Notes for 2025

June 9, 2025

1 Homological Algebra

1.1 Basic Tools

Definition 1. For $f : \mathbf{B} \to \mathbf{C}$, a map of cell complexes, the mapping cone of f is the cell complex following cell complex:

$$\cdots B_{n+1} \oplus C_{n+2} \xrightarrow{\begin{bmatrix} -d_B & 0 \\ -f & d_C \end{bmatrix}} B_n \oplus C_{n+1} \xrightarrow{\begin{bmatrix} -d_B & 0 \\ -f & d_C \end{bmatrix}} B_{n-1} \oplus C_n \cdots$$

Theorem 1. A chain map $f : \mathbf{B} \to \mathbf{C}$ is a quasi-isomorphism exactly when $\mathrm{C}(f)$ is exact.

Proof. There is a natural short exact sequence of chain complexes

$$0 \longrightarrow \mathbf{C} \longrightarrow \mathrm{C}(f) \longrightarrow \mathbf{B}[-1] \longrightarrow 0$$

Hence we get a long exact sequence on homology with differential f_*, explicitly this LES looks like

$$\cdots H_{n+1}(\mathrm{C}(f)) \longrightarrow H_n(B) \xrightarrow{f_*} H_n(C) \longrightarrow H_n(\mathrm{C}(f)) \cdots$$

□

1.2 Abelian Categories

Definition 2. A category $\mathcal{C}$ is called additive when

1. Each Hom set in $\mathcal{C}$ has an abelian group structure with composition distributing naturally over addition.
2. $\mathcal{C}$ has a zero (initial and terminal) object.
3. $\mathcal{C}$ has products.

Definition 3. We expand the definitions of kernel, cokernel, mono and epi to abelian categories. Let $f : C \to D$ be a map in $\mathcal{C}$, then

- ι is the **kernel** of f when for any j such that $fj = 0$ we have that j factors through ι.
- q is the **cokernel** of f when for any s, such that $sf = 0$ we have that s factors through q.
- f is an **epi** when for any $s : D \to D$, $qf = 0$ implies $q = 0$.
- f is a **mono** when for any $j : C \to C$, $fj = 0$ implies $j = 0$.

Definition 4. A category $\mathcal{C}$ is called abelian when

1. Every map in $\mathcal{C}$ has a cokernel and a kernel.
2. Every monic in $\mathcal{C}$ is the kernel of its cokernel.
3. Every epi in $\mathcal{C}$ is the cokernel of its kernel.

Definition 5. A subcategory $\mathcal{C} \subset \mathcal{A}$ is called an **exact subcategory** when any exact sequence in $\mathcal{C}$ is exact in $\mathcal{A}$.

Definition 6. Let $\mathcal{C}$ be an abelian category and X a topological space with $\mathcal{I}$ is its poset of open sets (ordered by inclusion), then a **pre-sheaf** on X is a contravarient functor $\mathcal{F}$ from $\mathcal{I}$ to $\mathcal{C}$ with $\mathcal{F}(\emptyset) = \{0\}$.

Definition 7. Let the objects be defined as in a presheaf, a sheaf on X is a presheaf $\mathcal{F}$, satisfying if $\{U_j\}_J$ is an open cover for $U \subset X$ open and $\{f_j \mid f_j \in \mathcal{F}(U_j)\}_J$ is such that $f_i = f_j$ on $U_i \cap U_j$ for any i, j, then there is a unique $f \in \mathcal{F}(U)$ such that $f|_{U_j} = f_j$ for all j.

Proposition 1. If $\mathcal{C} \subset \mathcal{A}$ is a full subcategory ($\mathcal{A}$ abelian), then $\mathcal{C}$ is additive iff $0 \in \mathcal{C}$ and $\mathcal{C}$ is closed wrt. $\oplus$.

Proposition 2. $\mathcal{C}$ and $\mathcal{A}$ as in Proposition 1, then $\mathcal{C}$ is abelian and $\mathcal{C}$ is an exact subcategory iff $\mathcal{C}$ is closed under $\ker$ and coker.

