Contents

Chapter 1

Benedict gross, Lecture 30: Gaussian integers

- math e222 L30 20031201
- YouTube link

1.1 Recap: Euclidian Algorithm

For any $a, b \in Z$ with $|b| < |a|$, we can decompose a as $a = \alpha \cdot b + r$ where $0 \leq r \lneq |d|$. This immediately implies certain facts about the structure of ideals in $\mathbb{Z}$.

Theorem 1. every ideal $I \neq 0$ in $\mathbb{Z}$ is principal. The generator of I is the smallest positive integer in the ideal. Formally: $I = (\min\{d \in I : d > 0\})$.

Proof. Let $i \in I$ be a general element. Find its decomposition into d using the Euclidian algorithm as $i = \alpha \cdot d + r$. Reasoning by ideals:

$$
\begin{aligned}
&\forall i \in I, \exists \alpha, r \in \mathbb{Z}, |r| \lneq d, \quad i = \alpha \cdot d + r \\
&\{\text{writing in ideal notation,}\} \\
&\exists r \in \mathbb{Z}, r \notin I, \quad I \subseteq Z \cdot d + r \\
&\{\text{since } I = (d),\} \\
&\exists r \in Z, r \notin \mathbb{Z}, \quad I \subseteq I + r \\
&\implies r = 0
\end{aligned}
$$

□

Theorem 2. Ideal $I = (a, b)$ is a principal ideal $I = (gcd(a, b))$.

Proof. We already know that every ideal I is generated by its smallest positive number d. We will show that $d = gcd(a, b)$. We first show that d is a divisor of a, and a divisor of b. Since $a \in (a, b) = I = (d)$, we know that $a = \alpha \cdot d$ for some $\alpha \in \mathbb{Z}$. Hence d divides a. Similarly, d divides b. To show that d is the *greatest common divisor*, let there be another divisor common divisor d' which divides a and b:

$d \in I = (a, b) \implies d = ma + nb$ (Any element in I can be written as $ma + nb$)
$d'|a \implies d'|ma, d'|b \implies d'|nb$
$d'|ma \wedge d'|nb \implies d'|[(ma + nb) = d]$
$d' \leq d$ (A divisor of a number must be less than or equal to the number)

Hence, $d = gcd(a, b)$. □

Theorem 3. If p is a prime and $p|ab$ then $p|a$ or $p|b$.

Proof. We know that $gcd(a, p) = p \vee gcd(a, p) = 1$, since the only divisors of p are 1 and p itself. If $p|a$ then we are done. If $p \not| a$, then $gcd(a, p) \neq p$, and we must have $gcd(a, p) = 1$. This means that $1 = \alpha a + \beta p$. Multiplying throughout by b, we get that $b = \alpha(ab)\beta(pb)$. We know that $p|ab$, and clearly $p|pb$. Hence, we must have that $p|(ab + pb)$. Therefore, $p|b$. □

Theorem 4. Every integer z has a unique decomposition into a product of primes of the form $z = \pm p_1 p_2 \dots p_n$.

Proof. Proof by induction on the number of factors and using the property that if $p|ab \implies p|a \vee p|b$. We prove this by induction on the size of the number. It clearly holds for 2 since 2 is prime. Now, let us assume it holds till number n. Now we consider $(n + 1)$. If $(n + 1)$ is prime, then the decomposition is immediate. Assume it is not. This means that $(n + 1) = \alpha\beta$, for $\alpha, \beta \leq n$. We know that α, β have unique factorization. We can easily show that the product of two unique factorizations also has a unique factorization. Hence proved. □

So really, given the Euclidian algorithm, we get this kind of prime decomposition and the unicity of factorization.

1.2 $\mathbb{Z}[i]$: The Gaussian integers

The size function is the absolute value $\delta(a+bi) \equiv |a+bi|^2 = a^2+b^2$. A corollary of this is that every ideal of $Z[i]$ is principal. In particular, the ideal I_p such that $\mathbb{Z}[i]/I_p \simeq \mathbb{Z}/p\mathbb{Z}$ where $p \equiv 1 \mod 4$ is principal, and is generated by a single element $a_p + b_p i$, and also that $a_p^2 + b_p^2 = p$. This is Fermat's theorem, which shows that every prime $p \equiv 1 \mod 4$ can be written as a sum of squares.

1.3 $\delta(r) = |r|$ is a size function

Let's try to show that δ is a good size function. Let us pick $B, A \in \mathbb{Z}[i]$. We can write $B = A \cdot w$, where $w = \alpha + \beta i$ where $\alpha, \beta \in \mathbb{Q}$. This is easy to do because in the complex numbers, we know that $B/A = B\bar{A}/(A\bar{A})$, where $\bar{A}$ is the complex conjugate. Hence $w = B/A = B\bar{A}/(A\bar{A})$. We split α, β into their integer and fractional parts by writing $\alpha = \alpha_0 + r_0$, $\beta = \beta_0 + s_0$ where $\alpha_0, \beta_0 \in \mathbb{Z}$ and $-1/2 \leq r_0, s_0 < 1/2$. This gives us:

$$B = Aw = A(\alpha + \beta i) = A(\lfloor \alpha \rfloor + i\lfloor \beta \rfloor) + A(r_0 + s_0 i)$$

Note that $A(\lfloor \alpha \rfloor + i\lfloor \beta \rfloor) \in \mathbb{Z}[i]$. What we have leftover is $r \equiv A(r_0 + s_0 i)$, the remainder. We claim that $\delta(r) < \delta(A)/2$. To prove this, we note that δ which is the absolute value is multiplicative: $\forall u, b \in \mathbb{C}, |ub| = |u||b|$. Hence, we get that $\delta(Ar) = \delta(A)\delta(r) = \delta(A)(r_0^2 + s_0^2)$. Hence we can conclude that:

$$\delta(Ar) = \delta(A)(r_0^2 + s_0^2) \leq \left[\delta(A)(1/2^2 + 1/2^2) = \delta(A)(1/4 + 1/4) = \delta(A)/2\right]$$
$$\delta(Ar) \leq \delta(A)/2$$

Note that the above trick of writing things in terms of $\alpha + \beta i = (\alpha_0 + \beta_0 i) + (r_0 + s_0 i)$ does not allow us to show that all rings of the form $\mathbb{Z}$ with stuff adjoined is Euclidian. For a concrete non-example, take $\mathbb{Z}[\sqrt{-5}]$. Here, the factorization works out to be $(r_0 + 5s_0 i) \leq 1/4 + 5/4$ which *does not decrease* the size. More drastically, $Z[\sqrt{-5}]$ cannot be a Euclidian domain for any choice of size function, since unique factorization fails. $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Chapter 2

Benedict gross, Lecture 31: Gaussian integers

- YouTube link

2.1 Goals for the leture

General version: If R is a domain with unique factorization into primes, then so is $R[X]$.

What we will show: $\mathbb{Z}[X]$ has unique factorization even though it is not a PID. Why is it not a PID? If it were a PID, then prime ideals are maximal. The ideal (X) is prime, but the quotient $\mathbb{Z}[X]/(X) \simeq \mathbb{Z}$ is not a field, hence (X) is not maximal though (X) is prime. Thus $\mathbb{Z}[X]$ is not a PID.

We will show that $\mathbb{Z}[X]$ still has unique factorization even though it is not a PID.

2.2 Investigating factorization in $\mathbb{Z}[x]$

Let's start off with $f(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$. So if we go to $\mathbb{Q}[x]$, we can definitely factor more polynomials than we could over $\mathbb{Z}[x]$.

We write $f(x) = c \cdot p_1(x) \cdot p_2(x) \dots p_n(x)$, where each of the $p_i(x)$ are monic irreducible in $\mathbb{Q}[x]$, and $c \in \mathbb{Q}^x$ is a unit. This factorization is unique because $\mathbb{Q}[x]$ is euclidian, and is thus PID, and is thus a UFD (unique factorization).

For example, if we take $f(x) = 2x + 1$, in the unique factor form, we would write it as $f(x) = 2(x + 1/2)$ since we need a monic polynomial. But we don't have $1/2 \in \mathbb{Z}$, so we are hosed. The problem is that the factors are not in $\mathbb{Z}[X]$.

We need to have a replacement of the notion of a monic polynomial over $\mathbb{Z}[X]$. The analogue of a monic polynomial is what is called as a **primitive polynomial**.

2.3 Primitive Polynomials

A primitive polynomial has the form:

$$f_0(x) \equiv a_n x^n + \cdots + a_0; a_i \in \mathbb{Z}$$
$$\gcd(a_1, a_2, \ldots, a_n) = 1$$
$$(a_1, a_2, \ldots, a_n) = \mathbb{Z} \quad \text{ideal generated by them is } \mathbb{Z}$$

Note that the ideal based condition allows us to multiply by -1 (ie, flip all signs) and still keep that $(a_1, a_2, \ldots, a_n) = \mathbb{Z}$. To remove this degree of freedom, we add the condition that $a_n > 0$.

Theorem 5. any polynomial f over the integers can be written uniquely as $f = cf_0$, where c is an integer and f_0 is primitive. Formally, for all $f \in \mathbb{Z}[x]$, we have $c \in \mathbb{Z}$ and $f_0 \in Z[X]$, f_0 primitive such that $f = cf_0$.

Proof. For a given f, pull out $c \equiv gcd(a_0, a_1, \ldots, a_n)$. Factorize $f = cf_0$, by setting $f_0 \equiv f/c$. If leading coefficient of f_0, $a_n < 0$, then flip the signs: $(c \mapsto -c; f_0 \mapsto -f_0)$. □

Example 6. If we have $f(x) = 6x^2 - 3x + 9$, then we get the factorization $f(x) = 3(2x^2 - x + 3)$.

What's nice is that we have such an expression for rational polynomials as well!

Theorem 7. If $f(x) \in \mathbb{Q}[x]$, we can write it as $f(x) = cf_0(x)$ where $f_0(x)$ is primitive in $\mathbb{Z}[x]$, while $c \in \mathbb{Q}$. This expression is *unique*.

Proof. Given a rational polynomial $f(x) \in \mathbb{Q}[x]$, first clear out all denominators, writing the polynomial as $1/ng(x)$ where $g(x) = nf(x)$, $g(x) \in \mathbb{Z}[x]$. Then write $g(x) = df_0(x)$ for $d \in Z$, $f_0(x)$ primitive in $\mathbb{Z}[x]$. We then write $f(x) = 1/ng(x) = (d/n)f_0(x)$ □

What is cool about this is that we can tell from this decomposition when the polynomial is integral and when it is not.

Theorem 8. Let $f(x) \in \mathbb{Q}[x]$. $f(x) in \mathbb{Z}[x]$ iff when we write $f(x) = cf_0(x)$ for $f_0 \in \mathbb{Z}[X]$ and $c \in \mathbb{Q}$, we have that $c \in \mathbb{Z}$. (Aside: This value c is called as the **content** of the polynomial f).

Proof. **forward:** $f(x) \in \mathbb{Z}[x] \implies c \in \mathbb{Z}$ We have that $f(x) \in \mathbb{Z}[x]$. we can write such a polynomial as $f(x) = cf_0(x)$ for $c \in \mathbb{Q}, f_0 \in \mathbb{Z}[x]$. Since the coefficients of $f(x)$, are the coefficients of f_0 times c, we have that $\mathbb{Z} = c\mathbb{Z}$, which implies that $c \in \mathbb{Z}$.

backward: $c \in \mathbb{Z} \implies f(x) \in \mathbb{Z}[x]$ We have that $f(x) = cf_0(x)$ for $c \in \mathbb{Z}, f_0 \in \mathbb{Z}[x]$. We already have $f_0 \in \mathbb{Z}[x]$. Multiplying the two out, we get that $f = cf_0 \in \mathbb{Z}[x]$, since the ith coefficient of f is the ith coefficient of f_0 times c, both of which are in $\mathbb{Z}$. □

2.4 Factorization of polynomials in $\mathbb{Z}[x]$

Let's now take an $f(x) \in \mathbb{Z}[x] \subset Q[x]$. We first factorize it in $Q[x]$, giving us $f(x) = cp_1(x) \dots p_n(x)$ with each $p_i(x)$ monic. Now we write each $p_i = c_i q_i(x)$ [the primitive decomposition] with each $q_i(x)$ primitive. This gives $f(x) = cc_1 q_1(x) c_2 q_2(x) \dots c_n q_n(x)$. We now write this as $f(x) = dq_1(x)q_2(x) \dots q_n(x)$ where $d = cc_1 \dots c_n$. We are now left with $q_i(x)$ where the $q_i(x) \in \mathbb{Z}[X]$. These $q_i(x)$ continue to be irreducible in $\mathbb{Q}[x]$. But our $d \in \mathbb{Q}$, since we have $c_1, c_2, \dots c_n \in Q$. We need to show that this $d \in \mathbb{Z}$.

2.5 Gauss' lemma

Theorem 9. If f_0 and g_0 are primitive polynomials, then so is $f_0 g_0$.

Proof. If not, say that the prime p divides all the coefficients of $f_0(x)g_0(x)$: By definition, the product is not primitive if the gcd of all the coefficients is not 1. Hence there exists some prime that divides all the coefficients.

Consider the morphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$, which sends $f(x) = \sum_i a_i x^i$ to $\overline{f}(x) = \sum_i \overline{a_i} x^i$.

Since p divides all the coefficients of $f_0 g_0$, we have that $\phi(f_0 g_0) = 0$. But this tells us that $\phi(f_0)\phi(g_0) = 0$. This means that either $\phi(f_0) = 0$ or $\phi(g_0) = 0$ since $\mathbb{Z}/p\mathbb{Z}$ is a field. This means that either f_0 or g_0 is not primitive, since p divides their coefficients. □

2.6 factorization of polynomials in $\mathbb{Z}[x]$: Redux

Now that we are armed with Gauss' lemma, note that we had $f(x) \in \mathbb{Z}[x]$. We wrote it as $f(x) = dq_1(x) \dots q_n(x)$ where each $q_i(x) \in \mathbb{Z}[x]$. From gauss' lemma, we know that the product $q(x) \equiv q_1(x) \dots q_n(x) \in \mathbb{Z}[x]$. Hence we have that $\mathbb{Z}(f(x)) = \mathbb{Q}(d)\mathbb{Z}(q(x))$, and thus $d \in \mathbb{Z}$.

We also have that that these $q_i(x)$ are irreducible in $\mathbb{Z}[x]$. If there we reducible in $\mathbb{Z}[x]$, then they are definitely reducible in $\mathbb{Q}[x]$. But this cannot be, by construction.

Hence we obtain a factorization:

$$f(x) \in Z[x]$$
$$f(x) = c\prod_i p_i(x) \quad p_i(x) \in \mathbb{Q}[x]; c \in \mathbb{Q}$$
$$f(x) = c\prod_i (d_i q_i(x)) \quad q_i(x) \in \mathbb{Z}[x]; c, d_i in \mathbb{Q}$$
$$f(x) = d\prod_i q_i(x) \quad q_i(x) \in \mathbb{Z}[x]; d \in \mathbb{Z}(\text{Gauss lemma})$$
$$f(x) = \pm\prod_j p_j \prod_i q_i(x) \quad q_i(x) \in \mathbb{Z}[x]; p_j \in \mathbb{Z}$$

so we get a full factorization in $\mathbb{Z}[x]$ in terms of irreducible primes $p_j \in \mathbb{Z}$ and polynomials $q_i \in \mathbb{Z}[x]$. These p_j divide the content of $f(x)$. Then the polynomials q_i correspond to the original factorization of $f(x)$ in $\mathbb{Q}[x]$.

A little more work will let us show that this factorization is unique.

