X_1, X_2$ both agree over Y. Thus, we obtain $A \to X_1 \times_Y X_2$. Hence, $X_1 \times_Y X_2$ satisfies the universal property of the fiber product, and we win. ∎

Problem 2.4 (Hartshorne II.4.4). *Let $f : X \to Y$ be a morphism of separated schemes of finite type over a noetherian base scheme S. Let $Z \subset X$ be a closed subscheme which is proper over S. Then, $f(Z)$ is closed in Y, and $f(Z)$ with its image subscheme structure is proper over S.*

Proof. Can assume $Z = X$.

As a special case of the magic diagram, we get a Cartesian square

$$\begin{array}{ccc} X & \xrightarrow{\Gamma_f} & X \times_S Y \\ \downarrow & & \downarrow{\scriptstyle (f,\mathrm{id})} \\ Y & \xrightarrow{\Delta} & Y \times_S Y \end{array}$$

where we note that $X = X \times_Y Y$. Since Y is separated, the diagonal is a closed immersion, so the graph morphism $\Gamma_f : X \to X \times_S Y$ is a closed immersion as well. Now, $f : X \to Y$ factors as

$$X \overset{\Gamma_f}{\hookrightarrow} X \times_S Y \xrightarrow{\mathrm{pr}_2} Y.$$

Note that $\mathrm{pr}_2 : X \times_S Y \to Y$ is proper since it is the base change of $X \to S$ (along $Y \to S$), so f is a composition of proper maps, and so itself proper.

Since f is quasi-compact, the underlying space of its scheme-theoretic image is $\overline{f(Z)} = f(Z)$, so we may as well replace Y with $f(Z)$ to assume that $f : X \to Y$ is a (proper) surjection from a proper S-scheme to a separated, finite-type S-scheme. Thus, to show that Y is proper/S, we only need show that $Y \to S$ is universally closed. First observe that the image of Y in S is the image of X is S (since $X \twoheadrightarrow Y$ surjective), so Y has closed image in S. Furthermore, for any $T \to S$, one obtains a diagram

$$\begin{array}{ccc} X_T & \xrightarrow{f_T} & Y_T \\ & \searrow \quad \swarrow & \\ & T & \end{array}$$

satisfying the same initial hypotheses, e.g. $X_T \to T$ is proper, $X_T \to Y_T$ is surjective, and $Y_T \to T$ is separated and of finite type. Thus, by the same reasoning, $Y_T \to T$ has closed image, so $Y \to S$ is indeed universally closed. ∎

Problem 2.5 (Hartshorne II.4.5). *Let X be an integral scheme of finite type over a field k, having function field K. We say that a valuation of K/k has **center** x **on** X if its valuation ring R dominates the local ring $\mathscr{O}_{X,x}$.*

(a) If X is separated over k, then the center of any valuation of K/k on X (if it exists) is unique.

Proof. This is the valuative criterion. Say v is a valuation of K/k with centers $x, y \in X$, i.e. $R \supset \mathscr{O}_{X,x}, \mathscr{O}_{X,y}$ inside the function field K. This gives morphism $x, y : \operatorname{spec} R \rightrightarrows \mathscr{O}_{X,x}, \mathscr{O}_{X,y} \rightrightarrows X$ fitting into the diagram

$$\begin{tikzcd} \operatorname{spec} K \arrow[r, "\eta"] \arrow[d] & X \arrow[d] \\ \operatorname{spec} R \arrow[r] \arrow[ur, bend left, "x"] \arrow[ur, bend right, "y"'] & \operatorname{spec} k \end{tikzcd}$$

Thus, $x = y$. ∎

(b) If X is proper over k, then every valuation of K/k has a unique center of X.

Proof. This is just the valuative criterion. ∎

(c) The converses of **(a)**,**(b)** hold.

(d) If X is proper over $k = \overline{k}$, then $\Gamma(X, \mathscr{O}_X) = k$.

Proof. Fix some $a \in \Gamma(X, \mathscr{O}_K)$. Suppose that $a \notin k$. Note that $a \in \Gamma(X, \mathscr{O}_K) \to \mathscr{O}_{X,x}$ for all $x \in X$, so a is present in every local ring. However, we claim there is a valuation ring R of K/k with $a^{-1} \in \mathfrak{m}_R$ (so $a \notin R$). This contradicts **(b)** as such an R cannot dominate any local ring of X.

Where does R come from? First consider the ring $k[a^{-1}] \subset K$. Since $k = \overline{k}$, this is a polynomial ring in one variable (i.e. a is transcendental over k). Let $\mathfrak{m} := (a^{-1}) \subset k[a^{-1}]$, so $k[a^{-1}]_{\mathfrak{m}} \subset K$ is a local ring (a dvr even) with a^{-1} in its maximal ideal. Since valuation rings are maximal local rings in K, we conclude there must be some valuation ring $R \subset K$ with $R \supset k[a^{-1}]_{\mathfrak{m}}$ and $\mathfrak{m}_R \cap k[a^{-1}]_{\mathfrak{m}} = \mathfrak{m} \ni a^{-1}$. ∎

Problem 2.6 (Ravi 8.4.E)**.** *Let M be an A-module. Say $x, y \in A$ form a regular sequence for M. Then, x^N, y is also an M-regular sequence.*

Proof. Clearly x^N is not a zero divisor in M since x isn't. We want to show that y is not a zero divisor of $M/(x^N M)$. Suppose $ym \equiv 0 \pmod{x^N}$ for some $m \in M$, i.e. that $ym = x^N k$ for some $k \in M$. Then, $ym = 0 \in M/xM$ which forces $m = 0 \in M/xM$ (since y not a zero divisor in M/xM), so $m = xm_1$ for some $m_1 \in M$ and $ym_1 = x^{N-1}k$ (x is not a zero divisor). This exponent is lower, so now we induct to conclude that $m = 0$. ∎

Corollary 2.26 (of argument)**.** *If $x_1, \dots, x_n$ is M-regular, then so is $x_1^{a_1}, \dots, x_n^{a_n}$ for any $a_1, \dots, a_n \in \mathbb{Z}_{\geq 1}$.*

We say X satisfies $(*)$ if X is a noetherian integral separated scheme which is regular in codimension one.

Problem 2.7 (Hartshorne II.6.1)**.** *Let X be a scheme satisfying $(*)$. Then, $X \times \mathbb{P}^n$ satisfies $(*)$, and $\operatorname{Cl}(X \times \mathbb{P}^n) \cong \operatorname{Cl}(X) \times \mathbb{Z}$.*

Proof. $X' := X \times \mathbb{P}^n$ is visibly noetherian, integral, and separated since it's factors are. That leaves regular in codimension one. Let $\pi : X' = X \times \mathbb{P}^n \to X$ denote the projection. Pick some $x' \in X'$ with $\dim \mathscr{O}_{X',x'} = 1$, set $x := \pi(x') \in X$, consider $\mathscr{O}_{X,x} \to \mathscr{O}_{X',x'}$ and notice that Corollary 1.7 tells us we have two cases

($\dim \mathscr{O}_{X,x} = 0$ – Type 1) In this case x is the generic point of X and $\mathscr{O}_{X,x} = K(X)$ is its function field. The pullback diagram

$$\begin{tikzcd} \mathbb{P}^n_{K(X)} \arrow[r] \arrow[d] \arrow[dr, phantom, "\ulcorner"] & X \times \mathbb{P}^n \arrow[d] \\ \operatorname{spec} K(X) \arrow[r] & X \end{tikzcd}$$

shows that the fiber above the generic point is $\mathbb{P}^n_{K(X)}$, so $x' \in \mathbb{P}^n_{K(X)}$ has a regular local ring.

Remember: smooth over a field = geometrically regular

($\dim \mathscr{O}_{X,x} = 1$ – Type 2) In this case $\overline{x'}$ does not project onto all of X, so x' must be the generic point of $Z \times \mathbb{P}^n$ with $Z = \overline{x} \subset X$ irreducible of codimension 1. Hence, the local ring $\mathscr{O}_{X',x'}$ here will be a localization of

$$\mathscr{O}_{X,x}[T_1, \dots, T_n]$$

and so will be regular local.

Alternatively, Hartshorne shows $X \times \mathbb{A}^1$ satisfies (*), so $X \times \mathbb{A}^n$ does too by induction, so $X \times \mathbb{P}^n$ does since regularity in codimension 1 can be checked locally

Now the class group computation. Consider the (commutative) diagram

$$\begin{tikzcd} 0 \arrow[r, dashed] & \mathbb{Z} \arrow[r, "1 \mapsto {[X \times \mathbb{P}^{n-1}]}"] & \mathrm{Cl}(X \times \mathbb{P}^n) \arrow[r] & \mathrm{Cl}(X \times \mathbb{A}^n) \arrow[r] & 0 \\ & \mathrm{Cl}(\mathbb{P}^n) \arrow[u, "\deg", "\wr"'] \arrow[ur, "\pi_2^*"] & & \mathrm{Cl}(X) \arrow[u, "\pi^*"', "\wr"] \arrow[ul, "\pi^*"] & \end{tikzcd}$$

with exact row (where $\pi_2 : X' \to \mathbb{P}^n$ the other projection). We claim $\pi_2^* : \mathrm{Cl}(\mathbb{P}^n) \to \mathrm{Cl}(X \times \mathbb{P}^n)$ is injective, which suffices to win. As far as I can tell, this is simply because, fixing any $x \in X$, we have a section $\sigma : \mathbb{P}^n \xrightarrow{\sim} \{x\} \times \mathbb{P}^n \hookrightarrow X \times \mathbb{P}^n$ to π_2, so $(\pi_2 \circ \sigma)^* = \sigma^* \circ \pi_2^* = \mathrm{Id}_{\mathrm{Cl}(\mathbb{P}^n)}$. ∎

Problem 2.8 (Hartshorne II.6.2). *Let X be a closed subvariety (nonsingular in codim 1) in $\mathbb{P}^n_k$ where $k = \overline{k}$ is algebraically closed. For a divisor $D = \sum n_i Y_i$ on X, we define its* ***degree*** *to be $\sum n_i \deg Y_i$ with $\deg Y_i$ the degree of Y_i as a projective variety.*

(a) For an irreducible hypersurface $V \subset \mathbb{P}^n_k$ containing X, the map $V \mapsto V.X$ extends to a well-defined homomorphism from the subgroup of $\operatorname{Div} \mathbb{P}^n$ consisting of divisors, none of whose components contain X, to $\operatorname{Div} X$.

Proof. We're extending linearly, so the only content is to show that $V.X$ is well-defined, i.e that $v_{Y_i}(\overline{f}_i)$ is independent of the choice of function f_i cutting out V near Y_i. Well, let $U, U' \subset \mathbb{P}^n$ be open sets intersecting Y_i non-trivially (so $\eta_{Y_i} \in U \cap U'$) and let f_i, f_i' be local equations for V on U, U', respectively. Then, $f_i|_{U \cap U'}, f_i'|_{U \cap U'}$ are both local equations for V on $U \cap U'$, so they must differ by a unit in the stalk at η_{Y_i}, and so $v_{Y_i}(\overline{f}_i) = v_{Y_i}(\overline{f}'_i)$ as desired. ∎

(b) If D is a principal divisor on $\mathbb{P}^n$ for which $D.X$ is defined, then $D.X$ is principal on X. Hence, we have a homomorphism $\operatorname{Cl}\mathbb{P}^n \to \operatorname{Cl} X$.

Proof. Write $D = \operatorname{div}_{\mathbb{P}^n}(f) = \sum_{i=1}^n n_i[V_i] \in \operatorname{Div}(\mathbb{P}^n)$. For each V_i, let Y_{ij} be the set of irreducible components of $V_i \cap X$, and let $U_{ij} \subset \mathbb{P}^n$ be an open set for which $U_{ij} \cap Y_{ij} \neq \emptyset$ and on which there exists a local equation g_{ij} for V on U_{ij}. Let $e_{ij} = \operatorname{ord}_{Y_{ij}}(\overline{g}_{ij})$ where $\overline{g}_{ij} = g_{ij}|_{U_{ij}\cap X}$. Then,

$$D.X = \sum_{i=1}^n \sum_j n_i e_{ij}[Y_{ij}],$$

and we claim that this is $\operatorname{div}_X(f)$ (i.e. that $n_i e_{ij} = \operatorname{ord}_{Y_{ij}}(f) =: m_{ij}$). To see this, note that we have $f|_{U_{ij}} \big/ g_{ij}^{n_i} \in \mathscr{O}_{\mathbb{P}^n}(U_{ij})$ vanishing only outside of V_i (by definition of n_i), so the same holds after restricting to X and hence $f|_{U_{ij}} \big/ g_{ij}^{n_i}$ is a unit in $\mathscr{O}_{X,\eta_{Y_{ij}}}$, but this says that

$$m_{ij} = \operatorname{ord}_{Y_{ij}}(f) = \operatorname{ord}_{Y_{ij}}(g_{ij}^{n_i}) = n_i e_{ij}$$

as desired. ■

(c) The integer n_i is the same as the intersection multiplicity $i(X, V; Y_i)$. As a consequence, generalized Bezout gives

$$\deg(D.X) = (\deg D)(\deg X)$$

whenever the LHS is defined.

Proof. We have $i(X, V; Y_i) = \mu_{Y_i}\left(\frac{S}{I_V + I_X}\right) = \operatorname{length}\left(\frac{S}{I_v + I_X}\right)_{Y_i}$ where I use the notation $blah_{Y_i}$ to denote localizing at (the prime corresponding to/generic point of) Y_i. Since,

$$\left(\frac{S}{I_v + I_X}\right)_{Y_i} \simeq \frac{(S/I_X)_{Y_i}}{I_{V,Y_i} \cap I_{X,Y_i}} \simeq \frac{\mathscr{O}_{X,Y_i}}{I_{V,Y_i}}$$

and $I_{V,Y_i} = (\pi)^{n_i}$ by definition ($\pi \in \mathscr{O}_{X,Y_i}$ a uniformizer), we have that $i(X, V; Y_i) = \operatorname{length}(\mathscr{O}_{X,Y_i}/(\pi)^{n_i}) = n_i$ e.g. since that is its dimension as a vector space over $\mathscr{O}_{X,Y_i}/(\pi)$. The second part is literally just generalized Bezout. ■

(d) If D is principal divisor on X, then there exists a rational function f on $\mathbb{P}^n$ such that $D = (f).X$, and hence $\deg D = 0$ by **(c)**. Thus, we get $\deg : \operatorname{Cl} X \to \mathbb{Z}$ which, by **(c)**, fits into a commutative diagram

$$\begin{tikzcd} \operatorname{Cl}\mathbb{P}^n \arrow[r] \arrow[d, "\deg"'] & \operatorname{Cl} X \arrow[d, "\deg"] \\ \mathbb{Z} \arrow[r, "(\deg X)"] & \mathbb{Z} \end{tikzcd}$$

In particular, $\operatorname{Cl}\mathbb{P}^n \to \operatorname{Cl}^X$ is injective.

Proof. Say $D = (f)$ on X, so $f \in K(X)^\times = \mathscr{O}_{X,\eta_X}^\times$ with $\eta_X \in X$ its generic point. Since $X \hookrightarrow \mathbb{P}^n$ is a closed immersion, we have a surjection

$$\mathscr{O}_{\mathbb{P}^n,\eta_X} \twoheadrightarrow \mathscr{O}X, \eta_X,$$

so f lifts to an element $F \in \mathscr{O}_{\mathbb{P}^n, \eta_X} \subset K(\mathbb{P}^n)$. By construction. $(F).X = (F|_X) = (f) = D$. ∎

Problem 2.9 (Hartshorne II.6.3)**.** *Let $V \hookrightarrow \mathbb{P}^n$ be a projective variety of dimension ≥ 1 which is nonsingular in codimension 1. Let $X = C(V)$ be the affine cone of V in $\mathbb{A}^{n+1}$, and let $\overline{X} \hookrightarrow \mathbb{P}^{n+1}$ be its projective closure. Let $P \in X$ be the vertex of the cone.*

(a) Let $\pi : \overline{X} \setminus P \to V$ be the projection map. V can be covered by opens $U_i \subset V$ s.t. $\pi^{-1}(U_i) \cong U_i \times \mathbb{A}^1$ for each i, and $\pi^* : \mathrm{Cl}(V) \to \mathrm{Cl}(\overline{X} \setminus P)$ is an iso. Hence,

$$\mathrm{Cl}(V) \xrightarrow{\sim} \mathrm{Cl}(\overline{X} \setminus P) \xrightarrow{\sim} \mathrm{Cl}(\overline{X}).$$

Remark 2.27. Let's say some stuff about coordinates first, just to orient ourselves. The points of $X \subset \mathbb{A}^{n+1}$ are those $(x_0, \dots, x_n) \in \mathbb{A}^{n+1}$ s.t. $[x_0 : \cdots : x_n] \in \mathbb{P}^n$ lies on V. We embed $\mathbb{A}^{n+1} \hookrightarrow \mathbb{P}^{n+1}$ via $(x_0, \dots, x_n) \mapsto [x_0 : \cdots : x_n : 1]$. Then, $\overline{X} \subset \mathbb{P}^{n+1}$ is the closure of $X \subset \mathbb{A}^{n+1}$ under this embedding. In particular, the homogeneous ideal defining $\overline{X}$ is generated by the same (homogeneous!) polynomials which define X (i.e. those which define V). Hence, we have a natural section $\sigma : V \hookrightarrow \overline{X} \setminus P$, $[x_0 : \cdots : x_n] \mapsto [x_0 : \cdots : x_n : 0]$ to the projection map $\pi : \overline{X} \setminus P \to V$. Anyways, let's actually do this problem...

Make this coordinate stuff rigorous by using the universal mapping properties of affine/projective space

Proof. Let $D_+(x_i) \subset \mathbb{P}^n$ be subspace where $x_i \neq 0$ (so $D_+(x_i) \cong \mathbb{A}^n$), and let $p : \mathbb{P}^{n+1} \setminus P \to \mathbb{P}^n$ be the projection map. Then, $p^{-1}(D_+(x_i)) \subset \mathbb{P}^{n+1}$ consists of points $[x_0 : \cdots : x_n : x_{n+1}]$ with $x_i \neq 0$, and so we have an iso

$$\begin{array}{ccc} D_+(x_i) \times \mathbb{A}^1 & \longrightarrow & p^{-1}(D_+(x_i)) \\ ([x_0 : \cdots : x_n], t) & \longmapsto & \left[\dfrac{x_0}{x_i} : \cdots : 1 : \cdots : \dfrac{x_n}{x_i} : t\right]. \end{array}$$

Since $\pi = p|_{\overline{X} \setminus P}$, and the above iso is compatible with projection, we conclude that $\pi^{-1}(U_i) \cong U_i \times \mathbb{A}^1$ where $U_i = D_+(x_i) \cap V$.

We now show π^* is an isom.[2] Recall the section $\sigma : V \hookrightarrow \overline{X} \setminus P$. $\pi \circ \sigma = \mathrm{Id}_V$ from which we conclude that $\pi^* : \mathrm{Cl}(V) \to \mathrm{Cl}(\overline{X} \setminus P)$ is injective. Furthermore, letting $\eta_V \in V$ be the generic point, we note that $\pi^{-1}(\eta_V) = \mathbb{A}^1_K$ has trivial class group (with $K = K(V)$ the function field of V). Let $D \in \mathrm{Div}(\overline{X} \setminus P)$ be any divisor. Then, there exists some $f \in K(t)^\times$ so that $D|_{\pi^{-1}(\eta_V)} = (f)$, so $D - (f) \in \mathrm{Div}(\overline{X} \setminus P)$ has no components meeting $\pi^{-1}(\eta_V)$, but this exactly says that D is linearly equivalent to a divisor (i.e. $D - (f)$) pulled back from V. ∎

(b) We have $V \subset \overline{X}$ as the "hyperplane section at infinity". The class $[V] \in \mathrm{Cl}(\overline{X})$ is equal to $\pi^*([V.H])$ where H is any hyperplane of $\mathbb{P}^n$ not containing V. Consequently, we have an exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{1 \mapsto [V.H]} \mathrm{Cl}\, V \to \mathrm{Cl}\, X \to 0.$$

[2]Following Eric's computation of class groups of vector bundles in 216B. I knew I'd understand it one day

Proof. It's clear that $\overline{X} \setminus V = X$, so we have an exact sequence

$$\mathbb{Z} \xrightarrow{1 \mapsto [V]} \mathrm{Cl}(\overline{X}) \to \mathrm{Cl}(X) \to 0.$$

Since $\pi^* : \mathrm{Cl}\, V \xrightarrow{\sim} \mathrm{Cl}\, \overline{X}$ is an iso, this means we have an exact sequence

$$\mathbb{Z} \xrightarrow{1 \mapsto (\pi^*)^{-1}([V])} \mathrm{Cl}\, V \to \mathrm{Cl}\, X \to 0.$$

To get the exact sequence in the problem statement, it suffices to show that $\pi^*([V.H]) = [V] \in \mathrm{Cl}\, \overline{X}$, and then observe that the map from $\mathbb{Z}$ is injective by **Problem 2.8(d)**.

By construction, there is a hyperplane H_1 (the hyperplane at infinity) s.t. $H_1.\overline{X} = V$. If there were a hyperplane H_2 s.t. $H_2.\overline{X} = \pi^*([V.H])$, then we'd win since $H_1 \sim H_2$. Let H_2 be the hyperplane defined by the same homogenous linear equation as H. ■

(c) Let $S(V)$ be the homogeneous coordinate ring of V (the affine coordinate ring of X). Then, $S(V)$ is a UFD iff **(1)** V is **projectively normal** (i.e. $S(V)$ is an integrally closed domain) and **(2)** $\mathrm{Cl}(V) \cong \mathbb{Z}$, generated by the class of $V.H$.

Proof. This is [Har77, Propostion II.6.2], a noetherian domain A is a UFD $\iff$ $\operatorname{spec} A$ is normal (i.e. A integrally closed) and $\mathrm{Cl}(A) = 0$. I guess also note that $\mathrm{Cl}\, S(V) = \mathrm{Cl}\, X$ and that we have the exact sequence of **(b)**. ■

(d) Let $\mathscr{O}_P$ be the local ring of P on X. The natural restriction $\mathrm{Cl}\, X \to \mathrm{Cl}(\operatorname{spec} \mathscr{O}_P)$ is an isomorphism.

Proof. ■

Problem 2.10 (Hartshore II.6.4). *Let k be a field with* $\operatorname{char} k \neq 2$, *and consider* $A = k[x_1, \dots, x_n, z]/(z^2 - f)$ *where* $f \in k[x_1, \dots, x_n]$ *is squarefree. This ring is integrally closed.*

Proof. The fraction field $K = \operatorname{Frac} A = k(x_1, \dots, x_n)[z]/(z^2 - f)$ is a degree two extension of $L = k(x_1, \dots, x_n)$ with Galois group generated by $z \mapsto -z$. For $\alpha = g + hz \in K$ with $g, h \in L$, its minimal polynomial is

$$(X - (g + hz))(X - (g - hz)) = X^2 - 2gX + (g^2 - h^2 f).$$

Now, α is integral over $B = k[x_1, \dots, x_n]$ iff its minimal polynomial has coefficients in B. This is clearly the case iff $g \in B$ and $h^2 f \in B$. Since $f \in B$ is squarefree, if $h^2 \in L$ had a nontrivial denominator, then $h^2 f$ could not be integral, so actually $h \in B$. In other words, α is integral over B iff $\alpha \in A$, so A is the integral closure of B in K. ■

Problem 2.11 (Hartshorne II.6.5). *Let* $\operatorname{char} k \neq 2$, *and let X be the affine quadric hypersurface*

$$X = \operatorname{spec} \frac{k[x_0, \dots, x_r]}{(x_0^2 + x_1^2 + \cdots + x_r^2)}.$$

(a) X is normal if $r \geq 2$.

Proof. Since $\operatorname{char} k \neq 2$, $f = x_0^2 + \cdots + x_r^2$ is squarefree for $r \geq 2$, so we win by Problem 2.10. ∎

(b) Setting $x = x_0 + ix_1$ and $y = x_0 - ix_1$ (and $z_i = ix_{i+1}$), we have

$$X \cong \operatorname{spec} \underbrace{\frac{k[x, y, z_1, \ldots, z_{r-1}]}{(xy = z_1^2 + \cdots + z_{r-1}^2)}}_{A}.$$

We compute $\operatorname{Cl} X$.

Proof. Let $Y' = (y)$, and let $\operatorname{Irr}(Y) = \{\text{irred. components of } Y\}$. Then, we have a right exact sequence

$$\mathbb{Z}^{\oplus \operatorname{Irr}(Y)} \to \operatorname{Cl}(X) \to \operatorname{Cl}(X \setminus Y) \to 0.$$

We note that $X \setminus Y \cong \operatorname{spec} A_y$ where

$$A_y \simeq \frac{k[x, y, y^{-1}, z_1, \ldots, z_{r-1}]}{(xy = z_1^2 + \cdots + z_{r-1}^2)} \simeq k[y, y^{-1}, z_1, \ldots, z_{r-1}]$$

(since x is determined from the rest of these) which is a UFD, so $\operatorname{Cl}(X \setminus Y) = \operatorname{Cl}(A_y) = 0$, and $\mathbb{Z}^{\oplus \operatorname{Irr}(Y)} \twoheadrightarrow \operatorname{Cl} X$ is a surjection. We next note that

$$Y \simeq \operatorname{spec} \frac{k[x, y, z_1, \ldots, z_{r-1}]}{(y, xy = z_1^2 + \cdots + z_{r-1}^2)} \simeq \operatorname{spec} \frac{k[x, y, z_1, \ldots, z_{r-1}]}{(y, z_1^2 + \cdots + z_{r-1}^2)} \left(\simeq \operatorname{spec} \frac{k[x, z_1, \ldots, z_{r-1}]}{(z_1^2 + \cdots + z_{r-1}^2)} \right).$$

We now split into cases

(1) First say $r = 2$. Then, $Y \simeq \operatorname{spec} k[x, y, z]/(y, z^2)$ is not reduced. We see that, as divisors $[Y] = (y) = 2[Y_{\text{red}}]$ where $Y_{\text{red}} = \operatorname{spec} k[x, y, z]/(y, z) = \operatorname{spec} k[x] \cong \mathbb{A}^1$ is integral (so a prime divisor). Since $[Y] = (y) = 0 \in \operatorname{Cl}(X)$, we conclude that we have a surjection $\mathbb{Z}/2\mathbb{Z} \twoheadrightarrow \operatorname{Cl}(X)$ sending $1 \mapsto [Y_{\text{red}}]$. The only quest that remains is, "is Y_{red} principal?" No, it's not.

Y_{red} is principal iff $I := (y, z)$ is a principal ideal in A. Let $0 \in \operatorname{spec} A$ be the origin (defined by the ideal (x, y, z)). If I were principal, then IA_0 would be as well. However, note that the maximal ideal $\mathfrak{m}_0 \subset A_0$ of the local ring at the origin is $\mathfrak{m}_0 = (x, y, z)$ so $\dim \mathfrak{m}_0/\mathfrak{m}_0^2 = 3$ with basis x, y, z (the origin is singular, so the tangent space there has dimension strictly greater than 2). We note that $IA_0/(\mathfrak{m}_0 IA_0) \to \mathfrak{m}_0/\mathfrak{m}_0^2$ surjects onto a 2-dimensional subspace (generated by x, y), so by Nakayama, IA_0 requires at least 2 generators, i.e. is not principle.

(2) Now say $r = 3$. Then, $Y \simeq \operatorname{spec} k[x, y, z, w]/(y, z^2 + w^2)$ is reducible. It's irreducible components are

$$Y_1 \simeq \operatorname{spec} k[x, y, z, w]/(y, z + iw) \text{ and } Y_2 \simeq \operatorname{spec} k[x, y, z, w]/(y, z - iw).$$

Since $[Y] = [Y_1] + [Y_2] = 0 \in \operatorname{Cl} X$, we have a surjection

$$\mathbb{Z} \simeq \frac{\mathbb{Z} \oplus \mathbb{Z}}{\mathbb{Z}(1, 1)} \twoheadrightarrow \operatorname{Cl}(X).$$

To show this is an isomorphism, we could do another Nakayama type argument (possibly appealing to Theorem 2.5) in order to show that $k[Y_1] \neq 0$ for all $k \neq 0$. Alternatively though, we can use Exercise 2.9(b) to see that we have an exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathrm{Cl}(\mathbb{P}^1 \times \mathbb{P}^1) \longrightarrow \mathrm{Cl}(X) \longrightarrow 0$$

so $\mathrm{rank}_{\mathbb{Z}} \mathrm{Cl}(X) = 1$. Since we have just shown it is cyclic, we conclude that $\mathrm{Cl}(X) \cong \mathbb{Z}$.

(3) Finally say $r \geq 4$. Then, $Y \simeq \operatorname{spec} k[x, y, z_1, \ldots, z_{r-1}]/(y, z_1^2 + \cdots + z_{r-1}^2)$ is integral. Hence, the surjection $\mathbb{Z} \twoheadrightarrow \mathrm{Cl}(X), 1 \mapsto [Y]$ is the zero map, so $\mathrm{Cl}(X) = 0$.

■

(c) Let Q be the quadratic hypersurface defined by the same equation. Then,

(1) If $r = 2$, $\mathrm{Cl}(Q) \cong \mathbb{Z}$, and the class of the hyperplane section $Q.H$ is twice the generator

(2) If $r = 3$, $\mathrm{Cl}\, Q \cong \mathbb{Z} \oplus \mathbb{Z}$

(3) If $r \geq 4$, $\mathrm{Cl}\, Q \cong \mathbb{Z}$, generated by $Q.H$

Proof. These all follow from Problem 2.9(b) + (b) of this problem (except **(c.2)** which was used in (b) of this problem. That follows from Hartshorne's computation[3] (II.6.6.1, maybe?)) ■

(d) (**Klein's Theorem**) If $r \geq 4$ and Y is an irreducible 1-dimensional subvariety of Q, then there is an irreducible hypersurface $V \subset \mathbb{P}^n$ such that $V \cap Q = Y$, with multiplicity one, i.e. Y is a complete intersection.

Proof. We know from **(c)** that $\mathrm{Cl}(Q) \cong \mathbb{Z}$, generated by $Q.H$. Thus, $[Y] = k[Q.H]$ for some $k \in \mathbb{Z}_{>0}$. ■

Problem 2.12 (Hartshorne II.6.7). *Let X be the nodal cubic*

$$X = \left\{y^2 z = x^3 + x^2 z\right\} \subset \mathbb{P}^2$$

The group of degree 0 Cartier divisor $\mathrm{CaCl}^0(X)$ is naturally isomorphic to the multiplicative group $\mathbb{G}_m$.