Proposition 3. The inclusion of Sheaves into Pre-Sheaves is left exact.

Theorem 2. Every additive category $\mathcal{A}$ can be embedded into an abelian category via the **Yoneda Embedding**.

Proof. The functor giving the Yoneda embedding is $\mathcal{F} : A \to \text{Hom}(-, A)$. Left exactness of $\mathcal{F}$ follows from left exactness of $\text{Hom}(M, -)$. □

Remark. (Important) If $\mathcal{A}$ is abelian, then the Yoneda embedding is into an abelian subcategory (the category of *left exact* contravarient functors from $\mathcal{A}$ to **abgp**)

Theorem 3. Yoneda Lemma. If for each M in an additive category $\mathcal{C}$ we have exactness of

$$\text{Hom}(M, A) \xrightarrow{f^*} \text{Hom}(M, B) \xrightarrow{g^*} \text{Hom}(M, C)$$

Then the original sequence

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is exact.

Theorem 4. Freyd-Mitchell Embedding Theorem. If $\mathcal{A}$ is a small abelian category, then there is a ring R, and an exact fully faithful functor from $\mathcal{A}$ into R-Mod. Such that for each $M, N \in \text{Ob}(\mathcal{A})$

$$\text{Hom}_{\mathcal{A}}(M, N) \cong \text{Hom}_R(M, N)$$

1.2.1 Exercises

–Environment– If M is a manifold show that $C^\infty(M)$ is a sheaf.

–Environment– Check that when $\mathcal{A}$ is abelian the category of left exact contravarient functors from $\mathcal{A}$ to **abgp** is abelian c.f. Yoneda Embedding Remark.

1.3 Derived Functors

Definition 8. A covarient 1. homological (2. cohomological) δ**-functor** from $\mathcal{A}$ to $\mathcal{C}$ is a collection of additive functors 1. $T_n : \mathcal{A} \to \mathcal{C}$ (2. $T^n : \mathcal{A} \to \mathcal{C}$) along with for each short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

morphisms 1. $\delta_n : T_n(C) \to T_{n-1}(A)$ (2. $\delta^n : T^n(C) \to T^{n+1}(A)$) such that (i) for each short exact sequence there is an induced long exact sequence

$$1.\ \cdots T_{n+1}(C) \xrightarrow{\delta_{n+1}} T_n(A) \longrightarrow T_n(B) \longrightarrow T_n(C) \xrightarrow{\delta_n} T_{n-1}(A) \cdots$$

$$(2.\ \cdots T^{n-1}(C) \xrightarrow{\delta^{n-1}} T^n(A) \longrightarrow T^n(B) \longrightarrow T^n(C) \xrightarrow{\delta^n} T^{n+1}(A) \cdots\ )$$

And δ commutes with morphisms of short exat sequences.

Remark. Homology is a homological δ-functor from $\mathrm{Ch}_*(\mathcal{A})$ to $\mathcal{A}$. Similarly, cohomology is a cohomological δ-functor from $\mathrm{Ch}^*(\mathcal{A})$ to $\mathcal{A}$

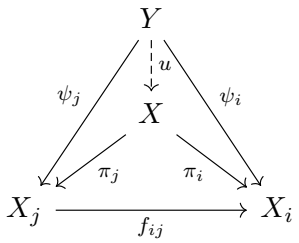
1.3.1 Exercises

–Environment– Show that $\pi : A \to A/p$

1.4 Misc. Category Theory

1.4.1 Properties of Inverse Limits

The **Universal Property** of the inverse limit X is that for any Y compatible with the inverse system $(X_i)_I$ we have a unique morphism u such that the following commutes.



Remark. If the objects of an inverse system are Rings/Modules, and the maps are Ring/Module homomorphisms, then the inverse limit has a Ring/Module structure. Note that this same observation should hold for other mathematical structures.

Proposition 4. If (S_i, π_i) is an inverse system of finite non-empty sets, then $\varprojlim S_i$ is nonempty.