2.7 Why care about irreduciblility in $\mathbb{Z}[x]$?

- we have a theorem: a polynomial is irreducible in $\mathbb{Z}[x]$ iff it is irreducible over $\mathbb{Q}[x]$.
- we can convert irreduciblity in $\mathbb{Q}[x]$ into irreduciblity in $\mathbb{Z}[x]$.
- It's easier to prove that polynomials are irreducible in $\mathbb{Z}[x]$ than in $\mathbb{Q}[x]$: deploy the homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$.
- If $f(x) = g(x)h(x)$, then we have$\phi(f(x)) = \phi(g(x))\phi(h(x))$. So if $f(x)$ is reducible over $\mathbb{Z}[x]$, it continues to be reducible over $\mathbb{Z}/pZ[x]$.
- Conversely, If $f(x)$ is irreducible over $\mathbb{Z}[x]/p\mathbb{Z}[x]$, it should continue to be irreducible over $\mathbb{Z}[x]$. If $f(x) = g(x)h(x)$ over $\mathbb{Z}[x]$, we must have that $\phi(f(x)) = \phi(g(x))\phi(h(x))$. But if $\phi(f(x))$ is irreducible, we cannot have $\phi(f(x)) = \phi(g(x))\phi(h(x))$.
- $\mathbb{Z}/p\mathbb{Z}[x]$ is finite, hence we can enumerate $\phi(g(x)), \phi(h(x))$.
- This makes it easy to check what happens in $\mathbb{Z}/p\mathbb{Z}[x]$.

Example 10. $f(x) = x^3 + x + 1$ is irreducible in $\mathbb{Z}[x]$.

Proof. Look at the image in $\mathbb{Z}/2\mathbb{Z}[x]$. Let $f(x) = m(x)n(x)$. If it factors, we would need one of them to be of degree 2, the other of degree 1, since that's the only non-trivial way to have $2 + 1 = 3$.

So it must be of the form $(x + a)(x^2 + bx + c) = f(x)$.

Thus, we need $f(-a) = 0$. We know that $\phi(f)(\overline{0}) = \overline{1}$, $\phi(f)(\overline{1}) = \overline{1}$. Thus f has no root in $\mathbb{Z}/2\mathbb{Z}$, and thus cannot be factored. □

Example 11. $f(x) = x^4 + x^2 + 1$ is irreducible in $\mathbb{Z}[x]$.

Proof. Once again, it doesn't factor as irreducibles of degrees $1 + 3$ since it has no roots:$f(0) = f(1) = 1$ modulo 2.

Maybe it factors into irreducibles of degrees $2+2$. Now we need these degree 2 to be irreducible. There's only one irreducible polynomial of degree 2 over $\mathbb{Z}/2\mathbb{Z}$: x^2+x+1. So we can only have that $f(x) =_? (x^2+x+1)^2$. That doesn't hold. □

2.8 A word of warning: reducibility of $\mathbb{Z}/p\mathbb{Z}[x]$ v/s $\mathbb{Z}[x]$

We can have polynomials which factorize over each $\mathbb{Z}/p\mathbb{Z}[x]$ (ie, are reducible) but continue to be irreducible over $\mathbb{Z}[x]$.

2.9 Irreducibility across degrees

We know that for any prime p and natural n, there is an irreducible polynomial of degree n in $\mathbb{Z}/p\mathbb{Z}[x]$ (**todo: how?**)

Chapter 3

Benedict gross, Lecture 32: Gaussian integers

- YouTube link

Knowing that $\mathbb{Z}[i]$ has unique factorization (or, stronger, that it is Euclidian) is only useful if we know what the primes look like. For example, is $\mathbb{Z}$ we know that the primes are prime, and in $\mathbb{R}[X]$ we know that it's the irreducible polynomials. But for $\mathbb{Z}[i]$, we don't know yet. So we're now going to figure out what the primes are.

3.1 Ideals of $\mathbb{Z}[i]$

Theorem 12. If $I \neq (0)$, then $Z[i]/I$ is finite. That is, I has finite index in $Z[i]$.

Proof. Let I be a non-zero principal ideal generated by α: $I = (\alpha)$. Then $\alpha\bar{\alpha} = a^2 + b^2 = n \in \mathbb{N}^+$. This integer $n \in I$, since $\alpha \in I, \bar{\alpha} \in Z[i]$, and the ideal is closed under multiplication with the rest of the ring. So $I \subseteq (n)$. We claim that $(n) \subseteq I \subseteq R$, and that (n) has finite index in R, and therefore I must have finite index in R. (n) has finite index in R because $(n) = \{na + nbi : a, b \in \mathbb{Z}\}$. The cosets of $R/(n) = \{a + bi : 0 \leq a < n, 0 \leq b < n\}$. There are n^2 such cosets. □

Theorem 13. If $I \neq (0)$, $I = (\alpha)$, then the index of I in R denoted by $\#(R/I)$ is equal to $\delta(\alpha)$, which is exactly how it works for the integers as well.

Proof. We write $\alpha = re^{i\theta}$. Now we know that $\delta(\alpha) = r^2$. We want to find $\alpha\mathbb{Z}[i] = \alpha\mathbb{Z} + i\beta\mathbb{Z}$. Notice that what we've done is to rotate the lattice by an angle θ, and scale the lattice by r. The index of a sublattice in a lattice is the square of the scaling factor.

The size of a basic parallelogram is 1. On scaling, we get have area r^2. Each element in the fundamental lattice is a coset, because after this the lattice repeats. □

Every Gaussian integer can be written as a unique factorization into primes upto the units, since it's a UFD. The primes are elements such that the ideal (p) is maximal with respect to the principal ideal. But in this ring, all ideals are principal ideals. Hence, (p) must be a maximal ideal. That is. $Z[i]/(p)$ must be a finite field. The problem is that we don't know what the units are, and we don't know what the primes are.

3.2 Units of the $\mathbb{Z}[i]$

$\delta : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$. $\alpha \mapsto \alpha\bar{\alpha}$. This cannot be a ring homomorphism because it is not additive. A different way of looking at it is that the image $\mathbb{Z}_{\geq 0}$ is not a group, so it can't be a ring homomorphism. However, it is multiplicative: $\delta(\alpha \cdot \beta) = \delta(\alpha)\delta(\beta)$. This is thanks to complex multiplication. With that note done, let's begin chipping away at the units.

Theorem 14. (1) α is a unit if and only if (2) $\delta(\alpha) = 1$.

Proof. We first show (2)$\delta(\alpha) = 1 \implies$ (1) α is a unit. Assume that $\delta(\alpha) = 1$. Hence, $|\alpha|^2 = 1$. So, it can be written as $e^{i\theta} = \cos(\theta) + i\sin(\theta)$. The only such numbers with $\cos(\theta), \sin(\theta) \in \mathbb{Z}$ are $\pm 1, \pm i$. These are all units. □

Proof. We wish to show (1) α is a unit $\implies$ (2) $\delta(\alpha) = 1$, Since α is a unit, there exists some element β such that $\alpha\beta = 1$. Now apply δ on both sides:

$$\delta(\alpha\beta) = \delta(1)$$
$$\delta(\alpha)\delta(\beta) = 1$$

Since $\delta(\alpha), \delta(\beta) \in \mathbb{Z}_{\geq 0}$ whose product is 1, we must have that $\delta(\alpha) = \delta(\beta) = 1$. □

Proof. A more complicated version of (1) α is a unit $\implies$ (2) $\delta(\alpha) = 1$. Since α is a unit, we know that $1 \in (\alpha)$ since $\alpha \times \alpha^{-1} \in (\alpha)$ as (α) is closed under multiplication. However, if $1 \in (\alpha)$, then every number is in the ring, since $z \cdot 1 \in (\alpha)$. Formally:

$$\forall z \in Z[i], \forall i \in (\alpha), zi \in (\alpha)$$
$$\text{pick } z = \alpha^{-1}, i = \alpha\text{:}$$
$$\alpha^{-1} \cdot \alpha = 1 \in (\alpha)$$
$$\text{pick } z \text{ as an arbitrary } z_0 \in Z[i], \text{ and } i = 1\text{:}$$
$$z_0 \cdot 1 = z_0 \in (\alpha)$$
$$R = (\alpha)$$

Therefore, $(\alpha) = Z[i]$. Now, we calculate $\delta(\alpha)$:

$$\delta(\alpha) = \#(R/(\alpha)) = \#(R/R) = 1$$

□

We now know the unit group of the ring. $Z[i]^\times = \{1, i, i^2, i^3\}$ which has order 4 in $\mathbb{Z}[i]$.

3.3 Primes of $\mathbb{Z}[i]$

We will use the letter π to denote a prime. We know that we need $\mathbb{Z}[i]/(\pi)$ is a finite field. Every finite field has order p^n for some prime $p \in \mathbb{Z}$ and $n \geq 1$. In our case, we claim that the dimension $(n = 1 \vee n = 2)$.

Theorem 15. Consider the quotient $F = \mathbb{Z}[i]/(\pi)$. This must be finite since it has finite order $\delta(pi)$, and is a field since π is prime. We claim that this finite field F of characteristic p with p^n elements has **size** p^1 **or** p^2. That is, it is a vector space of dimension 1 or 2 over Z/pZ but no larger.

Proof. Let $F = \mathbb{Z}[i]/(\pi)$ have characteristic p, and let $\phi : \mathbb{Z}[i] \to \mathbb{Z}[i]/(\pi)$ be the canonical map $\phi(z) \equiv z + \pi$. Now, we know that $p \in \mathbb{Z}[i]$, and also that $\phi(p) = 0$ since F is char. p. Therefore, $p \in \mathbb{Z}[i]/(\pi)$. This tells us that there is an inclusion of ideals $(p) \subseteq (\pi) \subsetneq \mathbb{Z}[i]$. Hence, $\#(Z[i] : (\pi)) \leq \#(Z[i] : (p))$ — intuitively, on squashing (p), we squash less elements than squashing (π). Hence, the number of elements in the quotient of (π) is upper-bounded by number of elements in the quotient in (p). Now recall that $\#(Z[i] : (p)) = \delta(p) = p^2$. Hence:

$$|F| = p^n \#(Z[i] : (\pi)) \leq \#(Z[i] : (p)) = \delta(p) = p^2$$
$$|F| = p^n \leq p^2 \implies |F| = p^1 \vee |F| = p^2$$

Hence proved. □

This is where number theory starts. We have two cases.

Theorem 16. If $R/(\pi)$ has order p^2. Then $(\pi) = (p)$

Proof. We argue by ideal-size-containment. Since

$$(p) \subseteq (\pi) \subseteq \mathbb{Z}[i]$$

If $\#(\mathbb{Z}[i] : (\pi)) = p^2$ and $\#(\mathbb{Z}[i] : p) = \delta(p) = p^2$, then we know that $\#(\mathbb{Z}[i] : p) = \#(\mathbb{Z}[i] : (\pi)) \times \#((\pi) : p)$, or $p^2 = p^2 \cdot ((\pi) : p)$. This means that $((\pi) : p) = 1$ or $(\pi) = (p)$. Hence, an ideal that's generated by a prime p in $\mathbb{Z}$ continues to be prime in $\mathbb{Z}[i]$. □

Theorem 17. If $R/(\pi)$ has order p, then TODO fill in structure!

Proof. In this case, $\mathbb{Z}[i]/(p)$ is not a field, so there are non-trivial ideal (π) between (p) and $\mathbb{Z}[i]$, such that $Z[i]/(\pi) \simeq \mathbb{Z}/p\mathbb{Z}$ (since it's a field of order p). □

To each Gaussian prime π we can associate a rational prime p as the characteristic of the field $\mathbb{Z}[i]/(\pi)$. We now try to make explicit the relationship between π, p, and the order of the field $\mathbb{Z}[i]/(\pi)$. Really, we should study the finite ring $R/(p)$. If it's a field, we are done. If it continues to be a ring, then there are ideals (pi) in it that generate fields.

3.4 The ring $Z[i]/(p)$

We study $\mathbb{Z}[i]/(p)$. We write:

$$\begin{aligned}\mathbb{Z}[i]/(p) &= (\mathbb{Z}[x]/(x^2+1))/(p) \\ &= \mathbb{Z}[x]/(x^2+1, p) \\ &= \mathbb{Z}[x]/(p, x^2+1) \\ &= (\mathbb{Z}[x]/(p))/(x^2+1) \\ &= \mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)\end{aligned}$$

The quotient ring of $\mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$ is a field if (x^2+1) to be an irreducible over $\mathbb{Z}/p\mathbb{Z}$. (TODO: link theorem). For it to be irreducible over $\mathbb{Z}/p\mathbb{Z}$, we need x^2+1 to not have roots over $\mathbb{Z}/p\mathbb{Z}$. That is, we need $x^2 \equiv (-1) \mod p$ to have **no solutions**.

Example 18. Over $p = 2$, we can write $x^2 + 1 \equiv (x+1)^2 \mod 2$. It has a repeated root $x = 1$. In this case, there is a unique prime $\pi = 1 + i$ with $(2) \subset (\pi) \subset Z[i]$

Theorem 19. If $p \equiv 3 \mod 4$, then x^2+1 is irreducible modulo p, and $\mathbb{Z}[i]/(p)$ is a field.

Proof. If $p \equiv 3 \mod 4$, then:

$$|\mathbb{Z}/p\mathbb{Z}^\times| = p - 1 = (4k+3) - 1 = 4k + 2 = 2(2k+1) = 2 \cdot \text{odd}$$

Let r be a root of $x^2 + 1$ in $\mathbb{Z}/p\mathbb{Z}$.

1. Since $r \neq 0$, r is invertible in $\mathbb{Z}/p\mathbb{Z}$ ($\mathbb{Z}/p\mathbb{Z}$ is a field). So $r \in \mathbb{Z}/p\mathbb{Z}^\times$.
2. $r^2 + 1 = 0 \implies r^2 = -1$.
3. r has order 4: $r^4 = (r^2)^2 = (-1)^2 = 1$.
4. $\mathbb{Z}/p\mathbb{Z}^\times$ has no elements of order 4, since the order of an element must divide the order of the group, but $|\mathbb{Z}/p\mathbb{Z}^\times| = 2 \cdot \text{odd}$, and hence is not divisible by 4.

5. Hence, $r \notin \mathbb{Z}/p\mathbb{Z}^{\times}$. Contradiction with (1).

Hence, there is no root r of $x^2 + 1$. □

Theorem 20. If $p \equiv 1 \mod 4$, then $x^2 + 1$ factors as $(x - a)(x + a)$, where $a^2 \equiv (-1) \mod p$.

Proof.

$$|Z/pZ|^{\times} = p - 1 = 4k + 1 - 1 = 4k = 2^n \quad \text{where } n \geq 2$$

Hence the Sylow-2 subgroup of $|Z/pZ|^{\times}$ has order 2^n (where $n \geq 2$). We claim that the only elements of order 2 is ± 1. Let us assume we have an element of order 2. This means that $a^2 = 1$. Hence $a^2 - 1 = 0$, or $p|a^2 - 1$. Hence, $p|(a^2 - 1)(a^2 + 1)$. Since p is prime, p has to divide either $(a^2 - 1)$ or $(a^2 + 1)$. Hence $a^2 = \pm 1$.

Now that we know this, we need more elements in $|Z/pZ|$ since it has order 2^n but we have only found 2 elements of order 2. So the other elements must have order 4 or larger. We can always take powers of such an element to create an element of order 4.

Spelling out the details, if an element $r \in Z/pZ^{\times}$ has order $4 \cdot m$, then $r^{4m} = 1$. So $(r^m)^4 = 1$. r^m is the element of order 4 we are looking for. □

Consider $1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} = \frac{\pi}{4}$. We will show that this is a theorem about Gaussian numbers.

Chapter 4

Benedict gross, Lecture 33: Gaussian integers

- YouTube link

Recap: We did primes in $\mathbb{Z}[i]$. We showed that:

- primes $p \equiv 1(\mod 4)$ gave two primes, π and π' in $\mathbb{Z}[i]$: $\pi \times \pi' = p$. This gives us that if $\pi = a + bi$, then $\pi' = a - bi$ and $\pi \times \pi' = a^2 + b^2 + p$. This is a proof of Fermat's theorem that the primes congruent to 1 mod 4 are the sum of two squares.