Proof. First note that the $[0:0:1] \in X$ is singular in codimension 1, so X does not satisfy $(*)$. This is why we're using Cartier divisors instead of Weil ones. We first need to define degree. ■

Problem 2.13 (Hartshorne II.6.9). *Let X be a projective curve over k with normalization $\pi : \widetilde{X} \to X$. For each $P \in X$, let $\mathscr{O}_P = \mathscr{O}_{X,P}$ be its local ring with integral closure $\widetilde{\mathscr{O}}_P$.*

Remember: For Hartshorne, **variety** means separated, integral, and finite type over $k = \overline{k}$

[3] Or from Problem 2.7 + verifying that $Q \cong \mathbb{P}^1 \times \mathbb{P}^1$ in this case

(a) There is an exact sequence

$$0 \longrightarrow \bigoplus_{P\in X} \frac{\widetilde{\mathscr{O}}_P^\times}{\mathscr{O}_P^\times} \longrightarrow \operatorname{Pic} X \xrightarrow{\pi^*} \operatorname{Pic} \widetilde{X} \longrightarrow 0.$$

Proof. On X, we have an exact sequence of sheaves[4]

$$0 \longrightarrow \frac{\pi_*\mathscr{O}_{\widetilde{X}}^\times}{\mathscr{O}_X^\times} \longrightarrow \frac{\mathscr{K}^\times}{\mathscr{O}_X^\times} \longrightarrow \frac{\mathscr{K}^\times}{\pi_*\mathscr{O}_{\widetilde{X}}^\times} \longrightarrow 0.$$

Recall that $\mathscr{K}^\times = \underline{K^\times}$, where $K = K(X)$ is its function field, and that $\operatorname{Pic} X$ is is group of Cartier divisors $\Gamma(X, \mathscr{K}^\times/\mathscr{O}_X^\times)$ modulo principal divisors $\Gamma(X, \mathscr{K}^\times)$. At this point, we cheat a little by using cohomology. In the above exact sequence, the kernel $\pi_*\mathscr{O}_{\widetilde{X}}^\times/\mathscr{O}_X^\times$ is supported on a finite scheme $Z \hookrightarrow X$, the singular points of X, so its H^1 vanishes. Hence, we get an exact sequence

We didn't actually have to say the word 'cohomology'. This sheaf is flasque as is clear e.g. from the description of its global sections (all X's singular points are closed since $k = \overline{k}$ and $\dim X = 1$, so the gluing axiom tells you it's a sum of skyscraper sheaves)

$$\begin{array}{ccccccc} 0 \longrightarrow \Gamma\left(X, \pi_*\mathscr{O}_{\widetilde{X}}^\times/\mathscr{O}_X^\times\right) & \longrightarrow & \Gamma(X, \mathscr{K}^\times/\mathscr{O}_X^\times) & \longrightarrow & \Gamma(X, \mathscr{K}^\times/\pi_*\mathscr{O}_{\widetilde{X}}^\times) \longrightarrow 0 \\ \| & & & & \| \\ \bigoplus_{P\in X_{\text{sing}}} \widetilde{\mathscr{O}}_P^\times/\mathscr{O}_P^\times & & & & \Gamma(\widetilde{X}, \mathscr{K}_{\widetilde{X}}^\times/\mathscr{O}_{\widetilde{X}}^\times) \end{array}$$

on global sections. Take the quotient by $\Gamma(X, \mathscr{K}^\times) = K^\times$, we see we have an exact sequence

$$0 \dashrightarrow \bigoplus_{P\in X} \frac{\widetilde{\mathscr{O}}_P^\times}{\mathscr{O}_P^\times} \to \operatorname{Pic} X \to \operatorname{Pic} \widetilde{X} \to 0,$$

and the only possibly unclear thing left is left exactness above. However, this follows from the fact that $K^\times \cap \left(\bigoplus \widetilde{\mathscr{O}}_P^\times/\mathscr{O}_P^\times\right) = 0$, i.e. the stalks of any rational function $f \in K^\times$... ∎

TODO: Finish this

(b) If X is a plane cuspidal cubic, there is an exact sequence

$$0 \longrightarrow \mathbb{G}_a \longrightarrow \operatorname{Pic} X \longrightarrow \mathbb{Z} \longrightarrow 0.$$

If it is plane nodal, then we instead have

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \operatorname{Pic} X \longrightarrow \mathbb{Z} \longrightarrow 0.$$

Proof. Say X is plane cuspidal, e.g. $X = \left\{y^2z = x^3 + z^3\right\} \subset \mathbb{P}^2_k$. This it's normalization is $\widetilde{X} \simeq \mathbb{P}^1$. Letting $P \in X$ be the cusp, we then get an exact sequence

$$0 \longrightarrow \widetilde{\mathscr{O}_P^\times}/\mathscr{O}_P^\times \longrightarrow \operatorname{Pic} X \longrightarrow \mathbb{Z} \longrightarrow 0.$$

So let's compute a stalk. We work in an affine chart, so consider the open $U = \operatorname{spec} k[x,y]/(y^2 - x^3) \subset X$ containing the cusp $P = (x,y) \in U$ at the origin. Then, $\widetilde{U} = k[t] \overset{\text{open}}{\subset} \widetilde{X}$ with normalization map

[4] Use that pushforwards are left-exact to get $\pi_*\mathscr{O}_{\widetilde{X}}^\times \hookrightarrow \mathscr{K}^\times$

$$\begin{array}{ccc} k[x,y]/(y^2-x^3) & \longrightarrow & k[t] \\ x,y & \longmapsto & t^2,t^3 \end{array}$$

(these have the same fraction field, $k[t]$ is integrally closed, and $k[t^2,t^3] \subset k[t]$ is integral). Integral closure commutes with localization, so we see that

$$\mathscr{O}_P = \frac{k[x,y]_{(x,y)}}{(y^2-x^3)} = k[t^2,t^3]_{(t^2,t^3)} \text{ and } \widetilde{\mathscr{O}}_P = k[t]_{(t)}.$$

Note that $\widetilde{\mathscr{O}}_P^\times = \{f(t)/g(t) : f(0) \neq 0 \neq g(0)\}$, so we get an isomorphism $\widetilde{\mathscr{O}}_P^\times/\mathscr{O}_P^\times \xrightarrow{\sim} k$ induced by the map (I never actually checked this was well-defined... or injective...)

$$\frac{f(t)}{g(t)} \mapsto \frac{f'(0)g(0)-f(0)g'(0)}{g(0)^2}$$

taking the "linear term".

I imagine the nodal case works out similarly. ■

Problem 2.14 (Hartshorne II.7.13)**.** *Let $k = \overline{k}$ with $\operatorname{char} k \neq 2$. Let $C \subset \mathbb{P}^2_k$ be the nodal cubic $y^2z = x^3 + x^2z$ with singular point $P_0 = (0,0,1)$. Hence, $C \setminus P_0$ is isomorphic to the multiplicative group $\mathbb{G}_m = \operatorname{spec} k[t,t^{-1}]$. Let $\varphi_a : C \to C$ be the automorphism restricted to $t \mapsto ta$ on $\mathbb{G}_m$ ($a \in k^\times$).*

Now, let $X_1 = C \times (\mathbb{P}^1 \setminus \{0\})$ and $X_2 = C \times (\mathbb{P}^1 \setminus \{\infty\})$. We glue their open subsets $C \times (\mathbb{P}^1 \setminus \{0,\infty\})$ together via

$$\varphi : \langle P, u\rangle \mapsto \langle \varphi_u(P), u\rangle$$

for $P \in C$ and $u \in \mathbb{G}_m = \mathbb{P}^1 \setminus \{0,\infty\}$. We call the resulting scheme X, and note it comes with a well-defined projection $\pi : X \to \mathbb{P}^1$.

(1) π is proper, so X is a proper variety over k.

Proof. Properness is local on the target, so can check it above the opens $\mathbb{P}^1 \setminus \{0\}$ and $\mathbb{P}^1 \setminus \{\infty\}$ where it's obvious (since C proper). ■

(2) $\operatorname{Pic}(C \times \mathbb{A}^1) \cong \mathbb{G}_m \times \mathbb{Z}$ and $\operatorname{Pic}(C \times \mathbb{G}_m) \cong \mathbb{G}_m \times \mathbb{Z} \times \mathbb{Z}$.

Proof. ■

Problem 2.15 (Hartshorne II.7.14)**.**

(a) There exists a noetherian scheme X with a locally free coherent sheaf $\mathscr{E}$, such that $\mathscr{O}(1)$ on $\mathbb{P}(\mathscr{E})$ is not very ample relative to X.

Proof. Let $X = C$ be a smooth genus 1 curve over $k = \overline{k}$, and fix a closed point $p \in C(k)$. Then, $\mathscr{E} := \mathscr{O}_C(p)$ is a locally free coherent sheaf. We first claim that $\mathscr{E}$ is not generated by global sections. Cheating by using cohomology, one easily check that the restriction map $\Gamma(C, \mathscr{E}) \to \Gamma(C, \mathscr{O}_p) = \kappa(p)$ is trivial, e.g. by Riemann-Roch + $0 \to \mathscr{O}_C \to \mathscr{O}_C(p) \to \mathscr{O}_p \to 0$.

Now, consider the scheme $\mathbb{P}(\mathscr{E})$, and suppose $\mathscr{O}(1)$ is very ample relative to X. Then, we have a closed embedding $\mathbb{P}(\mathscr{E}) \hookrightarrow \mathbb{P}^N_X$ for some $N > 0$, and so we must have a graded surjection $\varphi : \mathscr{O}_X[T_0, \ldots, T_N] \twoheadrightarrow \bigoplus_{d \geq 0} \mathscr{E}^{\otimes d}$. In particular, this would force $\mathscr{E}$ to be generated by the global sections $\varphi(T_0), \ldots, \varphi(T_n) \in \Gamma(C, \mathscr{E})$, a contradiction. Hence, $\mathscr{O}(1)$ on $\mathbb{P}(\mathscr{E})$ is not very ample. ■

(b) Let $f : X \to Y$ be a morphism of finite type, let $\mathscr{L}$ be an ample invertible sheaf on X, and let $\mathscr{S}$ be a sheaf of graded $\mathscr{O}_X$-algebras[5]. Let $P = \operatorname{Proj} \mathscr{S}$ with projection map $\pi : P \to X$, and associated invertible sheaf $\mathscr{O}_P(1)$. For all $n \gg 0$, the sheaf $\mathscr{O}_P(1) \otimes \pi^* \mathscr{L}^n$ is very ample on P relative to Y.

Proof. This is essentially [Har77, Proposition II.7.10], but we'll reproduce the argument anyways.

Since $\mathscr{L}$ is ample on X and $\mathscr{S}_1$ is a coherent $\mathscr{O}_X$-module, we see that $\mathscr{S}_1 \otimes \mathscr{L}^n$ is generated by global sections for $n \gg 0$. Hence, there is a graded surjection $\mathscr{O}_X[T_0, \ldots, T_N] \twoheadrightarrow \mathscr{S} * \mathscr{L}^n$ which gives rise to an embedding

$$P \simeq \operatorname{Proj}(\mathscr{S} * \mathscr{L}^n) \hookrightarrow \operatorname{Proj} \mathscr{O}_X[T_0, \ldots, T_N] = \mathbb{P}^N_X$$

with $\mathscr{O}_{\mathbb{P}^N_X}(1)$ pulling back to $\mathscr{O}_P(1) \otimes \pi^* \mathscr{L}^n$ on P. Thus, this sheaf is very ample on P relative to X. Now, $\mathscr{L}$ is ample on X, so $\mathscr{L}^m$ is very ample relative to Y for $m \gg 0$, i.e. there's an embedding $X \hookrightarrow \mathbb{P}^M_Y$ with $\mathscr{O}_{\mathbb{P}^M_Y}(1)$ restricting to $\mathscr{L}^m$ on X. Now we can stare at the diagram

$$\begin{tikzcd}
P \arrow[r, hook] \arrow[dr, "\pi"] & \mathbb{P}^N_X \arrow[r, hook] \arrow[d] & \mathbb{P}^N_Y \times_Y \mathbb{P}^M_Y \arrow[r, hook] \arrow[d] & \mathbb{P}^{NM+N+M}_Y \arrow[ddl] \\
& X \arrow[r, hook] \arrow[dr, "f"] & \mathbb{P}^M_Y \arrow[d] & \\
& & Y &
\end{tikzcd}$$

to see that $\mathscr{O}_P(1) \otimes \pi^* \mathscr{L}^n \otimes \pi^* \mathscr{L}^m$ is very ample relative to Y for $n, m \gg 0$.

Note above that $\mathbb{P}^N_Y \times_Y \mathbb{P}^M_Y = \mathbb{P}^N_{\mathbb{P}^M_Y}$ so the square is Cartesian (which is why the top map is a closed immersion). ■

Problem 2.16 (216B HW4 Exercise A)**.** *Fix an algebraically closed field k with $\operatorname{char} k \neq 2$.*

(i) Let $C = \{x^2 + y^2 = z^2\} \subset \mathbb{A}^3_k$ be the cone with singular point $P = (0, 0, 0)$. Then, the blowup $\mathrm{Bl}_P(C)$ is covered by $D_+(x)$ and $D_+(y)$ with exception divisor $\mathbb{P}^1_k$.

For a more detailed computation, scroll down a bit

[5] with $\mathscr{S}_0 = \mathscr{O}_X$, $\mathscr{S}_1$ coherent, and $\mathscr{S}$ generated by $\mathscr{S}_1$ as an $\mathscr{O}_X$-algebra

Proof. On $D_+(x)$, we have $y = ux$ and $z = vx$, so this part of the blowup is described by

$$x^2 + u^2x^2 = v^2z^2 \iff 1 + u^2 = v^2$$

Similarly, on $D_+(y)$, we have $x = wy$ and $z = vy$ giving $w^2 + 1 = v^2$, whereas on $D_+(z)$, we have $x = wz$ and $y = uz$ giving $w^2 + u^2 = 1$. Now, note that for any point in $D_+(z)$ we have $w \neq 0$ or $u \neq 0$, so one of these is a unit and hence the ideal $I = (x, y, z)$ at that point is generated by either x or y (i.e. $D_+(z) \subset D_+(x) \cup D_+(y)$). Hence, the $\mathrm{Bl}_P(C) = D_+(x) \cup D_+(y)$. For computing the exceptional divisor, consider the natural embedding $\mathrm{Bl}_P(C) \hookrightarrow \mathbb{P}^2$ constructed in class. Letting u, v, w be the homogeneous coordinates on $\mathbb{P}^2_k$, it is clear that, under this embedding, the exceptional divisor maps onto the projective cone $\{w^2 + u^2 = v^2\} \subset \mathbb{P}^2$ which is isomorphic to $\mathbb{P}^1_k$. This is because, dehomogenizations of this cone are $1 + u^2 = v^2, w^2 + 1 = v^2$, and $w^2 + u^2 = 1$ which are exactly the images of the exceptional divisor restricted to each of $D_+(x), D_+(y), D_+(z)$. ■

(ii) For the pinched surface $S = \left\{xy^2 = z^2\right\} \subset \mathbb{A}^3_k$, the singular locus is the x-axis L corresponding to the ideal (y, z), and the blowup along L is $\mathrm{Bl}_L(S) = D_+(y) = \mathbb{A}^2_k$.

Proof. The singular locus consists of where the partial derivatives vanish, i.e. where we have

$$y^2 = 0 \qquad\qquad 2xy = 0 \qquad\qquad 2z = 0$$

which is visibly exactly when $y = z = 0$, i.e. along the line L. Since the ideal corresponding to L is generated by y, z, we know that $\mathrm{Bl}_L(S)$ is covered by $D_+(y), D_+(z)$. On $D_+(z)$, we have $y = uz$, so the blowup is given by $uxz^2 = z^2$, ie. $ux = 1$ which tells us that $u \neq 0$, so $z = u^{-1}y$ and I is generated by y. In other words, $D_+(z) \subset D_+(y)$, so $\mathrm{Bl}_Z(S) = D_+(y)$. Finally, on $D_+(y)$, we has $z = uy$ and the blowup has equation $xy^2 = u^2y^2$, i.e. $x = u^2$. Since y is free, this tells us that

$$D_+(y) \simeq \operatorname{spec} k[y] \times_k \operatorname{spec} k[x, u]/(x - u^2) \simeq \mathbb{A}^2_k$$

using that $k[x, u]/(x - u^2) \simeq k[u]$ ■

(iii) Let $C = \left\{x^2y + xy^2 = x^4 + y^4\right\} \subset \mathbb{A}^2_k$ with "triple point" $P = (0, 0)$ (corresponding to the ideal $I = (x, y)$), the blowup $\mathrm{Bl}_P(C)$ has 3 points above P and is smooth at each of them.

Proof. This blow up is covered by $D_+(x)$ and $D_+(y)$, so we'll look at each of this sets. First, on $D_+(x)$, we have $y = ux$ and so the blowup is given by

$$ux^3 + u^2x^3 = x^4 + u^4x^4 \iff u + u^2 = x(1 + u^4).$$

The points above P are those with $x = 0$, i.e. those with $u + u^2 = 0 \iff u \in \{0, -1\}$ (note that the point with $u = -1$ lies in the intersection $D_+(x) \cap D_+(y)$). To check that $D_+(x) \subset \mathrm{Bl}_P(C)$ is smooth at these points, it suffices to check that the partials of this equation for $D_+(y)$ do not all vanish at them. These partials are

$$1 + 2u - 4xu^3 \qquad\qquad 1 + u^4$$

which indeed are nonzero when $u \in \{0, -1\}$ and $x = 0$. Now, on $D_+(y)$, we have $x = uy$ and so we get the equation

$$u^2y^3 + uy^3 = u^4y^4 + y^4 \iff u^2 + u = y(u^4 + 1).$$

Unsurprisingly, the analysis where is very similar to the case of $D_+(x)$. The only points above P are those with $y = 0$ and $u \in \{0, -1\}$ (the point with $u = -1$ is the same point we found before, while the one with $u = 0$ is a third and final point above P), and the same calculations show that the blowup is smooth at these points. ■

Problem 2.17 (Ravi 22.4.E)**.** *Let $C : x^2 + y^2 = z^2$ be an affine cone in $\mathbb{A}^3$. Let $S = \mathrm{Bl}_0 C$ be the blow-up of C at the origin. Then, S is regular and the exceptional divisor of $\pi : S \to C$ to $E := \pi^{-1}(0) \simeq \mathbb{P}^1$. Furthermore, the normal bundle to this $\mathbb{P}^1$ is $\mathscr{O}(-2)$.*

Proof. We use the 'blow-up closure lemma,' the blowup of C is the strict transform of C in the blowup of $\mathbb{A}^3$. Recall that we have $\mathrm{Bl}_0 \mathbb{A}^3 \hookrightarrow \mathbb{A}^3 \times \mathbb{P}^2$ cut out by the condition

$$\operatorname{rank} \begin{pmatrix} x & y & z \\ s_0 & s_1 & s_2 \end{pmatrix} \leq 1$$

In particular, we have relations like $xs_1 - ys_0 = 0$, $xs_2 - zs_0 = 0$, and $ys_s - zs_1 = 0$. Using the three usual charts on $\mathbb{P}^2$ – i.e. $D_+(s_0), D_+(s_1), D_+(s_2)$ – we see that the *total transform* $\pi^{-1}(C) \subset \mathrm{Bl}_0 \mathbb{A}^3$ is locally cut out by the equations (We say $\mathbb{A}^1$ instead of $\mathbb{A}^3$ below because there are implicitly also equations of the form $y = xs_{1/0}$, $z = xs_{2/0}$, etc.)

Think of $D_+(s_0)$ as the locus where x generates the ideal

$$\begin{aligned}
\mathbb{A}^1 \times D_+(s_0) : \quad & x^2 + (xs_{1/0})^2 = (xs_{2/0})^2 \iff 0 = x^2\left(1 + s_{1/0}^2 - s_{2/0}^2\right) \\
\mathbb{A}^1 \times D_+(s_1) : \quad & (ys_{0/1})^2 + y^2 = (ys_{2/1})^2 \iff 0 = y^2\left(1 + s_{0/1}^2 - s_{2/1}^2\right) \\
\mathbb{A}^1 \times D_+(s_2) : \quad & (zs_{0/2})^2 + (zs_{1/2})^2 = z^2 \iff 0 = z^2\left(1 - s_{0/2}^2 - s_{1/2}^2\right).
\end{aligned}$$

Now, the *strict transform* $\overline{\pi^{-1}(C \setminus 0)} \simeq \mathrm{Bl}_0 C$ is obtained by taking the closure of the locus away from the origin, i.e. where x, y, or z is nonzero. Hence, $S = \mathrm{Bl}_0 C$ is covered by the charts

$$\begin{aligned}
\mathbb{A}^1 \times D_+(s_0) : \quad & 0 = 1 + s_{1/0}^2 - s_{2/0}^2 \\
\mathbb{A}^1 \times D_+(s_1) : \quad & 0 = 1 + s_{0/1}^2 - s_{2/1}^2 \\
\mathbb{A}^1 \times D_+(s_2) : \quad & 0 = 1 - s_{0/2}^2 - s_{1/2}^2.
\end{aligned}$$

(in particular, each chart has one 'free variable'). From this, we see that the exceptional divisor (the part above $x = y = z = 0$) is

$$E = \mathrm{Proj}_k \left(\frac{k[s_0, s_1, s_2]}{(s_0^2 + s_1^2 - s_2^2)} \right) \simeq \mathbb{P}^1_k,$$

a quadric cone in $\mathbb{P}^2$. In particular, this shows that S is regular this $S \setminus E \cong C \setminus 0$ is clearly regular. To compute the normal bundle, first note we have a Cartesian square

$$\begin{tikzcd} \mathbb{P}^1 \arrow[r] \arrow[d] \arrow[dr, phantom, "\ulcorner", very near start] & \mathbb{P}^2 \arrow[d] \\ \mathrm{Bl}_0 C \arrow[r] & \mathrm{Bl}_0 \mathbb{A}^3. \end{tikzcd}$$

We claim that $N_{\mathbb{P}^1/S} = N_{\mathbb{P}^2/\mathrm{Bl}_0 \mathbb{A}^3}|_{\mathbb{P}^1}$, i.e. that

$$N_{\mathbb{P}^1/S} = \mathscr{O}_{\mathbb{P}^2}(-1)|_E = \mathscr{O}_{\mathbb{P}^1}(-2)$$

since $E \hookrightarrow \mathbb{P}^2$ is degree 2. This follows immediately from the fact that (e.g. by staring at the pullback diagram) we have $\mathscr{I}_{\mathbb{P}^2}|_{\mathrm{Bl}_0 C} = \mathscr{I}_{\mathbb{P}^1}$. ■

Problem 2.18 (Hartshorne II.8.4)**.** *A closed subscheme $Y \hookrightarrow \mathbb{P}^n_k$ is called a **(strict, global) complete intersection** if the homogeneous ideal I of Y in $S = k[x_0, \dots, x_n]$ is generated by $r := \operatorname{codim}(Y, \mathbb{P}^n)$ elements.*

(a) Let Y be an r-codimensional subscheme of $\mathbb{P}^n_k$. Then, Y is a complete intersection iff there are r **hypersurfaces** (i.e. locally principal subschemes of codimension 1) $H_1, \dots, H_r$ such that $Y = H_1 \cap \dots \cap H_r$ as schemes, i.e.

$$\mathscr{I}_Y = \mathscr{I}_{H_1} + \dots + \mathscr{I}_{H_r}.$$

Proof. This clearly holds if we show that hypersurfaces are themselves complete intersections, so we may assume $r = 1$. Say $Y = H_1$ is a hypersurface. We may suppose WLOG that Y is irreducible (since $V(I_1) \cup V(I_2) = V(I_1 I_2)$), so $Y = \operatorname{Proj} k[x_0, \dots, x_n]/\mathfrak{p}$ for some height 1 homogeneous prime ideal $\mathfrak{p}$. Since $k[x_0, \dots, x_n]$ is a UFD, every prime ideal contains a prime element, so, since $\operatorname{ht} \mathfrak{p} = 1$, we see that $\mathfrak{p} = (g)$ must be principal. Thus, we win. ■

(b) Let Y be a complete intersection of dimension ≥ 1 in $\mathbb{P}^n_k$. Then, Y is normal iff it is projectively normal.

Proof. Note that Y is projectively normal iff its affine cone $X = \operatorname{spec} S(Y) = \operatorname{spec} k[x_0, \dots, x_n]/I$ is normal. Since Y is a complete intersection, I is generated by $r := \operatorname{codim}(Y, \mathbb{P}^n_k) = \operatorname{codim}(X, \mathbb{A}^{n+1}_k)$ many elements, so X is a (local) complete intersection in $\mathbb{A}^{n+1}_k$. Now, [Har77, Prop. II.8.23] says that in this case (local complete intersection in a nonsingular k-variety), X is normal iff it is regular in codimension 1. ■

(c) With Y normal, the natural map $\Gamma(\mathbb{P}^n, \mathscr{O}(\ell)) \to \Gamma(Y, \mathscr{O}_Y(\ell))$ is surjective for all $\ell \geq 0$. In particular, taking $\ell = 0$ shows that Y is connected.

Proof. This is Hartshorne Exercise II.5.14.

We know Y is projectively normal. We claim that $S(Y) = S' := \bigoplus_{\ell \geq 0} \Gamma(Y, \mathscr{O}_Y(\ell))$. We have a natural inclusion $S(Y) \hookrightarrow S'$. Note that $S' = \Gamma\left(Y, \mathscr{S}' := \bigoplus_{\ell \geq 0} \mathscr{O}_Y(\ell)\right)$, and that Lemma 2.12

Question: Is this as obvious as I think it should be?

tells us that $\mathscr{S}'_{\mathfrak{p}} = \mathscr{O}_{Y,\mathfrak{p}}[x]$. Since Y is normal, $\mathscr{O}_{Y,\mathfrak{p}}$ is integrally closed, so $\mathscr{S}'_{\mathfrak{p}}$ is as well (for any $\mathfrak{p} \in Y \subset \mathbb{P}^n$). Thus, $\mathscr{S}'$ is a sheaf of integrally closed domains, so S' is integrally closed. $S(Y)$ is also integrally closed (Y projectively normal), so the inclusion $S(Y) \hookrightarrow S'$ must be an equality (really, there's more work to do. Need to show S' is the integral closure of Y, but meh).

Now $\Gamma(\mathbb{P}^n, \mathscr{O}(\ell)) \to \Gamma(Y, \mathscr{O}_Y(\ell)) = S(Y)_\ell$ is just the natural quotient map. ■

(d) Fix integers $d_1, \ldots, d_r \geq 1$ with $r < n$. Then there exists nonsingular hypersurfaces $H_1, \ldots, H_r$ in $\mathbb{P}^n$ with $\deg H_i = d_i$ s.t. $Y := H_1 \cap \cdots \cap H_r$ is irreducible and nonsingular of codimension r in $\mathbb{P}^n$.

Proof. Induct in r with base case $r = 1$ trivial. Let $X = H_1 \cap \cdots \cap H_{r-1}$ (exists by induction) and note that $\dim X = n - (r - 1) = (n - r) + 1 \geq 2$. Now apply Bertini, which holds not just for hyperplane sections, but for hypersurface sections of a given degree. ■

TODO: Prove this

(e) If Y is a nonsingular complete intersection as in **(d)**, then $\omega_Y \cong \mathscr{O}_Y\left(\sum d_i - n - 1\right)$.

Proof. We use adjunction. We start with the conormal sequence

$$0 \longrightarrow \bigoplus \mathscr{O}_Y(-d_i) \longrightarrow \Omega_{X/k}|_Y \longrightarrow \Omega_{Y/k} \longrightarrow 0,$$

and then take determinants to see that

$$\mathscr{O}_Y(-n-1) = \omega_X|_Y \cong \omega_Y \otimes \mathscr{O}_Y\left(\sum -d_i\right).$$

Rearrange gives what we want. ■

(f) Let Y be a nonsingular hypersurface of degree d in $\mathbb{P}^n$. Then,

$$p_g(Y) := h^0(\omega_Y) = \binom{d-1}{n}.$$

In particular, if $Y \hookrightarrow \mathbb{P}^2$ is a nonsingular plane curve of degree d, then $p_g(Y) = \frac{1}{2}(d-1)(d-2)$.

Proof. By **(e)**, we have an exact sequence of sheaves

$$\begin{tikzcd}
0 \arrow[r] & \mathscr{O}_{\mathbb{P}^n}(-n-1) \arrow[r] \arrow[d, equal] & \mathscr{O}_{\mathbb{P}^n}(d-n-1) \arrow[r] & \mathscr{O}_Y(d-n-1) \arrow[r] \arrow[d, equal] & 0 \\
& \mathscr{O}_{\mathbb{P}^n}(-Y) \otimes \mathscr{O}_{\mathbb{P}^n}(d-n-1) & & \omega_Y &
\end{tikzcd}$$

By **(b)**, this induces an exact sequence on global sections

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Gamma(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(-n-1)) & \longrightarrow & \Gamma(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(d-n-1)) & \longrightarrow & \Gamma(Y, \mathscr{O}_Y(d-n-1)) & \longrightarrow & 0 \\
 & & 0 & & \binom{(d-n-1)+n}{n} & & \binom{d-1}{n} & &
\end{array}$$

with the dimensions of the spaces written below them. ■

This only works for $d \geq n+1$, so what you actually do is twist by some $k \gg 0$ everywhere, compute $\dim \Gamma(Y, \omega_Y(k))$ and then say the phrase

(g) Let Y be a nonsingular curve in $\mathbb{P}^3$ which is the complete intersection of surfaces S, T of degrees d, e. Then,

$$p_g(Y) = \frac{1}{2}de(d+e-4)+1.$$

Proof. From **(e)**, we know that $\omega_Y = \mathscr{O}_Y(d+e-4)$ and $\omega_S = \mathscr{O}_S(d-4)$. We also know that $\mathscr{O}_S(-Y) = \mathscr{O}_{\mathbb{P}^n}(-T)|_S = \mathscr{O}_S(-e)$. We have exact sequences

Why didn't I just take the degree of this line bundle?

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Gamma(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(-4)) & \longrightarrow & \Gamma(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(d-4)) & \longrightarrow & \Gamma(S, \mathscr{O}_S(d-4)) & \longrightarrow & 0 \\ & & 0 & & \binom{d-1}{3} & & \binom{d-1}{3} & & \end{array}$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Gamma(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(e-4)) & \longrightarrow & \Gamma(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(d+e-4)) & \longrightarrow & \Gamma(S, \mathscr{O}_S(d+e-4)) & \longrightarrow & 0 \\ & & \binom{e-1}{3} & & \binom{d+e-1}{3} & & \binom{d+e-1}{3} - \binom{e-1}{3} & & \end{array}$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Gamma(S, \mathscr{O}_S(d-4)) & \longrightarrow & \Gamma(S, \mathscr{O}_S(d+e-4)) & \longrightarrow & \Gamma(Y, \mathscr{O}_Y(d+e-4)) & \longrightarrow & 0 \\ & & \binom{d-1}{3} & & \binom{d+e-1}{3} - \binom{e-1}{3} & & \binom{d+e-1}{3} - \binom{e-1}{3} - \binom{d-1}{3} & & \end{array}$$

Thus, we see that

$$p_a(Y) = \dim \Gamma(Y, \omega_Y) = \binom{d+e-1}{3} - \binom{e-1}{3} - \binom{d-1}{3} = \frac{1}{2}de(d+e-4)+1$$

as desired. ∎

Problem 2.19 (Hartshorne II.8.5)**.** *Let X be a nonsingular variety, and let Y be a nonsingular subvariety of codimension $r \geq 2$. Let $\pi : \widetilde{X} \to X$ be the blowup of X along Y, and let $Y' = \pi^{-1}(Y)$ be the exceptional divisor.*

(a) There is a natural isomorphism

$$\begin{array}{rccc} f: & \operatorname{Pic} X \oplus \mathbb{Z} & \longrightarrow & \operatorname{Pic} \widetilde{X} \\ & (\mathscr{L}, n) & \longmapsto & \pi^*\mathscr{L} \otimes \mathscr{O}_{\widetilde{X}}(nY'). \end{array}$$

Proof. We first show this map is surjective. Consider some prime divisor $Z \subset \widetilde{X}$. There are a few cases

($Z \cap Y' = \emptyset$) In this case, $\mathscr{O}_{\widetilde{X}}(Z) \cong \pi^*\mathscr{O}_X(\pi(Z)) = f(\mathscr{O}_X(\pi(Z)), 0)$ so we're good.

($Z = Y'$) In this case $\mathscr{O}_{\widetilde{X}}(Z) = f(0, 1)$ so we're good.

($\emptyset \subsetneq Z \cap Y' \subsetneq Y'$) In this case, Z must be the strict transform of $\pi(Z)$ (Z and the strict transform are both integral of the same dimension and Z is contained in the latter). Thus, $\pi^*\pi(Z) = Z + mY'$ for some $m \geq 0$, so $\mathscr{O}_{\widetilde{X}}(Z) = f(\mathscr{O}_X(\pi(Z)), -m)$.

The finishes surjectivity, so now injectivity. Say that $\mathscr{E} := \pi^*\mathscr{L} \otimes \mathscr{O}_{\widetilde{X}}(nY')$ is trivial. First restrict to Y' to see that

$$\mathscr{O}_{Y'}(nY') \simeq \mathscr{E}|_{Y'} \simeq \mathscr{O}_{Y'}.$$

Since (e.g. by [Har77, Theorem 8.24]) $Y' \simeq \mathbb{P}(\mathscr{I}/\mathscr{I}^2)$ with normal bundle $N_{Y'/\widetilde{X}} = \mathscr{O}_{Y'}(Y') \simeq \mathscr{O}_{\mathbb{P}(\mathscr{I}/\mathscr{I}^2)}(-1)$, the above says $\mathscr{O}_{\mathbb{P}(\mathscr{I}/\mathscr{I}^2)}(-n) \simeq \mathscr{O}_{\mathbb{P}(\mathscr{I}/\mathscr{I}^2)}$, so $n = 0$. Hence, $\mathscr{E} \simeq \pi^*\mathscr{L}$ is trivial. Now, since Y is in codimension ≥ 2, we have

$$\operatorname{Pic}(\widetilde{X} \setminus Y') \simeq \operatorname{Pic}(X \setminus Y) \simeq \operatorname{Pic}(X).$$

so we can restrict $\mathscr{E}$ to $\widetilde{X} \setminus Y'$ (recovering $\mathscr{L}$) in order to see that $\mathscr{L}$ is trivial. ■

Remark 2.28. A better approach is to just make use of the exact sequence

$$\mathbb{Z} \longrightarrow \operatorname{Pic}\widetilde{X} \longrightarrow \operatorname{Pic}(\widetilde{X} \setminus E) \longrightarrow 0$$

where $E = Y'$ is the exceptional divisor.

(b) $\omega_{\widetilde{X}} \simeq f^*\omega_X \otimes \mathscr{O}_{\widetilde{X}}((r-1)Y')$.

Proof. Write $\omega_{\widetilde{X}} = f^*\mathscr{L} \otimes \mathscr{O}_{\widetilde{X}}(nY')$. Restricting to $\widetilde{X} \setminus Y' \cong X \setminus Y$ shows that $\mathscr{L} = \omega_X$ To determine n, we use adjunction:

$$\mathscr{O}_{Y'}(nY') \simeq \omega_{\widetilde{X}}|_{Y'} \simeq \mathscr{O}_{Y'}(-Y') \otimes \omega_{Y'} \implies \mathscr{O}_{Y'}((n+1)Y') \simeq \omega_{Y'}.$$

Now, fix some closed point $y \in Y$ with fiber $Z = Y'_y$. Then, $Z \simeq \mathbb{P}^{r-1}$ so $\omega_{Y'}|_Z \simeq \mathscr{O}_{\mathbb{P}^{r-1}}(-r)$ and $\mathscr{O}_{Y'}(Y')|_Z \simeq \mathscr{O}_{\mathbb{P}^{r-1}}(-1)$. Restrcting the above to Z, we see that $-(n+1) = -r$, so $n = r-1$ as we win. ■

Problem 2.20 (Hartshorne II.8.8).

Problem 2.21 (Hartshorne III.2.2).

Problem 2.22 (Hartshorne III.2.3).