Proof. Let $F_{k,j},\ (k > j)$ be the image of $S_k \to \cdots \to S_j$, since these are finite non-empty sets $F_{k,j}$ is constant for sufficiently large k. Letting E_j be this eventual image, then the E_j form an inverse system with $E_{j+1} \to E_j$ surjective, hence we can choose some e_0, then choose e_1 in its preimage and so on to get an element of $\varprojlim S_i$. □

2 Algebraic Geometry

2.1 Prerequisites

Definition 9. Define the **ideal quotient** (in a ring A), $(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \subset \mathfrak{a}\}$.

2.1.1 Primary Decomposition

Definition 10. $I \subsetneq A$ is called primary if whenever $xy \in I$ we have either $x \in I$ or $y^n \in I$ for some n.

Remark. An equivalent definition is that I is primary when every zero divisor in A/I is nilpotent.

Definition 11. $I \subset A$ is called irreducible if $I = \mathfrak{a} \cap \mathfrak{b}$ implies $I = \mathfrak{a}$ or $I = \mathfrak{b}$.

Proposition 5. If I is primary, then $\sqrt{I}$ is prime. If $\mathfrak{p} = \sqrt{I}$, then I is called $\mathfrak{p}$-primary.

Proposition 6. Finite intersections of $\mathfrak{p}$-primary ideals are $\mathfrak{p}$-primary.

Proof. $\bigcap_1^n \sqrt{\mathfrak{p}_i} = \sqrt{\bigcap_1^n \mathfrak{p}_i}$. □

Proposition 7. If $\mathfrak{q}$ is $\mathfrak{p}$-primary, then for $x \notin \mathfrak{q}$ we have $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary.

Proof. $yz \in (\mathfrak{q} : x)$, then $xyz \in \mathfrak{q}$, if $y \in \sqrt{\mathfrak{q}} \supset (\mathfrak{q} : x)$ we are done, otherwise $xz \in \mathfrak{q}$, so that $z \in (\mathfrak{q} : x)$. □

Definition 12. A primary decomposition of an ideal $\mathfrak{a}$ is an intersection of finitely many primary ideals $\mathfrak{q}_i$, such that $\mathfrak{a} = \bigcap_1^n \mathfrak{q}_i$.

2.1.2 Multiple Complex Variables

Theorem 5. Cauchy's Integral Formula If f is C^∞ on a closed disc D, then $f(z_0) = \int_{\partial D} \frac{f(z)}{z-z_0} dz + \int_D \frac{\frac{\partial f}{\partial \overline{z}}(z)}{z-z_0} dz \wedge d\overline{z}$

Theorem 6. Elliptic Regularity Analytic complex functions are equal to their power series.

Proof. It will suffice to show that holomorphic functions are equal to their power series, let z_0 be in our domain, and γ be a circle of radius r about p in our domain (with z_0 in the interior of $gamma$), then by Cauchy's integral formula:

$$f(z_0) = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{z-z_0}dz = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{z-p}\frac{z-p}{z-p-(z_0-p)}dz = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{z-p}\frac{1}{1-\frac{z_0-p}{z-p}}dz$$
$$= \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{z-p}\sum_0^\infty \left(\frac{z_0-p}{z-p}\right)^n = \frac{1}{2\pi i}\int_\gamma \sum_0^\infty \frac{f(z)}{(z-p)^{n+1}}(z_0-p)^n$$

Since f is continuous and γ is compact, we have that $\sup_\gamma |f| = M$, and it is immediate that $|z_0 - p| < r = |z-p|$ for all $z \in \gamma$. In particular this implies that the sum of functions is abslutely convergent. Swapping the sum and integral gives us

$$f(z_0) = \frac{1}{2\pi i}\sum_0^\infty (z-p)^n \int_\gamma \frac{f(z)}{(z-p)^{n+1}}dz$$

□

Theorem 7. Poincare $\overline{\partial}$ Lemma For any $g \in C^\infty(D)$ we can solve for f defined on a slightly smaller disc, such that $\frac{\partial f}{\partial \overline{z}} = g$.