- primes $p \equiv 3(\mod 4)$ gave one prime p.

We study rings R analogous to $\mathbb{Z}[i]$ and try to understand their primes, even though the rings are not prime.

For example, the ring $R = \mathbb{Z}[\sqrt{-2}]$ where we have the δ function $\delta(a + b\sqrt{-2}) = a^2 + 2b^2$ which makes the ring Euclidian. On the other hand, we had $R = \mathbb{Z}[\sqrt{-5}]$ where $6 = 2 \times 3 = (1+\sqrt{5})(1-\sqrt{-5})$, and is thus not even a UFD!

So we could and take $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d}\} = \mathbb{Z}[x]/(x^2 - d)$. But this is not the right analogue of $\mathbb{Z}[i]$. The reason this is the wrong thing to do is as follows. Consider $f(x) = x^2 + x + 1$. It's roots are $\alpha = (-1 \pm \sqrt{-3})/2$. If we take $R = \mathbb{Z}[x]/(f(x))$, it'll give us $R = \mathbb{Z} + \mathbb{Z}\alpha$. This ring contains $S = \mathbb{Z} + \mathbb{Z}\sqrt{-3}$, because $2\alpha + 1 = \sqrt{-3}$. But these two rings are not equal, we need to divide by 2 to get from one to the other. In fact, S has index 2 in R.

Both R and S have the same fraction field $\mathbb{Q}[\sqrt{-3}]$. We want to work with the largest natural ring. So we would like to work with R, not S. So we need to learn how to get the largest rings. One reason why R is better is because R is Euclidian while S is not.

We're going to back off before we decide what the right rings are.

4.1 Algebraic integers

We need to talk about algebraic integer to get the right analogue. A complex number $z \in \mathbb{C}$ is an algebraic integer if it is the root of a monic polynomial $f(x) \in \mathbb{Z}[x]$.

Every integer is an algebraic integer, because it is the root of $f(x) = x - i$. $\sqrt{d}$ is an algebraic integer because it is the root of $f(x) = x^2 - d$. e is not an algebraic integer.

4.1.1 Rational coefficients

Suppose α is a root of $f(x) \in \mathbb{Q}[x]$ which is monic irreducible. Is it an algebraic integer? We claim that α is algebraic iff the monic irreducible $f(x) \in \mathbb{Q}[x]$ with α as a root has **integer** coefficients: that is, $f(x) \in \mathbb{Z}[x]$.

Example 21. $1/2$ is not an algebraic integer, because it satisfies the polynomial $x - 1/2$. How do we know? maybe there is *some other* polynomial in $\mathbb{Z}[x]$ whose root is $1/2$. We will prove that such a thing will not happen.

Example 22. any $\alpha \in \mathbb{Q}/\mathbb{Z}$ by the same reasoning.

Example 23. any $\alpha = \sqrt{2}/3$ is not an algebraic integer. **Proof:** This satisfies the polynomial $f(x) = x^2 - 2/9$ which is in $\mathbb{Q}[x]$.

Theorem 24. $\alpha \in \mathbb{C}$ is algebraic iff the monic irreducible $f(x) \in \mathbb{Q}[x]$ with α as a root has **integer** coefficients.

Re-stated, if we can write α as the root of some $g(x) \in \mathbb{Q}[x]/\mathbb{Z}[x]$, then we will have that α is not algebraic: that is, there is **no polynomial** in $g'(x) \in \mathbb{Z}[x]$ such that $g'(\alpha) = 0$.

Proof. Let $f_0(x)$ be the primitive polynomial in $\mathbb{Z}[x]$ with $f(x) = cf_0(x)$, for $c \in \mathbb{Q}, f_0 \in \mathbb{Z}[x]$.

claim: any $g(x) \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$ is of the form $g(x) = f_0(x)q(x)$ for some $q(x) \in \mathbb{Z}[x]$.

If the claim is available, we are done. □

Chapter 5

Atiyah MacDonald, Ch1 exercises

5.1 Q11

$2x = x + x = (x + x)^2 = x^2 + 2x + x^2 = x + 2x + x = 2 \cdot 2x$. This gives us the equation $2x = 2 \cdot (2x)$, and hence $2x = 0$.

5.2 Q15

Let X be the set of prime ideals of the ring A. We will denote elements of X as x, and when thinking of them as ideals, we will write them as $\mathfrak{p}_x$, though they are the same as sets ($x = \mathfrak{p}_x$).

Let $V(E)$ be the set of all points in X that contain E. That is, $V(E) = \{\mathfrak{p}_x \in X : E \subseteq \mathfrak{p}_x\}$. We need to show:

5.2.1 If $\mathfrak{a}$ is generated by E, then $V(E) = V(\mathfrak{a})$

$V(E) = \{\mathfrak{p}_x \in X : E \subseteq \mathfrak{p}_x\}$ $V(\mathfrak{a}) = \{\mathfrak{p}_x \in X : \mathfrak{a} \subseteq \mathfrak{p}_x\}$. The idea is to exploit that since we are collecting ideals when building $V(E)$, and ideals are closed under inclusion. if $e_1 \in \mathfrak{p}_x, e_2 \in \mathfrak{p}_x$, then all combinations $a_1e_1 + a_2e_2 \in \mathfrak{p}_x$. On the other hand, clearly the generated ideal will contain all elements of the original generating set. Hence, the points of x that we collect will be the same either way.

More geometrically, recall that for every (subset of A/polynomial) E, we let $V(E)$ to be the points over which E vanishes. That is, $x \in V(E) \iff E \xrightarrow{\mathfrak{p}_x} 0$, where $E \xrightarrow{frak p_x} \cdot$ is rewriting E using the fact that every element in $\mathfrak{p}_x$ is zero.

Now, notice that if we have that E rewrites to zero, then all elements in the ideal generated by E also rewrite to zero, since $a_1e_1 + a_2e_2 \xrightarrow{\mathfrak{p}_x} a_10 + a_20 = 0$.

Similarly, if the ideal generated by E rewrites to zero, then so does E, because E is a subset of the ideal generated by E.

5.2.2 If $\mathfrak{a}$ is generated by E, then $V(\mathfrak{a}) = V(radical(\mathfrak{a}))$

Recall that the radical of an ideal is defined as $radical(\mathfrak{a}) \equiv \{a \in A : a^n \in \mathfrak{a}\}$. X consists of *prime* ideals. Prime ideals contain the radicals of all of their elements. Recall that if $a^n \in \mathfrak{p}$ where $\mathfrak{p}$ is prime, then $a \cdot a^{n-1} \in \mathfrak{p}$, hence $a \in \mathfrak{p} \vee a^{n-1} \in \mathfrak{p}$ by definition of prime ideal. Induction on n completes the proof. Therefore, the additional elements we add when we consider $radical(\mathfrak{a})$ don't matter; if $a \xrightarrow{\mathfrak{p}} 0$, then $a \in \mathfrak{p}$, $radical(a) \subseteq \mathfrak{p}$, so $radical(\mathfrak{a}) \xrightarrow{\mathfrak{p}} 0$.

5.3 Q17

For each $f \in A$, We denote $X_f \equiv V(f)^{\complement}$ where we have $X = Spec(A)$. We first collect some information about these X_f and how to psychologically think of them. First, recall that $V(f)$ will contain all the points $x \in X$ such that f vanishes over the point x: $f \xrightarrow{\mathfrak{p}_x} 0$. Hence, the complement X_f will contain all those point $x' \in X$ such that f does *not* vanish over x': $f \xrightarrow{\mathfrak{p}_{x'}} \neq 0$. So we are to imagine X_f as containing those points x' over which f does not vanish.

We will first show that we can union and intersect these X_f, and we will then show how that these X_f form an open base of the Zariski topology.

5.3.1 $X_f \cap X_g = X_{fg}$

$X_f \cap X_g$ contains all the points in X where neither f nor g vanish. If neither f nor g vanish, then fg does not vanish. Conversely, if fg does not vanish at x, since the point x is prime, neither f nor g vanish over x (elements that do not belong to the prime ideal are a multiplicative subset: $xy \notin \mathfrak{p} \implies x \notin \mathfrak{p} \wedge y \notin \mathfrak{p}$).

Hence, the set where f and g do not both vanish, $X_f \cap X_g$ is equal to the set where fg does not vanish.

5.3.2 Incorrect conjecture: $X_f \cup X_g = X_{f+g}$

$X_f \cup X_g$ contais all the points in X where either f or g do not vanish. But that does not mean that $f + g$ has to not vanish. For example, let the the ring be $\mathbb{R}[X]$, and let $f = x^2 + 1$, $g = -x^2 - 1$. Both of these do not vanish over all of $\mathbb{R}$, and yet $f + g = 0$ which vanishes everywhere. So it's *not true* that $X_f \cup X_g = X_{f+g}$ because addition can interfere with non-vanishing.

5.3.3 $X_f = \emptyset \iff f$ is nilpotent

($\Longleftarrow$): Let f be nilpotent. We want to show that $X_f = \emptyset$. Recall that $X_f = \{x \in X : f \xrightarrow{\mathfrak{p}_x} \neq 0\}$. If f is nilpotent, then f belongs to every prime

ideal: $\forall x \in X, f \in \mathfrak{p}_x$. Thus f vanishes on all prime ideals: $\forall x \in X, f \xrightarrow{\mathfrak{p}_x} = 0$. Hence, X_f, which contains prime ideals x where f *does not vanish*, is empty.

($\implies$): Let $X_f = \emptyset$. We wish to show that f is nilpotent. This means that $\forall x \in X, f \in \mathfrak{p}_x$. But recall that the intersection of all prime ideals in a ring is the nilradical. Hence f is a nilpotent. We recollect the proof that the intersection of all prime ideals is the nilradical. (i) $Nil \subseteq \cap Prime$: The nilradical is contained in the intersection of all prime ideals. If an element $a \in A$ is nilpotent, then $a^n = 0 \in \mathfrak{p}$ for all ideals $\mathfrak{p}$. If $\mathfrak{p}$ is a prime ideal, then $a^{n-1} \in \mathfrak{p} \vee a \in \mathfrak{p}$. Induction on n proves that $a \in \mathfrak{p}$. (ii) $\cap Prime \subseteq Nil$: The multiplicative semigroup of elements that do not belong to $\cap Prime$ is $\cup Prime^{\complement}$. We claim that no nilpotent element belongs to $\cup Prime^{\complement}$. Assume it does. Then this nilpotent element n is in the complement of some prime ideal $\mathfrak{p}^{\complement}$.

[NOTE: I don't have good insight into why this works]. On the answer, someone told me to think of nilpotents as vanishing elements or infinitesimals, because in the case of an infinitesimal, we have that $\epsilon \neq 0, \epsilon^2 = 0$. This is exactly what happens with a nilpotent, where we have $f \neq 0, f^2 = 0$. [In general, it seems like a good way to get a handle on any ring theoretic definition is to simply adjoin constants that satisfy the definition into the ring and see what the geometry is. Thinking about constants is a good deal easier than thinking about polynomials]. Now, looking at the situation, it's intuitive that such an infinitesimal will "appear to vanish", since it cannot be distinguished from 0 by any polynomial. Hence, we will have that $X_\epsilon = 0$, since ϵ is zero everywhere, as far as polynomials are concerned, because no polynomial can pick up on the difference between ϵ and 0. What do I mean by that? Well, we have the relation that $p(x + \epsilon) = p(x) + \epsilon p'(x)$ inside the ring $\mathbb{R}[x][\epsilon]/(\epsilon^2)$. Now if we want a polynomial to detect epsilon, then it must be such that $p(\epsilon) = 0$;

$$
\begin{aligned}
&p(x) = q(x) + \epsilon r(x) \quad [q(x), r(x) \in \mathbb{R}[X]] \\
&p(\epsilon) = 0 \quad [\text{we want } p \text{ to detect } \epsilon] \\
&\text{Let } q(x) = q_0 + q_1 x + \cdots ; r(x) = r_0 + r_1 x + \cdots \\
&q(\epsilon) + \epsilon r(\epsilon) = 0 \\
&q_0 + q_1(\epsilon) + \epsilon(r_0) = 0 \quad [\text{truncate to } \epsilon \text{ since } \epsilon^2 = 0] \\
&q_0 + \epsilon(q_1 + r_0) = 0 \quad [\text{Recall that } q_0, q_1, r_0 \in \mathbb{R}] \\
&q_0 = 0 \wedge (q_1 = -r_0) \\
&p(0) = q(0) + \epsilon r(0)
\end{aligned}
$$

TODO: figure out the full story

5.3.4 $X_f = X \iff f$ is unit

Intutively, if f is a unit (eg. $f = 1$), then f does not vanish anywhere. Hence the set where f does not vanish, X_f is equal to the entire ring.

Formally, since f is a unit, f cannot be contained in any proper prime ideal of A. If it were contained in an ideal, then that ideal would become the full ring. the spectrum of a ring does not contain the full ring.

Elaborating, we must have that for each proper prime ideal $\mathfrak{p} \in X$, $f \notin \mathfrak{p}$. If $f \in \mathfrak{p}$, then we will have $f \times f^{-1} \in \mathfrak{p}$ [ideals are closed under multiplication with entire ring, and is hence closed under multiplication with f^{-1}]. This gives us $1 \in \mathfrak{p}$, and therefore $R = \mathfrak{p}$. But we disallow the full ring in the prime spectrum. Hence contradiction. Therefore $f \notin \mathfrak{p}$.

I asked about the intuition for the nilradical. Hoping for good answers.

5.3.5 the sets X_f form a basis (base) of open sets for the Zariski topology

Clear from the definition of closed sets. We define the closed sets as the intersection of vanishing sets of families of polynomials. By complementing, the open sets are the unions of non-vanishing sets of polynomials. We can write the union of non-vanishing sets in terms of the basic open sets X_f.

5.3.6 X is quasi-compact: every open covering of X has a finite subcovering

Assume we have an open covering of X. Since the open sets are generated from X_f, we need only consider an open covering in terms of $X_f[i]$ for some index set $i \in I$.

So we have elements $f[i]$ such that for each $x \in X$, there is some $f[x]$ such that $f[x]$ does not vanish on $\mathfrak{p}_x$: $f[x]/\mathfrak{p}_x \neq 0$. Now assume that we are given some element $a \in A$.

TODO

5.4 Q18

5.4.1 The set $\{x\}$ is closed in $Spec(A) \iff \mathfrak{p}_x$ is maximal

$\implies$: Let $\{x\}$ be closed. We wish to show that $\mathfrak{p}_x$ is maximal. This means that there is some $F \subseteq I$ such that $F(x) = 0; F/\mathfrak{p}_x = 0$, and F(all other prime ideals) $\neq 0$. Hence we have a containment of ideal $F \subseteq \mathfrak{p}_x \subseteq R$, and $F \subsetneq Spec(A)/\{x\}$. That is, F is not contained in any other prime ideal. Thus, $\mathfrak{p}_x$ is maximal.

Assume not. Then the ideal $\mathfrak{p}_x$ is contained in some maximal ideal M. Now note that if $F/\mathfrak{p}_x = 0$, then $F/M = 0$. Also, M is maximal, and is hence prime. Therefore, we will have that the zero set of F to be at least $\{\mathfrak{p}_x, M\}$. This contradicts our assumption that the zero set of F was just $\{\mathfrak{p}_x\}$.

$\impliedby$: Assume $\mathfrak{p}_x$ is maximal. We wish to show that $\{x\}$ is closed. Consider the zero set of $\mathfrak{p}_x$. We will have that $\mathfrak{p}_x$ can only vanish on $\mathfrak{p}_x$, since the ideal is maximal. Hence its zero set is the single point $\{x\}$.