Problem 2.23 (Hartshorne III.2.4).

Problem 2.24 (Hartshorne III.3.7).

Problem 2.25 (Hartshorne III.4.1). *Let $f : X \to Y$ be an affine morphism of noetherian separated schemes, and let $\mathscr{F}$ be a quasi-coherent sheaf on X. Then, there are natural isomorphisms*

$$\mathrm{H}^i(X, \mathscr{F}) \cong \mathrm{H}^i(Y, f_*\mathscr{F})$$

for all $i \geq 0$.

Proof. Let $\mathfrak{U}$ be an affine open cover of Y, so $f^{-1}\mathfrak{U} = \left\{f^{-1}(U) : U \in \mathfrak{U}\right\}$ is an affine cover of X. Furthermore, $f_*\mathscr{F}$ is a quasi-coherent sheaf on Y since X is noetherian[6]. This means we are in luck. For noetherian, separated schemes[7], sheaf cohomology can be computed as Čech cohomology of any affine covering. Since $\mathfrak{U}$ and $f^{-1}\mathfrak{U}$ have the same global sections by definition (and preimage commutes with intersections), we naturally have $\check{\mathrm{H}}^i(f^{-1}\mathfrak{U}, \mathscr{F}) \simeq \check{\mathrm{H}}^i(\mathfrak{U}, f_*\mathscr{F})$, and so we get isomorphisms

$$\mathrm{H}^i(X, \mathscr{F}) \simeq \check{\mathrm{H}}^i(f^{-1}\mathfrak{U}, \mathscr{F}) \simeq \check{\mathrm{H}}^i(\mathfrak{U}, f_*\mathscr{F}) \simeq \mathrm{H}^i(Y, f_*\mathscr{F}).$$

∎

Problem 2.26 (Hartshorne III.4.7). *Let X be a subscheme of $\mathbb{P}^2_k$ defined by a single homogeneous equation $f(x_0, x_1, x_2) = 0$ of degree d. Assume that $[1 : 0 : 0] \notin X$. Then, X can be covered by two open affines $U = X \cap \{x_1 \neq 0\}$ and $V = X \cap \{x_2 \neq 0\}$. We will compute the Čech complex*

$$\Gamma(U, \mathscr{O}_X) \oplus \Gamma(V, \mathscr{O}_X) \xrightarrow{\mathrm{d}} \Gamma(U \cap V, \mathscr{O}_X)$$

and see that

$$\dim \mathrm{H}^0(X, \mathscr{O}_X) = 1 \;\; \textit{while} \;\; \dim \mathrm{H}^1(X, \mathscr{O}_X) = \frac{1}{2}(d-1)(d-2).$$

Proof. U, V are affine since their closed subsets of $D_+(x_1) = \operatorname{spec} k[u, v]$ and $D_+(x_2) = \operatorname{spec} k[s, t]$.[8] In particular, we see that

$$U \simeq \operatorname{spec} \frac{k[u, v]}{(f(u, 1, v))} \;\; \text{and} \;\; V \simeq \operatorname{spec} \frac{k[s, t]}{(f(s, t, 1))}.$$

Similarly,

$$U \cap V \simeq \operatorname{spec} \frac{k[u, v][1/v]}{(f(u, 1, v))} \simeq \operatorname{spec} \frac{k[s, t][1/t]}{(f(s, t, 1))}$$

The differential in the Čech complex is

$$\mathrm{d}\left(g(u, v), h(s, t)\right) = g(u, v) - h(u/v, 1/v) \in \frac{k[u, v][1/v]}{(f(u, 1, v))}.$$

[6] We'd also be in good shape if f were separated and quasi-compact. Basically, intersections of affine opens need to be quasi-compact

[7] Need intersections of affines to be affine

[8] $u = x_0/x_1, v = x_2/x_1, s = x_0/x_2, t = x_1/x_2$

By considering v-degrees, we see that

$$\mathrm{H}^0(X, \mathscr{O}_X) \simeq \ker \mathrm{d} \simeq k$$

consists of constant polynomials (diagonally embedded). The cokernel seems trickier to determine... ■

Problem 2.27 (Hartshorne III.4.10)**.**

Problem 2.28 (Hartshorne III.5.3)**.** *Let X be a projective scheme of dimension r over a field k. We define the* ***arithmetic genus*** *p_a of X by*

$$p_a(X) = (-1)^r(\chi(\mathscr{O}_X) - 1).$$

(a) If X is integral, and $k = \overline{k}$, then $\mathrm{H}^0(X, \mathscr{O}_K) \cong k$, so

$$p_a(X) = \sum_{i=0}^{r-1} (-1)^i \dim_k \mathrm{H}^{r-i}(X, \mathscr{O}_X).$$

In particular, if X is a curve, we have $p_a(X) = \dim_k \mathrm{H}^1(X, \mathscr{O}_X)$.

Proof. This follows e.g. from Problem 2.5**(d)** since X is integral + proper ($\Longleftarrow$ projective). ■

(b) If X is a closed subvariety of $\mathbb{P}^r_k$, then $p_a(X)$ defined above agrees with its classical definition: $p_a(X) = (-1)^r(P_X(0) - 1)$.

Proof. The Hilbert polynomial literally is $P_X(n) = \chi(\mathscr{O}_X(n))$, so this follows from **(a)**. ■

(c) If X is a nonsingular plane curve over $k = \overline{k}$, then $p_a(X)$ is a birational invariant. In particular, a nonsingular plane curve of degree $d \geq 3$ is not rational.

Problem 2.29 (Hartshorne III.5.5)**.** *Let k be a field, let $X = \mathbb{P}^r_k$, and let Y be a closed subscheme of dimension $q \geq 1$ which is a complete intersection. Then,*

(a) *for all $n \in \mathbb{Z}$, the natural map*

$$\mathrm{H}^0(X, \mathscr{O}_X(n)) \to \mathrm{H}^0(Y, \mathscr{O}_Y(n))$$

is surjective (even if Y not normal).

(b) *Y is connected.*

(c) $\mathrm{H}^i(Y, \mathscr{O}_Y(n)) = 0$ *for $0 < i < q$ and all $n \in \mathbb{Z}$*

(d) $p_a(Y) = \dim_k \mathrm{H}^q(Y, \mathscr{O}_Y)$

Proof. It's clear that **(b)** follows from **(a)** since it implies $\mathrm{H}^0(Y, \mathscr{O}_Y(n)) = k$. Similarly, **(d)** follows from **(c)** + **(a)**. Thus, it suffices to prove **(a)**, **(c)**. We do these by induction on $c := \operatorname{codim}(\mathbb{P}^r_k, Y) = r - q$. When $c = 0$, both statements are known, so we only need to do the induction step.

Suppose **(a)**,**(c)** are known for complete intersections of codimension $c-1$. Write $Y = V \cap Z$ with V a degree d hypersurface and Z a complete intersection of codimension $c-1$. Then, we have exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathscr{O}_Z(n) \otimes \mathscr{O}_Z(-Y) & \longrightarrow & \mathscr{O}_Z(n) & \longrightarrow & \mathscr{O}_Y(n) & \longrightarrow & 0 \\ & & \| & & & & & & \\ & & \mathscr{O}_Z(n) \otimes \mathscr{O}_{\mathbb{P}^r}(-V)|_Z & & & & & & \\ & & \| & & & & & & \\ & & \mathscr{O}_Z(n-d) & & & & & & \end{array}$$

for all $n \in \mathbb{Z}$. This induces

$$0 \longrightarrow \mathrm{H}^0(Z, \mathscr{O}_Z(n-d)) \longrightarrow \mathrm{H}^0(Z, \mathscr{O}_Z(n)) \longrightarrow \mathrm{H}^0(Y, \mathscr{O}_Y(n)) \longrightarrow \mathrm{H}^1(Z, \mathscr{O}_Z(n-d)) = 0,$$

with the last equality holding by induction. In particular, we see that the natural map $\mathrm{H}^0(Z, \mathscr{O}_Z(n)) \to \mathrm{H}^0(Y, \mathscr{O}_Y(n))$ is surjective, so $\mathrm{H}^0(X, \mathscr{O}_X(n)) \to \mathrm{H}^0(Y, \mathscr{O}_Y(n))$ is as well. This proves **(a)** (and so **(b)**). For **(c)**, our earlier short exact sequence all induces

$$0 = \mathrm{H}^i(Z, \mathscr{O}_Z(n)) \longrightarrow \mathrm{H}^i(Y, \mathscr{O}_Y(n)) \to \mathrm{H}^{i+1}(Z, \mathscr{O}_Z(n-d)) = 0$$

for all $0 < i < q = \dim Y = \dim Z - 1$ (so $0 < i, i+1 < \dim Z$), from which we see that $\mathrm{H}^i(Y, \mathscr{O}_Y(n)) = 0$ in this range. ■

Remark 2.29. Taking $i = q$ at the end of the above proof, we see that $\mathrm{H}^q(Y, \mathscr{O}_Y(n)) \hookrightarrow \mathrm{H}^{q+1}(Z, \mathscr{O}_Z(n-d))$ and so we get as a bonus that

(e) $\mathrm{H}^q(Y, \mathscr{O}_Y(n)) \hookrightarrow \mathrm{H}^r\left(X, \mathscr{O}_X\left(n - \sum d_i\right)\right)$ when Y is a compete intersection of type $(d_1, d_2, \dots, d_{r-q})$.

Problem 2.30 (Hartshorne III.5.6)**.** *Let Q be the nonsingular quadric surface $xy = zw$ in $X = \mathbb{P}^3_k$ over a field k. We will consider locally principal closed subschemes of Q. These correspond to Cartier divisors on Q. Recall that $\operatorname{Pic} Q \simeq \mathbb{Z} \oplus \mathbb{Z}$, so we can talk about the type (a, b) of Y. The invertible sheaf $\mathscr{O}(Y)$ will be denoted $\mathscr{O}(a, b)$. In particular, for any $n \in \mathbb{Z}$, we have $\mathscr{O}_Q(n) = \mathscr{O}_Q(n, n)$.*

(a) We have

(1) If $|a - b| \le 1$, then $\mathrm{H}^1(Q, \mathscr{O}_Q(a, b)) = 0$

(2) if $a, b < 0$, then $\mathrm{H}^1(Q, \mathscr{O}_Q(a, b)) = 0$,

(3) if $a \le -2$, then $\mathrm{H}^1(Q, \mathscr{O}_Q(a, 0)) \ne 0$.

Proof. ■

(b)

(c) Say Y is a locally principal subscheme of type (a,b) in Q. Then, $p_a(Y) = ab - a - b + 1$.

Proof. We have the conormal sequence

$$0 \longrightarrow \mathscr{O}_Y(-Y) \longrightarrow \Omega_Q|_Y \longrightarrow \Omega_Y \longrightarrow 0.$$

Adjunction gives

$$\omega_Y \cong \omega_Q|_Y \otimes \mathscr{O}_Y(-a,-b)^\vee \cong \mathscr{O}_Y(a-2,b-2).$$

We can compute the degree of this as an intersection[9]

$$\deg \omega_Y = (a-2,b-2)\cdot(a,b) = a(b-2)+b(a-2) = 2ab-2a-2b = 2g(Y)-2 \implies g(Y) = ab-a-b+1.$$

Alternatively, we adjunct a second time since $Q \hookrightarrow \mathbb{P}^3$ is a quadric surface. We know that

$$\omega_Q \cong \omega_{\mathbb{P}^3}|_Q \otimes \mathscr{O}_Q(Q) \cong \mathscr{O}_Q(2-4) = \mathscr{O}_Q(-2).$$

This is actually not all that useful because we don't know the degree of Y in the ambient $\mathbb{P}^3$. ■

Actually, we do. $Q = \mathbb{P}^1 \times \mathbb{P}^1 \hookrightarrow \mathbb{P}^3$ via $\mathscr{O}_Q(1,1)$, so $Y \hookrightarrow Q \hookrightarrow \mathbb{P}^3$ has degree $(1,1)\cdot(a,b) = b+a$. Thus, $\omega_Y \cong \mathscr{O}_Y(-2) \otimes \mathscr{O}_Y(a,b)$, but then you still need to compute intersections to determine $\deg \omega_Y$, so this is no better than the first approach

---

Problem 2.31 (Hartshorne III.5.8)**.**

Problem 2.32 (Hartshorne III.7.4)**.**

Problem 2.33 (Hartshorne IV.1.3)**.**

Problem 2.34 (Hartshorne IV.1.8(a,b))**.** *Let X be an integral projective scheme of dimension 1 over $k = \overline{k}$, and let $\widetilde{X}$ be its normalization. Then, there is an exact sequence*

$$0 \longrightarrow \mathscr{O}_X \longrightarrow f_*\mathscr{O}_{\widetilde{X}} \longrightarrow \mathscr{C} \longrightarrow 0$$

where $\mathscr{C}$ is a sum of skyscraper sheaves concentrated at the singular points of X, and $\mathscr{C}_p = \widetilde{\mathscr{O}_{X,p}}/\mathscr{O}_{X,p}$ for $\widetilde{\mathscr{O}_{X,p}}$ the integral closure of $\mathscr{O}_{X,p}$. For each $p \in X$, let $\delta_p = \dim_k \mathscr{C}_p$. Then,

$$p_a(X) = p_a(\widetilde{X}) + \sum_{p\in X} \delta_p.$$

Furthermore, if $p_a(X) = 0$, then X is nonsingular and isomorphic to $\mathbb{P}^1$.

Hartshorne uses length for some reason. I'm not sure why...

[9] $(1,0)\cdot(1,0) = 0 = (0,1)\cdot(0,1)$ by moving fibers, while $(1,0)\cdot(0,1) = 1$

Proof. The given exact sequence shows that

$$\chi(f_*\mathscr{O}_{\widetilde{X}}) = \chi(\mathscr{O}_X) + h^0(\mathscr{C}).$$

By the Problem 2.25 (the normalization map is affine), $\chi(f_*\mathscr{O}_{\widetilde{X}}) = \chi(\mathscr{O}_{\widetilde{X}})$. Furthermore,[10] $\mathrm{H}^0(X, \mathscr{O}_X) = k = \mathrm{H}^0(\widetilde{X}, \mathscr{O}_{\widetilde{X}})$, so the above equation can be rearranged to read

$$p_a(X) = p_a(\widetilde{X}) + h^0(\mathscr{C})$$

from which the first part of the claim follows. For the second part, suppose now that $p_a(X) = 0$. Then, $\delta_p = 0$ for all p, so X must have no singular points, i.e. X is non-singular. Since we're working over an algebraically closed field, X must have some k-point p,and one easily shows that $\mathscr{O}_X(p)$ is very ample (so gives an isomorphism $X \simeq \mathbb{P}^1_k$ since it's degree 1). ■

Problem 2.35 (Hartshorne IV.1.9)**.** *Let X be an integral projective scheme of dimension 1 over k. Let X_{reg} be the set of regular points of X.*

(a) Let $D = \sum n_i P_i$ be a divisor with support in X_{reg}, i.e. $P_i \in X_{reg}$ for all i. Define $\deg D := \sum n_i$. Let $\mathscr{L}(D)$ be the associated invertible sheaf on X. Then,

$$\chi(\mathscr{L}(D)) = \deg D + 1 - p_a$$

Proof. This is true by definition when $D = 0$. In general, we induct. The exact sequence

$$0 \to \mathscr{L}(D - P) \to \mathscr{L}(D) \to \mathscr{O}_P \to 0$$

says that

$$\chi(\mathscr{L}(D)) = \chi(\mathscr{L}(D-P)) + \chi(\mathscr{O}_P) = \chi(\mathscr{L}(D-P)) + 1$$

so the claim holds for $D \iff$ it holds for $D - P$. ■

(b) Any Cartier divisor on X is the difference of two very ample Cartier divisors.

Proof. Let D be a Cartier divisor on X. Since X is projective, it has some very ample divisor, say $\mathscr{L}$. Then, $\mathscr{L}$ is also ample, so there exists n_0 s.t. $\mathscr{L}^n \otimes \mathscr{O}_X(D)$ is globally generated for $n \geq n_0$. Thus, $\mathscr{L}^n \otimes \mathscr{O}_X(D)$ is very ample for $n \geq n_0 + 1$. Hence,

$$\mathscr{O}_X(D) \cong \left(\mathscr{L}^{n_0+1} \otimes \mathscr{O}_X(D)\right) \otimes \left(\mathscr{L}^{n_0+1}\right)^{-1}$$

is a difference of two very ample Cartier divisors (all line bundles come from Cartier divisors on an integral scheme). ■

(c) Every invertible sheaf $\mathscr{L}$ on X is isomorphic to $\mathscr{L}(D)$ for some divisor D with support in X_{reg}.

[10] A global section is a map to $\mathbb{A}^1_k$. The image must be closed (X proper) and irreducible (i.e. a point), so all global sections are constant.

Proof. We may write $\mathscr{L} \cong \mathscr{L}(D_1 - D_2)$ with D_1, D_2 both very ample Cartier divisors. That is, D_i is a hyperplane section of some embedding $\iota_i : X \hookrightarrow \mathbb{P}^{n_i}$. Since $X \setminus X_{reg}$ is finite, there is a hyperplane $H_i \subset \mathbb{P}^{n_i}$ with $D_i' := H_i \cap X \subset X_{reg}$. Hence, $\mathscr{L} \cong \mathscr{L}(D_1' - D_2')$ and we win. ■

(d) Assume that X is a locally complete intersection in some projective space. Then, [Har77, Theorem III.7.11] tells us that the dualizing sheaf ω_X is a line bundle, so has an associated canonical divisor K (with support in X_{reg} by **(c)**). Now, **(a)** says that

$$l(D) - l(K - D) = \deg D + 1 - p_a.$$

Definition 2.30. Let $Y \hookrightarrow X$ be a closed subscheme of a nonsingular k-variety. We say Y is a **local complete intersection** in X if the ideal sheaf $\mathscr{I}_Y$ of Y in X can be locally generated by $r := \operatorname{codim}(Y, X)$ elements at every point.

Problem 2.36 (Hartshorne IV.1.10)**.** *Let X be an integral projective scheme of dimension 1 over k, which is locally a complete intersection, and has $p_a = 1$. Fix a point $P_0 \in X_{reg}$. The map $P \mapsto \mathscr{L}(P - P_0)$ gives a one-to-one correspondence between the points of X_{reg} and the elements of the group $\operatorname{Pic}^0 X$.*

Proof. By Problem 2.35**(c)**, every element of $\operatorname{Pic} X$ is of the form $\mathscr{L}(D)$ with D a divisor with support in X_{reg}. Thus, we only need show that if D is a degree 0 divisor with support in X_{reg}, then there is a unique $P \in X_{reg}$ s.t. $\mathscr{L}(D) \cong \mathscr{L}(P - P_0)$, i.e. s.t. $\mathscr{L}(D + P_0) \cong \mathscr{L}(P)$. We first note that, by Problem 2.35**(d)**, we have

$$0 = \chi(K) = l(K) - l(K - K) = \deg K + 1 - p_a = \deg K$$

since $1 = p_a = 1 - \chi(\mathscr{O}_X) = 1 + \chi(K)$. Thus, $\deg(K - (D + P_0)) = -1 < 0$, so $l(K - (D + P_0)) = 0$. Hence, another application of Riemann-Roch gives

$$l(D + P_0) = l(D + P_0) - l(K - (D + P_0)) = \deg(D + P_0) + 1 - p_a = \deg(D + P_0) = 1.$$

In other words, the complete local system $\mathbb{P}\,\mathrm{H}^0(\mathscr{L}(D + P_0))$ of effective divisors linearly equivalent to $D + P_0$ is a 0-dimensional projective space, i.e. consists of a single divisor, i.e. there is a unique point $P \in X$ s.t. $D + P_0 \sim P$. Why is P in X_{reg}? ■

Problem 2.37 (Hartshorne IV.2.1)**.**

Definition 2.31. Let P, Q be two distinct points of $X \in \mathbb{P}^n$. The **secant line** determined by P, Q is the line in $\mathbb{P}^n$ joining P and Q. If $P \in X$, the **tangent line** to X at P is the unique line $L \subset \mathbb{P}^n$ passing through P whose tangent space $T_P(L)$ is equal to $T_P(X)$ as a subspace of $T_P(\mathbb{P}^n)$.

Problem 2.38 (Hartshorne IV.2.3)**.** *Let X be a curve of degree d in $\mathbb{P}^2$. For each point $P \in X$, let $T_P(X)$ be the tangent line to X at P. Considering $T_P(X)$ as a point of the dual projective plane $(\mathbb{P}^2)^*$, the map $P \mapsto T_P(X)$ gives a morphism of X to its* ***dual curve*** *$X^* \subset (\mathbb{P}^2)^*$. This may be singular even if X is smooth. Assume* $\operatorname{char} k = 0$ *below.*

(a) Fix a line $L \subset \mathbb{P}^2$ which is not tangent to X. Define a morphism $\varphi : X \to L$ via $\varphi(P) = T_p(X) \cap L$, for each point $P \in X$. Then, φ is ramified at P iff **(1)** $P \in L$, or **(2)** P is an **inflection point** of X, i.e. the intersection multiplicity of $T_P(X)$ with X at P is ≥ 3. Hence, X has only finitely many inflection points.

Remark 2.32. $\deg \varphi = \#$ tangents to X through a generic point of L (equiv, of $\mathbb{P}^2$).

Proof. Fix a (closed) point $P \in X$. We want to understand ramification at P. Let $F(x_0, x_1, x_2) \in S := k[x_0, x_1, x_2]$ be the (degree d) homogeneous polynomial cutting out $X \subset \mathbb{P}^2$. After suitable automorphism of $\mathbb{P}^2$, we may assume $P = (0,0) \in D_+(x_0) = \operatorname{spec} k[x_{1/0}, x_{2/0}]$ with tangent line $T_P X$ given by $\{x_{2/0} = 0\}$, i.e. the "x-axis". We give two arguments...

(1) We have $\operatorname{char} k = 0$ (and $k = \overline{k}$), so we may as well assume $k = \mathbb{C}$ and work analytically. The implicit function theorem gives us a local parameterization where our tangent line is cut out by $(t, 0)$ and X is cut out by $(t, a(t))$ near $P = (0,0)$ (note $a(t)$ holomorphic vanishing to order ≥ 2 at $t = 0$) since "$\frac{\partial F}{\partial y} \neq 0$" (but "$\frac{\partial F}{\partial x} = 0$"). If $P \in L$, we make L the y-axis, and if $P \notin L$, we may it the line at infinity.

In the first case, $\varphi(Q)$ is the y-intercept of the tangent line at $(t, a(t))$ for t near 0; this tangent line is given by the equation

$$y = a'(t)x + (a(t) - a'(t)t)$$

so has y-intercept $y = a(t) - a'(t)t$ vanishing to second order, so φ is ramified at P.

In the second case, $\varphi(Q)$ is the slope of the tangent line at $(t, a(t))$ for t near 0, i.e. $\varphi(Q) = [1 : a'(t)]$. This will be ramified at P iff $a'(t)$ vanishes to the second order iff $a(t)$ vanishes to the third order iff the intersection multiplicity of $T_P(X)$ with X at P is ≥ 3.

(2) We note that the completed local ring of at P is $\widehat{\mathscr{O}}_{X,P} \simeq \widehat{\mathscr{O}}_{X \cap D_+(x_0), P} = k\llbracket x_{1/0}, x_{2/0} \rrbracket / (F(1, x_{1/0}, x_{2/0}))$. Since $k\llbracket x_{1/0} \rrbracket$ is a complete local ring, Weierstrass Preparation[11] says that we may write

$$F(1, x_{1/0}, x_{2/0}) = u\left(x_{2/0} - f_0\right) \in k\llbracket x_{1/0}, x_{2/0} \rrbracket \quad \text{with} \quad u \in k\llbracket x_{1/0} \rrbracket^{\times} \quad \text{and} \quad f_0 \in k\llbracket x_{1/0} \rrbracket .$$

Thus, $x_{2/0} = f_0(x_{1/0}) \in \widehat{\mathscr{O}}_{X,P}$ so we have a "local equation for X at P." We also see that

$$\widehat{\mathscr{O}}_{X,P} = \frac{k\llbracket x_{1/0}, x_{2/0} \rrbracket}{(F(1, x_{1/0}, x_{2/0}))} \simeq \frac{k\llbracket x_{1/0}, x_{2/0} \rrbracket}{(x_{2/0} + f_0(x_{1/0}))} \simeq k\llbracket x_{1/0} \rrbracket .$$

As before, if $P \in L$, make L the y-axis, and if $P \notin L$, make it the line at infinity. Let $t \in \mathscr{O}_{L,\varphi(P)}$ be a uniformizer.

In the first case, L is the y-axis, so $\varphi^*(t) \in \widehat{\mathscr{O}}_{X,P}$ is the "y-intercept of tangent line at $(x_{1/0}, f_0(x_{1/0}))$," i.e.

$$\varphi^*(t) = f_0(x_{1/0}) - f_0'(x_{1/0})x_{1/0}.$$

Since $f_0(x_{1/0})$ vanishes to order ≥ 2 (since the tangent line is by $x_{2/0} = f_0(x_{1/0}) = 0$), we conclude that $\varphi^*(t)$ vanishes to order ≥ 2, and so φ is ramified at P.

[11] s in that link is the minimal index so that $a_s \notin \mathfrak{m} \subset A$. Here $s = 1$ since X is smooth so $\frac{\partial F}{\partial x_{2/0}} \neq 0$ (since $\frac{\partial F}{\partial x_{1/0}} = 0$ by assumption

In the second case, L is the line at infinity, so $\varphi^*(t)$ is the slope of the tangent line, so $\varphi^*(t) = f_0'(x_{1/0})$ which vanishes to order ≥ 2 iff f_0 vanishes to order ≥ 3, so P ramified iff it is an inflection point. ■

Maybe need some Taylor series-type argument here

(b) A line of $\mathbb{P}^2$ is a **multiple tangent** if it is tangent to X at more than one point, and is a **bitangent** if it is tangent to X at exactly 2 points. If L is a multiple tangent of X, tangent at the points $P_1, \ldots, P_r$, and if none of the P_i are inflection points, then the corresponding point on X^* is an **ordinary r-fold point**, i.e. a point of multiplicity r with distinct tangent directions. Hence, X has only finitely many multiple tangents.

Proof. Let $F(x, y, z)$ be the equation for X. Then, X^* ■

(c) Let $O \in \mathbb{P}^2$ be a point not on X nor on any inflectional or multiple tangent of X. Let L be a line not containing O, and let $\psi : X \to L$ be projection away from O. Then, ψ is ramified at $P \in X$ iff OP is tangent to X at P, and in this case the ramification index is 2. By Hurwitz, there are exactly $d(d-1)$ tangents passing through O.

Proof. Fix $P \in X$. We claim $e_P = i(X, OP; P)$ is the intersection multiplicity of X and OP at P. We may assume $P = (0, 0) \in \mathbb{A}^2$ with L the y-axis and OP the x-axis. Also, X will locally be the graph of a function $(t, a(t))$. Say $O = (1, 0)$ so for $Q = (t, a(t))$ near P (i.e. t small), we have OQ given by

$$OQ : y = \frac{a(t)}{t-1}x - \frac{a(t)}{t-1} \iff (t-1)y - a(t)x = -a(t).$$

Thus, the y-intercept of OQ is $\psi(Q) = -\frac{a(t)}{t-1}$. This vanishes to order ≥ 2 at $t = 0$ iff $a(t)$ does iff $T_P X$ is the x-axis iff OQ is tangent to X at P. The ramification index must then be 2 by the assumptions on O.

Scratch that. Intersection multiplicity will be

$$i(X, OP; P) = \dim_k \left(\frac{\mathscr{O}_{\mathbb{P}^2, P}}{I_X + I_{OP}} \right) = \dim_k \left(\frac{\mathscr{O}_{X,P}}{I_{OP}} \right) = v_{X,P}(g)$$

where $g \in \Gamma(\mathscr{O}(1))$ is the equation defining OP. Similarly, $1 = i(L, OP; \psi(P)) = v_{L,\psi(P)}(g)$. This should do it, but I'm not convinced it does...

Hurwitz now gives

$$(d-1)(d-2)-2 = 2g(X)-2 = (\deg \psi)(2g(L)-2) + \sum_P (e_P - 1) = d(-2) + (\#R) \implies \#R = d(d-1)$$

as desired. ■

(d) For almost all points of X, a point O of X lies on exactly $(d+1)(d-2)$ tangents of X, not counting the tangent at O.

Proof. Let L be a line through O and consider $\varphi : X \to L$ as in **(a)**. By **(c)**, $\deg \varphi = d(d-1)$, so

$$d(d-1) = \sum_{P \in \varphi^{-1}(O)} e_P.$$

Generically, none of the preimages of O are inflection points, so the above really says

$$d(d-1) = e_O + (\#\varphi^{-1}(O)-1) = 2 + (\#\varphi^{-1}(O)-1) \implies \#\varphi^{-1}(O) - 1 = d^2 - d - 2 = (d+1)(d-2).$$

■

(e) The degree of φ from **(a)** is $d(d-1)$. If $d \geq 2$, then X has $3d(d-2)$ inflection points. An ordinary inflection point of X corresponds to cusp of the dual curve.

Proof. The first part follows from **(c)**. By **(a)** + **(d)**, the number of inflection points I satisfies

$$(d-1)(d-2) - 2 = 2g(X) - 2 = d(d-1)(-2) + d + I \implies I = 3d(d-2).$$

■

Problem 2.39 (Hartshorne IV.2.5)**.** *Let X be a curve of genus $g \geq 2$, and let $G = \operatorname{Aut} X$. Take for granted the fact that G is finite, and set $n = \#G$. Let $L = K(X)^G$ be the fixed field of the natural G-action, so the inclusion $L \hookrightarrow K(X)$ corresponds to a degree n finite morphism $f : X \to Y$ of curves.*

(a) Say $P \in X$ is a ramification point with ramification degree $e_P = r$. Then, $f^{-1}f(P)$ consists of exactly n/r points each with ramification degree r. Now, let $P_1, \dots, P_s$ be a maximal set of ramification points lying above distinct points of Y, and write $e_{P_i} = r_i$. Then,

$$\frac{2g(X)-2}{n} = 2g(Y) - 2 + \sum_{i=1}^{s}(1 - 1/r_i).$$

Proof. The second part follows immediately from Riemann-Hurwitz once we know the first part (and that f is separable). The first part holds because f is, by construction, a Galois cover with group G. In particular, for any $\sigma \in G = \operatorname{Aut} X$, by 'transfer of structure' $\sigma(P) \in X$ is a ramification point (still above $f(P)$![12]) of degree $e_P = r$. All points in $f^{-1}f(P)$ are of this form, so they all have ramification degree r; thus, $\sum_{P' \in f^{-1}f(P)} e_{P'} = n \implies \#f^{-1}f(P) = \frac{n}{r}$. ■

(b) Since $g = g(X) \geq 2$, the LHS of the equation at the end of **(a)** is > 0. Note that $g(Y), s \geq 0$ and $r_i \geq 2$ for all i. We claim the minimum possible value of

$$V := 2g(Y) - 2 + \sum_{i=1}^{s}(1 - 1/r_i) > 0$$

is $1/42$. Thus, $n \leq 84(g-1)$ as claimed.

[12] The composition $X \xrightarrow{\sigma} X \xrightarrow{f} Y$ corresponds on function fields to $L \hookrightarrow K(X) \overset{\sigma}{\hookrightarrow} K(X)$ which is just $L \hookrightarrow K(X)$ since L is fixed by G. Alternatively, $Y = X/G$

Proof. We consider various cases.

($g(Y) = 0$) If $g(Y) = 0$, then we have

$$\sum_{i=1}^{s} \left(1 - \frac{1}{r_i}\right) > 2.$$

This forces $s \geq 3$ (note $1 \geq 1 - 1/r_i \geq 1/2$). If $s \geq 5$, then $V \geq 1/2 > 1/42$, so we may assume $s \in \{3, 4\}$.

($s = 4$) In this case, there must be some i, with $r_i > 2$. Thus,

$$V \geq \left(\frac{3}{2} + \frac{2}{3}\right) - 2 = \frac{13}{6} - 2 = \frac{1}{6} > \frac{1}{42}.$$

($s = 3$) In this case, there must be two indices i, say $i = 1, 2$, with $r_i > 2$ and one index j, say $j = 1$, with $r_j > 3$. More subcases...

($r_3 = 2$) Say we have $r_1 \geq 4, r_2 \geq 3, r_3 = 2$. If $r_2 = 3$, then $(1 - 1/r_1) + 7/6 > 2$ which forces $r_1 > 6$. Thus,

$$V \geq \left(\frac{1}{2} + \frac{2}{3} + \frac{6}{7}\right) - 2 = \frac{85}{42} - 2 = \frac{1}{42}.$$

If $r_3 = 4$, then $(1 - 1/r_1) + 5/4 > 2$ which forces $r_1 > 4$ and so

$$V \geq \left(\frac{1}{2} + \frac{3}{4} + \frac{4}{5}\right) - 2 = \frac{41}{20} - 2 = \frac{1}{20} > \frac{1}{42}.$$

Finally, if $r_3 \geq 5$, then the above equation also holds since $r_1 \geq 4$.

($r_3 \geq 3$) Then,

$$V \geq \left(\frac{4}{3} + \frac{3}{4}\right) - 2 = \frac{25}{12} - 2 = \frac{1}{12} > \frac{1}{42}.$$

($g(Y) = 1$) In this case, we have

$$\sum_{i=1}^{s} \left(1 - \frac{1}{r_i}\right) > 0.$$

Thus, $s \geq 1$ and so $V \geq 1/2 > 1/42$.