Proof. I will just provide a sketch of the main ideas of this proof, it is written out in Griffiths and Harris. □

2.2 Honest AG

Remark. The starting point for algebraic geometry is studying the zero locus of a set of polynomials, $V(\{f_i(X_1, \ldots, X_n)\}_{i \in I}) \subset k^n$. The approach in this subject is to study the ring of functions $V \to k$, obtained by restriction of functions on k^n to functions on V.

Remark. I am taking these notes shortly after concluding a course on commutative algebra, as such I will be skipping over the going up theorem, Hilbert's Nullstellensatz, etc. Some definitions such as that of a variety, closed algebraic set, etc. I will go over again as to establish a convention.

Definition 13. A **closed algebraic set** is a set of the form $V(I)$, where $I \subset k[X_1, \ldots, X_n]$.

Definition 14. A closed algebraic set is **irreducible** if it cannot be written as the union of two strictly smaller algebraic sets.

2.3 Arithmetic Geometry

Definition 15. An **absolute value** on a field k is a function $|\cdot| : k \to \mathbb{R}_{\geq 0}$ satisfying

1. Positive definiteness.
2. $|xy| = |x| \cdot |y|$
3. $|\cdot|$ satisfies the triangle inequality.

Remark. When $k = \mathbb{Q}$ the euclidean absolute value $|\cdot|$ is often denoted as $|\cdot|_\infty$.

Definition 16. Two absolute values $|\cdot|$ and $|\cdot|'$ on a field k are **equivalent** when there is some $\alpha \in \mathbb{R}_{>0}$, such that for any $x \in k$ we have $|x|^\alpha = |x|'$.

Theorem 8. Ostrowski's classification theorem Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to $||_p$ for some $p \in \text{Primes} \cup \{\infty\}$

Definition 17. $\mathbb{Z}_p := \varprojlim \mathbb{Z}/(p^n)$

Proposition 8. $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p$

Proof. One direction is obvious, for the other direction if $(a_1, a_2, \ldots)$ is invertible, then note that inverses behave well with respect to projection, so that $(a_1^{-1}, a_2^{-1}, \ldots) \in \mathbb{Z}_p$. □

Remark. It is an important observation that any $a \in \mathbb{Z}_p \setminus \{0\}$ can be uniquely in the form $p^n u$ for $u \in \mathbb{Z}_p^\times$.

Definition 18. $\mathbb{Q}_p := \text{Frac}\, \mathbb{Z}_p$. I.e. the field of fractions of $\mathbb{Z}_p$.

Definition 19. The **p-adic valuation** $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ is defined via $p^n u \mapsto n$ (where $u \in \mathbb{Z}_p^\times$) and $0 \mapsto \infty$.

Definition 20. The **p-adic absolute value** $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}$ via $|x|_p := p^{-v_p(x)}$.

Theorem 9. $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. Note here that there is a natural inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.

Proof. Let (a_n) be a cauchy sequence in $\mathbb{Q}_p$, since it is bounded, we may multiply by p^k for some k and consider a sequence in $\mathbb{Z}_p$. Denote $(a_n) = S_0$, then for each $n \in \mathbb{Z}_{>0}$ there is some subsequence $S_n \subset S_{n-1}$ such that S_n is constant in $\mathbb{Z}/(p^n)$, choose a diagonal sequence then this forms a convergent subsequence of the cauchy sequence $S_0 = (a_n)$. This implies that $\mathbb{Q}_p$ is complete.

If a is in $\mathbb{Q}_p$, then there is a sequence in $\mathbb{Q}$ that converges to it, to see this we can first consider $a = (a_1, a_2, \ldots) \in \mathbb{Z}_p$ by clearing its denomenator, so that $a_1, a_2, \ldots$ is a convergent $\mathbb{Q}$-valued sequence. □

Proposition 9. Let $f \in \mathbb{Z}_p[X]$, then f has a root in $\mathbb{Z}_p$ if and only if f has a root in $\mathbb{Z}/(p^n)$ for each n.