5.4.2 $\overline{\{x\}} = V(\mathfrak{p}_x)$

(i) The vanishing set of $\mathfrak{p}_x$ is the set of points at which $\mathfrak{p}_x$ evaluates to 0: $V(\mathfrak{p}_x) = \{y \in Spec(A) : \mathfrak{p}_x/\mathfrak{p}_y = 0\}$. (ii) The closure of the set $\{x\}$ is the intersection of all closed sets that contain x. Note that the closed sets of $Spec(A)$ are the vanishing sets of subsets of A.

$\overline{\{x\}} = \bigcap$ closed sets that contain x

$= \bigcap_{E \subseteq A} V(E)[x \in V(E)]$

$= \bigcap_{E \subseteq A} [x \in V(E)]\{y \in Spec(A) : E \xrightarrow{\mathfrak{p}_y} 0\} \quad = \bigcap_{E \subseteq A} [E \xrightarrow{\mathfrak{p}_x} 0]\{y \in Spec(A) : E \xrightarrow{\mathfrak{p}_y} 0\}$

TODO

5.5 Q19

We wish to show that $Spec(A)$ is irreducible iff the nilradical of A is prime. Recall that a topological space is irreducible if $X \neq \emptyset$, and and every pair of non empty open sets intersect.

5.5.1 Incorrect intuition I was carrying about the nilradical

We note that the nilradical is a *set* of nilpotent elements. We can show that this set is an ideal. However, this ideal **need not be prime**. The intersection of prime ideals does not have to be prime! If we have that $p_1 \cap p_2 = p'$ where p' is prime, then we have that $p_1 p_2 \subseteq p'$. But because p' is prime, it must be that $p_1 \subseteq p' \vee p_2 \subseteq p'$. We also have that $p' \subseteq p_1 \wedge p' \subseteq p_2$ since p' is their intersection. Combining the two, we must have that $p' = p_1 \vee p' = p_2$, Hence the intersection of distinct prime ideals that do not contain each other cannot be prime.

A more down to earth example is to consider the ring $S \equiv \mathbb{R}[x, y]/(xy)$. We have that $x * y = 0; x^n \neq 0, y^n \neq 0$. We have that $x \notin Nil(S)$, $y \notin Nil(S)$, but $xy = 0 \in Nil(S)$. Therefore, the nilradical of S is not prime.

TODO

Chapter 6

AGITTOC: Pseudolecture1 1

- Open introduction to AG: algebraic geometry in the time of Covid.
- Pseudolecture 1 exercises.
- AGITTOC Zulip chat

For those comfortable with proofs, and perhaps familiar with modules, but not more:

- why is a group? (This problem is not a joke! Do you know about groups because someone told you to? Well, if they told you to go jump in lake, would you do that too?)
- Make a list of categories (both objects and morphisms) you are already friends with, and functors you already know about.
- You neednt know any definition of manifold, but figure out with others why the notion of a manifold is a reasonable one (even if you cant formalize it well), so we can use it in conversation.
- In the notes, try problems 1.2.B, 1.3.A. (Localization and tensor products are harder than people think!) 1.3.N, 1.3.Q, 1.3.O, 1.4.B, 1.4.C. Maybe 1.4.D and 1.4.G. Ponder 1.4.8. Pick another exercise on this list on the basis of your judgement and taste that you think is worth thiking about.
- Whats your favorite exercise (not necessarily from the notes), and why? (This is important: you are not a passive robot doing exercises. You are deliberately refining your thinking.)
- What was a big insight here (either new to you, or perhaps not), and why?

If you are already very comfortable with modules and point-set topology, and trying to digest the core material in a more systematic way: Read up to section 1.5. There are some notions (including adjoints) that one understands more completely and deeply the more times one revisits them, so if you think you know these ideas, then think harder. Read starred sections too. Truly digest tensor products, limits, and colimits as much as possible.

Some interesting questions to make friends with: 1.3.K, 1.3.N, 1.3.S, 1.3.Y (baby Yoneda). (1.3.Z is Yoneda but if you are just doing 1.3.Y now, then leave 1.3.Z for two weeks, other things can marinate in your mind.) 1.4.B, 1.4.D, 1.4.G. 1.5.D, 1.5.E, 1.5.F, 1.5.G.

A point of view: To learn as much as possible, we're going to be learn as much as we need, as little as possible.

> We don't want definitions! We want properties!
>
> **Parable of the musicians**: As the math courses get more complicated, the textbooks get thinner. How does one memorize an entire symphony? They don't. They remember certain key points in the piece, and the rest just falls into place. Just like mathematical proofs.

6.1 Why should we care about AG?

We want to solve for Pythagorean triples $x^2 + y^2 = z^2$. We can think of it as looking for rational points on a circle. We will generally just draw a circle. But a circle has real points! So why do we draw a circle (the real set of solutions?) Because it's psychologically easier.

To solve the problem of enumerating these triples, we can start with the point $(1, 0)$. We can then take a line with rational slope p/q passing through $(1, 0)$. This will cut the circle again.

That's both *geometry* and *arithmetic*

What about $x^2 + y^n = z^n$. The old trick doesn't work, but there are lots of complex solutions. We'll get a complex riemann surface , inside which we have real points, inside which we have rational points. How does it help to think of the complex surface? There is an amazing theorem (Falting's theorem) which says that if there is more than one hole of the riemann surface, then there are finitely many rational points. There is something liking the arithmetic, geometry, topology, and algebra.

The weil conjectures are a different flavour. Roughly, if we have a bunch of equations in $\mathbb{C}^\times$ with integer coefficients. We have a thing that is a variety, and it has a topology on it. We can take the equations (mod p). The Weil conjectures say that knowing solutions in (mod p), we can learn about the topology of $\mathbb{C}$.

Gauss Bonnet / Riemann roch grow up to become Atiyah Singer. It's about something discrete and something continuous being the same for no good reason.

We know how to think of elements of $\mathbb{C}[X]$ as smooth curves. AG allows us to think of elements of $\mathbb{Z}$ also as a smooth curve.

The other thing is "what is projective space".

6.2 Categories

(Read upto section 1.5 in the rising sea). Why categories? things and maps between them. We can compose maps, and we have a way an identity map. We also know that composition is associative.

6.2.1 Products

What is a product? Assume we have two sets U, V. We will define $U \times V$. It's a thing that has maps to U and V. If we have anything (called W) that has a map to U and to V, then we have a *unique* map to $U \times V$.

Now if we have another product, they must be the same. Why? Let's call the two product sets $U \times V$, $U \boxtimes V$. ... [TODO]

6.2.2 Moduli Space

What are the circles in the plane? They are things of the form $(x-a)^2+(y-b)^2 = r^2$. this is $\mathbb{R} \times \mathbb{R} \times \mathbb{R}^+$ [radius most be positive].

If we now want to to think of projective space? what is $\mathbb{RP}2$? Points in projective space correspond to lines through the origin of $\mathbb{R}3$. We have more structure on $\mathbb{R}3$ than just a set.

If we go to a riemann surfaces, we have a nice collection of these spaces called $M3$. It's basically a manifold. We have a set of Riemann surfaces. If I have a nice family of riemann surfaces, I have a point on $M3$ for every Riemann surface. If such a thing exists, there can only be one such upto unique isomorphism.

6.2.3 Sheaf

Why is a sheaf? Consider some nice space X, like a manifold. Consider continuous functions on X. We want information about continuous functions on all of X. $O(U)$ is the continuous functions on U where U is some open set in X. First note that $O(U)$ has a ring structure; we can add and multiply such functions.

If we have a continuous function on U, and we have a smaller open set $V \subseteq U$, we have a restriction map $O(U) \to O(V)$. Also, if we have an even smaller set $W \subseteq V$, we can either resstrict directly from $O(U)$ to $O(W)$, going as $O(U) \mapsto O(W)$, or we can pass through V: $O(U) \mapsto O(V) \mapsto O(W)$. This should yield the same result.

If we have an open set U, and a cover of U called C_i. If we now have two functions on U, called f and g which are the same on each set of the cover C_i, then f and g must have been the same function to begin with.

Similarly, if we have functions on the smaller open sets that agree on the overlap, we can glue them together to build a larger function.

The exact same story works with differentiable functions.

Chapter 7

AGITTOC: Pseudolecture 2

- Youtube video.
- Problem set link

If you are not super-comfortable with modules: How comfortable are you with localization and tensor products? (Tensor products in particular really are confusing, so dont be surprised, or feel stupid.) Perhaps try an exercise in each to see if you can do them. If you can, then declare victory and move on; youll digest these ideas better later, when you use them. Do 1.5.F (if you have to work hard, you are working too hard t has a one-sentence answer.) Do 1.5.G (and realize that if you understand negative numbers, you understand this exercise). Do exercise 2.1.A (even though I allegedly did it in the pseudolecture) If you have some background in differential geometry, you will find Exercise 2.1.B enlightening. Exercise 2.2.B will give you an idea of when things might not quite be sheaves, but still be presheaves. Do Exercise 2.2.E, 2.2.F, 2.2.H, and even 2.2.J. Do 2.3.A, , and 2.3.C.

If you are quite comfortable with modules over a ring: Make sure you can do all the localization and tensor product exercises without referring to anything. Exercise 1.5.H will ensure you understand the ification functor. Do 1.6.A, 1.6.B, 1.6.C, and 1.6.D (for modules over a ring). Do 1.6.I, and possibly 1.6.K Do 2.1.A, and (if you know some differential or complex geometry) 2.1.B. Do 2.2.E; 2.2.F or 2.2.G; 2.2.H; 2.2.I; 2.2.J; 2.3.A. Definitely do 2.3.C. You can do 2.3.E and 2.3.F, and in anticipation of the next problem set, 2.3.I and 2.3.J.

Reading: Section 2.1 - Section 2.3 of the rising sea. **Homework**: Week 2 of the problems from last week, Week 1 of 2 problems to be posted.

"We should never take a course on category theory". To learn to play a musical instrument, we should not spend a year learning how the key presses work.

As a linear algebra warmup, we're going to write down a 108 equations in 26 unknowns. The all have integer coefficients. I will also be told the solution $(14, \pi, 9, \sqrt{2}, dots)$. We should prove that there ought to be a rational solution as well.

7.1 Limit

An element of a limit gives one of each of its ingredients. For example, $K[[X]] = \lim_n\{\text{degree } n \text{ polynomials}\}$, since we can get a degree n polynomial for all n, from any power series by truncation.

RAPL: right adjoints preserve limits.

Limits commute with limits.

7.2 Colimit

An element of one of its ingredients is a colimit. (?) I don't understand this.

7.3 Adjoints

A really nice example of adjoints. Consider the fact that integral domains and fields are adjoints. We can build the field of fractions to get a field from an integral domain (free functor). Conversely, we can forget the field structure to treat a field as an integral domain. So we get a mapping of hom-sets:

$$Hom(IntegralDomain, Forget(Field)) \simeq Hom(Frac(IntegralDomain), Field)$$

7.4 Sheafs

Same story from last time. We want to talk about functions on sub parts of the space. We're interested in the space $X = \mathbb{R}^n$. So for every open set U, we want $\mathcal{O}(U)$ to be the set of continuous functions that are defined on U. $\mathcal{O}(U)$ is a ring. We can restrict functions, and restrictions can need to have the property that $f|v|w = f|w$. This is a **presheaf**.

Then we have the **identity axiom**: If we have a set U and a cover U_i, if two functions f and g agree on each element of the cover U_i, then f and g agree on U. Alternatively, if we have a bunch of functions on an open cover, we can have at most a single function on U that restricts to the bunch of functions.

Another axiom is the **gluing axiom**: if we have functions f defined on U, g defined on V, and f and g agree on $U \cap V$, then we must have a glued function h which is defined on $U \cap V$ such that $h|U = f$ and $h|V = g$. The gluing axiom gives us the conditions for us to be able to have *at least one* function which can be glued together from a bunch of functions using an open cover.

So if we find "at least one" function under the conditions of the gluing axiom [existence], the identity axiom allows us to show that this function is unique [uniqueness], since we can have "at most one" way to glue these functions together.

7.4.1 Example 1: Maps into a set

Sheaf of maps into Y. That is, given a set X, we can think for each open set $U \subseteq X$, we can consider the sheaf of functions from U to Y.

7.4.2 Example 2:Sections over a space

Given a space M (think manifold) and some bundle T over M (think tangent bundle), we want to consider, for each open set $U \subseteq M$, we want to consider the sheaf of sections of M over U (think sheaf of vector fields from M over U). Clearly, this is a presheaf since we can restrict vector fields. It's a sheaf because we can glue vector fields together.

7.4.3 Example 3: Pushfoward sheaf

We have a map of topological space $\pi : X \to Y$ and we have a sheaf on X, called $\mathcal{F}$, we can get a sheaf on Y. We can think of X as some sort of bundle over Y. The definition is $(\pi_* F)(u) \equiv F(\pi^{-1}(u))$.

7.4.4 Example 4: Skyscraper sheaf

For a point p, if the open set U does not contain p, then there are no sections. If the open set U contains p, then it will have one section.

7.4.5 Example 5: constant sheaf

The sheaf of locally constant functions. That is, for some open set U, we get the functions that are *constant* on U.

7.5 Maps of sheaves

For every open set, we need to have a map, and it should work well with restrictions. To meditate. We have a map $\pi : X \to Y$. We have the sheaf of functions on X, call it $\mathcal{O}_X$. We have a way to push forward this as a sheaf on Y using π as $\pi_* \mathcal{O}_X$. More importantly, there is a map from the sheaf of functions on Y to the pushfoward sheaf of O_X. This is because we can always pull back a continuous function $h_Y \in \mathcal{O}_Y$ on Y to get some continuous function $\pi^{-1}(h_Y) \in \mathcal{O}_X$ on X [TODO: how does one prove this?]. We can now push this forward through the sheaf map, giving us a way to embed $\mathcal{O}_Y$ into $\pi_* \mathcal{O}_X$.

7.6 Stalks and germs of presheaves

Two functions have the same germ near $x \in X$ if they are the same near X. If there's an honest open neighbourhood where the functions are the same. Each germ is a function. Is stalk F_p a colimit over the sheaf F_U, because we are picking some element of the sheaf.

7.7 Insight into local rings

If $X = \mathbb{C}^n$ is some geometric space, then $\mathcal{O}_p$ is a local ring. A local ring is a ring with a single maximal ideal. We consider a map $\mathcal{O} \to \mathbb{C}; f \mapsto f(p)$. We have a map to a field. The ideal $m_p \equiv \{g \in \mathcal{O}_p | g(p) = 0\}$, since it's the kernel of the evaluation map. The evaluation map goes to the field. Now, anything that is not in the maximal ideal is *invertible*, hence m_p is maximal. Thus the ring is a local ring.

7.8 $\mathcal{O}$-modules

Module: abelian group with the action of a ring on it, just like vector space is an abelian group with the action of a field on it.

Sheaf of modules over a sheaf of rings $\mathcal{O}$, which we will think of as functions. An $\mathcal{O}$ module is a sheaf of abelian groups with an action on each open set.

7.8.1 Example: Vector fields on a manifold

For every point, we have a tangent vector. If we have a vector field and a function on the manifold, we can act the function on the vector field by scaling. So vector fields on manifolds are a module over the ring of functions of the module.

7.8.2 Example: pushforward sheaf

The push forward is $\pi_* \mathcal{O}_X$ is an $\mathcal{O}_Y$ module, because given a function $f \in \mathcal{O}_Y$, I can have it act on $\pi_* \mathcal{O}_X$.

7.9 How to abstract out kernels, cokernels?

Grothendeick in the tohoku paper defined abelian categories. We need to remember that kernels are limits!

Given a map of R-modules $\phi : A \to B$, the kernel is the limit of the diagram:

TODO: Latex the diagram

That is, the map into 0 commutes with the embedding map into A.