($g(Y) \geq 2$) In this case $V \geq 2g(Y) - 2 \geq 2 > 1/42$.

Thus, we see that $V \geq 1/42$ in every possible case, and moreover that $1/42$ is possible, e.g. when

$$(g(Y), s, (r_i)_{i=1}^{s}) = (0, 3, (2, 3, 7)).$$

■

Problem 2.40 (Hartshorne IV.3.1)**.**

Problem 2.41 (Hartshorne IV.4.1)**.** *Let X be an elliptic curve over k, with $\operatorname{char} k \neq 2$, let $P \in X$ be a point, and let R be the graded ring*

$$R := \bigoplus_{n \geq 0} \mathrm{H}^0(X, \mathscr{O}_X(nP)).$$

For suitable choice of t, x, y, we have

$$R \cong \frac{k[t,x,y]}{(y^2 - x(x-t^2)(x-\lambda t^2))} \quad \textit{where} \quad |t| = 1, |x| = 2, |y| = 3.$$

Proof. First note that Riemann-roch says ($n \geq 0$)

$$\dim \mathrm{H}^0(X, \mathscr{O}_X(nP)) = \begin{cases} 1 & \text{if } n = 0 \\ n & \text{otherwise.} \end{cases}$$

So let $t \in \mathrm{H}^0(X, \mathscr{O}_X(P))$ be a generator. Choose $x \in \mathrm{H}^0(X, \mathscr{O}_X(2P))$ so that $\{t^2, x\}$ is a basis, and then choose $y \in \mathrm{H}^0(X, \mathscr{O}_X(3P))$ so that $\{t^3, tx, y\}$ forms a basis.[13] Now, $\mathrm{H}^0(X, \mathscr{O}_X(6P))$ is 6-dimensional, but contains the 7 elements $t^7, t^5x, t^4y, t^2xy, t^2x^2, x^3, y^2$. Hence, we must have a linear relationship among them which necessarily involves both x^3 and y^2 (as the remaining elements come from a basis of $\mathrm{H}^0(X, \mathscr{O}_X(5P))$. After scaling, we may assume our relationship is of the form

$$y^2 + a_1txy + a_3t^3y = x^3 + a_2t^2x^2 + a_4t^4x + a_6t^6.$$

Now, using $\operatorname{char} k \neq 2$, we complete the square on the left. That is we replace $y \mapsto \left(y + \frac{a_1tx + a_3t^3}{2}\right)$ in order to put this in the form

$$y^2 = \text{degree 3 homo. poly. in } x, t^2 = (\alpha_1 x - \beta_1 t)(\alpha_2 x - \beta_2 t^2)(\alpha_3 x - \beta_3 t^2).$$

Since $\alpha_1\alpha_2\alpha_3 = 1$, we can pull them out above (i.e. replace $\beta_i \mapsto \beta_i/\alpha_i$) to actually assume $\alpha_1 = \alpha_2 = \alpha_3$, so we have $y^2 = (x - \beta_1t^2)(x-\beta_2t^2)(x-\beta_3t^2)$. Next replace $x \mapsto x + \beta_1t^2$ to get $y^2 = x(x-\beta_2t^2)(x-\beta_3t^2)$. Then replace $x \mapsto x\beta_2$ (and $y \mapsto y/\beta_2^3$) to finally write

$$y^2 = x(x-t^2)(x-\lambda t^2).$$

This shows that we have a surjection.

$$\frac{k[t,x,y]}{(y^2 - x(x-t^2)(x-\lambda t^2))} \twoheadrightarrow R.$$

To show that this is an iso, one only needs show that the degree n part of this quotient algebra has dimension n... ■

Problem 2.42 (Hartshorne IV.4.3)**.**

[13] Multiplication by t is injective since it comes from the first map is the exact sequence $0 \to \mathscr{O}_X \otimes \mathscr{O}_X(nP) \to \mathscr{O}_X(P) \otimes \mathscr{O}_X(nP) \to \mathscr{O}_P \to 0$

Problem 2.43 (Hartshorne IV.4.6).

(a) Let X be a curve of genus g embedded birationally in $\mathbb{P}^2$ as a curve of degree d with r nodes. Then, X has $6(g-1)+3d$ inflection points, at least assuming $\operatorname{char} k = 0$.

Proof. ■

Problem 2.44 (Hartshorne IV.4.7). *Let X, X' be elliptic curves with basepoints P_0, P_0'.*

(a) If $f : X \to X'$ is a morphism, then $f^* : \operatorname{Pic} X' \to \operatorname{Pic} X$ induces a homomorphism $\widehat{f} : (X', P_0') \to (X, P_0)$.

Proof. By [Har77, Theorem 4.11], the **Jacobian** of X – i.e. the pair $(J, \mathscr{L})$ representing the functor $T \rightsquigarrow \operatorname{Pic}^0(X_T)/\operatorname{Pic}(T) = \operatorname{Pic}^0(X/T)$ – is $J = X$ with $\mathscr{L} = \mathscr{O}(\Delta) \otimes p_1^* \mathscr{O}(-P_0)$ on $X \times J$. Thus, a morphism $X' \to J = X$ is the same thing as a line bundle in $\operatorname{Pic}^0(X/X')$; we take $\mathscr{M} := \mathscr{O}(\Gamma_f) \otimes p_2^* \mathscr{O}(-P_0')$ on $X \times X'$, and let $\widehat{f} : (X', P_0') \to (X, P_0)$ be the resulting homomorphism. ■

Problem 2.45 (Hartshorne IV.4.15). *Let X be an elliptic curve over a field k of characteristic p, and let $F' : X_p \to X$ be the k-linear Frobenius map. Then, the dual morphism $\widehat{F}' : X \to X_p$ is separable iff the Hasse invariant of X is 1. Furthermore,*

$$X[p] \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} & \textit{if Hasse invariant } 1 \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. The Zariski tangent space to X at the origin is $\mathrm{H}^1(X, \mathscr{O}_X)$ since it is the Jacobian of X. Note that we have an exact sequence

$$\begin{tikzcd} X_p \arrow[r, "F'"'] \arrow[rr, bend left, "{[p]}"] & X \arrow[r, "\widehat{F}'"'] & X_p \end{tikzcd}$$

of k-morphisms. Since $\widehat{F}'$ is of degree p, it is inseparable iff it is Frobenius (which would force $X \simeq X_{p^2}$. Irrelevant for now, but fun fact). Consider the induced map on tangent spaces. The composition induces 0 on tangent spaces since $\operatorname{char} k = p$. By definition, F' is nontrivial on tangent spaces (note $T_0 X \simeq \mathrm{H}^1(X, \mathscr{O}_X)$) iff X has Hasse invariant 1. By staring at the diagram, we conclude X has Hasse invariant 1 iff $\widehat{F}'$ is trivial on tangent spaces (for $\Longleftarrow$ direction, is $\widehat{F}'$ is inseparable, it is frobenius, so both arrows induce same action on $\mathrm{H}^1(X, \mathscr{O}_X)$ which must be the trivial action).

For the last part, we just note that $\#X[p] = \deg_s[p] = \deg_s[\widehat{F}']$ and this is either p or 1. ■

Problem 2.46 (Hartshorne IV.4.16). *Let X/k be an elliptic curve in char p, and suppose X is defined over $\mathbb{F}_q$. Assume X has an $\mathbb{F}_q$-rational point, and let $F' : X_q \to X$ be the k-linear Frobenius w.r.t q.*

(a) $X_q \cong X$ as k-schemes, with $F' : X \to X$ given by take qth powers of coordinates on $X \hookrightarrow \mathbb{P}^2$.

Proof. By assumption $X = (X_0)_k$ with $X_0/\mathbb{F}_q$, so $X_q = (X_{0,q})_k = (X_0)_k = X$ since Frobenius of $\mathbb{F}_q$ is trivial. Inside $\mathbb{P}^2$, X is carried to X_q be the absolute Frobenius $F : \mathbb{P}^2 \to \mathbb{P}^2$ which acts by the qth power map on $\mathscr{O}_{\mathbb{P}^2}$, so $X_q \hookrightarrow \mathbb{P}^2$ defined by the qth power of X's equation... ■

(b) $1_X - F'$ is separable w/ kernel $X(\mathbb{F}_q)$.

Proof. In general, $\varphi : X \to Y$ is separable iff $\varphi^* : \Omega_{K(Y)/k} \to \Omega_{K(X)/k}$ is an iso. We know F' is inseparable, so $({}^*1_X - F')\omega = \omega - 0 = \omega$ and so this map is separable. The kernel is as claimed. ■

(c) $F' + \widehat{F}' = a_X$ for some integer a, and $N := \#X(\mathbb{F}_q) = q - a + 1$.

Proof. This follows from

$$n = (1 - F) \circ (1 - \widehat{F}) = 1 - F - \widehat{F} - q.$$

■

(d) $|a| \le 2\sqrt{q}$.

Proof. Note that $\deg(m + nF') > 0$ for all $m, n \in \mathbb{Z}$. That is,

$$m^2 + mna + qn^2 = (m + nF')(m + n\widehat{F'}) > 0$$

for all $m, n \in \mathbb{Z}$. Letting $t = m/n$ and dividing by n^2 to de-homogenize, this says

$$t^2 + at + q > 0$$

for all $t \in \mathbb{Q}$. Thus, this holds (with $>$ replaced by $\ge$) for all $t \in \mathbb{R}$. This is a concave up parabola, so we're saying that it has at most one real root. Hence, it's discriminant must satisfy

$$a^2 - 4q \le 0,$$

i.e. $a \le 2\sqrt{q}$. ■

(e) Now assume $q = p$. Then X has Hasse invariant 0 iff $a \equiv 0 \pmod{p}$. For $p \ge 5$, this holds iff $\#X(\mathbb{F}_p) = p + 1$.

Proof. Hass invariant 0 means $\widehat{F}'$ is inseparable, so multiplication by a must be zero on tangent space, so $p \mid a$. We know $|a| \le 2\sqrt{p}$. Since $p > 2\sqrt{p}$ for $p \ge 5$, $p \mid a$ forces $a = 0$ in these cases. ■

Problem 2.47 (Hartshorne IV.4.22)**.**

Problem 2.48 (Hartshorne IV.5.2)**.** *Let X be a curve of genus $g \ge 2$ over a field of characteristic* 0*. Then, $G := \operatorname{Aut} X$ is finite.*

2.4 Some Examples

2.4.1 Ramification Stuff

Example. Let $X : y^2 - y = x^{-(2m+1)}$ over k, and let $f : X \to \mathbb{A}^1$ be $(x, y) \mapsto x$. Furthermore, assume $\operatorname{char} k = 2$. We want to compute the ramification divisor R of f. This will only be ramified above the origin. Hence, R is supported at a single point (the unique point above the origin) $p \in X$.

Question: Why?

Answer: Elsewhere, there are two preimages w/ no funny business

Note that x is a uniformizer at the origin of $\mathbb{A}^1$. We would like a uniformizer of at $p \in X$. Let $v : \mathscr{O}_{\mathbb{A}^1,0} \to \mathbb{Z}$ be the normalized valuation with unique extension $w : \mathscr{O}_{X,p} \to \frac{1}{2}\mathbb{Z}$. Note that

$$w(y^2-y) = w(x^{-(2m+1)}) = -(2m+1)w(x) = -(2m+1)v(x) = -2m-1 \implies w(y) < 0 \implies w(y^2) < w(y),$$

so $2w(y) = w(y^2 - y) = -2m - 1$ and $w(y) = -\frac{2m+1}{2}$. Hence,

$$w\left(yx^{m+1}\right) = \frac{2m+2}{2} - \frac{2m+1}{2} = \frac{1}{2},$$

so $t := yx^{m+1} \in \mathscr{O}_{X,p}$ is a uniformizer. We would now like to rewrite the equation for X in terms of t:

$$\begin{aligned} & y^2 - y = x^{-(2m+1)} \\ \implies & \left(\frac{t}{x^{m+1}}\right)^2 - \left(\frac{t}{x^{m+1}}\right) = x^{-2m-1} \\ \implies & t^2 - x^{m+1}t = x. \end{aligned}$$

Thus, we see that $g(T) := T^2 - x^{m+1}T - x$ is the minimal polynomial for t (we also see that this is Eisenstein and reaffirm that $2w(t) = w(t^2 - x^{m+1}t) = w(x) = 1$). In any case, we see that $\mathscr{O}_{X,p} = \mathscr{O}_{\mathbb{A}^1,0}[t]$ has different

$$(g'(t)) = \left(x^{m+1}\right) = (t)^{2m+2},$$

so $R = (2m + 2)[p]$.

Alternatively, we could compute (recall $\operatorname{char} k = 2$)

$$\begin{aligned} \mathrm{d}x &= \mathrm{d}\left(t^2 - x^{m+1}t\right) = 2t\mathrm{d}t - (m+1)x^m t\mathrm{d}x - x^{m+1}\mathrm{d}t \\ \implies \mathrm{d}x &= \left(\frac{2t - x^{m+1}}{(m+1)x^m t + 1}\right)\mathrm{d}t = -\frac{x^{m+1}}{(m+1)x^m t + 1}\mathrm{d}t \end{aligned}$$

The coefficient above has (normalized) valuation $2m + 2$.

3 Algebraic Number Theory

3.1 Discriminant and Different

3.1.1 Norm and Trace

3.1.2 Basics

The different of a number field is inverse fractional ideal of the trace dual of the ring of integers.

Definition 3.1. Let L be a lattice in a number field K, so $L \cong \mathbb{Z}^{[K:\mathbb{Q}]}$. Its **dual lattice** is

$$L^\vee := \left\{\alpha \in K : \mathrm{Tr}_{K/\mathbb{Q}}(\alpha L) \subset \mathbb{Z}\right\}.$$

In particular, is $e_1, \ldots, e_n$ is a basis for L, the the dual basis $e_1^\vee, \ldots, e_n^\vee$ (w.r.t the trace paring $(x, y) \mapsto \mathrm{Tr}(xy)$) is a basis for $L^\vee$.

Example. Say $K = \mathbb{Q}(i)$ and $L = \mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i$. Then, $\alpha = a + bi \in \mathbb{Q}(i)$ is in $L^\vee$ iff $\mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(a + bi), \mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}((a + bi)i) \in \mathbb{Z}$. That is, we need $2a, -2b \in \mathbb{Z}$, so

$$\mathbb{Z}[i]^\vee = \frac{1}{2}\mathbb{Z} + \frac{1}{2}\mathbb{Z}i = \frac{1}{2}\mathbb{Z}[i].$$

Now say $L = (1 + 2i)\mathbb{Z}[i] = \mathbb{Z}(1 + 2i) + \mathbb{Z}(i - 2)$. Then,

$$L^\vee = \mathbb{Z}\left(\frac{1}{10} - \frac{i}{5}\right) + \mathbb{Z}\left(-\frac{1}{5} - \frac{i}{10}\right) = \frac{1}{2(1+2i)}\mathbb{Z}[i].$$

Lemma 3.2. *For lattices in K, one has*

(1) $L^{\vee\vee} = L$

(2) $L_1 \subset L_2 \iff L_1^\vee \supset L_2^\vee$

(3) $(L_1 + L_2)^\vee = L_1^\vee \cap L_2^\vee$

(4) $(L_1 \cap L_2)^\vee = L_1^\vee + L_2^\vee$

(5) $(\alpha L)^\vee = \frac{1}{\alpha}L^\vee$

Proof of (5). Say $x \in (\alpha L)^\vee$. Then, $\mathrm{Tr}(x\alpha y) \in \mathbb{Z}$ for any $y \in L$, so $x\alpha \in L^\vee$, i.e. $x \in \frac{1}{\alpha}L^\vee$. The converse is similarly easy. ■

Example. Say $K = \mathbb{Q}(\sqrt{d})$. Let $L_1 = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$ and $L_2 = \mathbb{Z} \oplus \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$.

The dual basis of $\{1, \sqrt{d}\}$ w.r.t the trace product on K is $\left\{\frac{1}{2}, \frac{1}{2\sqrt{d}}\right\}$, so

$$\left(\mathbb{Z} + \mathbb{Z}\sqrt{d}\right)^\vee = \mathbb{Z}\frac{1}{2} + \mathbb{Z}\frac{1}{2\sqrt{d}} = \frac{1}{2\sqrt{d}}\left(\mathbb{Z}\sqrt{d} + Z\right) = \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}].$$

Similarly,

$$\left(\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}\right)^\vee = \mathbb{Z}\left(-\frac{1}{2}\right) + \mathbb{Z}\frac{1}{\sqrt{d}} = \frac{1}{\sqrt{d}}\left(\mathbb{Z} - \mathbb{Z}\frac{\sqrt{d}}{2}\right) = \frac{1}{\sqrt{d}}\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

Theorem 3.3. *Say $K = \mathbb{Q}(\alpha)$, and let $f(T)$ be the minimal polynomial of α in $\mathbb{Q}[T]$. Write*

$$f(T) = (T-\alpha)\left(c_0(\alpha) + c_1(\alpha)T + \cdots + c_{n-1}(\alpha)T^{n-1}\right) \in K.$$

The dual basis of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is $\left\{\frac{c_0(\alpha)}{f'(\alpha)}, \ldots, \frac{c_{n-1}(\alpha)}{f'(\alpha)}\right\}$. In particular, when $\alpha \in \mathscr{O}_K$,

$$\left(\mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}\right)^\vee = \frac{1}{f'(\alpha)}\left(\mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}\right).$$

Proof. Let $\alpha_1, \ldots, \alpha_n$ be the $\mathbb{Q}$-conjugates of α in a splitting field, with $\alpha = \alpha_1$. Euler tells us that

$$\sum_{i=1}^n \frac{1}{f'(\alpha)} \frac{f(T)}{T - \alpha_i} = 1.$$

Both sides are polynomials of degree $< n$ which are equal at n values. The same argument shows that

$$\sum_{i=1}^n \frac{\alpha_i^k}{f'(\alpha_i)} \frac{f(T)}{T - \alpha_i} = T^k$$

for $0 \leq k \leq n-1$ (RHS needs to be a poly of degree $< n$). As a consequence

$$\sum_{i=1}^n \frac{\alpha_i^k}{f'(\alpha_i)} c_j(\alpha_i) = \delta_{jk}.$$

The LHS above is precisely $\mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{\alpha^k c_j(\alpha)}{f'(\alpha)}\right)$, so $\{c_j(\alpha)/f'(\alpha)\}$ is the dual basis to $\{\alpha^j\}$.

To finish, we need to show that

$$\mathbb{Z}c_0(\alpha) + \cdots + \mathbb{Z}c_{n-1}(\alpha) = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1},$$

when $\alpha \in \mathscr{O}_K$. To do these, we find a formula for $c_j(\alpha)$, the coefficient of T^j in $f(T)/(T-\alpha)$... see here. ■

Definition 3.4. The **codifferent** is the lattice

$$\mathscr{O}_K^\vee = \left\{\alpha \in K : \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\mathscr{O}_K) \subset \mathbb{Z}\right\}.$$

Theorem 3.5. *For a fractional ideal $\mathfrak{a}$ in K, $\mathfrak{a}^\vee$ is the fractional ideal $\mathfrak{a}^\vee = \mathfrak{a}^{-1}\mathscr{O}_K^\vee$.*

Proof. First check it's a fractional idea. It's a f.g. $\mathbb{Z}$-module, so we only need it to be preserved by multiplication by $\mathscr{O}_K$. This is obvious.

To show $\mathfrak{a}^\vee = \mathfrak{a}^{-1}\mathscr{O}_K^\vee$, pick some $\alpha \in \mathfrak{a}^\vee$. For $\beta \in \mathfrak{a}$, $\mathrm{Tr}(\alpha\beta\mathscr{O}_K) \subset \mathbb{Z}$, so $\alpha\beta \in \mathscr{O}_K^\vee$. Letting β vary in $\mathfrak{a}$, we see that $\alpha\mathfrak{a} \subset \mathscr{O}_K^\vee$, so $\alpha \in \mathfrak{a}^{-1}\mathscr{O}_K^\vee$. The reverse inclusion is even simpler. ■

Proposition 3.6. *The codifferent $\mathscr{O}_K^\vee$ is the largest fractional ideal in K all of whose elements have trace in $\mathbb{Z}$.*

Proof. For a fractional ideal $\mathfrak{a}$, $\mathfrak{a} = \mathfrak{a}\mathscr{O}_K$, so $\mathrm{Tr}(\mathfrak{a}) = \mathrm{Tr}(\mathfrak{a}\mathscr{O}_K)$ lies in $\mathbb{Z}$ iff $\mathfrak{a} \subset \mathscr{O}_K^\vee$. ■

Definition 3.7. The **different ideal** of K is

$$\mathcal{D}_K := (\mathcal{O}_K^\vee)^{-1} = \{x \in K : x\mathcal{O}_K^\vee \subset \mathcal{O}_K\}.$$

Since $\mathcal{O}_K \subset \mathcal{O}_K^\vee$, $\mathcal{D}_K \subset \mathcal{O}_K^{\vee\vee} = \mathcal{O}_K$, so its an integral ideal.

Example. $\mathbb{Z}[i]^\vee = \frac{1}{2}\mathbb{Z}[i]$, so $\mathcal{D}_{\mathbb{Q}(i)} = 2\mathbb{Z}[i]$.

Theorem 3.8. *If $\mathcal{O}_K = \mathbb{Z}[\alpha]$, then $\mathcal{D}_K = (f'(\alpha))$ where α has minimal polynomial $f(T) \in \mathbb{Z}[T]$.*

Example. For $K = \mathbb{Q}(\sqrt{d})$ with square $d \in \mathbb{Z} \setminus \{0, 1\}$,

$$\mathcal{D}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} (2\sqrt{d}) & \text{if } d \equiv 2, 3 \pmod 4 \\ (\sqrt{d}) & \text{if } d \equiv 1 \mod 4. \end{cases}$$

Theorem 3.9. *For a number field K, $N(\mathcal{D}_K) = |\operatorname{disc} K|$.*

Proof. Let $e_1, \ldots, e_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$, so $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbb{Z}e_i$. Then, $\mathcal{D}_K^{-1} = \mathcal{O}_K^\vee = \bigoplus_{i=1}^n \mathbb{Z}e_i^\vee$. The norm of an ideal is its index in $\mathcal{O}_K$, so

$$N(\mathcal{D}_K) = [\mathcal{O}_K : \mathcal{D}_K] = [\mathcal{D}_K^{-1} : \mathcal{O}_K] = [\mathcal{O}_K^\vee : \mathcal{O}_K].$$

This latter index is the determinant of the inclusion matrix $\mathcal{O}_K \hookrightarrow \mathcal{O}_K^\vee$. Note that we can write

$$e_j = \sum_{i=1}^n a_{ij}e_i^\vee \text{ with } a_{ij} = \operatorname{Tr}_{K/\mathbb{Q}}(e_ie_j),$$

so $N(\mathcal{D}_K) = [\mathcal{O}_K^\vee : \mathcal{O}_K] = |\det(a_{ij})| = |\operatorname{disc} K|$. ∎

Remark 3.10. One can define an ideal-theoretic norm map, and so directly say that $N(\mathcal{D}_K) = \operatorname{disc} K$. This is defined, on primes, by $N(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{q}|\mathfrak{p})}$ where $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_\mathbb{Q}$ and $f(\mathfrak{q} \mid \mathfrak{p}) = [(\mathcal{O}_K/\mathfrak{q}) : (\mathcal{O}_\mathbb{Q}/\mathfrak{p})]$ is the inertial degree.

Compare with push-forward of divisors on curves were $\varphi_*[P] = [\kappa(P) : \kappa(\varphi(P))] \cdot [\varphi(P)]$

Lemma 3.11. *For a nonzero ideal $\mathfrak{a} \subset \mathcal{O}_K$, $\mathfrak{a} \mid \mathcal{D}_K$ iff $\operatorname{Tr}_{K/\mathbb{Q}}(\mathfrak{a}^{-1}) \subset \mathbb{Z}$.*

Remember: $I \mid J \iff I \supset J$ in a Dedekind domain (e.g. $(3) \supset (6)$)

Theorem 3.12 (Dedekind)**.** *The prime ideal factors of $\mathcal{D}_K$ are the primes in K that ramify over $\mathbb{Q}$. More precisely, for each prime $\mathfrak{p}$ in $\mathcal{O}_K$ lying over a prime number p, with ramification index $e = e(\mathfrak{p} \mid p)$, the exact power of $\mathfrak{p}$ in $\mathcal{D}_K$ is $\mathfrak{p}^{e-1}$ if $p \nmid e$, and $\mathfrak{p}^e \mid \mathcal{D}_K$ if $p \mid e$.*

Proof. It suffices to check the divisibility statements, i.e. that $\mathfrak{p}^{e-1} \mid \mathcal{D}_K$ always (so $\mathfrak{p} \mid \mathcal{D}_K$ if $\mathfrak{p}$ ramified) and $\mathfrak{p}^e \mid \mathcal{D}_K$ iff $p \mid e$ (so $\mathfrak{p} \nmid \mathcal{D}_K$ if $e = 1$).

First write $(p) = \mathfrak{p}^{e-1}\mathfrak{a}$ so $\mathfrak{p} \mid \mathfrak{a}$. To say $\mathfrak{p}^{e-1} \mid \mathcal{D}_K$ is equivalent to saying that $\operatorname{Tr}_{K/\mathbb{Q}}(\mathfrak{p}^{-(e-1)}) \subset \mathbb{Z}$. Since $\mathfrak{p}^{-(e-1)} = \frac{1}{p}\mathfrak{a}$, this is the case iff $\operatorname{Tr}_{K/\mathbb{Q}}(\mathfrak{a}) \subset p\mathbb{Z}$, i.e. $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha) \equiv 0 \mod p$ for all $\alpha \in \mathfrak{a}$.

Well, for $\alpha \in \mathfrak{a}$,

$$\operatorname{Tr}_{K/\mathbb{Q}}(\alpha) = \operatorname{Tr}_{\mathcal{O}_K/\mathbb{Z}}(\alpha) \equiv \operatorname{Tr}_{(\mathcal{O}_K/(p))/\mathbb{F}_p}(\overline{\alpha}) \mod p.$$

This last trace is the trace of multiplication by $\overline{\alpha}$ on $\mathcal{O}_K/(p)$ as an $\mathbb{F}_p$-linear map, and $\overline{\alpha}$ is a general element of $\mathfrak{a}/(p)$. Since $\mathfrak{a}$ is divisible by every prime ideal factor of (p) (including $\mathfrak{p}$), a higher power of $\mathfrak{a}$ is divisible by (p). Therefore, $\overline{\mathfrak{a}}$ is nilpotent in $\mathcal{O}_K/(p)$, so has trace 0.

Now we want to show $\mathfrak{p}^e \mid \mathcal{D}_K \iff p \mid e$. Write $(p) = \mathfrak{p}^e\mathfrak{b}$ so $\mathfrak{p} \nmid \mathfrak{b}$. Then $\mathfrak{p}^e \mid \mathcal{D}_K$ iff

$$\mathrm{Tr}_{(\mathscr{O}_K/(p))/\mathbb{F}_p}(\overline{\beta}) = 0 \text{ for all } \beta \in \mathfrak{b}.$$

Write $\mathscr{O}_K/(p) \cong \mathscr{O}_K/\mathfrak{p}^e \times \mathscr{O}_K/\mathfrak{b}$ using coprimality. Then,

$$\mathrm{Tr}_{(\mathscr{O}_K/(p))/\mathbb{F}_p}(\overline{x}) = \mathrm{Tr}_{(\mathscr{O}_K/\mathfrak{p}^e)/\mathbb{F}_p}(\overline{x}) + \mathrm{Tr}_{(\mathscr{O}_K/\mathfrak{b})/\mathbb{F}_p}(\overline{x}).$$

Now, for any $y \in \mathscr{O}_K$, there is an $x \in \mathscr{O}_K$ s.t. $x \equiv y \mod \mathfrak{p}^e$ and $x \equiv 0 \mod \mathfrak{b}$ (i.e. $x \in \mathfrak{b}$), so

$$\mathrm{Tr}_{(\mathscr{O}_K/\mathfrak{p}^e)/\mathbb{F}_p}(\overline{y}) = \mathrm{Tr}_{(\mathscr{O}_K/\mathfrak{p}^e)/\mathbb{F}_p}(\overline{x}) = \mathrm{Tr}_{(\mathscr{O}_K/\mathfrak{p}^e)/\mathbb{F}_p}(\overline{x}) + \mathrm{Tr}_{(\mathscr{O}_K/\mathfrak{b})/\mathbb{F}_p}(\overline{x}) = \mathrm{Tr}_{(\mathscr{O}_K/(p))/\mathbb{F}_p}(\overline{x}).$$

Thus, $\mathfrak{p}^e \mid \mathcal{D}_K \iff \mathrm{Tr}_{(\mathscr{O}_K/\mathfrak{p}^e)/\mathbb{F}_p}(\overline{y}) = 0$ for all $y \in \mathscr{O}_K$.

Now, to study the trace down to $\mathbb{F}_p$ of y on $\mathscr{O}_K/\mathfrak{p}^e$, we first filter

$$\mathscr{O}_K/\mathfrak{p}^e \supset \mathfrak{p}/\mathfrak{p}^e \supset \mathfrak{p}^2/\mathfrak{p}^e \supset \cdots \supset \mathfrak{p}^{e-1}/\mathfrak{p}^e \supset \mathfrak{p}^e/\mathfrak{p}^e = 0.$$

Multiplication by y is well defined on each $\mathfrak{p}^i/\mathfrak{p}^e$ (since $\mathfrak{p}^i$ is an ideal), so we can compute the trace

$$\mathrm{Tr}_{(\mathscr{O}_K/\mathfrak{p}^e)/\mathbb{F}_p}(\overline{y}) = \sum_{i=0}^{e-1} \mathrm{Tr}\left(m_y : \mathfrak{p}^i/\mathfrak{p}^{i+1} \to \mathfrak{p}^i/\mathfrak{p}^{i=1}\right).$$

We claim all the traces in the above sum are equal. Fix some $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then, $\pi^i \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$, so $\mathfrak{p}^i = (\pi^i) + \mathfrak{p}^{i+1}$. Therefore, multiplication by π^i gives an $\mathscr{O}_K$-linear iso $\mathscr{O}_K/\mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^i/\mathfrak{p}^{i+1}$ commuting with multiplication by y, so the traces all agree. Thus,

$$\mathrm{Tr}_{(\mathscr{O}_K/\mathfrak{p}^e)/\mathbb{F}_p}(\overline{y}) = e\,\mathrm{Tr}_{(\mathscr{O}_K/\mathfrak{p})/\mathbb{F}_p}(\overline{y})$$

for all $y \in \mathscr{O}_K$. Since $\mathscr{O}_K/\mathfrak{p}$ is a finite field (so separable over $\mathbb{F}_p$), the trace map is not identically 0, so the above vanishes identically iff $e = 0 \in \mathbb{F}_p$, i.e. iff $p \mid e$. ∎

Corollary 3.13. *The prime factors of* $\mathrm{disc}(K)$ *are the primes in* $\mathbb{Q}$ *that ramify in* K*.*

Corollary 3.14. *Write* $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_g^{e_g}$ *for distinct prime ideals* $\mathfrak{p}_i$*, and set* $f_i = f(\mathfrak{p}_i \mid p)$*. If no* e_i *is a multiple of* p*, then the multiplicity of* p *in* $\mathrm{disc}(K)$ *is*

$$(e_1 - 1)f_1 + \cdots + (e_g - 1)f_g = n - (f_1 + \cdots + f_g).$$

If $p \mid e_i$ *for some* i*, then the multiplicity is strictly greater than the above.*

3.1.3 Differentials

Theorem 3.15. *Let* L/K *be an extension of number fields. Then, the different* $\mathcal{D}_{L/K}$ *is the annihilator of* $\Omega_{\mathscr{O}_L/\mathscr{O}_K}$*, i.e. the support of the sheaf of relative differentials for the map* $\operatorname{spec} \mathscr{O}_L \to \operatorname{spec} \mathscr{O}_K$ *of curves.*

Proof. Both the different and the discriminant play nicely with localization, so we may work with an extension $\operatorname{spec} B \to \operatorname{spec} A$ of complete dvrs. In this case, $B = A[x]$ for some $x \in B$ (i.e. B is monogenic), so $\Omega_{B/A}$ is generated by $\mathrm{d}x$, subject to $\mathrm{d}f(x) = 0$, i.e. $f'(x)\mathrm{d}x = 0$, where $f(T) \in A[T]$ is the minimal polynomial of x. Thus, $\mathrm{Ann}(\Omega_{B/A}) = (f'(x))$. At the same time, in this monogenic case, we calculated earlier that $\mathcal{D}_{L/K} = (f'(x))$ so we win. $\blacksquare$

3.2 Cyclotomic Fields

Let ζ_n denote a primitive nth root of unity, so $\mathbb{Q}(\zeta_n) = \mathrm{split}_{\mathbb{Q}}(x^n - 1)$.

Goal. Compute $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ as well as $\mathscr{O}_{\mathbb{Q}(\zeta_n)}$.

We start by observing that all (primitive) nth roots of unity are powers of ζ_n, so we have a natural injection

$$\begin{array}{rccc} a: & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ & \sigma & \longmapsto & a(\sigma) \end{array}$$

characterized by $\sigma(\zeta_n) = \zeta_n^{a(\sigma)}$. In particular, this shows that $\#\,\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \le \varphi(n)$. The first thing we will do is show that this is an equality (so a is a canonical isomorphism).