Proof. One direction is obvious, in the other direction the solution sets are finite and non-empty, thus a categorical result completes the proof. □

Theorem 10. Hensel's lemma Let $f \in \mathbb{Z}_p[X]$ and $\alpha \in \mathbb{Z}/(p)$ such that $f(\alpha) = 0 + (p)$ and $f'(\alpha) \neq 0 + (p)$, then α lifts to a unique root in $\mathbb{Z}_p$.

Proof. This is an elementary proof using p-adic Newton's method. □

The following definitions and results serve to establish the structure of the groups $\mathbb{Z}_p^\times$ and $\mathbb{Q}_p^\times$.

Definition 21. $\mu_{p-1} := \{x \in \mathbb{Z}_p \mid x^{p-1} = 1\}$, note that this is a group under multiplication.

Definition 22. $U_n := 1 + p^n\mathbb{Z}_p$

Proposition 10. $\mathbb{Z}_p^\times = U_1 \times \mu_{p-1}$

Proof. $U_1 \cap \mu_{p-1} = \{1\}$ since by hensels lemma there is a unique solution to $x^{p-1} = 1$ in mod p. Then notice that $\mathbb{Z}_p^\times = U_1 \cdot \mu_{p-1}$, since we can divide any unit by an element of μ_{p-1} to get an element of U_1. □

Theorem 11. $\mathbb{Z}_2^\times \cong \mathbb{Z}/(2) \times \mathbb{Z}_2$ and for $p \neq 2$, $\mathbb{Z}_p^\times \cong \mathbb{Z}/(p-1) \times \mathbb{Z}_p$

Proof. First note that by the binomial theorem, if $x \in U_{n-1} \setminus U_n$, then $x^p \in U_n \setminus U_{n-1}$, we also have that $U_1/U_{n+1} \cong \mathbb{Z}/(p^n)$, by considering $x \mapsto x^p$ and $n \mapsto pn$ respectively we get isomorphic inverse systems:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \mathbb{Z}/(p^n) & \longrightarrow & \mathbb{Z}/(p^{n-1}) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & U_1/U_{n+1} & \longrightarrow & U_1/U_n & \longrightarrow & \cdots \end{array}$$

By taking inverse limits, we get $\mathbb{Z}_p \cong U_1$.

In the case $p = 2$, by taking the generator $1 + 4$ for U_2 we can repeat the inverse limit argument, then $U_1/U_2 \cong \mathbb{Z}/(2)$. □

Theorem 12.

$$\mathbb{Q}_2^\times \cong \mathbb{Z} \times \mathbb{Z}/(2) \times \mathbb{Z}_2 \text{ and } \mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}/(p-1) \times \mathbb{Z}_p,\ p \neq 2$$

Proof. $\mathbb{Z} \times \mathbb{Z}_p^\times \cong \mathbb{Q}_p^\times$ via $(n, x) \mapsto p^n x$. □

Theorem 13. $2^n u$ is square in $\mathbb{Q}_2^\times$ if and only if n is even and $u \equiv 1 \bmod 8$. Similarly, $p^n u$ is square if and only if n is even and u is square in $F_p^\times \cong \mathbb{Z}/(p-1)$.

Proof. $p = 2$: $\mathbb{Q}_2^{\times 2}$ corresponds under the isomorphism to $2\mathbb{Z} \times 2\mathbb{Z}_2$, where $2\mathbb{Z}_2$ is the image of U_3.

$p \neq 2$: Use the same correspondence, but $2\mathbb{Z}_p = \mathbb{Z}_p$, and $2\mathbb{Z}/(p-1)$ corresponds to $F_p^{\times 2}$, so $\mathbb{Q}_p^{\times 2}$ corresponds under the isomorphism to $2\mathbb{Z} \times F_p^{\times 2} \times \mathbb{Z}_p$. □

Definition 23. If G is a group, and I is the poset of normal subgroups having finite index ordered by reverse inclusion, then for $K \subset N$ we get the quotient homomorphism $G/K \to G/N$. The profinite completionof G is defined as $\hat{G} := \varprojlim_N G/N$.