Because limits commute with limits, we have things like "limits of kernels = kernels of limits". Also because of RAPL, we know that right adjoints preserve kernels because right adjoints preserve limits.

Similarly, we can show that cokernels are colimits.

Chapter 8

AGITTOC: Pseudolecture 3

- Youtube video
- Link to exercise
- Get solid on Chapter 2 up until 2.3. Try Exercise 2.3.J. Read sections 2.4 and 2.5. Im not sure how hard you will find these sections, as it doesnt involve much algebra, but does involve geometric intuition. Try 2.4.A, 2.4.B, 2.4.C. 2.4.E is worth doing, as youll see how sheaves are better. 2.4.F is good to practice earlier idea. You might even like to try the exercise describing sheafification (2.4.H through 2.4.J). Try 2.4.O too. (And of course, try others if you can.) In 2.5, think through 2.5.A (no need to write it up, but just convince yourself.) See if you can do one of the important exercises here.

8.1 Last time

We talked about sheaves on topological spaces. for example, presheaves of abelian groups associate to each open set U an abelian group $F(U)$. We also have restriction maps.

8.1.1 Adjoints

The category of integral domains must have as morphisms as inclusions for the previous argument to work out. Otherwise, we will have the map $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. This is a map of integral domains. This does not give us a map from $\mathbb{Q}$ to $\mathbb{Z}/2\mathbb{Z}$ as promised by the adjunction.

8.2 Ringed spaces

We have a set, a topology on it, and a sheaf of rings on it. we're going to call the rings functions. Formally, it's a space $(X, \mathcal{O}_X)$ where $\mathcal{O}_X$ is a ring of functions

on the space.

8.3 Manifold

A manifold is a ringed space which is covered by open sets, where each open set (plus its sheaf data) is isomorphic to ($U \subseteq \mathbb{C}^\kappa$, sheaf of homolorphic functions).

8.4 Locally ringed space

It's a ringed space where all stalks are local rings. Spelling this out, It's a ringed space $(X, \mathcal{O})$ such that for all $p \in X$, $\mathcal{O}_p$ is a local ring. If we have $f \in \mathcal{O}_p$, we define the value of f at p as $f \mod m_p$, where m_p is the (unique, since the ring O_p is local) maximal ideal of O_p This will give us a value in some field because ring quotient maximal ideal is field. We say that f vanishes at p if $f(p) = 0$. that is, $f \in m_p$.

8.4.1 Beware!

A function on a locally ringed space, by definition, we can get the value of a point. In general, given a sheaf, we can only find $f|p$, the value of "f near p". In that, we can talk about the germ, not about the value.

8.5 Varieties and Schemes

think of the ring $A \equiv \mathbb{C}[X_1, X_2, \ldots X_n]/I$ which allow us to define schemes.

We define $\operatorname{Spec}(A)$ to be the set of prime ideals of A, which are used to talk about schemes.

We define $\mathfrak{m}\operatorname{Spec}(A)$ to be the set of maximal ideals of A, which are used to talk about varieties.

This will be our set. We need to know the geometry. We need to understand how $\operatorname{Spec}\mathbb{Z} \simeq \operatorname{Spec}\mathbb{C}[t]$.

Theorem 25. Zariski's Lemma If E/F is a field extension and E is finitely generated over F as an algebra, then E is finitely generated over F as a vector space. This means that E/F is a finite extension of fields. This is supposedly equivalent to nullstellensatz (what?!).

8.6 Kernel and Cokernel presheaves

Suppose we have $V \subseteq U$, and we have a map of presheaves $\phi : \mathcal{F} \to \mathcal{G}$. We can define the kernel presheaf as $(ker\phi)(U) = ker(\phi(U))$.

8.7 Kernel and Cokernel sheaves

We need to show that the kernel will also be a sheaf. Why? This is complicated, because we need to show that it all works out. **exercise**

8.8 Properties of sheaves are preserved by stalks

Exercise: Sections of a sheaf on X are determined by their germs.

8.9 Sheaf on a base

Base of a topology is a collection of open set of X such that every open set of X is a union of the base. Because balls (which are the base of $\mathbb{R}^n$ are nice and topologically trivial) it's easier to work with balls.

So we want to know what it means to have a sheaf on a base. A base is a bunch of open set $B \equiv \{B_i\}$ such that every open set $U \subseteq X$ is a union of some base: $U = \cup_j B_j$.

NOTE: I will use ball and base interchangably in the next section as Ravi does, since any base can be morally thought of as a collection of balls. We need a sheaf on a base $\mathcal{F}(B)$. The presheaf data works because we can clearly nest and restrict functions on balls. However, we need to be careful when we define the identity and gluing axioms, because the intersection (and union) of balls need not be balls! However, we know that the union and intersection will be *covered* by balls (since the balls are a base).

If we have a bunch of sections $f_i \in F(B_i)$ **TODO**

8.10 Where are we going?

We will be forced into the notion of varieties and schemes. We may then go do line bundles, curves, etc. There's also questions about smoothness, dimension, etc. Two examples of good food for thought:

If I have one 5-dimensional manifold as a ringed space, how do we recover the dimension? If we only know the topological space can we know the dimension? What about only the set?

If I have a complex analytic variety as a ringed space, how do whether it is smooth?

8.11 What is the functor of points?

It's just a terrible name. It's the functor of maps to X. Let's say we have a category C. then we have the functor $H_X : C \to Sets$, which sends Y to $Mor(Y, X)$. A complex point is a Spec($\mathbb{C}$) valued point.

8.12 Why don't people use sheaves in diffgeo?

They are. They're used a lot in differential operators.

Another answerer said that the do not use the language much, but sheaves are everywhere.

8.13 Often manifolds are required to satisfy countability / Haussdorf. How do we impose this?

We should add those conditions. There is the Haussdorf condition, which is the wrong way of saying it categorically. We should state it in terms of "separatedness" which is actually categorical. The second condition (second countability) is some kind of finiteness condition.

8.14 What is a ringed space which is not a locally ringed space?

Why do we bother with locally ringed space? Ravi's answer is that in general, such ringed spaces which are not locally ringed are pathological. The good ones that come from geometry will be locally ringed.

8.15 Nullstellensatz: How does one get a good geometric feel for Nullstellensatz? There are so many statements of Nullstellensatz, how do we navigate about them?

Anything interesting called Nullstellensatz will follow from Zariski's lemma.

It tells you that the maximal ideals that we can "see" are all there are. Ie, maximal ideals will correspond to points. We can also do it for non algebraically closed case by thinking about $\mathbb{R}$ in terms of galois orbits.

8.16 When will thinking about adjoints be useful?

For me, it is black magic which you learn to use by experimenting with certain lesser dark spells. Essentially, we dream for things to be adjoints.

8.17 Why did people bother setting up abelian categories?

To talk about kernels and cokernels. We're also going to be fooled into thinking about them correctly.

8.18 Do we use spectral sequences?

Yes, they're just a machine. Cohomology is local to global. Spectral sequences

8.19 Krull PID theorem

if we have a single linear equations on a vector space and we ask where it vanishes, it's going to knock the dimension down by 1 or 0.

8.20 What is the big deal with espace etale?

the best kind of sheaf of sections is that we have a space X, and sheaf of sections are literally sections of the space above it. What is the advantage of doing it this way? All sorts of stuff comes for free. Serre does this in FAC.

Math overflow question

8.21 How do we know that sheaves are the right way to talk about geometry?

It's an empirical question. Sheaves just work so well.

Chapter 9

The rising sea, solutions for first 3 pseudolectures

9.1 Q1.3C: $A \to S^{-1}A$ is injective iff S has no zero divisors

($\implies$): Assume $A \to S^{-1}A$ is injective. We wish to show that S has no zero divisors. Also assume for contradiction that S has zero divisors. So there is an element z such that for some element $z' \neq 0$ we have $zz' = 0$. Since S is multiplicatively closed, we must have that $zw \in S \implies 0 \in S$. Hence, for any two elements $a, a' \in A$, we will have that $a/1 = a'/1 : \ 0(1 \cdot a - 1 \cdot a') = 0$, and hence $a/1 = a'/1$. This the mapping $a \mapsto a/1$ is not injective. This is a contradiction. Hence S has no zero divisors.

($\impliedby$): Assume S has no zero divisors. We wish to show that the map $A \to S^{-1}A$ is injective. Let us have that $a/1 = a'/1$ for some $a, a' \in A$. We wish to show that $a = a'$. $a/1 = a'/1$ means that $s(a \cdot 1 - a' \cdot 1) = 0$ for some $s \in S$. Since S does not have zero divisors, we can conlude that either $s = 0 \vee (a \cdot 1 - a' \cdot 1) = 0$. But 0 itself is a zero divisor in a non-zero ring (since for all other elements $a \in A$, we have $a0 = 0$), so we have $s \neq 0$ since S contains no zero divisors. Thus, $a \cdot 1 - a' \cdot 1 = 0$. Hence $a = a'$.

9.2 1.3D: The map $A \to S^{-1}A$ is initial among A-algebras B such that every element of S is sent to an invertible element of B

Recall that an A-algebra B is an A-module which has a bilinear operator $* : B^2 \to B$.

9.2.1 A-algebra B gives ring map $A \to B$

Let us assume we have an A algebra B. We need to construct a ring map $\phi : A \to B$. this only makes sense if the algebra is assumed to be unital, so let's assume we have a unit 1_B. Now we can simply treat B as a ring where the multiplication from the algebra is the ring multiplication. **TODO:** Question on math.se where I got confused.

9.2.2 ring map $A \to B$ gives rise to B as an A-algebra

Assume the ring map is called $\phi : A \to B$. This is naturally an action of the ring A on the ring B, and hence allows us to view B as an A-module. We can view the multiplication on B as the product of the algebra. This naturally satisfies the bi-linearity axiom.

9.3 Q1.3G: $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$

Let us define a map $f : (a+10\mathbb{Z}, b+12\mathbb{Z}) \in \mathbb{Z}/10\mathbb{Z} \otimes_Z \mathbb{Z}/12\mathbb{Z} \mapsto ab+2m \in \mathbb{Z}/2\mathbb{Z}$. The map f is clearly bi-linear.

Hence by the universal property of the tensor product, it must be that we have a linear map:

$$f' : \mathbb{Z}/10\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} f'((a+10\mathbb{Z}) \otimes (b+12\mathbb{Z})) \equiv ab + 2\mathbb{Z}$$

We can construct the inverse of the map f as the map

$$g : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/12\mathbb{Z} g(a+2\mathbb{Z}) \equiv (1+10\mathbb{Z}) \otimes (a+12\mathbb{Z})$$

These are inverses:

$$\begin{aligned}
&(g \circ f')((a+10\mathbb{Z}) \otimes (b+12\mathbb{Z})) \\
&\quad = g(f'((a+10\mathbb{Z}) \otimes (b+12\mathbb{Z}))) \\
&\quad = g(ab+2\mathbb{Z}) \\
&\quad = (1+10\mathbb{Z}) \otimes (ab+12\mathbb{Z}) \\
&\quad = a(1+10\mathbb{Z})(b+12\mathbb{Z}) = (a+10\mathbb{Z})(b+12\mathbb{Z}) \quad \square \\
&(f' \circ g)(x+2\mathbb{Z}) \\
&\quad = f'(g(x+2\mathbb{Z})) \\
&\quad = f'((1+10\mathbb{Z}) \otimes (x+12\mathbb{Z})) \\
&\quad = (1 \cdot x + 2\mathbb{Z}) = x + 2\mathbb{Z} \quad \square
\end{aligned}$$

https://math.stackexchange.com/questions/72284/proof-of-mathbbz-m-mathbbz-otimes-mathbbz-mathbbz-n-mathbbz

9.4 Q1.4.A Suppose that the poset J has an initial object e. Show that the limit of any diagram indexed by J exists.

Let us assume that e has an initial object. This means that for any other object $j \in J$, we have a unique morphism $\exists! e2j : Hom_J(e, j)$.

Let us assume we have a diagram. This means that we have a functor $F : J \to C$ such that the arrows commute.

We will show that an initial object must be mapped to another initial object by a functor $F : J \to C$.

TODO

9.5 Q1.4.B Limits in the category of sets are products with equalities

More formally, we are to show that:

$$\lim_J A_i \equiv \left\{ (a_i)_{i \in J} \in \prod_i A_i : F(j \xrightarrow{m} k)(a_j) = a_k \text{ for all } j \xrightarrow{m} k \in Hom(j,k) \in Hom(J) \right\}$$

along with the obvious projection maps $\pi_k : \lim_J A_i \to A_k$.

9.5.1 A notational issue I have been confused with for a while

When someone asks for a limit, they first need to provide a diagram $F : J \to C$. Once they give us the diagram, they have the right to ask us for the limit of the diagram.

For example, in the case of products, one first gives us the diagram $d \equiv J(\bullet;\bullet) \xrightarrow{F} C(A;B)$ then cranks the limit machine with "what is the limit of the above diagram d". The limit machine returns us the product $A \times B$.

So the "type" of the limit is really:

lim **inputs:**
(i)diagram $F:$ functor $J \to C$
(the diagram identifies both objects *and* arrows in C as the image of F)
lim **outputs:**
$(i) limit : C$
$(ii) proj : (j : J) \to Hom(limit, F(j))$

$$proj[j \in J] \equiv limit \xrightarrow{proj[j]} F(j) \in Hom(limit, F(J))$$

$(iii) commutes :$

$\forall (j \xrightarrow{m} j' \in J)$

$$\begin{array}{ccc} & limit(\lim F)) & \\ proj[j](\lim F) \swarrow & & \searrow proj[j'](\lim F) \\ F(j) & \xrightarrow{F(m)} & F(j') \end{array}$$

$(iv) initial/universal$: If there is another object $W \in C$ and maps $proj' : (j : J) \to Hom(W, F(j))$:

$\forall (j \xrightarrow{m} j' \in J)$

$$\begin{array}{ccc} & W & \\ proj'[j] \swarrow & & \searrow proj'[j'] \\ F(j) & \xrightarrow{F(m)} & F(j') \end{array}$$

then this factorizes through $limit(\lim F)$

9.5.2 OK, back to the proof

We essentially need to show that:

$$\lim_J A_i \equiv \left\{ (a_{j_1}, a_{j_2}, \ldots a_{j_n}) \in \prod_{j \in J} F(j) : \forall j_p \xrightarrow{m} j_q, F(m)(a_{j_p}) = a_{j_q} \right\}$$

[Intuition: we take the large cartesian product of the images of all the $F(j)$, and we then equalize the domain of every $F(m)$ with its image. If we have an arrow between x and y, we set $f(x) = y$ to ensure that they equalize.]
along with the obvious projection maps $\pi_k : \lim_J A_i \to A_k$.

9.6 Q1.4.B Colimits in the category of sets are disjoint unions with equivalences

TODO

9.7 Q2.2.B Presheaf that is not a sheaf: Presheaf of bounded functions

Consider the function $f(x) \equiv x$. This is bounded on every open interval $I \equiv (l, r)$: $l \leq f(I) \leq f(r)$ But the full function $f(x)$ is unbounded. Hence it does not satisfy the gluing axiom.