Suppose $n = mk$ with $(m, k) = 1$. Then $\zeta_m := \zeta_n^k$ is a primitive mth root of unity, so we have extensions

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\zeta_m) \arrow[dr, dash] & & \mathbb{Q}(\zeta_k) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

We claim that $\mathbb{Q}(\zeta_m), \mathbb{Q}(\zeta_k)$ are linearly disjoint, so that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q}).$$

Remark 3.16. I guess first note that $\zeta_m = \zeta_n^k$ and $\zeta_k = \zeta_n^m$, so fixing $x, y \in \mathbb{Z}$ s.t. $xm + yk = 1$, we have $\zeta_n = \zeta_n^{xm+yk} = \zeta_k^x \zeta_m^y$, so $\mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_k) = \mathbb{Q}(\zeta_n)$ as implicitly claimed.

To show that they are linearly disjoint, we will compute $\mathscr{O}_{\mathbb{Q}(\zeta_n)}$ when $n = p^r$ is a prime power, and then show it's ramified only at p, ad if furthermore totally ramified at p. This + a simple induction argument will show that $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_k) = \mathbb{Q}$ when $\gcd(m, k) = 1$. For example, if $m = p^r$ and $k = q^s$, then this intersection will be (totally) ramified at p, q but also unramified at q, p, so it must be $\mathbb{Q}$.

With that said, let's analyze the prime power case.

Claim 3.17. *Fix a prime p, and some $r \ge 1$. Let*

$$\Phi_{p^r}(x) := \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{p^{r-1}(p-1)} + x^{p^{r-1}(p-2)} + \cdots + x^{p^{r-1}} + 1,$$

i.e. $\Phi_{p^r}(x) = \frac{Y^p - 1}{Y - 1}$ *where* $Y = x^{p^{r-1}}$. *Then,* $\Phi_{p^r}(x)$ *is the minimal polynomial of* ζ_{p^r}*, so* a *is an isomorphism by counting.*

Proof. It's obvious that $\Phi_{p^r}(\zeta_{p^r}) = 0$, so only need to show it is irreducible. For this, define

$$f(x) := \Phi_{p^r}(x+1) = \frac{(x+1)^{p^r} - 1}{(x+1)^{p^{r-1}} - 1}.$$

We claim f is irreducible, and specifically, that f is p-Eisenstein. Indeed,

$$f(x) \equiv \frac{x^{p^r}}{x^{p^{r-1}}} \equiv x^{p^r - p^{r-1}} \equiv x^{\varphi(p^r)} \pmod{p},$$

so p divides all of f's coefficients except it's leading one. Furthermore, $f(0) = \Phi_{p^r}(1) = 1+1+\dots+1+1 = p$ is not divisible by p^2, so f is p-Eisenstein as claimed. Thus, $\Phi_{p^r}(x) = f(x-1)$ is irreducible as well, and we win. ∎

Corollary 3.18. *Let $\zeta = \zeta_{p^r}$ and $K = \mathbb{Q}(\zeta)$. Then $\mathbb{Z}[\zeta] \subset \mathscr{O}_K$ is a finite index subgroup.*

We claim that in fact $\mathbb{Z}[\zeta] = \mathscr{O}_K$. To show this, note that we have

$$\operatorname{disc}_{\mathbb{Z}}(\mathbb{Z}[\zeta]) = [\mathscr{O}_K : \mathbb{Z}[\zeta]]^2 \operatorname{disc}_{\mathbb{Z}}(\mathscr{O}_K)$$

so the index $[\mathscr{O}_K : \mathbb{Z}[\zeta]]$ divides $\operatorname{disc}_{\mathbb{Z}}(\mathbb{Z}[\zeta])$. Next observe

Lemma 3.19. $\operatorname{disc}_{\mathbb{Z}}(\mathbb{Z}[\zeta])$ *is $\pm$ a p-power*

Proof. Since it is monogenic, we have

$$\operatorname{disc}_{\mathbb{Z}}(\mathbb{Z}[\zeta]) = (-1)^{\binom{\varphi(p^r)}{2}} \mathrm{N}_{\mathrm{K}/\mathbb{Q}}(f'(\zeta)),$$

where $f(x) = \Phi_{p^r}(x) \in \mathbb{Z}[x]$ is the minimal polynomial of ζ. We have

$$f'(\zeta) = \frac{p^r \zeta^{p^r - 1}(\zeta^{p^{r-1}} - 1) - p^{r-1}(\zeta^{p^r} - 1)\zeta^{p^{r-1}-1}}{(\zeta^{p^{r-1}} - 1)^2} = \frac{p^r \zeta^{-1}}{\zeta_p - 1},$$

where $\zeta_p := \zeta^{p^{r-1}}$ is a primitive pth root of unity. Note that $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\zeta^{-1}) = \pm 1$ since $\zeta^{-1} \in \mathbb{Z}[\zeta]^\times \subset \mathscr{O}_K^\times$ so $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(f'(\zeta)) = \pm p^{r\varphi(p^r)} / \mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\zeta_p - 1)$ is a $\pm$ a p-power as $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\zeta_p - 1) \in \mathbb{Z}$. Technically, this completes the proof.

We can do better though. First observe that

$$\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\zeta_p - 1) = \mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\mathrm{N}_{K/\mathbb{Q}(\zeta_p)}(\zeta_p - 1)) = \mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1)^{[K:\mathbb{Q}(\zeta_p)]} = \mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1)^{\varphi(p^r)/\varphi(p)} = \mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1)^{p^{r-1}}.$$

Next we observe that the minimal polynomial of ζ_p is

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1 = \prod_{a=1}^{p-1}(x - \zeta_p^a),$$

so

$$\mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1) = \prod_{a=1}^{p-1}(\zeta_p^a - 1) = (-1)^{p-1}\prod_{a=1}^{p-1}(1 - \zeta_p^a) = (-1)^{p-1}\Phi_p(1) = (-1)^{p-1}p \implies \mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\zeta_p - 1) = (-1)^{\varphi(p^r)}p^{p^{r-1}}$$

(note that this sign is +1 unless $p = 2$ and $r = 1$, but that case is dumb so it's +1 always). Hence, we see that

$$\operatorname{disc}_{\mathbb{Z}}(\mathbb{Z}[\zeta]) = \pm p^{p^{r-1}(pr-r-1)}.$$

This only leaves the sign which is $(-1)^{\binom{\varphi(p^r)}{2}}$ times

$$\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\zeta^{-1}) = \prod_{a \in (\mathbb{Z}/p^r\mathbb{Z})^\times} \zeta^a = (-1)^{\# \deg \Phi_{p^r}} \Phi_{p^r}(0) = (-1)^{\varphi(p^r)}.$$

The upshot is that (even when $p^r = 2$!), we see that

$$\operatorname{disc}_{\mathbb{Z}}(\mathbb{Z}[\zeta]) = (-1)^{\binom{\varphi(p^r)}{2}} p^{p^{r-1}(pr-r-1)}.$$

■

Corollary 3.20. *$\operatorname{disc}_{\mathbb{Z}}(\mathscr{O}_K)$ is $\pm$ a p-power, so p is the only ramified prime in $\mathscr{O}_K$. Furthermore, p is totally ramified, with $(p) = (1-\zeta)^{\varphi(p^r)}$.*

Proof. The first part follows from the lemma + the fact that $\operatorname{disc}_{\mathbb{Z}}(\mathscr{O}_K) \mid \operatorname{disc}_{\mathbb{Z}}(\mathbb{Z}[\zeta])$. For the latter part, first note that

$$\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(1-\zeta) = \prod_{a \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (1-\zeta^a) = \Phi_{p^r}(1) = p,$$

so the ideal $\mathfrak{p} := (1-\zeta) \subset \mathscr{O}_K$ has norm p, i.e. $\mathscr{O}_K/\mathfrak{p} = \mathbb{F}_p$. Thus, (p) factors as $(p) = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_g$ with each $f(\mathfrak{p}_i \mid \mathfrak{p}) = 1$ for all i. Hence, it suffices to show that $g = 1$, i.e. that $\mathscr{O}_K/(p)$ has a unique prime. From the above, we in fact see that

$$\prod_{a \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (1-\zeta^a) = (p)$$

as ideals in $\mathscr{O}_K$. Thus, it suffices to show that $(1-\zeta^a) = (1-\zeta)$, i.e that $\frac{1-\zeta}{1-\zeta^a} \in \mathscr{O}_K^\times$. For this we observe that

$$\frac{1-\zeta^a}{1-\zeta} = \zeta^{a-1} + \zeta^{a-2} + \cdots + \zeta + 1 \in \mathscr{O}_K.$$

Similarly, fixing b so that $ab \equiv 1 \pmod{p^r}$ and letting $\omega := \zeta^a$, we see that

$$\frac{1-\zeta}{1-\zeta^a} = \frac{1-\zeta^{ab}}{1-\zeta^a} = \frac{1-\omega^b}{1-\omega} = \omega^{b-1} + \omega^{b-2} + \cdots + \omega + 1 \in \mathscr{O}_K,$$

so we win. ■

Lemma 3.21. $(1/p)\mathbb{Z}[\zeta] \cap \mathscr{O}_K = \mathbb{Z}[\zeta]$

Proof. It suffices to show that $\mathbb{Z}[\zeta] \cap p\mathscr{O}_K = p\mathbb{Z}[\zeta]$. For this, note that $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta - 1]$, and write any $x \in \mathbb{Z}[\zeta] \cap p\mathscr{O}_K$ as

$$x = c_0 + c_1(\zeta-1) + c_2(\zeta-1)^2 + \cdots + c_d(\zeta-1)^d \text{ where } d = \varphi(p^r) - 1.$$

First observe that

$$c_0 = x - (\zeta-1)(c_1 + c_2(\zeta-1) + \cdots + c_d(\zeta-1)^{d-1}) \in (p\mathscr{O}_K + (\zeta-1)\mathbb{Z}[\zeta]) \cap \mathbb{Z} = p\mathbb{Z} \subset p\mathbb{Z}[\zeta].$$

Thus, we may as well assume $c_0 = 0$. Inductively, suppose we may as well assume $c_0 = c_1 = \cdots = c_k = 0$. Then,

$$c_{k+1}(\zeta-1)^{k+1} = x - c_{k+2}(\zeta-1)^{k+2} + \cdots + c_d(\zeta-1)^d.$$

Since $x \in p\mathscr{O}_K = (\zeta-1)^{d+1}\mathscr{O}_K$ (and since $k+1 \le d$), we can divide above to get

$$c_{k+1} = \frac{x}{(\zeta-1)^{k+1}} + (\zeta-1)(c_{k+2} + \cdots + c_d(\zeta-1)^{d-(k+2)}) \in \left((\zeta-1)^{d-k}\mathscr{O}_K + (\zeta-1)\mathbb{Z}[\zeta]\right) \cap \mathbb{Z} = p\mathbb{Z}.$$

Thus, $p \mid c_i$ for all i, so $x \in p\mathbb{Z}[\zeta]$. ■

Corollary 3.22. $\mathscr{O}_K = \mathbb{Z}[\zeta]$

Proof. We know $[\mathscr{O}_K : \mathbb{Z}[\zeta]]$ is a p-power, so $\mathscr{O}_K \subset \frac{1}{p^N}\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta]$ for some $N > 0$. ■

What about general n? Since we understanding ramification in $\mathbb{Q}(\zeta_{p^r})$, we can now conclude that $a : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism is general by inducting with diamonds

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_m) \arrow[dr, dash] & & \mathbb{Q}(\zeta_k) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

where $\gcd(m,k) = 1$ and $n = mk$. This computes the Galois group. For the ring of integers, we use the following fact.

Proposition 3.23. *Let $K, K'/\mathbb{Q}$ be linearly disjoint number fields with compositum $F = KK'$. If* $\gcd(\operatorname{disc} K, \operatorname{disc} K') = 1$*, then*

(1) $\mathscr{O}_F = \mathscr{O}_K\mathscr{O}_{K'}$*; and*

(2) $\operatorname{disc} F = (\operatorname{disc} K)^{[F:K]}(\operatorname{disc} K')^{[F:K']}$.

Proof. First note that $\mathrm{Tr}_{F/K'}|_K = \mathrm{Tr}_{K/\mathbb{Q}}$. Indeed, if $\{e_i\}$ is a $\mathbb{Q}$-basis for K, then it is also a K'-basis for F, and multiplication by α has the same matrix, whether viewed as a map $F \to F$ or $K \to K$. To show **(1)**, we show that $[\mathscr{O}_F : \mathscr{O}_K\mathscr{O}_{K'}] \mid \operatorname{disc} K$ (by symmetry, it also divides $\operatorname{disc} K'$ and so must be 1). That is, for $\alpha \in \mathscr{O}_F$, we will show that

$$\alpha \in \frac{1}{\operatorname{disc} K}\mathscr{O}_K\mathscr{O}_{K'}.$$

Write $\alpha = \sum_i c_i' e_i$ (with $e_i \in \mathscr{O}_K$ a $\mathbb{Q}$-basis for K, and $c_i' \in K'$). It will suffice to show $c_i' \in \frac{1}{\operatorname{disc} K}\mathscr{O}_{K'}$. We can control denominators via trace (think to how one shoes $\mathscr{O}_K$ is $\mathbb{Z}$-finite); observe that

$$\begin{pmatrix} \mathrm{Tr}_{F/K'}(\alpha e_1) \\ \vdots \\ \mathrm{Tr}_{F/K'}(\alpha e_m) \end{pmatrix} = \underbrace{\left(\mathrm{Tr}_{F/K'}(e_ie_j)\right)_{i,j=1}^m}_{M} \begin{pmatrix} c_1' \\ \vdots \\ c_m' \end{pmatrix} \quad \text{where } m = [F:K'] = [K:\mathbb{Q}].$$

Note above that $\alpha e_i \in \mathscr{O}_F \implies \mathrm{Tr}_{F/K'}(\alpha e_1) \in \mathscr{O}_{K'}$ and that $e_i e_j \in \mathscr{O}_K \implies \mathrm{Tr}_{F/K'}(e_i e_j) = \mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j)$. Cramer's formula tells us that $M^{-1} = \frac{1}{\det M} M'$ for some $M' \in \mathrm{GL}_m(\mathbb{Z})$, so we conclude that

$$\begin{pmatrix} c_1' \\ \vdots \\ c_m' \end{pmatrix} \in M^{-1} \cdot \mathscr{O}_{K'}^m = \frac{1}{\det M} M' \cdot \mathscr{O}_{K'}^m = \frac{1}{\operatorname{disc}(K/\mathbb{Q})} \cdot \mathscr{O}_{K'}^m,$$

which proves **(1)**.

What about **(2)**? Picking bases for $\mathscr{O}_K$ and $\mathscr{O}_{K'}$ and taking the composite basis for $\mathscr{O}_F = \mathscr{O}_K \mathscr{O}_{K'}$, this boils down to the fact that if $T : V \to V$ and $S : W \to W$ are (invertible) linear transformations, then

$$\det(T \otimes S) = (\det T)^{\dim W} (\det S)^{\dim V}$$

as can be seen e.g. by considering eigenvalues. ■

3.3 Class Groups

3.3.1 S-integers

3.3.2 Calculations

Theorem 3.24. *Let K be a number field, and write $n = r_1 + 2r_2$ with the usual meanings. Define* ***Minkowski's constant***

$$\lambda_K := \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\operatorname{disc} K|}.$$

Each element of $\mathrm{Cl}(K)$ is the ideal class $[\mathfrak{a}]$ of a nonzero ideal $\mathfrak{a} \subset \mathscr{O}_K$ such that $N(\mathfrak{a}) \le \lambda_K$.

Corollary 3.25. *$\mathrm{Cl}(K)$ is generated by the classes $[\mathfrak{p}]$ for the finitely many primes $\mathfrak{p}$ over the finitely many primes $p \in \mathbb{Z}^+$ s.t. $p \le \lambda_K$.*

Example. Say $K = \mathbb{Q}(\sqrt{d})$ for some squarefree $d \in \mathbb{Z} \setminus \{0, 1\}$.

(1) If $d > 0$, then $(r_1, r_2) = (2, 0)$, so

$$\lambda_K = \begin{cases} \dfrac{2!}{2^2}\left(\dfrac{4}{\pi}\right)^0 \sqrt{d} = \dfrac{\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \\ \dfrac{2!}{2^2}\left(\dfrac{4}{\pi}\right)^0 \sqrt{4d} = \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

(2) If $d < 0$, then $(r_1, r_2) = (0, 1)$, so

$$\lambda_K = \begin{cases} \dfrac{2!}{2^2}\left(\dfrac{4}{\pi}\right)^1 \sqrt{|d|} = \dfrac{2\sqrt{|d|}}{\pi} & \text{if } d \equiv 1 \pmod 4 \\ \dfrac{2!}{2^2}\left(\dfrac{4}{\pi}\right)^1 \sqrt{4\,|d|} = \dfrac{4\sqrt{|d|}}{\pi} & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

In particular, $\lambda_K < 2$ precisely when

$$d \in \{5, 13\} \cup \{2, 3\} \cup \{-3, -7\} \cup \{-1, -2\},$$

so all those number fields have trivial class group. These are not all quadratic number fields with trivial class group though.

Example. Say $K = \mathbb{Q}(\sqrt{-14})$. We want to show that $\mathrm{Cl}(K) \simeq \mathbb{Z}/4\mathbb{Z}$, generated by either prime above 3.

We have $(n, r_1, r_2) = (2, 0, 1)$ and $\operatorname{disc} K = 4(-14) = -56$, so Minkowski's constnat is $\lambda_K \approx -4.764\ldots$. In particular, $\mathrm{Cl}(K)$ is generated by the classes of primes above $2, 3$. Note that $\mathscr{O}_K = \mathbb{Z}[\sqrt{-14}] = \mathbb{Z}[x]/(x^2+14)$. We see

$$x^2 + 14 \equiv x^2 \pmod 2 \text{ and } x^2 + 14 \equiv x^2 - 1 \equiv (x-1)(x+1) \pmod 3,$$

so we have $2\mathscr{O}_K = \mathfrak{p}_2^2$ while $3\mathscr{O}_K = \mathfrak{p}_3\mathfrak{p}_3'$ where

$$\mathfrak{p}_2 = (2, \sqrt{-14}),\ \ \mathfrak{p}_3 = (3, \sqrt{-14} - 1),\ \text{ and }\ \mathfrak{p}_3' = (3, \sqrt{-14} + 1).$$

In particular, $[\mathfrak{p}_2]^2 = 0 \in \mathrm{Cl}(K)$ and $[\mathfrak{p}_3][\mathfrak{p}_3'] = 0 \in \mathrm{Cl}(K)$, so $\mathrm{Cl}(K)$ is generated by the 2-torsion $[\mathfrak{p}_2]$ and the element $[\mathfrak{p}_3]$.

Let's first check if $[\mathfrak{p}_2]$ has order 1 or 2. If $[\mathfrak{p}_2] = 1 \in \mathrm{Cl}(K)$, then $\mathfrak{p}_2 = (\alpha)$ for some $\alpha \in \mathscr{O}_K$ with $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\alpha) = \pm 2$. Writing $\alpha = u + v\sqrt{-14}$, we need $2 = \mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\alpha) = u^2 + 14v^2$, but this is clearly impossible. Thus, $[\mathfrak{p}_2] \neq 1 \in \mathrm{Cl}(K)$ and so has order exactly 2.

What about $[\mathfrak{p}_3]$? The key idea is to look for elements of norm divisibly by $2, 3$ to get relations involving $\mathfrak{p}_2, \mathfrak{p}_3$. Note that $N(1 + \sqrt{-14}) = 15 = 3 \cdot 5$ and $N(2 + \sqrt{-14}) = 18 = 2 \cdot 3^2$. Therefore, for some prime $\mathfrak{p}_5$ above 5, we have

$$(1 + \sqrt{-14}) = \mathfrak{p}_5\mathfrak{p}_3 \text{ or } \mathfrak{p}_5\mathfrak{p}_3' \text{ and } (2 + \sqrt{-14}) = \mathfrak{p}_2\mathfrak{p}_3^2 \text{ or } \mathfrak{p}_2\mathfrak{p}_3'^2 \text{ or } \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'.$$

Since $\mathfrak{p}_3\mathfrak{p}_3' = (3) \nmid (2 + \sqrt{-14})$, we can rule out the last case above. Thus, we see that $(2 + \sqrt{-14}) = \mathfrak{p}_2\mathfrak{p}_3^2$. Hence, $[\mathfrak{p}_2] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_3]^2 \in \mathrm{Cl}(K)$, so $[\mathfrak{p}_3]^2 \neq 1 \in \mathrm{Cl}(K)$ but $[\mathfrak{p}_3]^4 = [\mathfrak{p}_2]^2 = 1 \in \mathrm{Cl}(K)$, so $[\mathfrak{p}_3]$ has order exactly 4 and generates $\mathrm{Cl}(K)$, i.e. $\mathrm{Cl}(K) = \langle [\mathfrak{p}_3] \rangle \cong \mathbb{Z}/4\mathbb{Z}$.

Example. Say $K = \mathbb{Q}(\sqrt{-65})$, so $\mathscr{O}_K = \mathbb{Z}[\sqrt{-65}]$. We claim $\mathrm{Cl}(K) = (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

The Minkowski constant is $\lambda_K = \frac{4}{\pi}\sqrt{65} \sim 10.26$, so we need to look a primes above $2, 3, 5, 7$. We first factor

$$\begin{aligned}
x^2 + 65 &\equiv x^2 + 1 \equiv (x+1)^2 && \pmod 2 \implies (2) = \mathfrak{p}_2^2 \\
x^2 + 65 &\equiv x^2 + 2 \equiv (x+1)(x-1) && \pmod 3 \implies (3) = \mathfrak{p}_3\mathfrak{p}_3' \\
x^2 + 65 &\equiv x^2 && \pmod 5 \implies (5) = \mathfrak{p}_5^2 \\
x^2 + 65 &\equiv x^2 + 2 && \pmod 7 \implies (7) = \mathfrak{p}_7
\end{aligned}$$

Thus, $[\mathfrak{p}_7] = 1 \in \mathrm{Cl}(K)$ while $\mathfrak{p}_2, \mathfrak{p}_5$ are both 2-torsion. Note that $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5$ are all not principal, since you cannot write $2, 3$ or 5 in the form $u^2 + 65v^2$ for $u, v \in \mathbb{Z}$. To find some relations, let's compute $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(a + \sqrt{-65})$ for some small values of a, and hope we get lucky.

Trying $a = 4, 5$ gives $N(4 + \sqrt{-65}) = 81 = 3^4$ and $N(5 + \sqrt{-65}) = 90 = 2 \cdot 3^2 \cdot 5$. Therefore, $\mathfrak{p}_3$ is 4-torsion (we know $(4 + \sqrt{-65}) = \mathfrak{p}_3^4$ or $\mathfrak{p}_3'^4$ since $\mathfrak{p}_3\mathfrak{p}_3' = (3) \nmid (4 + \sqrt{-65})$). Relabeling if necessary, we may write $(4+\sqrt{-65})=\mathfrak{p}_3^4$. Since $(4+\sqrt{-65})$ is coprime to $(5+\sqrt{-65})$ and $3\nmid(5+\sqrt{-65})$, we then conclude that $(5+\sqrt{-65})=\mathfrak{p}_2\mathfrak{p}_3'^2\mathfrak{p}_5$. Therefore,

$$1=[\mathfrak{p}_2][\mathfrak{p}_3']^2[\mathfrak{p}_5]=[\mathfrak{p}_2][\mathfrak{p}_3]^{-2}[\mathfrak{p}_5]=[\mathfrak{p}_2][\mathfrak{p}_3]^2[\mathfrak{p}_5]\in\mathrm{Cl}(K),$$

so $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2],[\mathfrak{p}_3]$.

Next, we claim $[\mathfrak{p}_3]$ has order exactly 4. In order to have $\mathfrak{p}_3^2=(\alpha)$, we need $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\alpha)=9$, but this is only possible if $\alpha=\pm3$, but 3 is not ramified as we checked earlier. Hence, $[\mathfrak{p}_3]^2\neq1\in\mathrm{Cl}(K)$. This gives a surjection

$$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\twoheadrightarrow\mathrm{Cl}(K).$$

This is injective unless $\mathrm{Cl}(K)=\langle[\mathfrak{p}_3]\rangle$, but that would force $[\mathfrak{p}_3]^2=[\mathfrak{p}_2]$. In this case, $[\mathfrak{p}_2][\mathfrak{p}_3]^2=[\mathfrak{p}_3]^4=1\in\mathrm{Cl}(K)$ so there's some $\alpha=u+v\sqrt{-65}$ with $\mathfrak{p}_2\mathfrak{p}_3^2=(\alpha)$. In particular,

$$18=\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\alpha)=u^2+65v^2.$$

This is impossible. Thus, $\mathrm{Cl}(K)\simeq\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Example. Now say $K=\mathbb{Q}(\sqrt{82})$ is real quadratic, so $\mathscr{O}_K=\mathbb{Z}[\sqrt{82}]$. We have $(n,r_1,r_2)=(2,2,0)$ and $\operatorname{Disc}K=4(82)=328$, so

$$\lambda_K=\frac{2!}{2^2}\left(\frac{4}{\pi}\right)^0\sqrt{328}\sim9.055.$$

Hence, $\mathrm{Cl}(K)$ is generated by primes above $2,3,5,7$. One quickly checks that

$$(2)=\mathfrak{p}_2^2,\;\;(3)=\mathfrak{p}_3\mathfrak{p}_3',\;\;(5)=\mathfrak{p}_5,\;\;\text{and}\;\;(7)=\mathfrak{p}_7,$$

so $\mathrm{Cl}(K)$ is generated by $\mathfrak{p}_2,\mathfrak{p}_3$.

Now we compute small norms $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(a+\sqrt{82})=a^2-82$. Taking $a=10$ shows that $(10+\sqrt{82})=\mathfrak{p}_2\mathfrak{p}_3^2$ (not divisibly by $(3)=\mathfrak{p}_3\mathfrak{p}_3'$), possibly after rearrangement. Thus, $[\mathfrak{p}_3]^2=[\mathfrak{p}_2]^{-1}=[\mathfrak{p}_2]$, so $\mathrm{Cl}(K)$ is cyclic, generated by $[\mathfrak{p}_3]$ (which we now see is 4-torsion). We wish to show that it has order exactly 4, i.e. that $[\mathfrak{p}_2]$ is nontrivial.

Say $\mathfrak{p}_2=(\alpha)$ for some $\alpha=u+v\sqrt{82}\in\mathbb{Z}[\sqrt{82}]=\mathscr{O}_K$. Then,

$$2=N(\mathfrak{p}_2)=\left|\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\alpha)\right|\implies u^2-82v^2=\pm2.$$

Thus, we wish to show $x^2-82y^2=\pm2$ has no solutions over $\mathbb{Z}$. We take for granted that $\mathscr{O}_K^\times$ has fundamental unit $\varepsilon:=9+\sqrt{82}$ and note that $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\varepsilon)=-1$.

Now, note that $(\alpha^2)=(\alpha)^2=\mathfrak{p}_2^2=(2)$, so $\alpha^2=2u$ for some unit $u\in\mathscr{O}_K^\times$. Taking norms, we see that

$$4\,\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(u)=\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(2u)=\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\alpha^2)=\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\alpha)^2=4\implies\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(u)=1,$$

so $u=\pm\varepsilon^{2k}$ for some k. In particular, $\pm2=(\varepsilon^{-k}z)^2$ is a square. Thus, it suffices to show that neither of ±2 is a square in $\mathscr{O}_K$. For $a,b\in\mathbb{Z}$, we have

$$(a+b\sqrt{82})^2=(a^2+82b^2)+2ab\sqrt{82}.$$

This can't be -2 since the coefficient of 1 is always positive. It also can't be $+2$ since that would force $b = 0$ and 2 is not a square in the rational integers.

Exercises These are from Conrad classes.

Problem 3.1 (248A HW9 Prob. 2)**.** *Say $K = \mathbb{Q}(\alpha)$ where $\alpha^5 - \alpha + 1 = 0$. We will show* $\mathrm{Cl}(K) = 1$.

Proof. We first want to compute $\mathscr{O}_K$. For this, we note that

$$\mathrm{disc}(\mathbb{Z}[\alpha]/\mathbb{Z}) = \pm\,\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(f'(\alpha)) = \mathrm{N}_{\mathrm{K}/\mathbb{Q}}(5\alpha^4 - 1) = \pm 2869 = \pm 19 \cdot 151$$

is square-free, and so conclude that $\mathbb{Z}[\alpha] = \mathscr{O}_K$. Now, let's compute the Minkowski bound. We have $(n, r_1, r_2) = (5, 1, 2)$, so

$$\lambda_K = \frac{5!}{5^5}\left(\frac{4}{\pi}\right)^2\sqrt{2869} \sim 3.334$$

so $\mathrm{Cl}(K)$ is generated by primes above $2, 3$. Next, we factor

$$\begin{aligned} x^5 - x + 1 &\equiv (x^2 + x + 1)(x^3 + x^2 + 1) \pmod 2 \implies (2) = \mathfrak{p}_2\mathfrak{p}_2' \\ x^5 - x + 1 &\equiv x^5 + 2x + 1 \pmod 3 \implies (3) = \mathfrak{p}_3 \end{aligned}$$

Thus, $\mathrm{Cl}(K)$ is cyclic, generated by $\mathfrak{p}_2$. Actually, we can say more. $\mathrm{Cl}(K)$ is generated by primes ideals $\mathfrak{p}$ with norm $N(\mathfrak{p}) \le \lambda_K$. However, we see from the above that $N(\mathfrak{p}_3) = 3^5 > \lambda_K$ and $N(\mathfrak{p}_2) = 2^2 > \lambda_K$ and $N(\mathfrak{p}_2') = 2^3 > \lambda_K$, so $\mathrm{Cl}(K)$ has no prime ideals with norm $\le \lambda_K$. Thus, it's generated by the empty set, which is to say, $\mathrm{Cl}(K) = 1$. ∎

3.4 Group Cohomology

3.4.1 Inflation-restriction

Proposition 3.26. *Let $H \triangleleft G$ (both finite, or at least H of finite index), and let A be a G-module. Then, there is an exact sequence*

$$0 \longrightarrow \mathrm{H}^1(G/H, A^H) \longrightarrow \mathrm{H}^1(G, A) \longrightarrow \mathrm{H}^1(H, A).$$

Direct verification on cochains.

Proposition 3.27. *Fix $q \ge 1$. If $\mathrm{H}^i(H, A) = 0$ for $1 \le i \le q - 1$, then*

$$0 \longrightarrow \mathrm{H}^q(G/H, A^H) \longrightarrow \mathrm{H}^q(G, A) \longrightarrow \mathrm{H}^q(H, A)$$

is exact, and so

$$\mathrm{H}^i(G/H, A^H) \simeq \mathrm{H}^i(G, A) \ \textit{for}\ 1 \le i \le q - 1.$$

Example. Let E/F be a Galois extension containing a Galois extension K/F. Let $G = \mathrm{Gal}(E/F)$ and $H = \mathrm{Gal}(E/K) \triangleleft G$. Hence, $G/H \simeq \mathrm{Gal}(K/F)$. Hilbert 90 says that $\mathrm{H}^1(\mathrm{Gal}(E/K), E^\times) = 0$, so we get an exact sequence

$$0 \longrightarrow \mathrm{H}^2(\mathrm{Gal}(K/F), K^\times) \longrightarrow \mathrm{H}^2(\mathrm{Gal}(E/F), E^\times) \longrightarrow \mathrm{H}^2(\mathrm{Gal}(E/K), E^\times)$$

Taking a direct limit over Galoi extensions E/K, we obtain the exact sequence

$$0 \longrightarrow \mathrm{H}^2(\mathrm{Gal}(K/F), K^\times) \longrightarrow \mathrm{Br}(F) \longrightarrow \mathrm{Br}(K)$$

involving Brauer groups $\mathrm{Br}(F) = \mathrm{H}^2(\mathrm{Gal}(\overline{F}/F), \overline{F}^\times)$.

3.5 Artin-Schreier Theory

Let's understand p-power cyclic extension in characteristic p. Actually, we'll only look at $\mathbb{F}_p$-extensions, but same difference. Fix some field k with $\operatorname{char} k = p > 0$. We then have the following exact sequence

$$0 \longrightarrow \underline{\mathbb{F}}_p \longrightarrow \mathbb{G}_a \xrightarrow{x \mapsto x^p - x} \mathbb{G}_a \longrightarrow 0$$

(equivalently, $0 \to \mathbb{F}_p \to \overline{k} \xrightarrow{x \mapsto x^p - x} \overline{k} \to 0$). In cohomology, this gives

$$0 \longrightarrow \mathbb{F}_p \longrightarrow k \xrightarrow{x^p - x} k \xrightarrow{\delta} \mathrm{Hom}(G_k, \mathbb{F}_p) \longrightarrow \mathrm{H}^1(G_k, \overline{k}) = 0.$$

Remark 3.28. Why does $\mathrm{H}^1(G_k, \overline{k}) = 0$ above? Say L/k is a finite Galois extension. The **normal basis theorem** (see e.g. here) says that there is some $\alpha \in L$ so that L has a k-basis of the form $\{\sigma(\alpha)\}_{\sigma \in \mathrm{Gal}(L/k)}$. In other words, we have a G_k-module isomorphism

$$\begin{array}{ccc} k[G_k] & \longrightarrow & L \\ e_\sigma & \longmapsto & \sigma(\alpha), \end{array}$$

so $L \simeq \mathrm{Hom}_k(k[G_k], k)$ is (co-)induced and hence has trivial cohomology. In particular, $\mathrm{H}^1(G_k, L) = 0$. Now take (direct) limits.