Remark. In the case $G = \mathbb{Z}$ the ordering is equivalent to divisibility.

Definition 24. A **profinite group** is the inverse limit of finite groups.

Proposition 11. $\hat{\mathbb{Z}} \cong \prod_{\text{Primes}} \mathbb{Z}_p$

Proof.

$$\mathbb{Z}/(n) \cong \prod_{\text{Primes}} \mathbb{Z}/p^{v_p(n)}$$

Now take the inverse limit of both sides. □

Definition 25. The **profinite topology** on a profinite group $G = \varprojlim G_i$ is defined by giving each G_i the discrete topology, then giving G the subspace topology of $\prod_i G_i$ (since G has projections π_i onto each G_i).

Proposition 12. The **profinite topology** is compact.

Proof. Each G_i with the discrete topology is compact, since they are finite. Furthermore, by Tychonoff's theorem $\prod_i G_i$ is compact. Then define $F_{ij} := \{(x_k)_I \mid \varphi(x_j) = x_i\}$ since each φ_{ij} is continuous (trivial!) F_{ij} is in the preimage of the diagonal on $X_j \times X_i$ which is a closed set, hence F_{ij} is closed. It follows that $\varprojlim G_i = \bigcap_{i \leq j} F_{ij}$ is a closed subset of a compact set, hence compact. □

Definition 26. An **open subgroup** of a profinite group is a subgroup of the form $\pi_i^{-1}(H_i)$, where $\pi_i : \hat{G} \to G_i$, and H_i is a subgroup of G_i.

Definition 27. A **closed subgroup** H of a profinite group is given by taking H_i, H_j compatible with φ_{ij} for all $i, j \in I$ and taking $H := \varprojlim H_i$.

Remark. Open subgroups of a profinite group are the closed subgroups of finite index.

Example 1. The open subgroups of $\mathbb{Z}_p$ are all of the form $p^d\mathbb{Z}_p$, and the closed subgroups are the open subgroups together with $\{0\}$.

Proposition 13. Let E/k be Galois, and let I be the poset of finite Galois extensions F such that $k \subset F \subset E$. Then

$$\text{Gal}(E/k) \cong \varprojlim \text{Gal}(F/k)$$

Proof. We can take $\sigma \mapsto (\sigma|_F)_I$, these maps are compatible by definition, so by the universal property this defines a map into the inverse limit. Furthermore, any compatible system defines an automorphism on E/k, which provides an inverse for this map. □

Remark. By the previous proposition, every Galois group is a profinite group.

Example 2. Recall that finite extensions of finite fields correspond to splitting fields of the polynomials $x^q - x$. And that $\text{Aut}(F_{p^n}/F_p) \cong \mathbb{Z}/(n)$ is cyclic and generated by the Frobenius automorphism. It follows that:

$$\text{Gal}(\overline{F_p}/F_p) \cong \hat{\mathbb{Z}}$$

Definition 28. $k^{\text{ab}} \subset \overline{k}$ is defined as the field generated by all the finite abelian extensions of k.

Theorem 14. Kroneker-Weber $\mathbb{Q}^{\text{ab}} = \bigcup_1^\infty \mathbb{Q}(\zeta_n)$

Proposition 14.

$$\text{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q}) \cong \prod_{\text{Primes}} \mathbb{Z}_p^\times$$

Proof.

$$\text{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/(n))^\times \cong \hat{\mathbb{Z}}^\times \cong \prod_{\text{Primes}} \mathbb{Z}_p^\times$$

To jusify the second isomorphism, take the inverse limit as a ring, then the additive/multiplicative structure is still compatible with that of the additive/multiplicative group so we can specialize after taking the limit. □

2.3.1 Exercises

Exercise 1. Show that a Dedekind domain with finitely many prime ideals is a PID.