9.8 Q2.2.C Identity and gluability as a limit

Content stolen from the wikipedia on gluing axiom. We want to identify $F(\cup_{i\in I} U_i)$ as the limit of a certain diagram. We will write down the digram:

$$F(U) \xrightarrow{\prod_i Res(U,U_i)} \prod_i F(U_i) \underset{F(U_j)\to F(U_i\cap U_j)}{\overset{F(U_i)\to F(U_i\cap U_j)}{\rightrightarrows}} \prod_{i,j} F(U_i \cap U_j)$$

If F should be a sheaf, then we need F to be a limit of the diagram (?) **TODO: WTF does that even mean?**

9.9 Q2.2D (a) Verify that functions on a manifold do indeed form a sheaf.

It is clear that they form a presheaf, as the restriction of a differentiable function to a smaller domain remains differentiable.. For the identity axiom, if the functions f_i and g_i agree on open sets U_i, then they must agree on $\cup U_i$, by definition of equality. So this is also immediate. Only non-trivial property is gluing, as we need to verify that the gluing of two functions continues to be differentiable. Let us try to glue (f, U) to (g, V). If $U \cap V = \emptyset$, then we can consider the function $h \equiv f \cup g$ and and are done. Otherwise at $U \cap V$, we need to check that we can really glue f and g and that the glued function remains differentiable. Define the the function as:

$$h(x) \equiv \begin{cases} f(x) & x \in U - V \\ f(x) = g(x) & x \in V \cap U \\ g(x) & x \in V - U \end{cases}$$

If we have a neighbourhood entirely in $U-V$ or in $V-U$, the differentiability in that neighbourhood follows from the differentiability of f or g. If we need to consider differentiability in some neighbourhood that is in $U \cap V$, then we can consider the differentiability of either f or g.

9.10 Q2.2D (b) Verify that real valued continuous functions on open sets of a topological space X form a sheaf

Is the same as the differentiable case. Basically, continuity is also a local property so everything works out.

9.11 Q2.2E Show that the sheaf of functions that are locally constant is indeed a sheaf

For gluing, assume we have $f(x) = c$ on U, $g(x) = d$ on V. If we have non-empty $U \cap V$, then we must have that $f(x)|U \cap V = g(x)|U \cap V$ and hence $c = d$. Thus we just build the constant function $h(x) \equiv c = d$. Otherwise, if U and V are disjoint, we build a piecewise function:

$$h(x) \equiv \begin{cases} c & x \in U \\ d & x \in V \end{cases}$$

and we are done.

9.12 Q2.2F Let Y be a topological space. Show that continuous maps to Y forms a sheaf on X

Pre-sheaf-ness is clear since it's just functions.

Let's first do gluing. Assume we have two continuous function $f : U \to Y$ and $g : V \to Y$, such that they agree on $U \cap V$. We can define

9.13 Q2.2G Let Y be a topological space. Let $\mu : Y \to X$. Show that sections of μ form a sheaf

9.14 Q2.2H Show that the pushforward of a sheaf is a sheaf

Let $\pi : (X, \tau) \to (Y, \tau')$ be a continuous map and $F : \tau \to \mathcal{O}$ is a presheaf on X. Then we define a sheaf on Y, let's call it $G : \tau' \to \mathcal{O}$. Note that G is a presheaf of Y taking values the same as presheaf F. We define $G(V) \equiv F(\pi^{-1}(V))$. We need to show that this is a presheaf, and also, is a sheaf if F is a sheaf

9.14.1 G is a presheaf

If we have two subsets $V, W \in tau'$ such that $V \subseteq W$, then we need to be able to restrict $G(W)$ to $G(V)$. But $G(W) = F(\pi^{-1}(W)), G(V) = F(\pi^{-1}(V))$. Since $V \subseteq W$, we have $\pi^{-1}(V) \subseteq \pi^{-1}(W)$. Hence there's a restriction map in F, $Res_F(\pi^{-1}(W), \pi^{-1}(V)) : \pi^{-1}(W) \to \pi^{-1}(V)$, which is the same as $Res_G(W, V) : \pi^{-1}(W) \to \pi^{-1}(V)$.

9.14.2 G is a sheaf

We can once again similarly pushforward the sheaf gluing and identity.

9.15 Q2.2I Pushforward induces maps of stalks

9.16 Q2.2I Describe $\mathcal{O}_{X,p}$ modules

9.17 Q2.3A Morphisms of sheaves induce morphisms of stalks

9.18 Q2.4A Sections are determined by germs

9.19 Q2.4B Support of a section is closed

9.20 Compatible germs, an exposition

Taken from the document Let F be a presheaf on (X, τ) and let $U \in \tau$ be an open set. We now now want to consider a collection of germs f_x, one for each $x \in U$. So we write this as $(f_x)_{x \in U}$ that has one f_x for every point in U. This lives in in the product of stalks $\prod_{x \in U} F_x$. Such a collection of germs f_x is said to be compatible over U if ..

Formally, we have an open cover $C[i]$ of U, and sections of the sheaf $s[i] \in F(C[i])$. [recall that a section of a sheaf the value the sheaf takes at a set. If $C[i]$ is an open set, then elements of $s[i] \in F(U[i])$ are called as sections of $F(U_i)$] These sections $s[i]$ are such that their germs at the point x is equal to the function f_x. That is, $s[i]_x = f_x$.

So in our minds eye, we should see a space U, and function f_x hanging above for each $x \in U$. Next, we should see an open cover of U, covered by $C[i]$. On each $C[i]$, we have an element $s[i] in F(C[i])$ whose germs at each point x agree with the f_x below it. If such an open cover and its sections exist, then the germs f_x are said to be compatible.

We note that any section of the sheaf $g \in F(U)$ creates a collection of compatible germs $(g_x)_{x \in U}$.

9.21 Q2.4C Any choice of compatible germs for a sheaf of sets $F(U)$ is the image of a section of F over U

This is in some sense asking the converse: it's clear that the image of a section creates compatible germs. Now we are to show that compatible germs come from the image of a section.

Proof strategy is clear. We have an open cover C_i of U, and the sections $s[i]$ of $F(C_i)$ which lower to f_x. So we need to show that for all i, j, $s[i]|_{C_i \cap C_j} = s[j]|_{C_i \cap C_j}$ This way, we can glue the $s[i]$ together to get a section.

Assume that we have sections $s[i], s[j]$ that cannot be glued. Hence, $s[i](p) \neq s[j](p)$. But if this is the case, then we ought to have that $s[i]_p \neq s[j]_p$: That is, their germs at p cannot be the same. But this is absurd, since by assumption, the germs all agree: $s[i]_p = s[j]_p = f_p$.

Hence we can indeed glue all the $s[i]$ together to build an element of $F(U)$.

9.22 Q2.4E Isomorpshisms are determined by stalks

9.23 Q2.4F Counterexamples for pre-sheaves. Take 2-element set with discrete topology

9.24 Q2.4O Epi on sheaves

9.25 Q2.5A Recovering a sheaf from a sheaf on a base

Chapter 10

AGITTOC Pseudolecture 4

- Youtube video
- Link to exercise
- Exercise 2.2.J might give you some practice with modules over rings. Try 2.3.C if you havent already. Get somewhat happy with why we can understand things about sheaves in terms of stalks, by picking a do-able problem or two in Section 2.4. Understand examples in Section 3.3 as much as you can, and practice drawing pictures of rings. **If you came in happy with commutative algebra:**Do 2.3.C if you havent already. Understand sheaves via stalks and sheaves on a base well by picking an interesting problem in each of those sections (2.4 and 2.5). Understand the examples of Section 3.3 as completely as possible. **If you are complex analytically minded:** Have you fully figured out how to think about complex analytic varieties (including morphisms between them) in the language we are using? Do you see why the fibered product of complex analytic varieties exists, for example? **If youve seen some commutative algebra to think about it:** Can you answer the second question I posed before the start (with rigorous proof!)? Can you describe how the maximal ideals of the polynomial ring in n variables over a field k should be identified with the Galois-orbits of n-tuples of elements of the algebraic closure $\overline{k}$ of k? **If you have already become comfortable with the ideas we are talking about:** (This is only for those who have already seen the above, because otherwise I fear you will become a lotus-eater.) Try to mix Yoneda with maps to a space form a sheaf. Do this without looking up the definition of a Grothendieck topology you should try to do this (even if you fail) without being told what to do. Here is a precise case to think through. Suppose $\mathcal{G}$ is the category of balls (or if you prefer, polydiscs) in $\mathbb{C}^n$ (where n is not specified), where morphisms are holomorphic maps. Let the functor category ($\mathrm{Fun}_{\mathcal{G}}$) of $\mathcal{G}$ be defined by taking the objects as contravariant functors from $\mathcal{G}$ to the category of (Sets), and morphisms are "natural transformations of functors", so we

have a (covariant!) functor $Yo : \mathcal{G} \to (\mathrm{Fun}_{\mathcal{G}})$, given by $X \mapsto h_X$. Two big things: (1)(Yoneda) Yonedas Lemma says that this is a faithful functor, which is why we call Yo the "Yoneda embedding" of $\mathcal{G}$ into its functor category $(\mathrm{Fun}_{\mathcal{G}})$. (2) (maps glue) Second, h_X is a sheaf on any $Y \in \mathcal{G}$ (considered as a topological space). Now $\mathcal{G}$ sits in a bigger category, the category of complex manifolds. Show that a complex manifold X (not necessarily a ball!) gives an element of $(\mathrm{Fun}_{\mathcal{G}})$, and it still satisfies "Yonedas Lemma for $\mathcal{G}$" (i.e., this element of the functor category h_X determines X up to unique isomorphism of manifolds), and also h_X is a sheaf for all $Y \in \mathcal{G}$. So: figure out what it should mean for an element of $(\mathrm{Fun}_{\mathcal{G}})$ to be "a sheaf" on all elements $Y \in \mathcal{G}$, and see what information you need to make this make sense. (Hint: you need to know when a bunch of open embeddings into some $Y \in \mathcal{G}$ "cover" Y.) You are basically going to invent an approximation of the notion of a topology on this category (otherwise known, roughly, as a Grothendieck topology).

10.1 While you are waiting:

we have 34 linear equations in 10 variables, with coefficients in $\mathbb{Z}$. If there is a solution in $\mathbb{C}^{10}$, then there is a solution in $\mathbb{Q}^{10}$. Why? Also, if there is only one solution in $\mathbb{C}^{10}$, then it is in $\mathbb{Q}^{10}$.

Next, assume we have 34 polynomial equations in $\mathbb{Z}$. If there is a solution in $\mathbb{C}^10$, then there is a solution in $\overline{\mathbb{Q}}^{10}$. Why? Also, if there are only finitely many solutions in $\mathbb{C}^{10}$, then they are all in $\overline{\mathbb{Q}}^{10}$. Why?

We're trying to learn and understand something. The complication is that everyone has different goals. How to think categorically, think of sheaves, how to think of a geometric space. By the end of today, we should be comfy with most of chapter 1, most of chapter 2, the start of chapter 3.

Today, we ought to understand:

- geometric spaces as ringed spaces
- sheaves
- varieties/schemes
- sheaves on a category

10.2 Thinking about geometric spaces

Complex manifolds, varieties, schemes, etc. We want to think of it as $((X, \tau), \mathcal{O})$. where $\mathcal{O}$ is a sheaf of functions. For every point $p \in X$, we have the stalk $\mathcal{O}_p$. There is an evaluation map $\mathfrak{m}_p \to \mathcal{O}_p \xrightarrow{\text{evaluation at } p} \mathbb{C}$ $\mathfrak{m}_p$ is a maximal ideal. The ring $(\mathcal{O}_p, \mathfrak{m}_p)$ is a local ring.

This ring is a local ring based on the following fact: If f is a function on an open set U, then the locus where f vanishes is a closed subset. Let us denote

this by $V(f) \equiv \{p \in U : f(p) = 0\}$ (V for vanish). We need to show that $V(f)$ is closed.

10.3 What is a map of complex manifolds?

We have the spaces $((X, \tau), \mathcal{O}_X)$ and $((Y, \tau'), \mathcal{O}_Y)$. We have a map from $(X, \tau) \xrightarrow{\pi} (Y, \tau')$. Let X have dimension m, Y have dimension n. We map from $U \in \tau$ to $V \in \tau'$. We have local coordinates for U, V that provide homeomorphisms into $\mathbb{C}^m, \mathbb{C}^n$. As a diagram, it looks like:

$$\begin{array}{ccccccc} & & \mathbb{C}^m & \leftarrow & U & \hookrightarrow & X \\ y_j = f_j(\{x_i\}) & & \downarrow & & & & \downarrow \pi \\ & & \mathbb{C}^n & \leftarrow & V & \hookrightarrow & Y \end{array}$$

So we have a map that written in local coords looks like:

$$\begin{aligned} y_1 &= f_1(x_1, x_2, \ldots x_m) \\ y_2 &= f_1(x_1, x_2, \ldots x_m) \\ &\ldots \\ y_n &= m_1(x_1, x_2, \ldots x_m) \end{aligned}$$

where each of these $y_1, \ldots, y_n$ is homolorphic.

Let's restate this. We have a continuous map of topological spaces. We want the the pullback $\pi^{-1}(y_i)$ is a $\mathbb{C}$ valued function on U. For any holomorphic function g on V, we require $\pi^{-1}(g)$ to be holomorphic. This statement is independent of coordinates on V and coordinates on U. For any open set U, pulling back $\mathcal{O}_Y(V)$ to $\mathcal{O}_X(\pi^{-1}(V))$. Recall that $\mathcal{O}_Y, \mathcal{O}_X$ were the sheaf of functions on Y, X respectively. So we get a statement like:

$$\pi^{-1}\mathcal{O}_Y(V) \to \mathcal{O}_X(\pi^{-1}(V))$$

10.4 Sheaves

How do we work with a sheaf? Our initial definition was open set at a time. We get a good definition for pre-sheaves and pushforwards.

We can also work stalk by stalk, which will be good for sheaves, and good for pulling back.

We can also talk about this in terms of nice open set by nice open set, by considering sheaves defined on a base.

10.5 Understading sheaves through their stalks

If F is a sheaf on X and we have $U \subseteq X$ open, then the natural map $F(U) \to \prod_{p \in U} F_p$ that takes a section of a sheaf to the tuple of all germs in the section,

stalk by stalk. This is an injection. Why? if $f, g \in F(U)$ have the same germs, this means that near a point p, we have an honest open set U_p where $f|U_p = g|U_p$. This is true at every single point. By the identity axiom, they must be equal.

Now the converse: how do we know that if we are given some element $\prod_{p \in U} F_p$ which is a germ in each stalk, how do we know if it comes from a section? Asked differently, what is the image of $F(U) \to \prod_{pinU} F_p$?

Given $s[p] \in F_p$ which is a whole bunch of germs, how do we tell if there is some $f \in F(U)$ with $f_p = s(p)$? **answer**: If there is an honest section, then the germs ought to be compatible with each other. For each $p \in U$, there are representatives for $s(p)$ that has all the right germs.

That is, there exists $p \in V_p \subset U$ and an honest section $r[p] \in F(V_p)$ which gives the correct germs: $r[p]_q = s[q]$ for all $q \in V_p$.

10.6 Sheafification of a presheaf

the sheafification of a presheaf F gives us a sheaf F^{sh} and a mapping $f : F \to F^{sh}$ such that F^{sh} is universal across all maps from F into G^{sh}. That is, for any other $g : F \to G^{sh}$, there exists a **unique map** $e : F^{sh} \to G^{sh}$ such that $g = e \circ f$. Alternatively, it's a free functor that's adjoint to the forgetful functor.

10.6.1 Does the sheafification exist?

Yes! If F is a presheaf on X, define F^{sh} to be the sheaf of compatible germs of F.

We should check that it's a sheaf! Then, we need to show that there's a map from F to F^{sh}. We need to show that it is surjective on stalks.

Finally, we need to check the universal property.

10.7 Cokernel Sheaf

Suppose $\phi : F \to G$ is a morphism of sheaves. We have the cokernel presheaf $\text{coker}^{pre}(\phi)$, in the category of presheaves of abelian groups on X.

We claim that the sheaf $(\text{coker}^{pre})^{sh}$ is the cokernel in the category of sheaves of abelian groups on X.

10.8 How to think about cokernel sheaf

Assume we have $\phi : F \to G$, which is a morphism of sheaves of abelian groups on the topological space X. To have an example, let ϕ be an injection. Now the cokernel ought to be something like G/F.