Alternatively,

$$\mathrm{H}^1(G_k, \overline{k}) = \mathrm{H}^1(\operatorname{spec} k_{\text{ét}}, \mathbb{G}_a) = \mathrm{H}^1(\operatorname{spec} k_{\text{ét}}, \mathscr{O}_k^{\text{ét}}) = \mathrm{H}^1(\operatorname{spec} k, \mathscr{O}_k) = 0$$

since coherent sheaf cohomology vanishes for affine schemes.

Returning to the problem at hand, we see that

$$\mathrm{Hom}(G_k, \mathbb{F}_p) \simeq \operatorname{coker}\left(k \xrightarrow{x \mapsto x^p - x} k\right).$$

In particular,

$$\left\{\begin{array}{c} \mathbb{F}_p\text{-extensions} \\ \text{of } k \end{array}\right\} \simeq \mathrm{Sur}(G_k, \mathbb{F}_p) \simeq \text{nonzero elements of } \operatorname{coker}\left(k \xrightarrow{x^p - x} k\right) =: Q.$$

Let's say I choose some $t \in k$ representing some nonzero $[t] \in Q$. What's the corresponding extension k_t/k? First note that the boundary map $\delta : k \to \mathrm{Hom}(G_k, \mathbb{F}_p)$ from before sends $s \in k$ to

$$\delta(s)(\sigma) = \sigma(\beta) - \beta \text{ with } \beta \in \overline{k} \text{ satisfying } \beta^p - \beta = s.$$

For peace of mind, note that if β' is another choice of β, then $\beta' - \beta \in \mathbb{F}_p$, so $\sigma(\beta') - \beta' = \sigma(\beta + a) - (\beta + a) =$

$\sigma(\beta) - \beta$ for some $a = \beta' - \beta \in \mathbb{F}_p$. Now that we have the homomorphism $G_k \to \mathbb{F}_p$ corresponding to t, we claim that the $\mathbb{F}_p$-extension is $k_t = k(\alpha)$ where α is a root of $x^p - x - t \in k[x]$. That is, we claim

$$k(\alpha) = \overline{k}^{\ker \delta(t)} =: k_t.$$

The containment $k(\alpha) \subset \overline{k}^{\ker \delta(t)}$ is obvious. To show equality, we compare degrees. Note that $[k_t : k] = [G_k : \ker \delta(t)] = \#\mathbb{F}_p = p$.

At this point, we're done since p is prime and $k(\alpha) \neq k$. However, we really also want to allow for $\mathbb{F}_q$ extensions with q a p-power, so we continue with an argument that works in that case too

Actually, I guess there's no need to compare degrees. We know exactly how $\mathrm{Gal}(k_t/k)$ acts on $k(\alpha)$. By construction, we have an isomorphism $\delta(t) : \mathrm{Gal}(k_t/k) \xrightarrow{\sim} \mathbb{F}_p$ defined by the fact that, for any root β of $x^p - x = t$, we have $\sigma(\beta) = \beta + \delta(t)(\sigma)$ for all $\sigma \in \mathrm{Gal}(k_t/k)$. In particular, $\sigma(\alpha) = \alpha + \delta(t)(\sigma)$, so $\sigma|_{k(\alpha)} = \mathrm{id} \implies \sigma = 1$. That is, $\mathrm{Gal}(k_t/k) \xrightarrow{\sim} \mathrm{Gal}(k(\alpha)/k)$, so $k_t = k(\alpha)$.

3.6 Class Field Theory

4 Algebraic Topology

4.1 Poincaré Duality

Following Haynes' notes.

4.1.1 Cap product

Given a space X, we let $S^p(X)$ denote its space of singular p-cochains, and similarly for $S_p(X)$.

Remark 4.1. One can form the composite

$$\cap : S^p(X) \otimes S_n(X) \xrightarrow{1\times(\alpha\circ\Delta_*)} S^p(X) \otimes S_p(X) \otimes S_{n-p}(X) \xrightarrow{\langle -,-\rangle\otimes 1} S_{n-p}(X).$$

Above, α is the Alexander-Whitney map. More concretely,

$$\beta \cap \sigma = \beta(\sigma \circ \alpha_p) \cdot (\sigma \circ \omega_q)$$

We evaluate the cochain on part of the chain, leaving a lower dimensional chain remaining.

The composite above is a chain map so induces a **cap product**

$$\frown = \cap : \mathrm{H}^p(X) \otimes \mathrm{H}_n(X) \to \mathrm{H}_{n-p}(X)$$

is homology.

Proposition 4.2. *The cap products satisfies the following*

(1) $(a \cup b) \cap x = a \cap (b \cap x)$ *and* $1 \cap x = x$*. That is,* $\mathrm{H}_*(X)$ *is an* $\mathrm{H}^*(X)$*-module.*

(2) *Given a map* $f : X \to Y$*,* $b \in \mathrm{H}^p(Y)$ *and* $x \in \mathrm{H}_n(X)$*,*

$$f_*(f^*(b) \cap x) = b \cap f_*(x).$$

(projection formula)

(3) *Let* $\varepsilon : \mathrm{H}_*(X) \to \mathrm{H}_*(*) = R$ *be the augmentation. Then,*

$$\varepsilon(b \cap x) = \langle b, x\rangle .$$

(4) *Cap and cup are adjoint:*

$$\langle a \cup b, x\rangle = \langle a, b \cap x\rangle .$$

Proof. **(2)** Let β be a cocycle representing b, and σ an n-simplex in X. Then,

$$\begin{aligned} f_*(f^*(\beta) \cap \sigma) &= f_*\left(f^*(\beta)(\sigma \circ \alpha_p) \cdot (\sigma \circ \omega_q)\right) \\ &= f_*\left(\beta(f \circ \sigma \circ \alpha_p) \cdot (\sigma \circ \omega_q)\right) \\ &= \beta(f \circ \sigma \circ \alpha_p) \cdot f_*(\sigma \circ \omega_q) \\ &= \beta(f \circ \sigma \circ \alpha_p) \cdot (f \circ \sigma \circ \omega_q) \end{aligned}$$

$$= \beta \cap f_*(\sigma)$$

(3) Get 0 unless $p = n$. This case is easy. **(4)** Let α, β be cocycles representing a, b ($|a| = p, |b| = q, p + q = n$), and let σ be an n-simplex in X. Then,

$$\langle \alpha \cup \beta, \sigma \rangle = (-1)^{pq} \alpha(\sigma \circ \alpha_p) \beta(\sigma \circ \omega_q) \text{ while } \langle \alpha, \beta \cap \sigma \rangle = \alpha(\sigma \circ \omega_p) \beta(\sigma \circ \alpha_q).$$

Thus, we win by (graded) commutativity of the cup product on H^*. ■

Our goal is to prove the following.

Theorem 4.3 (**Poincaré duality**). *Let M be a topological n-manifold that is compact and oriented w.r.t a PID R. Then there is a unique class $[M] \in \mathrm{H}_n(M; R)$ that restricts to the orientaion class in $\mathrm{H}_n(M, M - a; R)$ for every $a \in M$. It has the property that*

$$- \cap [M] : \mathrm{H}^p(M; R) \to \mathrm{H}_{n-p}(M; R)$$

is an isomorphism for all p.

The proof will be an inductive argument proving a substantially more general theorem involving relative homology and cohomology. Hence, we first form a relative cap product. Note that $0 \to S_n(A) \to S_n(X) \to S_n(X, A) \to 0$ is split and so remains exact after any tensor product (e.g. when tensored with the non-free $S^p(X)$). Thus, we get a diagram ($Ai : A \hookrightarrow X$)

$$\begin{tikzcd}
0 \arrow[r] & S^p(X) \otimes S_n(A) \arrow[r, "1 \otimes i_*"] \arrow[d, "i^* \otimes 1"] & S^p(X) \otimes S_n(X) \arrow[r] \arrow[dd, "\cap"] & S^p(X) \otimes S_n(X, A) \arrow[r] \arrow[dd, dashed, "\cap"] & 0 \\
& S^p(A) \otimes S_n(A) \arrow[d, "\cap"] & & & \\
0 \arrow[r] & S_q(A) \arrow[r, "i^*"] & S_q(X) \arrow[r] & S_q(X, A) \arrow[r] & 0
\end{tikzcd}$$

This commutes by the projection formula, so the dashed map exists, yielding the **relative cap product**

$$\cap : \mathrm{H}^p(X) \otimes \mathrm{H}_n(X, A) \to \mathrm{H}_q(X, A).$$

Remark 4.4. Say $K \subset X$ is a subspace. Then, one should think of $\mathrm{H}_*(X, X - K)$ as giving information about K (we're killing information in the complement of K). Note these group behave *contravariantly* with K, i.e. if $K \subset L$, we get a map

$$\mathrm{H}_*(X, X - L) \to \mathrm{H}_*(X, X - K).$$

Excision tells us about how these depend on K. Say $K \subset U \subset X$ with $\overline{K} \subset \mathrm{Int}(U)$ (e.g. K closed and U open). Then the map

$$\mathrm{H}_*(U, U - K) \xrightarrow{\sim} \mathrm{H}_*(X, X - K)$$

is an iso.

The cap product says $\mathrm{H}_*(X, X-K)$ is a module over $\mathrm{H}^*(X)$. By the above remark, it's actually a module over $\mathrm{H}^*(U)$ for any open U containing K. These various actions are all compatible by the projection formula (if $V \subset U$, the $\mathrm{H}^*(U)$-action on K factors through the $\mathrm{H}^*(V)$-action).

4.1.2 Čech Cohomology

Let $\mathcal{U}_K$ be the set of open neighborhoods of K in X, partially ordered by reverse inclusion.

Definition 4.5. The **Čech cohomology** of K is

Question: Why are we calling this Čech cohomology?

$$\check{\mathrm{H}}^p(K) := \varinjlim_{U \in \mathcal{U}_K} \mathrm{H}^p(U).$$

Tensor products commute with direct limits (tensoring is a left adjoint), we get a cap product

$$\cap : \check{\mathrm{H}}^p(K) \otimes \mathrm{H}_n(X, X-K) \to \mathrm{H}_q(X, X-K) \text{ where } p+q=n.$$

Can can form a natural map $\check{\mathrm{H}}^*(K) \to \mathrm{H}^*(K)$ which is often an isomorphism.

Lemma 4.6. *Suppose $K \subset X$ satisfies the following "regular neigborhood" condtion: for every open $U \supset K$, there is an open V with $U \supset V \supset K$ s.t. $K \hookrightarrow V$ is a homotopy equivalence (or even just a homology isomorphism). Then, $\check{\mathrm{H}}^*(K) \to \mathrm{H}^*(K)$ is an iso.*

Proof. Easy to directly check injectivity and surjectivity. ■

We now want to show that Čech cohomology behaves like a cohomology theory. Say $L \subset K$ is a pair of closed subsets of a space X. Let (U, V) be a "neighborhood pair" for (K, L). These again form a directed set $\mathcal{U}_{K,L}$ with partiial order given by reverse inclusion of pairs. We define

$$\check{\mathrm{H}}^p(K, L) = \varinjlim_{(U,V) \in \mathcal{U}_{K,L}} \mathrm{H}^p(U, V).$$

Theorem 4.7. *Let (K, L) be a closed pair in X. There is a long exact sequence*

$$\cdots \to \check{\mathrm{H}}^p(K, L) \to \check{\mathrm{H}}^p(K) \to \check{\mathrm{H}}^p(L) \to \check{\mathrm{H}}^{p+1}(K, L) \to \cdots$$

natural in the pair.

Theorem 4.8. *Suppose A, B are closed subsets of a normal space, or compact subsets of a Hausdorff space. Then the map*

$$\check{\mathrm{H}}^p(A \cup B, A) \xrightarrow{\sim} \check{\mathrm{H}}^p(B, A \cap B)$$

induced by the inclusion is an iso.

The point is that $\mathcal{U}_{K,L}$ is cofinal in $\mathcal{U}_K, \mathcal{U}_L$ (and $\mathcal{U}_A \times \mathcal{U}_B$ is cofinal in $\mathcal{U}_{A \cup B, A}, \mathcal{U}_{B, A \cap B}$) so all direct limits can be computed with it. Direct limits are exact, so get these from comparision with usual cohomology.

Corollary 4.9. *There's a Mayer-Vietoris sequence too.*

Fully relative cap product Fix some $x_K \in \mathrm{H}_n(X, X-K)$ and consider the map

$$-\cap x_K : \check{\mathrm{H}}^p(K) \to \mathrm{H}_q(X, X-K) \text{ where } p+q=n.$$

We want to show this is often an iso. This will come from some five-lemma argument.

To start, how do these maps vary as we change K. Let L be a closed subset of K, so $X-K \subset X-L$ and we get a restriction map $i_* : \mathrm{H}_n(X, X-K) \to \mathrm{H}_n(X, X-L)$. Let $x_L := i_*(x_K)$. The projection formula tells us that

$$\begin{tikzcd}
\check{\mathrm{H}}^p(K) \arrow[r] \arrow[d, "-\cap x_K"'] & \check{\mathrm{H}}^p(L) \arrow[d, "-\cap x_L"] \\
\mathrm{H}_q(X, X-K) \arrow[r] & \mathrm{H}_q(X, X-L)
\end{tikzcd}$$

commutes.

Theorem 4.10. *There is a* ***full relative cap product***

$$\cap : \check{\mathrm{H}}^p(K, L) \otimes \mathrm{H}_n(X, X-K) \to \mathrm{H}_q(X-L, X-K) \text{ where } p+q=n$$

such that for any $x_K \in \mathrm{H}_n(X, X-K)$ and any $x \in \mathrm{H}_n(X)$, the two ladders below commute:

$$\begin{tikzcd}
\cdots \arrow[r] & \check{\mathrm{H}}^p(K,L) \arrow[r] \arrow[d, "\cap x_K"] & \check{\mathrm{H}}^p(K) \arrow[r] \arrow[d, "\cap x_K"] & \check{\mathrm{H}}^p(L) \arrow[r, "\delta"] \arrow[d, "\cap x_L"] & \check{\mathrm{H}}^{p+1}(K,L) \arrow[r] \arrow[d, "\cap x_K"] & \cdots \\
\cdots \arrow[r] & \mathrm{H}_q(X-L, X-K) \arrow[r] & \mathrm{H}_q(X, X-K) \arrow[r] & \mathrm{H}_q(X, X-L) \arrow[r, "\partial"] & \mathrm{H}_{q-1}(X-L, X-K) \arrow[r] & \cdots
\end{tikzcd}$$

$$\begin{tikzcd}
\cdots \arrow[r] & \check{\mathrm{H}}^p(X,K) \arrow[r] \arrow[d, "\cap x"] & \check{\mathrm{H}}^p(X,L) \arrow[r] \arrow[d, "\cap x"] & \check{\mathrm{H}}^p(K,L) \arrow[r] \arrow[d, "\cap x_K"] & \check{\mathrm{H}}^{p+1}(X,K) \arrow[r] \arrow[d, "\cap x"] & \cdots \\
\cdots \arrow[r] & \mathrm{H}_q(X-K) \arrow[r] & \mathrm{H}_q(X-L) \arrow[r] & \mathrm{H}_q(X-L, X-K) \arrow[r] & \mathrm{H}_{q-1}(X-K) \arrow[r] & \cdots
\end{tikzcd}$$

with the obvious relationships between x, x_K, x_L. In particular,

$$(\delta b) \cap x_K = \partial(b \cap x_L).$$

Notation 4.11. $\mathrm{H}_q(X|A) := \mathrm{H}_q(X, X-A)$.

Corollary 4.12. *Let A, B be closed in a normal space or compact in a Hausdorff space. The Čech cohomology and singular cohomology Mayer-Vietoris sequences are compatible: for any $x_{A\cup B} \in \mathrm{H}_n(X, X - A \cup B)$, there is a commutative ladder*

$$\begin{tikzcd}
\cdots \arrow[r] & \check{\mathrm{H}}^p(A\cup B) \arrow[r] \arrow[d, "\cap x_{A\cup B}"] & \check{\mathrm{H}}^p(A) \oplus \check{\mathrm{H}}(B) \arrow[r] \arrow[d, "(\cap x_A)\oplus(\cap x_B)"] & \check{\mathrm{H}}^p(A\cap B) \arrow[r, "\delta"] \arrow[d, "\cap x_{A\cap B}"] & \check{\mathrm{H}}^{p+1}(A\cup B) \arrow[r] \arrow[d, "\cap x_{A\cup B}"] & \cdots \\
\cdots \arrow[r] & \mathrm{H}_q(X|A\cup B) \arrow[r] & \mathrm{H}_q(X|A) \oplus \mathrm{H}_q(X|B) \arrow[r] & \mathrm{H}_q(X|A\cap B) \arrow[r, "\partial"] & \mathrm{H}_{q-1}(X|A\cup B) \arrow[r] & \cdots
\end{tikzcd}$$

The point being that Mayer-Vietoris comes from the ladder between the LESs of the pairs $(A \cup B, B)$

and $(A, A\cap B)$ (in which every third vertical map is an iso by excision), so inherit compatibility between Čech and singular cohomology.

4.1.3 Some Exercises

Problem 4.1. *The cup product on* $\mathrm{H}^*(X)$ *is graded commutative.*

4.2 Complex Oriented Cohomology Theories

For the most part, see these notes. If there's anything more I want to record, I'll add it here I guess.

4.2.1 Computation of the Lazard Ring

Thank ~~Naminé~~ Lurie.

We let L denote the **Lazard ring**, the ring supporting the universal formal group law. Write

$$f_L(x,y) = x +_L y = \sum_{i,j} a_{ij}x^iy^j = x + y + \sum_{i,j\geq 1} a_{ij}x^iy^j$$

for the universal formal group law. Inspired by cohomology (i.e. thinking of $x \in E^2(\mathbb{CP}^\infty)$ above as some complex orientation), we grade this by setting

$$|a_{ij}| = 2(i+j-1)$$

so that $x, y, f_L(x,y)$ are all in degree -2. In other words,

Definition 4.13. A **formal group law on a $\mathbb{Z}$-graded ring** A is a formal group law of the form

$$f(x,y) = \sum_{i,j} c_{ij}x^iy^j$$

with $|c_{ij}| = 2(i+j-1)$.

The Lazard ring is universal for both graded and ungraded formal group laws.

We wish to shows that $L \simeq \mathbb{Z}[t_1, t_2, \dots]$ is a polynomial ring on generators in even degrees $|t_i| = 2i$. To show this, we compare with another polynomial ring. Inspired by the Hurewicz map $\pi_*(MU) \hookrightarrow \mathrm{H}_*(MU) = \mathbb{Z}[b_i \mid i \geq 1]$, we consider the graded commutative ring

$$R = \mathbb{Z}[b_1, b_2, \dots, b_i, \dots]$$

with b_n of degree $2n$. Consider the formal power series $\exp(y) = \sum_{i\geq 0} b_iy^{i+1} \in R[\![y]\!]$ (where $b_0 := 1$), and let $\log(x) \in R[\![x]\!]$ be its compositional inverse (which exists since b_0 is a unit and there's no constant term). We define the formal product

$$f_R(x,y) = x +_R y := \exp(\log x + \log y)$$

which gives rise to a map $\theta : L \to R$. We will show that θ is injective (with image a polynomial algebra) by analyzing it "one degree at a time," i.e. by looking at the induced maps

$$Q_{2n}(L) := (I_L/I_L^2)_{2n} \to (I_R/I_R^2)_{2n} =: Q_{2n}(R),$$

where $I_L = \sum_{n>0} L_n$ and $I_R = \sum_{n>0} R_n$ are the (augmentation?) ideals of positive degree elements.

Computing $Q_{2n}(\theta)$ Our goal is to show the following.

Lemma 4.14. *The map $Q_{2n}(\theta) : Q_{2n}(L) \to Q_{2n}(R) = \langle [b_{2n}] \rangle \cong \mathbb{Z}$ is an isomorphism when $n+1 \neq p^k$ for any prime p (and $k > 0$), while it is an inclusion of an index p subgroup otherwise.*

Since L supports the universal (graded) formal group law, understanding $Q_{2n}(L)$ basically amounts to understanding formal group laws on rings of the form $A_{2n}^+ \cong \mathbb{Z} \oplus A$ with $\mathbb{Z}$ in degree 0 and A in degree $2n$. That is, for any abelian group A, we have

$$\mathrm{Hom}\left(Q_{2n}(L), A\right) = \mathrm{Hom}^{gr}\left(Q_{2n}(L)_{2n}^+, A_{2n}^+\right) = \mathrm{Hom}^{gr}(L, A_{2n}^+) = \mathrm{FGL}^{gr}(A_{2n}^+),$$

where the superscript ^{gr} denotes graded homomorphisms.

Any formal group law on $M := A_{2n}^+$ will be of the form

$$f(x,y) = x +_M y = \sum_{i,j \geq 0} c_{ij} x^i y^j \quad \text{with} \quad |c_{ij}| = 2(i+j-1).$$

Since M is nonzero only in degrees 0 and $2n$, we see that

$$c_{ij} \neq 0 \implies i + j \in \{1, n+1\}$$

so

$$f(x,y) = x + y + \sum_{i+j=n+1} c_{ij} x^i y^j = x + y + \sum_{i=0}^{n+1} c_i x^i y^{n+1-i} \quad \text{where} \quad c_i := c_{i,n+1-i}.$$

Commutativity says that $f(x,y) = f(y,x)$ so $c_i = c_{n+1-i}$. One can check that associativity amounts to the identity

$$c_{i+j}\binom{i+j}{i} = c_{j+k}\binom{j+k}{j} \quad \text{when} \quad i+j+k = n+1.$$

How can we find (all) such sequences of elements? One thing we can do is note that $Q_{2n}(R) = \mathbb{Z}$ (generated by the image of $b_{2n} \in R_{2n}$), and so $Q_{2n}(\theta)$ induces a map

$$\lambda : M = \mathrm{Hom}(\mathbb{Z}, M) \xrightarrow{\sim} \mathrm{Hom}(Q_{2n}(R), M) \xrightarrow{\mathrm{Hom}(Q_{2n}(\theta), -)} \mathrm{Hom}(Q_{2n}(L), M) \xrightarrow{\sim} \mathrm{FGL}^{gr}(M_{2n}^+).$$

Note that this map is equivalently

$$\lambda : M = \mathrm{Hom}(\mathbb{Z}, M) \xrightarrow{\sim} \mathrm{Hom}(Q_{2n}(R), M) \xrightarrow{\sim} \mathrm{Hom}^{gr}(R, M_{2n}^+) \xrightarrow{\mathrm{Hom}(\theta, -)} \mathrm{Hom}^{gr}(L, M_{2n}^+) \xrightarrow{\sim} \mathrm{FGL}^{gr}(M_{2n}^+).$$

Thus, $m \in M$ gets associated first to the ring homomorphism $\psi_m : \mathbb{Z}[b_1, \dots] \to \mathbb{Z} \oplus M$ sending $b_n \mapsto m$ (and $b_i \mapsto 0$ for $i \neq n$). This induces the exponential map $\exp_m(x) = x + mx^{n+1}$ $\left(= \psi_m\left(\sum_{i \geq 0} b_i x^{i+1}\right)\right)$ with inverse $\log_m(x) = x - mx^{n+1}$ (as can be easily checked). Thus, m is associated to the formal group law

$$\begin{aligned}\exp_m(\log_m(x)+\log_m(y)) &= \exp_m(x+y-m(x^{n+1}+y^{n+1})) \\ &= x+y-m(x^{n+1}+y^{n+1})+m(x+y-m(x^{n+1}+y^{n+1}))^{n+1} \\ &= x+y+m\left((x+y)^{n+1}-x^{n+1}-y^{n+1}\right)\end{aligned}$$

(recall all powers of $m \in M_{2n}^+$ vanish).

Notation 4.15. Let $F(M)$ denote the set of all sequences $\{c_i\}_{i=0}^{n+1} \subset M$ so that $c_i = c_{n+1-i}$, $c_0 = 0$, and

$$c_{i+j}\binom{i+j}{i} = c_{j+k}\binom{j+k}{j} \text{ when } i+j+k = n+1.$$

Thus, the functor $M \rightsquigarrow F(M)$ is naturally isomorphic to $\mathrm{FGL}^{gr}((-)_{2n}^+)$.

The computation above shows that $\lambda : M \to F(M)$ sends $m \in M$ to the sequence

$$c_i = \begin{cases} 0 & \text{if } i \in 0, n+1 \\ \binom{n+1}{i} m & \text{otherwise.} \end{cases}$$

Let $d_n := \gcd\left\{\binom{n+1}{i} : 1 \le i \le n\right\}$, so

$$d_n = \begin{cases} p & \text{if } n+1 = p^f \\ 1 & \text{otherwise.} \end{cases}$$

If $n+1 = p^f$, then all these coefficients is divisible by p (since the factor of p^f in $(i+j)!/i!$ cannot be cancelled by anything appearing in $j!$), and if $n+1 \neq p^f$, then at least one of them is not divisible by p. Finally, if $n+1 = p^f$, then the coefficient with $i = \lambda p^{f-1}$ and $j = \mu p^{f-1}$ (where $\lambda + \mu = p$) is $p!/(\lambda!\mu!) \pmod{p^2}$ which is divisible by p but not p^2.

Proposition 4.16. *The map $\varphi : m \mapsto \frac{\lambda(m)}{d_n}$ is a (functorial) isomorphism $M \xrightarrow{\sim} \mathrm{Hom}(Q_{2n}(L), M)$. In particular, by (co-)Yoneda, $Q_{2n}(L) \cong \mathbb{Z}$ and $Q_{2n}(\theta)$ is multiplication by d_n.*

Proof. We can check this locally at each prime, so assume M is a $\mathbb{Z}_{(p)}$-module. Each coefficient c_i gives a map

$$c_i : \mathrm{Hom}(Q_{2n}(I), M) \to M.$$

Fix i so that $\binom{n+1}{i}$ has the smallest p-adic valuation. Then the composition $c_i \circ \varphi$ is multiplication by a unit (by definition of d_n), so φ is injective (and c_i is surjective). For surjectivity, it suffices to show this particular c_i is injective... ∎

The consequence

Theorem 4.17. *$\theta : L \to R$ is a monomorphism, and L is a polynomial algebra on generators in even degrees.*

This is saying that $\pi_*(MU)$ is a polynomial algebra on generators in

Proof. Choose $t_n \in L_{2n}$ projecting onto a generator of T_n. This gives a map

$$\mathbb{Z}[t_1, t_2, \dots, t_n, \dots] \xrightarrow{\alpha} L$$

which, by the previous corollary, induces isomorphisms $Q_{2n}(\alpha)$ for each n. Thus, α is an epimorphism. At the same time, the composite map

$$\mathbb{Z}[t_1, t_2, \dots, t_n, \dots] \xrightarrow{\alpha} L \xrightarrow{\theta} R = \mathbb{Z}[b_1, b_2, \dots, b_n, \dots]$$

is monomorphic since $\theta \circ t_n$ is a nonzero multiple of b_n, modulo decomposables. Therefore, α is an isomorphism and θ is a monomorphism. ■

4.2.2 Computation of MU_*

Instead of Adams, trying to follow Lurie's Chromatic Homotopy Theory notes, Lectures 8 – 10.

Adams Spectral Sequence Jk, I'm never gonna actually understand this...

4.3 Lens Spaces

Fix an integer m along with integers $\ell_1, \dots, \ell_n$ relatively prime to m. Let $L = L_m(\ell_1, \dots, \ell_n)$ be the **lens space** given as the quotient of the unit sphere $S^{2n-1} \subset \mathbb{C}^n$ by the μ_m-action given by

$$\zeta \cdot (z_1, \dots, z_n) = \left(e^{2\pi i \ell_1/m} z_1, \dots, e^{2\pi i \ell_n/m} z_n\right).$$

Example. When $m = 2$, $\ell_i = 1$ for all i, so $\zeta \in \mu_2$ acts by the antipodal map and $L \simeq \mathbb{RP}^{2n-1}$.

Remark 4.18. The projection $S^{2n-1} \to L$ is a covering map (action is free or whatever), so $\pi_1(L) = \mu_m \simeq \mathbb{Z}/m\mathbb{Z}$.

We want to give L a CW-structure. First, for $r = 0, 1, \dots, m-1$, consider the cells

$$\begin{aligned} e_r^{2n-2} &= \{(z_1, \dots, z_{n-1}, z_n) : \arg(z_n) = 2\pi r/m\} && \subset S^{2n-1} \\ e_r^{2n-1} &= \{(z_1, \dots, z_{n-1}, z_n) : 2\pi r/m \le \arg(z_n) \le 2\pi(r+1)/m\} && \subset S^{2n-1} \end{aligned}$$

Note that S^{2n-1} can be formed by attaching these cells to S^{2n-3} (i.e. $\{z_n = 0\} \subset S^{2n-1}$) simply because all the points with $z_n \neq 0$ lie on one of these cells. Thus, we can inductively defines cells e_r^k for all $0 \le k \le 2n-1$ and $0 \le r \le m-1$ so as to give S^{2n-1} a CW-structure with m cells in each dimension. It's clear that μ_m acts simply transitively on the cells in a given dimension, so taking quotients shows this CW-structure descends to one of L with a single cell e^k in each dimension $k \in \{0, \dots, 2n-1\}$.

Remark 4.19. The even attaching maps $\varphi_{2k} : \partial e^{2k} \cong S^{2k-1} \to L_{2k-1} = L_m(\ell_1, \dots, \ell_k)$ are the natural quotient maps.

We claim the cellular chain complex looks like

$$\mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{m} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \to \cdots \to \mathbb{Z} \to 0.$$

Fact. If $f : S^n \to S^n$ has no fixed points, then $\deg f = (-1)^{n+1}$ because f is homotopic to the antipodal map $x \mapsto -x$ via a straight line homotopy.

For even cells, the boundary map in the cellular chain complex is multiplication by m since the attaching map is the natural quotient $S^{2k-1} \to L_m(\ell_1, \dots, \ell_k)$ and the cells $e_r^{2k} \subset S^{2k-1}$ are permuted cyclically by the degree $+1 = (+1)^{2k-1+1}$ map given by the action of ζ. Put another way, this map is multiplication by the degree of the following map (the top row of the commutative diagram)

$$\begin{tikzcd}
\partial e^{2k} \arrow[r, equal] & S^{2k-1} \arrow[r, "\varphi_{2k}"] \arrow[d] & L_{2k-1} \arrow[r] & L_{2k-1}/L_{2k-2} \arrow[d, equal] \\
& S^{2k-1}/(S^{2k-1})_{2k-1} \arrow[r, equal] & \bigwedge_{i=1}^m S^{2k-1} \arrow[r, "1\wedge\zeta\wedge\zeta^2\wedge\cdots\wedge\zeta^{m-1}"] & S^{2k-1}
\end{tikzcd}$$

This degree is

$$\sum_{i=0}^{m-1} \deg(\zeta^i) = 1 + \sum_{i=1}^{m-1} (-1)^{2k-1+1} = m$$

since ζ^i has no fixed points. For odd cells, the boundary map must be 0 in order to have $\partial^2 = 0$.

The upshot is that

$$\mathrm{H}_*(L; \mathbb{Z}) \cong \begin{cases} \mathbb{Z} & \text{if } * = 0, 2n-1 \\ \mathbb{Z}/m\mathbb{Z} & \text{if } * \text{ odd and } 0 < * < 2n-1 \\ 0 & \text{if otherwise} \end{cases}$$

(nontrivial homology in odd degrees).

Remark 4.20. Let $X = S^1 \cup_\varphi e_2$ with attaching map $\varphi : \partial e_2 = S^1 \to S_1$ an m-fold cover. Then, the cellular chain complex of X is $\mathbb{Z} \xrightarrow{m} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \to 0$, so X is an $M(\mathbb{Z}/m\mathbb{Z}, 1)$. Hence, L_2 and $X \vee S^3$ have the same homology, but $L_2 \not\simeq X \wedge S^3$ since their mod m cohomology rings differ.

From the cellular chain complex, we see that the mod m (co)homology of L is

$$\mathrm{H}^*(L; \mathbb{Z}/m\mathbb{Z}) \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{if } * \leq 2n-1 \\ 0 & \text{otherwise.} \end{cases}$$

Since L is a manifold, we can use Poincaré duality to help us compute its cup product structure. Let $x \in \mathrm{H}^1(L; \mathbb{Z}/m\mathbb{Z})$ and $y \in \mathrm{H}^2(L; \mathbb{Z}/m\mathbb{Z})$ be generators.

Assumption. Assume m is odd.

We'll show that

$$\mathrm{H}^*(L_n; \mathbb{Z}/m\mathbb{Z}) \cong \frac{(\mathbb{Z}/m\mathbb{Z})[x, y]}{(x^2, y^n)}$$

Note that $x^2 = -x^2 \implies 2x^2 = 0$ by graded commutativity, so $x^2 = 0$ since m odd. The inclusion $L_{n-1} \hookrightarrow L_n = L$ respects x, y, so we can induct (base case $n = 1$, so $L_1 = S^1$, being obvious), assuming things work up to degree $2n-3$ (with $n > 1$). Now, Poincaré tells us that cup products give perfect pairings (secretly, we need to mod out by ($R = \mathbb{Z}/m\mathbb{Z}$)-torsion, but there is none so we're fine)

$$\mathrm{H}^{2n-3}(L; \mathbb{Z}/m\mathbb{Z}) \times \mathrm{H}^2(L; \mathbb{Z}/m\mathbb{Z}) \to \mathrm{H}^{2n-1}(L; \mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z}$$

and

$$\mathrm{H}^{2n-2}(L; \mathbb{Z}/m\mathbb{Z}) \times \mathrm{H}^1(L; \mathbb{Z}/m\mathbb{Z}) \to \mathrm{H}^{2n-1}(L; \mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z}.$$

The first pairing tells us that H^{2n-1} is generated by $(xy^{n-2})y = xy^{n-1}$ as desired. Given this, the second pairing then tells us that H^{2n-2} is generated by any γ such that $x\gamma = \pm xy^{n-1}$. Visibly, we can take $\gamma = y^{n-2}$, as desired.