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be the prime ideals, then since they are maximal, they are coprime, let $y_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$, then by the chinese remainder theorem there is some x_i such that $x_i = y_i + \mathfrak{p}_i$, and $x_i = 1 + \mathfrak{p}_j,\ j \neq i$. Then (x_i) factors as a product $\prod_1^n \mathfrak{p}_i^{e_i}$, it follows that $(x_i) = \mathfrak{p}_i$ is principle, all other ideals are products of principle ideals hence principle. □

Exercise 2. Let $\mathcal{O}$ be a Dedekind domain, and $\mathfrak{a} \subset \mathcal{O}$ an ideal. Show that $\mathcal{O}/\mathfrak{a}$ is a PID.

Proof. Firstly, the properties of all prime ideals being maximal $\mathfrak{a}$ admits a prime factorization $\prod_1^r \mathfrak{p}_i^{e_i}$, by the correspondence theorem the prime ideals of $\mathcal{O}/\mathfrak{a}$ are exactly the images of the prime ideals containing $\mathfrak{a}$ via the quotient, thus $\mathcal{O}/\mathfrak{a}$ has prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$, the previous argument can still be applied, since any factors of the (x_i) given by some prime ideal $\mathfrak{q} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ get sent to the ideal $1 + \mathfrak{a}$ in the quotient, so that each $\mathfrak{p}_i + \mathfrak{a} = (x_i) + \mathfrak{a}$ is principally generated. It follows that each ideal in $\mathcal{O}/\mathfrak{a}$ is a product of principle ideals hence principle. □

Exercise 3. Show that every ideal of a Dedekind domain $\mathcal{O}$ is generated by two elements.

Proof. Let $\mathfrak{a} \subset \mathcal{O}$, let $x \in \mathfrak{a}$, then $\mathcal{O}/(x)$ is a PID by the previous exercise, it follows that $\mathfrak{a} + (x) = (y) + (x)$, so that $\mathfrak{a} = (x, y)$. □

Exercise 4. Show that if A is a Noetherian ring where every prime ideal is maximal, then A is Artinian.

Proof. First, note that 0 is not prime since it is not maximal. Assume for contradiction that not all ideals of A contain a finite product of prime ideals, and let $\mathfrak{a}$ be maximal with respect to this property. Tautologically, $\mathfrak{a}$ cannot be prime, so let $xy \in \mathfrak{a}$, but $x, y \notin \mathfrak{a}$. It follows that $(\mathfrak{a}+x)(\mathfrak{a}+y) \subset \mathfrak{a}$, and by the maximality assumption both contain products of prime ideals, hence as does $\mathfrak{a}$ a contradiction. So all ideals of A, including zero contain a finite product of prime ideals.

Consider the descending chain of A modules

$$A \supset \mathfrak{p}_1 \supset \mathfrak{p}_1\mathfrak{p}_2 \supset \cdots \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r = 0$$

It is immediate that each of the A-modules

$$A/\mathfrak{p}_1,\ \mathfrak{p}_1/\mathfrak{p}_1\mathfrak{p}_2,\ \ldots,\ \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{r-1}/\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{r-1}$$

is equivalent to an $A/\mathfrak{p}_\mathrm{i}$ (where i is the largest index of the primes in the denomenator) vectorspace V_i. The Noetherian condition implies that each of these vectorspaces must be finite dimensional, which suffices to prove the Artinian condition by allowing for the construction of a composition series via adding a $\dim V_i - 1, \dim V_i - 2, \ldots, 1$ dimensional subspaces to the descending series at each step, since any intermediary module will be a $A/\mathfrak{p}_i$ vectorspace this constitutes a composition series. The length of a composition series is an upper bound for the length of any descending chain by taking common refinements and the Jordan-Holder theorem, hence any descending chain has length at most $\sum_1^r \dim V_i$ and A is Artinian. □

Exercise 5. Let $X \subset \mathbb{A}^2$ be the algebraic curve defined by the equation $y^2 = x^3$, and $f : \mathbb{A}^1 \to X$ be the regular mapping defined via $t \mapsto (t^3, t^2)$. Then f is not an isomorphism.