10.8.1 Cokernel sheaf in terms of stalks:

for all $p \in X$, $(\operatorname{coker} \phi)_p = \operatorname{coker} \phi_p$, where $\phi_p : F_p \to G_p$. **Homework: prove this!**

10.8.2 Cokernel sheaf in terms of open sets:

We can't do it open set by open set. It is not true that $(\operatorname{coker} \phi)(U) = \operatorname{coker}(F(U) \to G(U))$.

We want to say that given the following data, we can get a section of a cokernel. This is morally true, but we need to setup equivalence relations for it really work. The **Homework: what should the equivalence relations be?**

We take the U which has an open cover by smaller open U_i. We want sections $s_i \in G(U_i)$. We want that on each $U_i \cap U_j, s_i - s_j = \phi(t_{ij})$ where $t_{ij} \in F(U_i \cap U_j)$. What does this mean? What is the equivalence relation?

10.9 Sheaves on the base of a topology

The base of a topology is a collection of sets $\{B_i\}$ such that any open set $U \subseteq X$ can be written as the union of sets from the base: $U = \cup_{i \in I} B_i$.

It should be enough to have the data of $F(B_i)$ along with the restriction maps $F(B_i) \to F(B_j)$ for $B_j \subseteq B_i$ to reconstruct the full sheaf. *Note that we only have the restriction for the base!, not for arbitrary opens!*

There are various levels of niceness. One extremely nice base would be a base of convex sets, where the intersection of convex sets continues to remain convex!

On the other hand, there are worse bases (eg. open balls) where the intersection of two open balls need not be an open ball. So some times, we can recover the full sheaf with only information about some (enough) open balls.

Conversely, there should be some way to check that the information of some $G(B_i)$ with $G(B_i) \to G(B_j)$ comes from a sheaf. So we need "sheafy" conditions.

10.9.1 Sheaf on the base

If $\{B_i\}$ is a base for the topology of the topological space X, then a sheaf on the base $\{B_i\}$ is the data:

- Sets $F(B_i)$
- Restriction maps $F(B_i) \to F(B_j)$ for $B_j \subset B_i$
- Restriction maps satisfy presheaf condition: For $B_i \subseteq B_j \subseteq B_k$, we have that $F(B_k) \subseteq F(B_j) \subseteq F(B_i)$.
- Identity axiom: If $f, g \in F(B)$ satisfy $f|_{B_i} = g|_{B_i}$ for every $B_i \subseteq B$ then $f = g$. This is interesting: why *every?* We should show that this is the

- Gluability: If $\{B_i\}$ cover the base open B and we have $f_i \in F(B_i)$ such that they agree on pairwise overlaps, then there is a unique $f \in F(B)$ with $f_i = f|_{B_i}$.

10.9.2 Germs of Sheaf on a base

Germs still make sense. A germ of a sheaf at p should be a section on some honest open set. In this case, we will need honest *basic* open sets $p \in B_i$. We again declare the same germ definition, etc. This works because categorically, it's just a colimit: $F_p \equiv \operatorname{colim}_{p \in B_i} F(B_i)$.

compatible germs also make sense, so we indeed have a sheaf on the base. If we have a sheaf on the base, we have an actual sheaf. So we have an equivalence:

$$\text{Sheaves on } (X, \tau) \leftrightarrow \text{Sheaves on the base } (X, \{B_i\})$$

10.10 Sheaves of abelian groups on X form an abelian category

If we have $F \xrightarrow{\phi} G$, we have kernel, cokernel, etc. We just need to work stalk by stalk, germ by germ and we're done. germ-by-germ, we just have maps of abelian groups. It just works!

10.11 Thinking more about varieties and schemes

To define a new kind of geometric space, we need to define a local model:

- as a set.
- with a ring of functions.
- with the topology where vanishing set of the functions are closed.
- with a sheaf of rings (functions), built out of the functions we considered before.

10.12 Complex varities / Varieties over an algebraically closed field / Variety over a field / Schemes

We have subsets of $\mathbb{C}^n$ cut out by polynomials. This is our set. Our functions are the restrictions of polynomials $\mathbb{C}[X_1, X_2, \ldots, X_n]$

Rings are called A (Anneaux).

Our set / space is the maximal ideals of the ring R. This is called $\mathfrak{m}\operatorname{Spec} R$

The functions are just polynomials. $R = k[x_1, x_2, \ldots, x_n]/I$. We need the condition that if $f^2 = 0$ then $f = 0$. That is, the only nilpotent function is 0 for varieties.

10.13 Examples with pictures

> If you read EGA, you will find no pictures, and that was because pictures were invented in the latter half of the 20th century

$\mathbb{C}[X]$ is a single dimension, because the maximal ideals $\mathfrak{m}\,\mathrm{Spec}\ (x - a)$ are in bijection with $\mathbb{C}$. We draw $\mathbb{C}$ as a single line (1D). We have one other ideal, the prime ideal (0). Where does it go in the picture of a single line?

What about $\mathbb{C}[X, Y]$? Assume Nullstellensatz, we know that the maximal ideals are just $(x - a, y - b)$. $\mathfrak{m}\,\mathrm{Spec}$ is just $\mathbb{C}^2$ so we have a 2D space. This is sane, because if I were to ask "what is the value of a polynomial $p(x, y)$ at (a, b)?" We would evaluate $p(a, b)$ which is the same as $p(x, y)$'s image in the quotient $C[X, Y]/(x - a)(x - b)$.

We have many prime ideals, though. For example, (0), $(f(x, y))$ where f is irreducible. (A prime ideal is one where the quotient is an integral domain. The quotient cannot have divisors of zero. If $f(x, y)$ is irreducible, then we cannot have divisors of 0).

We have to fit additional points. For example, $(x - 2)$ which is prime in $C[X, Y]$. What point does it correspond to? Well, is it on $(xy - 2y = 0)$ Yes, because this function is on the ideal $(x - 2)$. So the "point" is contained in $x = 2$. The point is on $(x = 2)$, but is nowhere in particular on the line $x = 2$. Similarly, the prime ideal 0 is somewhere on the plane, but nowhere in particular. Similarly, if we think of $(y^2 - x^3)$, the ideal is a point somewhere on $y^2 = x^3$ but nowhere in particular.

10.14 Why algebra should be geometry?

Consider $\mathbb{C}[X, Y, Z]$. What are the maximal ideals? By nullstellensatz, it must be $(x - a, y - b, z - c)$ — we think of this as a point (a, b, c).

We also have prime ideals $(f(a, b, c))$, (0). We've seen how to think about these: the points that correspond to these ideals lie somewhere on $f(a, b, c)$ but nowhere in particular.

We are also missing some prime ideals, such as (x, y). This is prime because the quotient ring is just $C[Z]$ which is an integral domain. But where do we draw this? it's not an ideal generated by a *function*. It should be one-dimensional thing, but how do we make it precise?

10.15 Problem: Maximal ideals and Galois orbits

Show that the maximal ideals of $K[X_1, X_2, \ldots, X_n]$ can be identified with orbits $Gal(\overline{k}/k)$ on $\overline{k}^n$.

10.16 Topologies on sets to topologies on categories

Let G be a category of geometric spaces. If $X \in G$ we have two key ideas:

- We can recognize X by maps into it: By Yoneda, Let FG be the functor category whose objects are contravariant functors $G \to Sets$. Then $G \xrightarrow{Yo} FG$ is faithful.
- Maps to X glue. For any $Y \in G$, maps to X form a sheaf on Y. A (pre)-sheaf is again a contravariant functor from C to Set.

Now recall that any complex manifold also satisfies both of these properties. How do we come up with a definition for an element in the functor category FG to be a sheaf? Then we can define a complex manifold as a sheaf in FG, which can be *covered (?)* by *open subsheaves (?)* each of which is an element of G.

An examaple is projective space. Which is $\mathbb{P}^n \equiv (\mathbb{C}^{n+1} - \{\vec{0}\})/\mathbb{C}^*$: that is, vectors in C^{n+1} quotiented by scaling.

Does this mean that maps into $\mathbb{P}^n$ are just maps to $C^{n+1} - \{\vec{0}\}$ modulo maps to $\mathbb{C}^*$? Alternatively, is $Yo(\mathbb{P}^n) = Yo(C^{n+1} - \{vec0\})/Yo(C^*)$? No because $Yo(C^{n+1} - \{vec0\})/Yo(C^*)$ is not a sheaf. We need to sheafify it! What does this "mean"?

This is a good example for why quotients are interesting in geometry, not not just algebra.

10.17 Is $\mathcal{O}$ being local an assumption for geometric space?

For a geometric space, we have not defined a geometric space, so it should be part of a definition. So in general, anything that is geometric will have stalks as local rings. The key idea is that zero sets of functions are closed.

10.18 Is there a connection between section of a sheaf and section as a thing with a right inverse?

Yes, espace etale.

10.19 Does sheafification preserve colimits?

RAPL: Right adjoints preserve limits, left adjoints preserve colimits. Sheafification is a left adjoint.

10.20 Spec as being divided into layers

Dimension zero is on the bottom, which percolates into all layers. Russian lecture notes? Manin?

10.21 Why $\mathfrak{m}\,\mathrm{Spec}$ versus Spec?

For algebraically closed fields, $\mathfrak{m}\,\mathrm{Spec}$ has the same information as Spec. This is non-trivial and Nullstellensatz-y.

$\mathfrak{m}\,\mathrm{Spec}$ and Spec are not the same thing over non algebraically closed fields.

10.22 Generic point as point at infinity?

It's not a compactification. We don't know where to put the point.

10.23 Differentiate between prime ideals which are contained in the exact same set of maximal ideals?

For a variety, a prime ideal must be determined by the maximal ideals it is contained in, so its fine for varieties.

10.24 Noncommutative ringed spaces?

Yes, but it's hard. We should think of the center of the noncommutative ring as capturing Spec, and we need to figure out what the larger space is that holds the non commutativity.

10.25 Why isn't the quotient presheaf a sheaf in the $C^{n+1} - \vec{0}$ quotiented by $\mathbb{C}^\star$

I will give you a map to projective space which is not a map into $C^{n+1} - \vec{0}/\mathbb{C}^\star$. Map projective space to itself as the identity. This cannot be written as a map from projective space to $C^{n+1} - \vec{0}/\mathbb{C}^\star$. In some sense, the identity map is the "largest" projective space map which allows us to exhibit this deficiency. [I have no idea what this means].

10.26 What was Grothendeick guided by? Geometry? Abstraction?

no reasonable's person of geometry. He was trying to understand things from a very general point of view. Some of his false prophets assume that he was making stuff general for its own sake.

10.27 Ring that is not Jacobson?

A DVR is not Jacobson, such as the p-adics. Mumford's red book has a picture of what localization should look like. Jacobson rings should be learnt about only when forced upon you.

10.28 Does identity and gluability relate to injectivity and surjectivity of the Sh functor?

Perhaps, go read zulip.

10.29 Plus construction

Identity axiom says sameness glues. Gluing axiom says that objects glue. So in the first level, we lose objects, because we are forcing equivalence relations between objects. For gluing, we are make arrows equal (?)

Chapter 11

Solutions for pseudolecture 4 exercises

Chapter 12

AGITTOC Pseudolecture 5

- Youtube video
- Link to exercise
- Today, I finished (for the most part) discussing sheaves in particular, we discussed inverse image sheaves. Weve talked more about the underlying set of an affine variety or scheme (mSpec and Spec). In particular, weve begun to flesh out a dictionary between algebra and geometry. We saw why maps of rings give maps of Specs (or mSpecs, if appropriate) in the other direction.

  Things to think about in the next couple of weeks: Youre undoubtedly still thinking about things from the previous week, so here are some more things to ponder. If you are relatively new to commutative algebra, and you find that you can do exercises, then declare victory you can learn commutative algebra as you need it. It is worth thinking through the properties we need on quotient rings, localization of rings, and Noetherian rings. **Things to read this week:** On top of the things you read as of last week, you should now read the final section 2.7 on sheaves, and basically all of Chapter 3. We havent really discussed the topology on (m)Specs (the Zariski topology), but you have already told me how it should work — sets cut out by a bunch of functions should be declared to be closed sets, and nothing else. So you can now read all of Chapter 3 (and also think through what things mean even in the case of mSpec).

  Problems to think about this week and next: For everyone: please do the same three meta-problems of what was interesting, and what was challenging, and what was confusing. You may have noticed that your answers have a big effect on what I choose to say in the pseudolectures.

  If you are new to commutative algebra: There are a bunch of things in commutative algebra that are now coming up — you may be able to understand them all, by judiciously working through exercises. I hesitate to suggest any in particular — just pick several that you think are at the

border of your understanding. I am hoping that a number of you will think about the same problems, and discuss them (and call in me or some shepherds if you have questions or things to talk about). For example, you might be able to learn all you need (for now) about Noetherian rings by doing a few exercises in *section 3.6*. Do what you kind to understand the inverse image sheaf. For example, *2.7.B. Exercise 3.4.E and 3.4.F* will help see what nilpotents do (or more precisely dont do) geometrically. Weve seen that maps of rings induce maps of (m)Specs in the opposite direction; *3.4.H* will show you that this is a continuous map, and *3.4.I* will give a bit more insight. Definitely do 3.4.J.

When you read *3.5* on distinguished open subsets, definitely solve *3.5.E* if you can.

Section 3.6 has a lot of words in it, but the important concepts have already happened by *3.5*. *3.6.A* and *Remark 3.6.3* relate to Taylors comments on idempotents. *3.6.B* and *3.6.C* give examples that help you see the weirdness of Zariski topologies. *3.6.E* and *3.6.F* are concrete problems that might test your understanding; perhaps 3.7.G and 3.7.H too. In section 3.7, do *3.7.E* and *3.7.F*. And next Saturday, Ill quickly review things you have read on the Zariski topology, and we will define schemes (and, almost, varieties)!

We have compatible stalks / espace etale. We imagine ourselves picking a germ of a section of F at each point, which should extend to an honest section over some open set. If we do this, we get the sheaf of compatible germs. This gives us a map from a presheaf to its sheaf of compatible germs (sheafification).

12.1 Recall: sheaves on a base

It's enough to have the sheaf data defined just on the base of a sheaf. Because we know what the germs are, we can build the germs, and then build the sheaf of compatible germs. This lets us expand it into a "full sheaf".

12.2 Inverse image sheaf

We have a map of topological space $\pi : X \to Y$. We can make a pushforward sheaf $\pi_\star : Sh(Sets, X) \to Sh(Sets, Y)$ which pushes forward sheaves of sets on X to sheaves of sets on Y.

The inverse image sheaf gives us a map $\pi^{-1} : Sh(Sets, Y) \to Sh(Sets, X)$. Why don't we call it the pullback sheaf? We don't call it $\pi^\star F$ because the notation is reserved for something else.

12.2.1 Definition 1: Left adjoint to $\pi_\star$:

$$Hom_X(\pi^-1\mathcal{G}, \mathcal{F}) \leftrightarrow \mathrm{Hom}_Y(\mathcal{G}, \pi_\star\mathcal{F})$$

The nice thing is that we get the hom set adjunction automatically, along with all the data we would "expect". The problem is that we don't even know if this thing exists.

We also lose the geometry of what's going on.

12.2.2 Definition 2: Compatible stalks/espace etale

we have $\pi : X \to Y$, we have a sheaf G on Y. We want to build $\pi^{-}1G$ which is a sheaf on X. This is hard to define (need to think about it).

The advantage is that this gives us stalkiness. So for example, it is clear that for sheaf of abelian groups, we have that $\pi^{-}1 : Sh(Ab, Y) \to Sh(Ab, X)$ is exact, since we just need to check on stalks.

How do we make this precise? Exercise!