Remark 4.21. If m is even, $m = 2k$, then apparently $x^2 = ky$. Graded commutativity forces $x^2 = 0$ or $x^2 = ky$ (since $2x^2 = 0$), and one somehow shows it's the latter...

5 Lie Theory

5.1 Complete Reducibility of reps of semisimple Lie algebras

Let $\mathfrak{g}$ be a semisimle Lie algebra (in characteristic 0). We want to show that all f.dim reps are completely reducible, i.e. that all f.dim extensions split. We'll start with the following:

Fact. Extensions $0 \to V \to E \to W \to 0$ of W by V are characterized by the group

$$\mathrm{Ext}^1_{\mathfrak{g}}(W, V) = \mathrm{H}^1(\mathfrak{g}, \mathrm{Hom}_k(W, V))$$

(uses the fact that all extensions of vector spaces are split).

Goal. If V is a f.dim $\mathfrak{g}$-rep, then $\mathrm{H}^1(\mathfrak{g}, V) = 0$.

Let k denote the field we're working over.

Lemma 5.1. *Say E is a f.dim $\mathfrak{g}$-rep and $C \in U(\mathfrak{g})$ is central with $C|_k = 0$ and $C|_E = \lambda\,\mathrm{Id}$ for $\lambda \neq 0$. Then,* $\mathrm{H}^1(\mathfrak{g}, E) = \mathrm{H}^1(\mathfrak{g}, \mathrm{Hom}_k(k, E)) = \mathrm{Ext}^1(k, E) = 0$.

Proof. Need to show that any extension

$$0 \longrightarrow E \longrightarrow V \longrightarrow k \longrightarrow 0$$

of k by E splits. We claim $\exists! v \in V$ such that $p(v) = 1$ and $Cv = 0$. Indeed, pick any $w \in V$ s.t. $p(w) = 1$; then $Cw \in E$ since p is equivariant. Now set $v = w - \lambda^{-1}Cw$, so $Cv = Cw - \lambda^{-1}C^2 w = Cx - \lambda^{-1}\lambda Cw = 0$ (C acts on $Cw \in E$ by λ). This gives existence of v. For uniqueness, with v' has the same property, then

$$v - v' \in E \implies 0 = C(v - v') = \lambda(v - v') \implies v = v'.$$

Now consider the space $kv \subset V$, a complement of E invariant under $\mathfrak{g}$. Indeed, given $x \in \mathfrak{g}$, one has

$$C(xv) = xCv = 0 \implies xv \in kv$$

with the implication coming from uniqueness of v. Thus, $V = E \oplus k \cdot v$ and we win. ■

Remark 5.2. One can construct such a C for any irrep of $\mathfrak{g}$ (mirroring the construction of the Casimir element). You let $I = \ker B_V \subsetneq \mathfrak{g}$ (where $B_V(x, y) = \mathrm{Tr}(xy)$), write $\mathfrak{g} = I \oplus \mathfrak{g}'$ and then let $C = \sum x_i x^i$ with $x_i \in \mathfrak{g}'$ a basis (with dual basis x^i). Then $C|_k = 0$ since x_i acts trivially on the trivial $\mathfrak{g}$-rep, and $C|_V = \lambda\,\mathrm{Id}$ where

$$\lambda \dim V = \mathrm{Tr}_V\, C = \sum_i \mathrm{Tr}(x_i x^i) = \sum_i B(x_i, x^i) = \sum_i 1 = \dim \mathfrak{g}' \implies \lambda \neq 0.$$

The upshot is that $\mathrm{H}^1(\mathfrak{g}, V) = 0$ for any irrep V. To finish, form a Jordan series for an arbitrary $\mathfrak{g}$-rep V and then induct with the LES in cohomology.

5.2 Root decompositions

Definition 5.3. A **Cartan subalgebra** $\mathfrak{h} \subset \mathfrak{g}$ is a *toral subalgebra* (i.e. abelian with every element semisimple) such that $\mathfrak{g}_0 = \mathfrak{h}$, where

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{0 \neq \alpha \in \mathfrak{h}^*} \mathfrak{g}_\alpha \text{ with } \mathfrak{g}_\alpha = \{x \in \mathfrak{g} : [h, x] = \alpha(h)x \text{ for all } h \in \mathfrak{h}\},$$

i.e. such that $C(\mathfrak{h}) = \mathfrak{h}$ ($\mathfrak{h}$ is its own centralizer). Equivalently, $\mathfrak{h}$ is a maximal toral subalgebra.

Remark 5.4. $\mathfrak{g}_0$ is always reductive (for $\mathfrak{h}$ any toral subalgebra), and if B is a non-degenerate, invariant, bilinear form, then $\mathfrak{g}_\alpha \perp \mathfrak{g}_\beta$ for $\alpha + \beta \neq 0$ while $B : \mathfrak{g}_\alpha \times \mathfrak{g}_{-\alpha} \to k$ is a nondegenerate pairing.

Remark 5.5. nilpotent + reductive = abelian

Let $\mathfrak{g}$ be a semisimple Lie algebra with Cartan subalgebra $\mathfrak{h} \subset \mathfrak{g}$ and nondegenerate, invariant symmetric form $(-,-)$ (e.g. the Killing form). Let $A : \mathfrak{h} \xrightarrow{\sim} \mathfrak{h}^*$ given by $A(h) = (h, -)$. Given $\alpha \in \mathfrak{h}^*$, we set $H_\alpha := A^{-1}(\alpha)$. We then get a pairing on $\mathfrak{h}^*$ defined by

$$(\alpha, \beta) := (H_\alpha, H_\beta) = \alpha(H_\beta).$$

Lemma 5.6. *For any $e \in \mathfrak{g}_\alpha$ and $f \in \mathfrak{g}_{-\alpha}$, we have*

$$[e, f] = (e, f)H_\alpha \in \mathfrak{h}.$$

Proof. Since $(-,-)$ is non-degenerate, suffices to show they both have the same inner product with any $h \in \mathfrak{h}$. Observe,

$$([e, f], h) = -(f, [e, h]) = (f, [h, e]) = \alpha(h)(f, e) = (H_\alpha, h)(f, e) = \big((f, e)H_\alpha, h\big) = \big((e, f)H_\alpha, h\big).$$

■

Remark 5.7. nilpotent $\implies$ solvable ($\implies$ upper triangularizable by Lie's theorem)

Fact. If $\alpha \in R$ is a root, then $(\alpha, \alpha) \neq 0$.

If we pick $e \in \mathfrak{g}_\alpha$ and $f \in \mathfrak{g}_{-\alpha}$ so that $(e, f) = 2/(\alpha, \alpha)$ (easy by scaling), then letting $h_\alpha := 2H_\alpha/(\alpha, \alpha)$, we have that h_α, e, f satisfy the relations of $\mathfrak{sl}_2$. Also, h_α is independent of the choice of $(-,-)$.

$h_\alpha = \frac{2H_\alpha}{(\alpha,\alpha)} \in \mathfrak{h}$ is the coroot $\alpha^\vee$

Proposition 5.8.

(i) $\dim \mathfrak{g}_\alpha = 1$ *for all* $\alpha \in R$

(ii) *If $\alpha \in R$, then $\mathfrak{g}_{k\alpha} = 0$ for $k \geq 2$.*

Proof. Let $\mathfrak{a}_\alpha := kh_\alpha \oplus \bigoplus_{m \in \mathbb{Z} \setminus 0} \mathfrak{g}_{m\alpha}$. This is a Lie subalgebra of $\mathfrak{g}$, and more importantly, an $\mathfrak{sl}_2(k)_\alpha$-rep. The weights of $h = h_\alpha$ acting of $\mathfrak{a}_\alpha$ are ($x \in \mathfrak{g}_{m\alpha}$)

$$[h_\alpha, x] = m\alpha(h_\alpha)x = m\frac{2(H_\alpha, H_\alpha)}{(\alpha, \alpha)}x = 2mx.$$

Thus, all the eigenvalues are even integers and the 0-eigenspace is 1-dimensional. This forces $\mathfrak{a}_\alpha = L_{2r}$ to be the irrep with highest weight $2r$ for some $r \in \mathbb{Z}_{>0}$. This force all weight spaces to be 1-dimensional, giving **(i)**. For **(ii)**, rep theory of $\mathfrak{sl}_2$ says that $\mathfrak{g}_{k\alpha} = e^{k-1} \cdot \mathfrak{g}_\alpha$ for all $k \geq 1$. But $\mathfrak{g}_\alpha = \langle e \rangle$, so $\mathfrak{g}_{k\alpha} = 0$ for $k \geq 2$. ■

Theorem 5.9. *Let $\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha$ be a root decomposition of a semisimple Lie algebra, and let $(-,-)$ be a nondeg, invariant, symmetric form on $\mathfrak{g}$. Then,*

(i) *$\alpha \in R$ span $\mathfrak{h}^*$, and the h_α span $\mathfrak{h}$.*

(ii) *For all roots α, β, $a_{\alpha\beta} = 2(\alpha,\beta)/(\alpha,\alpha)$ is an integer*

(iii) *For all $\alpha \in R$, define the **reflection operator***

$$s_\alpha(\lambda) = \lambda - \lambda(h_\alpha)\alpha = \lambda - \frac{2(\lambda,\alpha)}{(\alpha,\alpha)}\alpha$$

(so $s_\alpha^2 = 1$). If $\beta \in R$, then $s_\alpha(\beta) \in R$, so $s_\alpha(R) = R$.

(iv) *For roots $\alpha, \beta \neq \pm\alpha$, the space $V_{\alpha,\beta} = \bigoplus_{m \in \mathbb{Z}} \mathfrak{g}_{\beta+m\alpha}$ is an irrep of $\mathfrak{sl}_2(k)_\alpha$.*

Proof. **(i)** Let $h \in \mathfrak{h}$ be such that $\alpha(h) = 0$ for all $\alpha \in R$. Then, $\operatorname{ad} h = 0$ (acts by 0 on $\mathfrak{h}$ and by $0 = \alpha(h)$ on $\mathfrak{g}_\alpha$) so $h = 0$ since $\mathfrak{g}$ semisimple. This means the α span $\mathfrak{h}^*$.

(ii) Note that $[h_\alpha, e_\beta] = \beta(h_\alpha)e_\beta = \beta\left(\frac{2H_\alpha}{(\alpha,\alpha)}\right)$ so $2(\alpha,\beta)/(\alpha,\alpha)$ is an eigenvalue of h under a f.d. rep of $\mathfrak{sl}_2(\mathfrak{h})_\beta$ which must then be an integer.

(iii) $s_\alpha^2(\beta) = s_\alpha(\beta - \beta(h_\alpha)\alpha) = \beta - \beta(h_\alpha)\alpha - (\beta - \beta(h_\alpha)\alpha)(h_\alpha)\alpha = \beta - 2\beta(h_\alpha)\alpha + \beta(h_\alpha)\alpha(h_\alpha)\alpha = \beta$. Let $\beta \in R$ and $x \in \mathfrak{g}_\beta$ nonzero. Then,

$$[h_\alpha, x] = \frac{2(\alpha,\beta)}{(\alpha,\alpha)}x = \beta(h_\alpha)x.$$

We now want to shift eigenspaces by applying f (to lower eigenvalue) or e (to raise eigenvalue). First note that

$$s_\alpha(\beta) = \beta - \beta(h_\alpha)\alpha,$$

as well as that $[f,x] \in \mathfrak{g}_{\beta-\alpha}$ and $[e,x] \in \mathfrak{g}_{\beta+\alpha}$ (and that $\alpha(h_\alpha) = 2$). If $\beta(h_\alpha) \geq 0$, then $y = (\operatorname{ad} f)^{\beta(h_\alpha)}x \neq 0 \in \mathfrak{g}_{s_\alpha(\beta)}$ so $s_\alpha(\beta) \in R$. If $\beta(h_\alpha) \leq 0$, then $y = (\operatorname{ad} e)^{-\beta(h_\alpha)}x \neq 0 \in \mathfrak{g}_{s_\alpha(\beta)}$, so $s_\alpha(\beta) \in R$.

This is $\neq 0$ since we're going from the $\beta(h_\alpha)$-eigenspace to the $-\beta(h_\alpha) = s_\alpha(\beta)(h_\alpha)$-eigenspace

(iv) $V_{\alpha,\beta} \subset \mathfrak{g}$ is a subspace. It is clearly a subep since $\{\beta + m\alpha\}$ is invariant under shifting by $\pm\alpha$. The eigenvalues of h_α are

$$2\frac{(\alpha,\beta)}{(\alpha,\alpha)} + 2m$$

which are all even. Since its eigenspaces are also all 1-dim, we conclude by rep theory of $\mathfrak{sl}_2$ that $V_{\alpha,\beta}$ is irreducible. ■

Proposition 5.10. *Let $\mathfrak{h}_\mathbb{R}$ be the $\mathbb{R}$-span of the $h_\alpha \in \mathfrak{h}$ for $\alpha \in R$. Then, $\mathfrak{h} = \mathfrak{h}_\mathbb{R} \oplus i\mathfrak{h}_\mathbb{R}$ and the restriction of the Killing form to $\mathfrak{h}_\mathbb{R}$ is positive definite.*

Proof. The eigenvalues of $\operatorname{ad} h_\alpha$ are integers, so the eigenvalues of an $\mathbb{R}$-linear combo $h = \sum c_\alpha h_\alpha \in \mathfrak{h}_\mathbb{R}$ are also real numbers. Hence, $\mathfrak{h}_\mathbb{R} \cap i\mathfrak{h}_\mathbb{R} = 0$. If λ_i are the eigenvalues of $\operatorname{ad} h$, then $K(h,h) = \sum \lambda_i^2 \geq 0$ w/ equality iff $\lambda_i = 0$ for all i. ■

5.2.1 Example/Exercise

Problem 6.5. *Let $\mathfrak{h} \subset \mathfrak{so}(4, \mathbb{C})$ be the subalgebra consisting of matrices of the form*

$$x_{a,b} := \begin{pmatrix} 0 & a & 0 & 0 \\ -a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \\ 0 & 0 & -b & 0 \end{pmatrix}.$$

This is Cartan.

Proof. Say $y = (y_{i,j})_{i,j=1}^4 \in \mathfrak{so}(4, \mathbb{C})$ commutes with every element of $\mathfrak{h}$. Then, $yx_{1,0} = x_{1,0}y$ tells us that the upper right and bottom left 2×2 blocks of y both vanish. It also tells us that $y_{1,2} = -y_{2,1}$ and $y_{1,1} = y_{2,2}$. Similarly, $yx_{0,1} = x_{0,1}y$ tells us that $y_{3,3} = y_{4,4}$. Thus, to get $y \in \mathfrak{h}$, it suffices to show $y_{1,1} = y_{2,2} = 0 = y_{3,3} = y_{4,4}$. Well, $y \in \mathfrak{so}(4, \mathbb{C})$ tells us that $y + y^t = 0$ which immediately gives that its diagonal vanishes, so indeed $y \in \mathfrak{h}$. This makes $\mathfrak{h}$ a maximal abelian[14] subalgebra, so $\mathfrak{h}$ is Cartan.

Let's determine the root system. Let $a_{i,j} = E_{ij} - E_{ji}$ where E_{ij} is the elementary matrix with a 1 in slot ij and 0's elsewhere. Now, there's probably some smart, systematic way to find roots, but I just kinda messed around for a while until I stumbled across the following. Let

$$\begin{aligned} P &= (a_{1,3} - a_{2,4}) - i(a_{1,4} + a_{2,3}) \\ Q &= (a_{1,3} - a_{2,4}) + i(a_{1,4} + a_{2,3}) \\ R &= (a_{1,3} + a_{2,4}) + i(a_{1,4} - a_{2,3}) \\ S &= -(a_{1,3} + a_{2,4}) + i(a_{1,4} - a_{2,3}) \end{aligned}$$

One can calculate by hand or by Mathematica that

$$[x_{a,b}, P] = -i(a+b)P, \;\; [x_{a,b}, Q] = i(a+b)Q, \;\; [x_{a,b}, R] = -i(a-b)R, \;\text{ and }\; [x_{a,b}, S] = i(a-b)S.$$

Thus, we have four roots $\alpha = \pm i(a+b), \pm i(a-b)$ (where $a, b \in \mathfrak{h}^*$ are the linear functionals $x_{a,b} \mapsto a, b$ respectively). We know these are all the roots since $\dim \mathfrak{so}(4, \mathbb{C}) - \dim \mathfrak{h} = \binom{4}{2} - 2 = 4$. ■

Remark 5.11. How do diagonal matrices act? Say $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ and $M = (m_{ij})_{i,j=1}^n$. Then, $DM = (\lambda_i m_{ij})_{i,j=1}^n$ and $MD = (\lambda_j m_{ij})_{i,j=1}^n$, so

$$[D, M] = DM - MD = \left((\lambda_i - \lambda_j) m_{ij}\right)_{i,j=1}^n.$$

Example. Let's compute the root decomposition for C_2, i.e. for $\mathfrak{g} = \mathfrak{sp}(4)$. Let

$$J = \begin{pmatrix} & -I_2 \\ I_2 & \end{pmatrix} \;\text{ so }\; \mathfrak{g} = \left\{x \in \mathfrak{gl}_4(\mathbb{C}) : xJ + Jx^t = 0\right\}$$

$(xJx^t = J \implies xJ = J\left(x^t\right)^{-1} \rightsquigarrow xJ = -Jx^t)$. The natural choice of Cartan subalgebra is the diagonal

[14] $x_{a,b}x_{c,d} = -\operatorname{diag}(ac, ac, bd, bd)$ so matrices in $\mathfrak{h}$ commute since this expression is symmetric about switching $(a, b) \leftrightarrow (c, d)$.

matrices[15]

$$\mathfrak{h} = \{\operatorname{diag}(x_1, x_2, -x_1, -x_2)\}.$$

What are the roots? First, what are the elements? Write $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ as a block matrix. Then,

$$\begin{pmatrix} b & -a \\ d & -c \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} & -I_2 \\ I_2 & \end{pmatrix} = AJ = -JA^t = \begin{pmatrix} & I_2 \\ -I_2 & \end{pmatrix} \begin{pmatrix} a^t & b^t \\ c^t & d^t \end{pmatrix} = \begin{pmatrix} b^t & d^t \\ -a^t & -c^t \end{pmatrix},$$

so $a = -d^t$ and b, c are symmetric, so A must be of the form

$$A = \begin{pmatrix} a & b = b^t \\ c = c^t & -a^t \end{pmatrix}.$$

Example. The root $e_1 - e_2$ has space spanned by $E_{1,2} - E_{4,3}$

In general, for each 'part' (a, b, or c), we get a root for each possible coordinate (off the diagonal). From a, we have root spaces spanned by ($n = 2$)

$$E_{i,j} - E_{j+n,i+n} \rightsquigarrow \alpha = e_i - e_j \text{ for } 1 \le i < j \le n$$

From b, we get

$$E_{i,j+n} + E_{j,i+n} \rightsquigarrow \alpha = e_i - e_{j+n} = e_i + e_j \text{ for } 1 \le i \le j \le n$$

From c, we get

$$E_{i+n,j} + E_{j+n,i} \rightsquigarrow \alpha = e_{i+n} - e_j = -e_i - e_j \text{ for } 1 \le i \le j \le n$$

These are all the roots since the corresponding spaces (along with $\mathfrak{h}$) are visibly spanning.

5.3 Conjugacy of Cartan subalgebras

Intuition. Regular elements are like matrices w/ distinct eigenvalues.

Definition 5.12. The **nullity** of $x \in \mathfrak{g}$, denoted $n(x)$, is the multiplicity of the 0-eigenvalue of $\operatorname{ad} x$, i.e. the dimension of the generalized 0-eigenspace of $\operatorname{ad} x$. The **rank** of $\mathfrak{g}$ is the minimal value of $n(x)$. We say $x \in \mathfrak{g}$ is **regular** if $n(x) = \operatorname{rank} \mathfrak{g}$.

Example. Say $\mathfrak{g} = \mathfrak{sl}_n(\mathbb{C})$. Then apparently x regular $\iff$ diagonalizable w/ distinct eigenvalues. We have $\operatorname{ad} x.y = [x, y] = xy - yx = 0 \iff x, y$ commute. If x is diagonalizable w/ distinct eigenvalues, this happens iff y preserves all of x's eigenspaces, so iff y is diagonalizable w.r.t. to same basis as x. Hence, $\ker(\operatorname{ad} x)$ has dimension $n - 1$ (choice of diagonal elements + trace must be 0). This is the main idea.

Lemma 5.13. *The set of regular elements is connected, dense, and open.*

---

[15]
$$\begin{pmatrix} & & -x_1 & \\ & & & -x_2 \\ x_3 & & & \\ & x_4 & & \end{pmatrix} + \begin{pmatrix} & & -x_3 & \\ & & & -x_4 \\ x_1 & & & \\ & x_2 & & \end{pmatrix} = 0$$

Proof. The characteristic polynomial of $\operatorname{ad} x$ will be of the form

$$P_x(t) = t^{\operatorname{rank}(\mathfrak{g})}(t^m + a_{m-1}(x)t^{m-1} + \cdots + a_0(x)),$$

where $m = \dim \mathfrak{g} - \operatorname{rank} \mathfrak{g}$ and the $a_i(x)$ are polynomial functions of x, so $\mathfrak{g}^{reg} = \{x \in \mathfrak{g} : a_0(x) \neq 0\}$ is open, path-connected, and dense. ■

Proposition 5.14. *Let $\mathfrak{g}$ be a complex semisimple Lie algebra w/ Cartan subalgebra $\mathfrak{h} \subset \mathfrak{g}$. Then,*

(i) $\dim \mathfrak{h} = \operatorname{rank} \mathfrak{g}$*; and*

(ii)

$$\mathfrak{h}^{reg} := \mathfrak{h} \cap \mathfrak{g}^{reg} = \{h \in \mathfrak{h} : \alpha(h) \neq 0 \text{ for all } \alpha \in R\} =: V.$$

The idea is to let G be a connected complex Lie group with Lie algebar $\mathfrak{g}$ (e.g. $\operatorname{Aut}(\mathfrak{g})^\circ$), and then consider the regular map

$$\begin{array}{rccc} \varphi : & G \times V & \longrightarrow & \mathfrak{g} \\ & (g, x) & \longmapsto & \operatorname{Ad} g \cdot x. \end{array}$$

One computes the derivative to show that this is a submersion (use derivatives are additive). One checks that $\ker \varphi_* \cong C(x) = \mathfrak{h}$ (note $x \in V$) and then dimension counts to see that the map is a submersion. Hence the image U of φ contains a neighborhood of x, so U is open (translate via adjoint action), so $U \cap \mathfrak{g}^{reg}$ is open and nonempty. For $u = \varphi(g, x) \in U \cap \mathfrak{g}^{reg}$, $n(u) = n(x) = \dim C(x) = \dim \mathfrak{h}$ which proves **(i)**. **(ii)** follows from the root decomposition showing that $n(x) = \dim \mathfrak{h} + \#\{\alpha \in R : \alpha(x) = 0\}$.

At this point, one can (but we won't) show that every Cartan subalgebra is the centralizer of some regular (semisimple) element.

Remark 5.15. The image of the map $\varphi : G \times \mathfrak{h}_y^{reg} \to \mathfrak{h}$ from before is the equivalence class of y under the relation $x \sim y \iff \mathfrak{h}_x$ is conjugate to $\mathfrak{h}_y$ on $\mathfrak{g}^{reg}$. It is open by the argument above, so $\mathfrak{g}^{reg}$ splits into a union of disjoint opens (the equiv classes). It's connected, so there's only one equiv class, i.e. all Cartan subalgebras are conjugate.

5.4 Root systems

Let $E \cong \mathbb{R}^n$ be a **Euclidean space**, i.e. real vector space with positive inner product.

Definition 5.16. A **root system** $R \subset E \setminus 0$ is a *finite* subset of nonzero vectors s.t.

- **(R1)** R spans E
- **(R2)** For all $\alpha, \beta \in R$, the number
$$n_{\alpha\beta} := \frac{2(\alpha, \beta)}{(\alpha, \alpha)}$$
is an integer.
- **(R3)** If $\beta \in R$, then
$$s_\alpha(\beta) := \beta - \frac{2(\alpha, \beta)}{(\alpha, \alpha)}\alpha = \beta - n_{\alpha\beta}\alpha$$
is also a root (i.e. in R).

The number $r = \dim E$ is called the **rank** of the root system.

Remark 5.17. Applying R3 for $\beta = \alpha$ shows that

$$\alpha \in R \implies s_\alpha(\alpha) = -\alpha \in R$$

so R is centrally symmetric.

Remark 5.18. s_α is really the reflection with respect to the hyperplane $H = \{x \in E : (\alpha, x) = 0\}$. In particular, $s_\alpha^2 = \mathrm{Id}$.

Remark 5.19. We can "take slices." If $R \subset E$ is a root system, and $F \subset E$ is a subspace, then $R' = R \cap F$ inside $E' = \operatorname{span}\{R'\} \subset F$ is also a root system.

Definition 5.20. A root system $R \subset E$ is **reduced** if whenever $\alpha, \beta \in R$ are collinear, we have $\alpha = \pm\beta$.

Exercise. $\{1, 2, -1, -2\} \subset \mathbb{R}$ is a nonreduced root system.

Definition 5.21. Given $\alpha \in R$, $\alpha^\vee \in E^\vee$ is defined by the formula

$$\alpha^\vee(x) = \frac{2(\alpha, x)}{(\alpha, \alpha)}$$

and called a **coroot**.

Let $R \subset E$ be a reduced root system, and let $t \in E$ be a polarization, so we have a set $\Pi = \{\alpha_1, \dots, \alpha_r\} \subset R$ be the set of simple roots (note $r = \dim E$).

Definition 5.22. A **simple reflection** is $s_{\alpha_i} = s_i \in W$.

We will see that these generate W and one can even write down some relations for them.

Lemma 5.23. *For every Weyl Chamber C, there exists $i_1, \dots, i_n$ s.t. $s_{i_1} \dots s_{i_m}(C_+) = C$.*

Proof. Pick $t \in C$ and $t_+ \in C_+$ generically, and draw a line segment connecting t and t_+. Let m be the number of root hyperplanes ($h_\alpha = \{x \in E : \alpha(x) = 0\}$) intersected by this segment. We induct on m. The base case ($m = 0$, so $C = C_+$) is trivial, so assume $m > 0$. Let C' be the chamber entered from C along this segment. To get from C' to C_+, we only need cross $m - 1$ hyperplanes, so by inductive hypothesis, $C' = s_{i_1} \dots s_{i_{m-1}}(C_+)$. Now C, C' are adjacent, so they are separated by a wall L_α. Letting $u = s_{i_1} \dots s_{i_{m-1}}$, we have $u^{-1}(C') = C_+$ so $u^{-1}L_\alpha = L_{\alpha_i}$ for some i (as $u^{-1}L_\alpha$ is a wall adjacent to C_+). Thus, reflection across L_α is $s_\alpha = u s_i u^{-1}$ (change coordinates so L_α becomes L_i, reflect across L_i, and then change coordinates back to normal). This implies that $C = s_\alpha(C') = u s_i u^{-1}(C') = u s_i u^{-1} u(C_+) = u s_i(C_+) = s_{i_1} \dots s_{i_{m-1}} s_i(C_+)$ which completes the induction. ∎

Note that we build $s_1 \dots s_{i_m}$ by appending elements to the right because of this conjugation trick

Corollary 5.24. ***(i)*** *Simple reflections generate W, and* ***(ii)*** *$W(\Pi) = R$.*

Proof. **(i)** For all α, L_α is a wall of some chamber $C = u(C_+)$ which implies $s_\alpha = u s_i u^{-1}$ for some i where $u = s_{i_1} \dots s_{i_{m-1}}$. Thus, s_α is a product of simple reflections. Hence, W is generated by the s_i. Now, **(ii)** follows from **(i)**. ∎

In particular, the root system R be reconstructed from Π as $W = \langle s_i = s_{\alpha_i} \rangle$ and $R = W(\Pi)$.

Example. A_{n-1}. Then $s_i = s_{e_i - e_{i+1}} = (i, i+1)$ is a transposition of neighbors. Thus, we recover the statement that the symmetric group S_n is generated by transpositions of neighbors.

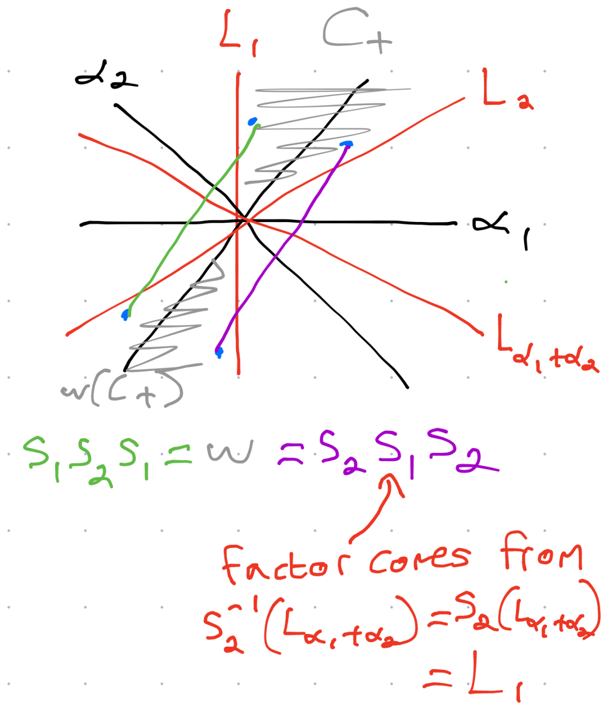

Figure 1: An example of carrying out the process in the proof of Lemma 5.23

5.4.1 Exercises

Problem 7.11.

(1) Let R be a reduced root system of rank 2, with simple roots α_1, α_2. Then, the longest element in the corresponding Weyl group is

$$w_0 = s_1 s_2 s_1 \cdots = s_2 s_1 s_2 \ldots$$

s.t. each product has m factors where the angle between α_1, α_2 is $\varphi = \pi - \frac{\pi}{m} = \pi\left(1 - \frac{1}{m}\right)$.

Proof. w_0 can be written as a product of simple transpositions. Since $s_i^2 = 1$, the shortest such product (corresponding to some path from C_+ to C_-) must be of the form $s_1 s_2 s_1 s_2 \ldots$ or $s_2 s_1 s_2 s_1 \ldots$,[16] and must have $\ell(w_0) = \#R_+ =: m$ factors. Now, let L_1, L_2 be the root lines corresponding to α_1, α_2, and let ψ be the angle between them. Since there are m lines between $C_0 := C_+$ and $C_m := w_0(C_+)$, there must be $m-1$ chambers $C_1, \ldots, C_{m-1}$ between them, so the region covered by $\bigcup_{i=0}^m C_i$ sweeps out a sector of angle $(m+1)\psi$. At the same time, $C_0 = -C_m$, so this region is a half-plane + a chamber, and hence sweeps out a sector of angle $\pi + \psi$. Thus, $\pi = m\psi$.

How does ψ relate to φ? Let A_1 be the line spanned by α_1, and let A_2 be the line spanned by α_2. Consider the four lines A_1, A_2, L_2, L_1. Imagine starting at α_1, moving counterclockwise until you

[16]Either form is possible, depending on if the path in question first crosses L_1 or first crosses L_2. Either starting wall is fine since w_0 is the longest element; geometrically, a $180°$ arc (clockwise or counterclockwise) from C_+ to $-C_+$ must cross π/ψ walls where ψ is the angle between L_1 and L_2

hit (a point on the line) A_2, then moving counterclockwise until you hit L_2, then continuing until you hit L_1, and the continuing until you get back to A_1 (equivalently, α_1). As you do this, you sweep out a total angle of $\varphi+\frac{\pi}{2}+\psi+\frac{\pi}{2}$. At the same time, since you end up where you start, you also sweep out an angle of size $2\pi k$ for some $k>0$, so

$$\varphi+\frac{\pi}{2}+\psi+\frac{\pi}{2}=2\pi k.$$

Since $\varphi,\psi<\pi$, we see that $k=1$ which gives $\psi=\pi-\varphi$, so (recall $\pi=m\psi$) $\varphi=\pi-\frac{\pi}{m}$ as desired. ∎

(2) The following relations hold in W:

$$s_i^2=1 \text{ and } (s_is_j)^{m_{ij}}=1$$

where $\varphi_{ij}=\pi-\pi/m_{ij}$ is the angle between α_i,α_j.