Proof. Suppose for contradiction that f is an isomorphism, then we have some g, such that $gf = 1_{\mathbb{A}^1}$, by the quotient structure we have that $g = P(x) + Q(x)y$, so that $g \circ f(t) = P(t^2) + Q(t^2)t^3 = t$, but it is immediate by degree considerations that this is impossible. □

Exercise 6. Let X be the curve defined by $y^2 = x^2 + x^3$, then $f : \mathbb{A}^1 \to X$ via $t \mapsto (t^2 - 1, t(t^2 - 1))$. Show that f^* is an isomorphism onto the subring $k[t] \cap \{g(1) = g(-1)\}$.

Proof. first note that f^* is surjective, since $\{g(1) = g(-1)\} = k[t^2 - 1, t^3 - t]$. Now to check that f is injective, first note that $y^2 - x^2 - x^3$ is irreducible, so that $k[X]$ is a domain, we can define a map from $\operatorname{Frac} k[X] \to k(t)$ via the same rule as f^* □

3 Cryptography

3.1 Computational Complexity

Remark. Solving $x^2 = y + (n)$ for arbitrary n is equivalent to integer factorization.

Remark. The Euclidean algorithm has runtime $\mathcal{O}(\log n)$, same for finding the coefficients guaranteed by Bezout's identity. The significance of this is that when additional information about the variables is known $\gcd$ can be used as an efficient route to deal with factorization problems.

Remark. *Encryption as an algebraic expression:* The term "confusion" (Shannon 1945) was coined to express the degree of complexity separating a cypher text and key. For example, a Caeser cypher has weak or linear confusion, being cypher $=$ key $+$ plaintext. In general substitution steps performed in cypher's aim to maximize their algebraic complexity, (or ability to be approximated linealry).

3.2 Encryption methods

3.2.1 RSA Cryptography

The RSA encryption scheme is as follows:

1. Choose large random prime numbers p, q and define $n = pq$
2. Compute $\lambda(n) = [\phi(p), \phi(q)] = [p-1, q-1]$ (here λ is the Carmichael totient, i.e. the smallest n such that for any a coprime to n we have $a^n = 1 + (n)$). Furthermore this is efficient since we have efficient algorithm for gcd and $[p, q] = \frac{pq}{(p,q)}$.
3. Take $1 < e < \lambda(n)$ with $(e, \lambda(n)) = 1$, e is commonly taken to be $2^{16} + 1$.
4. Compute the key $d = e^{-1} \bmod \lambda(n)$
5. The public key is then the tuple (n, e), and encryption is given via $m \mapsto m^e \bmod n$, this can easily be decrytped by the private key (n, d) as we can simply compute $s \mapsto s^d \bmod n$, where $m^{de} \equiv m$.

Remark. Keys with lesser hamming weight can be encrypted much more efficiently due to the repeated squaring operation for computing exponents.

3.2.2 Symmetric Cryptography (AES)

3.3 Elementary Number Theoretic Tools

Theorem 15. Consider the integer n with prime factorization $n = 2^d p_1^{d_1} \cdots p_k^{d_k}$ and $(m, n) = 1$, then

$$x^2 \equiv a \bmod n$$

exactly when both of the following are satisfied

1. $a^{\frac{p_i - 1}{2}} \equiv 1 \bmod p_i$ for all i
2. $a \equiv 1 \bmod 4$ for $d \in \{1, 2\}$
3. $a \equiv 1 \bmod 8$ for $d \geq 3$

3.4 Prime Factorization

Definition 29. A number n is called p smooth when for any prime factor q of n we have $q \leq p$.

Theorem 16. The **AKS primality test** is a polynomial time algorithm (although not practical) for determining whether or not a number is prime. In the next step, we want to find

Theorem 17. The **Quadratic Sieve** algorithm can factor an integer n in time complexity $\mathcal{O}(\exp((\log n)^{1/2}(\log\log n)^{1/2}))$.

For the quadratic sieve method, we first come up with a smoothness bound (the "standard" choice is $Y = \exp(\sqrt{\log n \log\log n})$)

Theorem 18. The **General Number Field Sieve (GNFS)** can factor an integer n in time complexity $\mathcal{O}(\exp((\log n)^{1/3}(\log\log n)^{2/3}))$.