Proof. The first relation is obvious. For the second relation, assume $i\neq j$ (when $i=j$ we recover the first relation). Let $w=s_is_j$. Since s_j is reflection across the root hyperplane $L_j=L_{\alpha_j}$, it in particular fixes L_j. Similarly, s_i is reflection across the root hyperplane L_i, so fixes L_i. Thus, their composition w fixes the codimension 2 subplane $L_{ij}:=L_i\cap L_j$. Let $P\subset E$ be the orthogonal complement of L_{ij}. Since $w\in \mathrm{SO}(E)$ and $w(L_{ij})=L_{ij}$, we conclude that $w(P)=P$. Note that $\alpha_i,\alpha_j\in P$ since $(\alpha_i,L_{ij})\subset(\alpha_i,L_i)=0$ and similarly for j. Now, $R':=R\cap P\subset P$ is a rank 2 root system with simple roots α_i,α_j. Thus, $w^{m_{ij}}|_P=1$ by part **(1)**.[17] We already knew that $w^{m_{ij}}|_{L_{ij}}=1$, so we conclude that indeed $w^{m_{ij}}=1$. ∎

5.4.2 Descriptions

A_n **Root System** We start with the root system A_n of $\mathfrak{sl}_{n+1}$.

Let $\mathfrak{g}=\mathfrak{sl}_{n+1}(\mathbb{C})=\{\text{traceless matrices}\}$. The usual Cartan subalgebra is $\mathfrak{h}=\{\text{diagonal matrices}\}\cong\mathbb{C}^n$. Let $e_i:\mathfrak{g}\to\mathbb{C}$ be the functional picking out the i diagonal entry, so

$$\mathfrak{h}^*=\frac{\bigoplus_{i=1}^{n+1}\mathbb{C}e_i}{\mathbb{C}(e_1+\cdots+e_{n+1}}.$$

The Euclidean space is $E=\mathfrak{h}_{\mathbb{R}}^*$ with the usual dot product w.r.t this basis, i.e.

$$E\cong\left\{x\in\mathbb{R}^{n+1}:\sum x_i=0\right\}.$$

The roots are given by $R=\{e_i-e_j:i\neq j\}$, and given $\alpha=e_i-e_j$, we have

$$\mathfrak{g}_\alpha=\mathbb{C}E_{ij}.$$

[17] $(s_is_j)^{m_{ij}}=w_0^2=(s_is_js_i\dots)(s_js_is_j\dots)$ or $(s_is_js_i\dots)(s_is_js_i\dots)$ depending on if m is odd or even.

The coroot to α is $h_\alpha = \alpha^\vee = E_{ii} - E_{jj} \in \mathfrak{h}$. Thinking of E as an abstract root system and identifying $E \cong E^*$, one has $\alpha^\vee = e_i - e_j$ as well (since $(\alpha, \alpha) = 2$). The positive and simple roots are

$$R_+ = \{e_i - e_j : i < j\} \text{ and } \Pi = \{\alpha_i := e_i - e_{i+1}\}$$

($\#R_+ = \binom{n+1}{2}$). The A_n Dynkin diagram is a path of length n. The Weyl group is $W = S_{n+1}$ with the

$$\bullet \text{ —— } \bullet \text{ —— } \cdots \text{ —— } \bullet \text{ —— } \bullet$$

Figure 2: The Dynkin Diagram A_n

simple reflection $s_i = s_{\alpha_i}$ acting via the transposition $(i\, i+1)$. The weight and root lattices are

$$P = \left\{(\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{R}^{n+1} : \sum \lambda_i = 0 \text{ and } \lambda_i - \lambda_j \in \mathbb{Z}\right\} \text{ and } Q = \left\{(\lambda_1, \ldots, \lambda_{n+1}) : \lambda_i \in \mathbb{Z}, \sum \lambda_i = 0\right\},$$

so

$$\frac{P}{Q} \simeq \frac{\mathbb{Z}}{(n+1)\mathbb{Z}} \text{ via } (\lambda_1, \ldots, \lambda_{n+1}) \mapsto \lambda_1 \in \frac{1}{n+1}\mathbb{Z}/\mathbb{Z}$$

(note $\sum \lambda_i = 0 \in \mathbb{Z}$)

B_n **Root System** This is the root system of $\mathfrak{g} = \mathfrak{so}_{2n+1}$. We use the split quadratic form $q(x) = x_{2n+1}^2 + \sum_{i=1}^n x_i x_{i+n}$ attached to the symmetric bilinear form represented by the matrix

$$B = \begin{pmatrix} & I_n & \\ I_n & & \\ & & 1 \end{pmatrix}.$$

Hence,

$$\mathfrak{g} = \mathfrak{so}(B) = \left\{a \in \mathfrak{gl}_{2n+1}(\mathbb{C}) : a + B^{-1}a^t B = 0\right\}.$$

This has Cartan subalgebra

$$\mathfrak{h} = \mathfrak{g} \cap \{\text{diagonal matrices}\} = \{\operatorname{diag}(x_1, \ldots, x_n, -x_1, \ldots, -x_n, 0)\}.$$

Let $e_i : \mathfrak{h} \to \mathbb{C}$ pick out the ith diagonal component, so $e_1, \ldots, e_n$ give a basis of $\mathfrak{h}^*$. The inner product is given by $(e_i, e_j) = \delta_{ij}$. The root system is

$$R = \{\pm e_i \pm e_j : i \neq j\} \cup \{\pm e_i\}$$

with arbitrary signs. These have the following root subspaces and coroots

α	$\mathfrak{g}_\alpha$	h_α	$\alpha^\vee$
$\alpha = e_i - e_j$	$\mathbb{C}(E_{ij} - E_{j+n,i+n})$	$H_i - H_j$	α
$\alpha = e_i + e_j$	$\mathbb{C}(E_{i,j+n} - E_{j,i+n})$	$H_i + H_j$	α
$\alpha = -e_i - e_j$	$\mathbb{C}(E_{i+n,j} - E_{j+n,i})$	$-H_i - H_j$	α
$\alpha = e_i$	$\mathbb{C}(E_{i,2n+1} - E_{2n+1,n+i})$	$2H_i$	2α
$\alpha = -e_i$	$\mathbb{C}(E_{n+i,2n+1} - E_{2n+1,i})$	$-2H_i$	-2α

where $H_i := E_{ii} - E_{i+n,i+n}$. The positive and simple roots are

$$R_+ = \{e_i \pm e_j : i < j\} \cup \{e_i\} \text{ and } \Pi = \{\alpha_i := e_i - e_{i+1} : 1 \le i < n\} \cup \{\alpha_n := e_n\}$$

($\#R_+ = n^2$). The fundamental weights are

$$\omega_i = (\underbrace{1, \dots, 1}_{i}, 0, \dots, 0) \text{ for } i = 1, \dots, n-1$$

and

$$\omega_n = \left(\frac{1}{2}, \dots, \frac{1}{2}\right).$$

The Dynkin diagram is

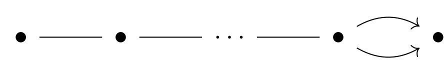

Figure 3: The Dynkin Diagram B_n

The Weyl group is $W = S_n \ltimes (\mathbb{Z}/2\mathbb{Z})^n$ (permute coordinates and change signs). The weight are root lattices are

$$P = \left\{(\lambda_1, \dots, \lambda_n) : \lambda_i \in \frac{1}{2}\mathbb{Z}, \lambda_i - \lambda_j \in \mathbb{Z}\right\} \text{ and } Q = \mathbb{Z}^n,$$

so $P/Q \cong \mathbb{Z}/2\mathbb{Z}$ via $(\lambda_1, \dots, \lambda_n) \mapsto \lambda_1$.

C_n **Root System** This is the root system of $\mathfrak{g} = \mathfrak{sp}_{2n}$. We use the standard symplectic form

$$J = \begin{pmatrix} & I_n \\ -I_n & \end{pmatrix}$$

so

$$\mathfrak{g} = \mathfrak{sp}_{2n}(\mathbb{C}) = \left\{a \in \mathfrak{gl}_{2n}(\mathbb{C}) : a + J^{-1}a^t J = 0\right\}$$

with Cartan subalgebra $\mathfrak{h}$ consisting of diagonal matrices $\operatorname{diag}(x_1, \dots, x_n, -x_1, \dots, -x_n)$. Can apparently think of J as $J = \sum_{i=1}^n x_i \wedge x_{i+n}$.

The root system is

$$R = \{\pm e_i \pm e_j : i \ne j\} \cup \{\pm 2e_i\}$$

with arbitrary signs. These have the following root subspaces and coroots

α	$\mathfrak{g}_\alpha$	h_α	$\alpha^\vee$
$\alpha = e_i - e_j$	$\mathbb{C}(E_{ij} - E_{j+n,i+n})$	$H_i - H_j$	α
$\alpha = e_i + e_j$	$\mathbb{C}(E_{i,j+n} + E_{j,i+n})$	$H_i + H_j$	α
$\alpha = -e_i - e_j$	$\mathbb{C}(E_{i+n,j} + E_{j+n,i})$	$-H_i - H_j$	α
$\alpha = 2e_i$	$\mathbb{C}E_{i,i+n}$	H_i	α
$\alpha = -2e_i$	$\mathbb{C}E_{i+n,i}$	$-H_i$	$-\alpha$

where $H_i := E_{ii} - E_{i+n,i+n}$. The positive and simple roots are

$$R_+ = \{e_i \pm e_j : i < j\} \cup \{2e_i\} \text{ and } \Pi = \{\alpha_i := e_i - e_{i+1} : 1 \leq i < n\} \cup \{\alpha_n := 2e_n\}$$

($\#R_+ = n^2$). The fundamental weights are

$$\omega_i = (\underbrace{1, \ldots, 1}_{i}, 0, \ldots, 0) \text{ for } i = 1, \ldots, n.$$

The Dynkin diagram for C_n is

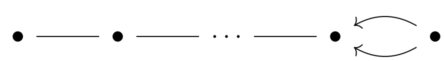

Figure 4: The Dynkin Diagram C_n

The Weyl group is $W = S_n \rtimes (\mathbb{Z}/n\mathbb{Z})^n$ (S_n permutes while $(\mathbb{Z}/n\mathbb{Z})^n$ changes signs).

Remark 5.25. B_n and C_n are dual root systems.

The weight and root lattices are

$$P = \mathbb{Z}^n \text{ and } Q = \left\{(\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n : \sum \lambda_i \in 2\mathbb{Z}\right\},$$

so $P/Q \cong \mathbb{Z}/2\mathbb{Z}$.

D_n **Root System** Now the Root System of $\mathfrak{g} = \mathfrak{so}(2n)$. We use the split quadratic form $q(x) = \sum_{i=1}^n x_i x_{i+n}$ attached to

$$B = \begin{pmatrix} & I_n \\ I_n & \end{pmatrix},$$

so $\mathfrak{g} = \mathfrak{so}(B) = \left\{a \in \mathfrak{gl}_{2n+1} : a + B^{-1}a^t B = 0\right\}$ with $\mathfrak{h}$ consisting of diagram matrices $\operatorname{diag}(x_1, \ldots, x_n, -x_1, \ldots, -x_n)$. We let e_i pick out the ith diagonal component. The roots are

$$R = \{\pm e_i \pm e_j : i \neq j\}$$

with arbitrary signs. These have the following root subspaces and coroots

α	$\mathfrak{g}_\alpha$	h_α	$\alpha^\vee$
$\alpha = e_i - e_j$	$\mathbb{C}(E_{ij} - E_{j+n,i+n})$	$H_i - H_j$	α
$\alpha = e_i + e_j$	$\mathbb{C}(E_{i,j+n} - E_{j,i+n})$	$H_i + H_j$	α
$\alpha = -e_i - e_j$	$\mathbb{C}(E_{i+n,j} - E_{j+n,i})$	$-H_i - H_j$	α

where $H_i := E_{ii} - E_{i+n,i+n}$. The positive and simple roots are

$$R_+ = \{e_i \pm e_j : i < j\} \text{ and } \Pi = \{\alpha_i := e_i - e_{i+1} : 1 \le i < n\} \cup \{\alpha_n := e_{n-1} + e_n\}$$

($\#R_+ = n(n-1)$). The Dynkin diagram is

$$\begin{tikzcd}[arrows=dash]
 & & & & \alpha_{n-1} \\
\alpha_1 \arrow[r] & \alpha_2 \arrow[r] & \cdots \arrow[r] & \alpha_{n-2} \arrow[ur] \arrow[dr] & \\
 & & & & \alpha_n
\end{tikzcd}$$

Figure 5: The Dynkin Diagram D_n

The fundamental weights are $\omega_1 = (1, 0, \ldots, 0), \omega_2 = (1, 1, 0, \ldots, 0)$ up to $\omega_{n-2} = (1, \ldots, 1, 0, 0)$ and then

$$\omega_{n-1} = \left(\frac{1}{2}, \ldots, \frac{1}{2}, -\frac{1}{2}\right) \text{ and } \omega_n = \left(\frac{1}{2}, \ldots, \frac{1}{2}, \frac{1}{2}\right).$$

The Weyl group here is $S_n \ltimes (\mathbb{Z}/2\mathbb{Z})_0^n$ where the 0 subscript means elements whose coordinates sum to 0. The weight and root lattices are

$$P = \left\{(\lambda_1, \ldots, \lambda_n) : \lambda_i \in \frac{1}{2}\mathbb{Z}, \lambda_i - \lambda_j \in \mathbb{Z}\right\} \text{ and } Q = \left\{(\lambda_1, \ldots, \lambda_n) : \lambda_i \in \mathbb{Z}, \sum \lambda_i \in 2\mathbb{Z}\right\},$$

so we have an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}^n/Q \arrow[r] \arrow[d, "\sum \lambda_i"', "\wr"] & P/Q \arrow[r, "\lambda_1"] & \frac{1}{2}\mathbb{Z}/\mathbb{Z} \arrow[r] \arrow[d, "\wr"] & 0 \\
 & \mathbb{Z}/2\mathbb{Z} & & \mathbb{Z}/2\mathbb{Z} &
\end{tikzcd}$$

which is split iff n is even, i.e.

$$P/Q \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{if } n \text{ even} \\ \mathbb{Z}/4\mathbb{Z} & \text{if } n \text{ odd.} \end{cases}$$

G_2 **Root System** This root system consists of the vectors in $\mathbb{R}_0^3 := \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0\}$ with squared-length 2 or 6, i.e. the roots are $\pm\alpha_i$ for $1 \le i \le 6$, where (e_1, e_2, e_3 an orthonormal basis for $\mathbb{R}^3$)

$$\alpha_1 = (e_1 - e_2),\ \ \alpha_2 = (e_1 - e_3),\ \ \alpha_3 = (e_2 - e_3),\ \ \alpha_4 = (2e_1 - e_2 - e_3),\ \ \alpha_5 = (e_1 - 2e_2 + e_3), \text{ and } \alpha_6 = (e_1 + e_2 - 2e_3),$$

and we can choose a polarization so that $R_+ = \{\alpha_1, \alpha_2, \ldots, \alpha_6\}$, e.g. by polarizing with respect to $t = (t_1, t_2, t_3)$ with $t_1 > 2t_2 > 2t_3$. With this polarization, the simple roots are[18] $\Pi = \{\alpha_3, \alpha_5\}$. The

[18] $\alpha_1 = \alpha_3 + \alpha_5$, $\alpha_2 = \alpha_1 + \alpha_3$, $\alpha_4 = \alpha_5 + \alpha_6$, and $\alpha_6 = \alpha_2 + \alpha_3$ so these aren't simple.

coroots are

$$\alpha_i^\vee = \alpha_i \text{ for } 1 \le i \le 3 \text{ and } \alpha_i^\vee = \frac{1}{3}\alpha_i \text{ for } 4 \le i \le 6.$$

The fundamental weights are $\omega_1 = e_1 - e_3 = \alpha_2$ and $\omega_2 := 2e_1 - e_2 - e_3 = \alpha_4$. One can check that $P = Q$ (i.e. the Cartan matrix has determinant 1). Furthermore, the Weyl group is D_{12}, the dihedral group of order 12.

Computation. We compute the Weyl group of G_2. It is generated by the simple reflections $s_1 := s_{\alpha_3}$ and $s_2 := s_{\alpha_5}$. Since the angle between α_3 and α_5 is

$$\cos^{-1}\left(\frac{(\alpha_3, \alpha_5)}{\sqrt{(\alpha_3, \alpha_3)(\alpha_5, \alpha_5)}}\right) = \cos^{-1}\left(\frac{-3}{\sqrt{2 \cdot 6}}\right) = \frac{5\pi}{6} = \pi - \frac{\pi}{6},$$

we see that these satisfy $s_1^2 = 1 = s_2^2$ and $(s_1s_2)^6 = 1$,[19] so the Weyl group $W = W(G_2)$ is a quotient of

$$\left\langle s_1, s_1 \mid s_1^2, s_2^2, (s_1s_2)^6 \right\rangle \cong \left\langle s, r \mid s^2, r^6, (sr)^6 \right\rangle \cong D_{12},$$

where $s = s_1$, $r = s_1s_2 = s_1^{-1}s_2$, and D_{12} is the group of symmetries of a hexagon. There are only 12 elements here, so one can simply check by hand that the natural map $D_{12} \twoheadrightarrow W$ is injective, i.e. that $W \simeq D_{12}$.

The Cartan matrix is

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

and the Dynkin diagram is

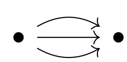

Figure 6: The Dynkin Diagram G_2

F_4 **Root System** Let $F_4 \subset \mathbb{R}^4$ be the union of B_4 and the vectors $\left(\pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}\right) = \frac{1}{2}\sum_{i=1}^4 (\pm e_i)$ for all choices of signs. Recall that B_4 had roots $\pm e_i \pm e_j$ for $1 \le i \ne j \le 4$. and $\pm e_i$ for $1 \le i \le 4$. Hence, B_4 has $4\binom{4}{2} + 2(4) = 32$ roots. We've just added 16 more, so altogether F_4 has 48 roots.

Exercise. Show this is an irreducible root system.

Pick a polarization $t = (t_1, t_2, t_3, t_4)$ such that $t_1 \gg t_2 \gg t_3 \gg t_4 > 0$ (e.g. $t_i = N^i$ for $N \gg 1$) where $\gg$ informally means "much bigger." Clearly e_4 is a simple root (it has positive inner product t_4 and also minimizes the inner product of t with any positive root). We now look at roots involving t_3, t_4. The simple root here will be $e_3 - e_4$ since it has the smallest positive inner product with t (after through away e_4). The next one is $e_2 - e_3$ and then finally we have $\frac{1}{2}(e_1 - e_2 - e_3 - e_4)$. We call these

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \left(\frac{1}{2}(e_1 - e_2 - e_3 - e_4), e_4, e_3 - e_4, e_2 - e_3\right).$$

[19] e.g. by Kirillov **Problem 7.11(2)** from HW9 last semester

Then,

$$\begin{aligned}
\alpha_1^\vee &= 2\alpha_1 = e_1 - e_2 - e_3 - e_4 \\
\alpha_2^\vee &= 2\alpha_2 = 2e_4 \\
\alpha_3^\vee &= \alpha_3 \\
\alpha_4^\vee &= \alpha_4
\end{aligned}$$

Finally, we draw the diagram

$$\alpha_1 \text{ —— } \alpha_2 \Leftarrow \alpha_3 \text{ —— } \alpha_4$$

Figure 7: A Dynkin diagram of type F_4

Remark 5.26. The F_4 root system is like the units in the ring of Hamilton integers or something like this.

Problem 22.{3,4}. *Let $F_4 \subset \mathbb{R}^4$ consist of the vectors*

$$\sum_{i=1}^{4} \left(\pm \frac{1}{2} e_i\right), \quad \pm e_i \pm e_j, \quad \textit{and} \quad \pm e_i$$

where $i \neq j$ in the second case. This gives an irreducible root system with Dynkin diagram F_4.

Proof. These vectors span $\mathbb{R}^4$ e.g. since they contain $e_1, \dots, e_4$. We next show $n_{\alpha\beta} \in \mathbb{Z}$ for all $\alpha, \beta \in F_4$. First note that $(\alpha, \beta) \in \frac{1}{2}\mathbb{Z}$ for all $\alpha, \beta \in F_4$. When $\alpha = \sum_{i=1}^4 \left(\pm\frac{1}{2}e_i\right)$ or $\alpha = \pm e_i$, we have $(\alpha, \alpha) = 1$, so $n_{\alpha\beta} = 2(\alpha, \beta)/(\alpha, \alpha) = 2(\alpha, \beta) \in \mathbb{Z}$ for all $\beta \in F_4$. Finally, when $\alpha = \pm e_i \pm e_j$, we have $(\alpha, \beta) = 0, \pm 1, \pm 1 \pm 1$, or $\pm\frac{1}{2} \pm \frac{1}{2}$ depending on the form of β; in any case $n_{\alpha\beta} = 2(\alpha, \beta)/(\beta, \beta) = (\alpha, \beta) \in \mathbb{Z}$, so we're good there. Finally, we need to check that the reflection of a root is a root. When $\alpha = \sum_{i=1}^4 (\frac{1}{2}c_i e_i)$, we have (below $c_i = \pm 1$)

$$s_\alpha(e_j) = e_j - \left(\sum_{i=1}^4 c_i e_i, e_j\right)\alpha = e_j - \frac{1}{2}\sum_{i=1}^4 (c_j c_i) e_i = \frac{1}{2}e_j - \frac{1}{2}\sum_{\substack{i=1\\ i\neq j}}^4 (c_j c_i) e_i \in F_4.$$

Similarly,

$$s_\alpha(e_j \pm e_k) = \frac{1}{2}e_j \pm \frac{1}{2}e_k - \frac{1}{2}\sum_{\substack{i=1\\ i\neq j}}^4 (c_j c_i) e_i \mp \frac{1}{2}\sum_{\substack{i=1\\ i\neq k}}^4 (c_k c_i) e_i = \frac{1}{2}(1 \mp c_k c_j) e_j + \frac{1}{2}(\pm 1 - c_j c_k) e_k - \frac{1}{2}\sum_{\substack{i=1\\ i\neq j,k}}^4 (c_j \pm c_k) c_i e_i = \pm e_s \pm e_t \in F_4$$

with s, t and their coefficients depending on the choice of c_i an $\pm$ on the LHS above. Furthermore ($d_j = \pm 1$),

$$s_\alpha\left(\frac{1}{2}\sum_{j=1}^4 d_j e_j\right) = \frac{1}{2}\left[\sum_{i=1}^4 d_i e_i - \frac{1}{2}\left(\sum_{i=1}^4 c_i d_i\right)\sum_{i=1}^4 c_i e_i\right] = \frac{1}{2}\sum_{i=1}^4 \pm e_i \in F_4.$$

We still need to check that $s_\alpha(\beta) \in F_4$ when $\beta = \frac{1}{2}\sum_{i=1}^4 (\pm e_i)$ (when neither α nor β is of this form, we're fine since we know about the B_4 root system); I'll save you the joy of staring and more ugly expressions with lots of $\pm$'s floating around and just promise you that the remaining cases work out as well, so F_4 really is a root system.

We now turn to determining its Dynkin diagram. Once we see that it is connected, we'll immediately conclude that F_4 is irreducible. Fix $t \in \mathbb{R}^4$ with $t_1 \gg t_2 \gg t_3 \gg t_4$.[20] This will give us our polarization. What are our simple roots? Well, we know $\alpha_2 := e_4$ must be simple; any other positive root β has a positive coefficient on e_i for some $i < 4$ and so (since $t_i \gg t_4$) will have $(t, \beta) > t_4$. This means e_4 can't be a sum of other positive roots. Continuing with this line of thought, the root with next smallest inner product with t is $\alpha_3 = e_3 - e_4$ (other positive roots include a e_2 or $\frac{1}{2}e_1$ or e_1 which are all too "big"), so this is simple as well by similar reasoning. This is followed by $\alpha_4 = e_2 - e_3$ and finally $\alpha_1 = \frac{1}{2}(e_1 - e_2 - e_3 - e_4)$. $\operatorname{rank} F_4 = 4$, so these are all the simple roots.

Now, the Dynkin diagram. One easily checks that $\alpha_1^\vee = 2\alpha_1$ so $\alpha_1^\vee(\alpha_i) \neq 0$ iff $i \in \{1, 2\}$. Similarly, $\alpha_2^\vee = 2\alpha_2$ so $\alpha_2^\vee(\alpha_i) \neq 0 \implies i \in \{2, 1, 3\}$, and finally, $\alpha_3^\vee(\alpha_i) \neq 0 \implies i \in \{3, 2, 4\}$. Thus, the vertices of the Dynkian diagram are connected in a chain $1 - 2 - 3 - 4$ with

- $\alpha_1^\vee(\alpha_2)\alpha_2^\vee(\alpha_1) = (-1)^2 = 1$ edge $1 - 2$
- $\alpha_2^\vee(\alpha_3)\alpha_3^\vee(\alpha_2) = (-2)(-1) = 2$ edges $2 \leftleftarrows 3$
- $\alpha_3^\vee(\alpha_4)\alpha_4^\vee(\alpha_3) = (-1)(-1) = 1$ edge $3 - 4$

This is the F_4 Dynkin diagram

$$\begin{tikzcd} 1 \arrow[r, dash] & 2 & 3 \arrow[l, bend right] \arrow[l, bend left] \arrow[r, dash] & 4 \end{tikzcd}$$

as desired. ∎

E_6, E_7, E_8 Root Systems

(E_8) Here, $E_8 \subset \mathbb{R}^8$ is the union of D_8 and the vectors

$$\frac{1}{2}\sum_{i=1}^{8}(\pm e_i)$$

with an *even* number of minuses. The roots are $\pm e_i \pm e_j$ with $1 \le i \neq j \le 8$ (112 of them) and $\frac{1}{2}\sum_{i=1}^{8} \pm e_i$ (128 of them (7 choices of sign)). Thus, we have 240 roots in total.

Exercise. Show this is a reduced, irreducible root system.

Note that all roots in this case have the same length $|\alpha|^2 = 2$. We need to find the simple roots. As before, choose a polarization with

$$t_1 \gg t_2 \gg \cdots \gg t_8 > 0.$$

The first simple root will be $e_7 - e_8$, followed by $e_7 + e_8$. We next have $e_6 - e_7$ and then $e_5 - e_6$, then $e_4 - e_5$, then $e_3 - e_4$, then $e_2 - e_3$. Finally, we have $\frac{1}{2}(e_1 - e_2 - e_3 - \cdots - e_7 + e_8)$. We label these

$$(\alpha_1, \alpha_2, \ldots, \alpha_8) = \left(\frac{1}{2}(e_1 - e_2 - \cdots - e_7 + e_8), e_7 + e_8, e_7 - e_8, e_6 - e_7, e_5 - e_6, e_4 - e_5, e_3 - e_4, e_2 - e_3\right)$$

[20] I think something like $t_i > 3\sum_{j=i+1}^{4} t_j$ will work

We obtain the diagram pictured in Figure 8.

$$\begin{tikzcd}[arrows=dash]
 & & \alpha_2 \arrow[d] & & & & \\
\alpha_1 \arrow[r] & \alpha_3 \arrow[r] & \alpha_4 \arrow[r] & \alpha_5 \arrow[r] & \alpha_6 \arrow[r] & \alpha_7 \arrow[r] & \alpha_8
\end{tikzcd}$$

Figure 8: A Dynkin diagram of type E_8

(E_7) Note that E_7 is a subdiagram of E_8 obtained by throwing away the 8th vertex. Hence, we can describe it as the subsystem of E_8 generated by $\alpha_1, \ldots, \alpha_7$. Note that these all satisfy the equation $x_1 + x_2 = 0$. Hence, $E_7 = E_8 \cap \{x \in \mathbb{R}^8 : x_1 + x_2 = 0\}$. The roots are $\pm e_i \pm e_j$ for $3 \leq i \neq j \leq 8$ (60 of these), $\pm(e_1 - e_2)$ (2 of these), and $\frac{1}{2}\sum_{i=1}^{8}(\pm e_i)$ with evenly many $-$'s and sign of e_1 opposite to sign of e_2 (64 of these). Hence, 126 roots in total.

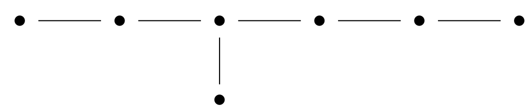

Figure 9: The Dynkin Diagram E_7

(E_6) Like before, this is a subsystem of E_7 (and of E_8) generated by $\alpha_1, \ldots, \alpha_6$ (cut $7, 8$ from the E_8 diagram). These roots have the equations $x_1 + x_2 = 0$ and $x_2 + x_3 = 0$ (but not for α_7, α_8) so $E_6 = E_8 \cap \{x \in \mathbb{R}^8 : x_1 + x_2 = 0 = x_2 + x_3\}$. What are the roots? Our vectors are of the form $(a, -a, a, b, c, \ldots)$. We have roots $\pm e_i \pm e_j$ with $4 \leq i \neq j \leq 8$ (40 of these) and $\frac{1}{2}\left(\sum_{i=1}^{8}(\pm e_i)\right)$ with evenly many $-$'s and the signs of e_1, e_3 both opposite to that of e_2 (32 of these). Hence, 72 roots in total.

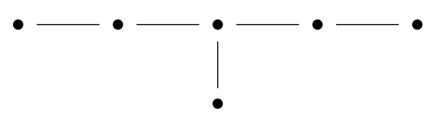

Figure 10: The Dynkin Diagram E_6

Problem 22.{6.7}. *Let $E_8 \subset \mathbb{R}^8$ consist of the vectors*

$$\sum_{i=1}^{8}\left(\pm\frac{1}{2}e_i\right) \quad \textit{and} \quad \pm e_i \pm e_j$$

where there are evenly many $-$ signs in the first case, and $i \neq j$ in the second case. This gives an irreducible root system with Dynkin diagram E_8.

Proof. These generate $\mathbb{R}^8$ since their span contains $2e_1 = (e_1 - e_2) + (e_1 + e_2)$ as well as $2e_i = (e_i - e_1) + (e_i + e_1)$ when $i \neq 1$. We have $n_{\alpha\beta} \in \mathbb{Z}$ for all $\alpha, \beta \in E_8$ since all roots have square length 2 and $(\alpha, \beta) \in \mathbb{Z}$ for $\alpha, \beta \in E_8$; this is maybe not immediately obvious when α, β are both of the form $\sum \pm \frac{1}{2} e_i$, but in this case the fact that each has evenly many $-$'s tells us that they will have differing signs in evenly many, say $2k$, slots and so will have inner product

$$(\alpha, \beta) = \frac{1}{4}(8 - 2k) - \frac{1}{4}(2k) = 2 - k \in \mathbb{Z}.$$

Typing a bunch of calculations showing that $s_\alpha(\beta) \in E_8$ when $\alpha, \beta \in E_8$ seems like a slog, so I'll just appeal to the fact that there are only finitely many cases to check, and so one can see this easily e.g. by writing a few loops in Mathematica. This tells us that E_8 forms a (reduced) root system.

We now calculate its Dynkin diagram. Polarize using $t \in \mathbb{R}^8$ with

$$t_1 \gg t_2 \gg t_3 \gg t_4 \gg t_5 \gg t_6 \gg t_7 \gg t_8.$$

As in the previous problems, if α is a root such that (t, α) is sufficiently small (and α is not an integral combination of other known simple roots), then α must itself be simple as $\alpha = \beta_1 + \beta_2$ (with $\beta_1, \beta_2 \in R$ s.t. $(t, \beta_i) > (t, \alpha)$), for example, would imply $(t, \alpha) = (t, \beta_1) + (t, \beta_2) > (t, \beta_1) > (t, \alpha)$, a contradiction. Thus, the simple roots will be the unique roots $\beta_1, \beta_2, \ldots, \beta_8$ with

$$\beta_i = \operatorname*{arg\,min}_{\substack{\beta \in R_+ \\ \beta \notin \operatorname{span}\{\beta_1, \ldots, \beta_{i-1}\}}} (t, \beta).$$

These are

$$(\beta_1, \beta_2, \ldots, \beta_8) = \left(e_7 - e_8, e_7 + e_8, e_6 - e_7, e_5 - e_6, e_4 - e_5, e_3 - e_4, e_2 - e_3, \frac{1}{2}(e_1 - e_2 - \cdots - e_8)\right).$$

To make the Dynkin diagram show up in the standard form, we relabel these as

$$\begin{aligned} (\alpha_1, \alpha_2, \ldots, \alpha_8) &:= (\beta_8, \beta_2, \beta_1, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7) \\ &= \left(\frac{1}{2}(e_1 - e_2 - \cdots - e_7 + e_8), e_7 + e_8, e_7 - e_8, e_6 - e_7, e_5 - e_6, e_4 - e_5, e_3 - e_4, e_2 - e_3\right). \end{aligned}$$

Now, $(\alpha_1, \alpha_i) \neq 0 \iff i \in \{1, 3\}$ so the 1 vertex is only connected to the 3 vertex. The 3 vertex is in addition connected to the 4 vertex as $(\alpha_3, \alpha_i) \neq 0 \iff i \in \{3, 1, 4\}$. The 4 vertex is a little more friendly; its connected to 2 and 5 in addition to 3. The 2 vertex is connected to nothing else. From 5 to 8, the vertices appear in a chain as each α_i has one basis vector in common with α_{i+1} and none in common with α_j (where $i \geq 4$ and $j > i + 1$). One easily calculates the there is only one edge between any two adjacent vertices, so we do obtain the E_8 Dynkin diagram

$$\begin{array}{ccccccccccccccc} & & & & 2 & & & & & & & & & & \\ & & & & | & & & & & & & & & & \\ 1 & — & 3 & — & 4 & — & 5 & — & 6 & — & 7 & — & 8 \end{array}$$

as claimed. ∎

References

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

6 List of Marginal Comments

Index