12.2.3 Definition 3: Constructive

We first define a presheaf $\pi^{-}1G$.

$$(\pi^{-}1G)^{psh}(U) = \text{colim}_{V \subset \pi(U)} G(V)$$

Then sheafify to get $\pi^{-}1G$. Why is this not a sheaf? what fails?

This gives neither formal insight nor definitional insight.

12.2.4 Coming to terms

For every $U \subseteq X$ we have $V = \pi(U) \subseteq Y$. We have a map from $G(V)$ to $F(U)$ which is compatible with restriction maps on both X and Y.

12.2.5 Example: a single point

If $X = \{*\}$ is just a point that maps to Y, with $\pi(*) = y_0$ then the inverse image sheaf retrieves a stalk at y_0, G_{y0} for us.

12.2.6 Example: a subset

If $X \subseteq Y$ where X is open with $\pi : X \hookrightarrow Y$, then we have $\pi^{-}1G \simeq G|_X$.

12.2.7 Example: Covering space

12.3 Support of a section of a sheaf

We have a topological space (X, τ) and a sheaf of abelian groups F, because we want to talk about when things are zero. $s \in F(U)$, a section of the sheaf over some open set $U \in \tau$. Define the support of s, $\text{Support}(s) \equiv \{p \in U : s_p \neq 0\}$: the set of points whose germs are non-zero. Non-zero value has no meaning! It is not zero in a *neighbourhood* of p.

Show that the set Support(s) is a closed subset (equivalently, the complement is open). The complement is where it is zero. If the complement is zero, then by compatible germs, we can build a neighbourhood where it comes from, which is open?

12.3.1 Confusion!

If we have a complex manifold with the sheaf of holomorphic functions, let $s \in F(U)$ a section of the sheaf (so a holomorphic function).

- the locus $\{p : S(p) \neq 0\}$ is an open set[non-zero *value*]. Where is s not 0?
- The locus $\{p : S_p \neq 0\}$ is a closed set [non-zero *germ*]. Near which points is s not the zero *function*?

There is a strong diffrence between **at** and **near**.

12.4 Support of the entire sheaf

We can define Support$(F) \equiv \overline{\{p \in X : F_p \neq 0\}}$.So we take the closure of all points where the sheaf is nonzero.

This is useful because we have an inclusion map i : Support$(F) \hookrightarrow X$. The sheaf on top of Support(F), $i^{-1}F$ pushes forward to the "full sheaf" $F = i_\star(i^{-1}F)$.

12.5 Thinking more about affine varieties and affine schemes

$\mathfrak{m}\,\mathrm{Spec}(A) \equiv \{\mathfrak{m} \subseteq A : \mathfrak{m} \text{ is a maximal ideal of } A\}$. $\mathrm{Spec}(A) \equiv \{p \subseteq A : p \text{ is a prime ideal of } A\}$.

12.5.1 Definition: $n-$space over a field

$\mathbb{A}^n_k \equiv \mathfrak{m}\,\mathrm{Spec}\,k[X_1, \ldots X_n]$ If k algebraically closed, then $\mathbb{A}^n_k = k^n$ $\mathbb{A}^n_k \equiv \mathrm{Spec}\,k[X_1, \ldots X_n]$

But this is a generalization of n-space. the $\mathbb{A}$ stands for affine.

12.6 What is a ring?

Commutative ring. Every ring has a 1 and a 0. We allow that $0 = 1$. In this case, the ring is the zero-ring 0. It has only one element.

12.7 Axiom of choice

Every nonzero ring has a maximal ideal (by Zorn).

12.8 The angel and the devil

Algebra	Geometry
ring A	$\mathrm{Spec}(A)$
ring A, finitely generated over field k	$\mathfrak{m}\,\mathrm{Spec}(A)$
$k[X_1, \ldots, X_n]$	n space
$p \subseteq A$ prime	point $p \in \mathrm{Spec}(A)$
$\mathfrak{m} \subseteq A$ maximal	point $p \in \mathfrak{m}\,\mathrm{Spec}(A)$
$f \in A$	function defined on $\mathfrak{m}\,\mathrm{Spec}(A)$, and on $\mathrm{Spec}(A)$
$f \mod \mathfrak{p}$	value of function at point $[\mathfrak{p}] : f([\mathfrak{p}])$
$f \in \mathfrak{p}$	f vanishes at $\mathfrak{p}$.

12.9 Example on $\mathbb{A}^2_k = (\mathfrak{m})\,\mathrm{Spec}\,k[x, y]$

Recall that $(2, 3)$ the point in Spec is just the ideal $I = (x - 2, y - 3)$. The function $x + y$ on $(2, 3)$. We can check that $x + y \equiv 5 \pmod I$, because the ideal says to rewrite xt to 2 and y to 3.

What about $x + y$ on the prime ideal (0)? It stays as $x + y$, because the ideal (0) asks us to perform no rewrites.

On Spec Z, 60 is a function. It's value at 6 is $60 \mod 7 = 4$. At point 2, it has value 0.

This function vanishes to order 2 at the point 2, a single zero at $3, 5$ and does not vanish at, say, 7.

12.10 $\mathrm{Spec}(A/I) \subseteq \mathrm{Spec}(A)$

Ideals of a quotient A/I are equivalent to ideals of A that contain I. This respects all reasonable things. For example, the correspondence holds on restricting to prime and maximal ideals.

Example: what are the prime ideals of $\mathbb{Z}/(60)$? TODO!

12.11 $\mathrm{Spec}(S^{-1}A) \subseteq \mathrm{Spec}(A)$

For some multiplicative subset S, we have:

$$S^{-1}A \equiv \{a/s : a \in A, s \in S\}$$

we use an equivalence relation: $a_1/s_1 \sim a_2/s_2$ iff there is an $s_3 \in S$ such that $s3(a_1 s_2 - a_2 s_1) = 0$. (What is the s_3 really doing?)

Nothing stops us from inverting zero. But if we invert zero, then everything collapses.

12.11.1 Example: powers of f

If we localize at $S = \{1, f, f^2, \ldots\}$ then we get $S^{-1}A = A[x]/(xf - 1)$. That is, add a new element $x = 1/f$.

12.11.2 The correspondence theorem

Correspondence for localizations says that ideals of I not meeting S are in corresponce with ideal of $S^{-1}A$.

Here, prime ideals remain prime. Maximal ideals need not remain maximal.

12.11.3 Conclusion

$$\operatorname{Spec} S^{-1}A \subset \operatorname{Spec} A\mathfrak{m} \operatorname{Spec} A_f \subset \mathfrak{m} \operatorname{Spec} A$$

where A_f is the localization of the ring at f.

12.12 Exampe: $\mathbb{C}[X,Y]/(y^2 - x^3)$

We will have all the "points" on $y^2 = x^3$. So we will have those things that lie inside the ideal. So for example, we will not have the point corresponding to the entire plane, but we will have the points that are on the curve, and the ideal of the curve itself.

I am confused, I feel that we should have all the points which *contain* $y^2 = x^3$. ideals in the quotient of R/I are in correspondence with ideals in the original that contain I.

Geometry: Stuff that is on the curve $y^2 - x^3$

12.13 Example: $\mathbb{C}[X,Y]_(x,y)$

primes of $\mathbb{C}[x,y]$ contained in (x,y). In this case, we know that we will have the point $(x = 0, y = 0)$. But we will also have all ideals that pass through the origin. So for example, in the quotient ring, we will remember $y^2 - x^3$. We will remember (0). We will not remember $x + y + 1$ since it does not meet the ring (x,y).

Geometry: Stuff that touches (x,y)? Stuff that contains (x,y)? Not sure, need a larger example.

12.14 Functions are not determined by their values!

This has been encountered before with polynomials. Eg. $p(x) = X^2 + X$ over F_2. By values, it's the same as $z(x) = 0$. But as a polynomial, it's different.

In the case of rings, the reason is because of nilpotents. If we have $f(p) = 0$ for all points $p \in \operatorname{Spec}(A)$ is $f = 0$?

No. Because every prime ideal $p \in spec(A)$ contains nilpotents, we can have a non-zero nilpotent f which vanishes at each point p, but is still nonzero.

Example: $A = \operatorname{Spec} C[X]/(x^3)$. Has only one prime ideal (x). It has a function $2x$. $2x \neq 0$ but $2x \in x$

This is the *only way* this problem can come up. We define the nilradical:

nilradical $= \mathfrak{N} = \sqrt{(0)} \equiv \{x \in A : x^n = 0 \text{for some } n \in \mathbb{Z}^+\} \sqrt{I} \equiv \{x \in A : x^n \in I \text{ for some } n \in \mathbb{Z}^+\}$

If $I = \sqrt{I}$ we say that I is a radical ideal here.

12.15 Claim: $\cap_{p \subseteq A, \textbf{prime}} p = \mathfrak{N}$

Geometrically, this is saying that functions that vanish at every point are exactly those that have a power that is zero. devastating proof!

12.15.1 $\sqrt{(0)} \subseteq p$

This is easy. if $x \in \sqrt{(0)}$ then $x^n = 0$. but $0 \in p$, hence $x^n \in \mathfrak{p}$. Quick induction over n gives $x \in p$.

12.15.2 The other direction

Suppose we have $x \in \mathfrak{p}$ for all prime ideals $\mathfrak{p}$. We need to show that it is nilpotent: there exists an $n \in N$ such that $x^n = 0$. How do we find out what power of it is zero?

Consider $A_x \equiv A[T]/(Tx-1)$ [localization at x]. What are the the primes of A_x? They are the primes of A not meeting $\{1, x, x^2, \dots\}$. But by assumption, every prime ideal of A contains x!. This means that A_x contains no prime ideals, no maximal ideals. So A_x must be the zero ring.

This means that $1/1 = 0/1$. So there must be an element in the multiplicative subset $\{1, x, x^2, \dots\}$ such that $x^\alpha(1 \times 1 - 0 \times 1) = 0$ [by cross multiplication, defn of localization]. Hence, we have that there is some power α such that $x^\alpha \cdot 1 = 0$, implies $x^\alpha = 0$.

Note that we need the axiom of choice to argue that if a ring has no prime ideals, then it must be the zero ring.

12.16 If a function f is nozero at all points, then it is a unit

Hint: consider the ideal (f). Show that it is the unit ideal $(f) = A$. **TODO!**

12.17 Practice: the radical of an ideal I is the intersection of all prime ideals containing I

There is a one-line proof: consider A/I.

12.18 Maps of rings give maps of spectra in the opposite direction

Situation: $\phi : B \to A$ is a ring homomorphism.

12.18.1 Primes

We want to induce a map of sets $\operatorname{Spec} A \to \operatorname{Spec} B$ from $\phi : B \to A$.

The prime ideal $p \in \operatorname{Spec} A$ **is** (carries the same data) as a map from A into an integral domain $A/\mathfrak{p}$. Call this map $/\mathfrak{p} : A \to A/\mathfrak{p}$. So we can get a map from B into $A/\mathfrak{p}$ by composition: $/p \circ \phi : B \to A/\mathfrak{p}$. This is an element of $\operatorname{Spec} B$.

We can go from $\operatorname{Spec} A$ to $\operatorname{Spec} B$ by going from $\mathfrak{p}A \circ A/\mathfrak{p}$ to $\mathfrak{p} \circ \phi : B \to A/\mathfrak{p}$.

12.18.2 Maximals

We want to induce a map of sets $\mathfrak{m}\operatorname{Spec} A \to \mathfrak{m}\operatorname{Spec} B$ from $\phi : B \to A$.

If A is finitely generated over a field k, then the maximal ideal $\mathfrak{m} \in \mathfrak{m}\operatorname{Spec}(A)$ corresponds to a map from A into a finite extension of k, $A \to A/\mathfrak{m}$. This uses Nullstellensatz! is hard!

Now given $\phi : B \to A$, we compose.

TODO: I don't understand, why can't we just use that $A \to A/\mathfrak{m}$ is a field?

12.18.3 Functions

Functions pull back reasonably as well.

12.19 Example 1

$A \to A/I$, $A \to S^{-1}A$.

Geometry: send (t) to (t^2, t^3). Algebra, map $\mathbb{C}[x, y]$ to $\mathbb{C}[t]$. $x \mapsto t^2; y \mapsto t^3$ [WTF, it is actually going in the opposite direction?]

12.20 Example 2

Take a geometric map $\mathbb{C}^3 \to \mathbb{C}^4$; $(x, y, z) \to (x^2 + y^3, 3yz, xz, 3y^9)$. The algebra should give us a map $\mathbb{C}[a, b, c, d] \to \mathbb{C}[x, y, z]$. What is the map? $a \mapsto x^2 + y^3$, $b \mapsto 3yz$, $c \mapsto xz$, $d \mapsto 3y^9$.

Why does this work? what does this do?

12.21 Example 3

Take the ring map $\mathbb{C}[a,b,c,d] \to \mathbb{C}[x,y,z]$. $a \mapsto x^2 + y^3$, $b \mapsto 3yz$, $c \mapsto xz$, $d \mapsto 3y^9$. What is the corresponding geometric map?

12.22 Next week: the topology of $\mathfrak{m}\operatorname{Spec}(A)$

We have the set. We need to learn the topology next time! We need the locus where a function vanishes to be closed. This is the definition of Zariski.

Chapter 13

Problem set 5

Chapter 14

AGITTOC, pseudolecture 6

Today we want to understand the space $\operatorname{Spec} A/\mathfrak{m}\operatorname{Spec} A$ as a ringed space: a set with a topology and a sheaf of rings. So far, we have the set. Today, we do the topology, and maybe the sheaf.

14.1 Reminders from last week

14.1.1 Inverse image of a sheaf

It should be simple, but it's strangely complicated. we have a $\pi : (X, U) \to (Y, V)$ and a sheaf $\mathcal{G} : V \to \mathbf{Set}$ on Y. We want to pull back to get a sheaf $\mathcal{F} \equiv \pi^{-1}\mathcal{G}; \mathcal{F} : U \to \mathbf{Set}$ on X.

We have three ways to think about it:

- Adjoint to pushforward: $\operatorname{Hom}(\pi^{-}1G, F) \leftrightarrow \operatorname{Hom}(G, \pi_\star F)$.
- Compatible stalks: $\pi^{-}1\mathcal{G}$ has the same stalks as $\mathcal{G}$.
- Constructive definition: First build the inverse image presheaf, then sheafify. $\pi^{-}1_{pre}\mathcal{G} \equiv \operatorname{colim}_{\pi(U)\subseteq V} G(V)$. $\pi^{-}1\mathcal{G} = (\pi^{-}1_{pre})^{sh}$.

We have two examples:

- The pullback at a single point $(\pi : \star \mapsto y_0)$, that is, the function $\pi : \{\star\} \to Y$ gives us the inverse image sheaf $\mathcal{F} = \pi^{-}1\mathcal{G} \simeq \mathcal{G}_p$: it's isomorphic to the stalk data
- The pullback along an injection of a open set $\pi : U \hookrightarrow Y$ gives us a pullback sheaf which is the same as the restriction of the sheaf: $\mathcal{F} = \pi^{-}1G \simeq G|_U$

14.2 Picturing Rings

If A is finitely generated over field $\urcorner$: imagine $\mathfrak{m}\operatorname{Spec} A$. If A is any old ring, then think of $\operatorname{Spec} A$. Then we define $\mathbb{A}^n_k \equiv \mathfrak{m}\operatorname{Spec}$.

14.3 The grand dictionary

Algebra	Geometry
ring A	$\operatorname{Spec}(A)$
ring A, finitely generated over field k	$\mathfrak{m}\operatorname{Spec}(A)$
$k[X_1, \ldots, X_n]$	n space
$p \subseteq A$ prime	point $p \in \operatorname{Spec}(A)$
$\mathfrak{m} \subseteq A$ maximal	point $p \in \mathfrak{m}\operatorname{Spec}(A)$
$f \in A$	function defined on $\mathfrak{m}\operatorname{Spec}(A)$, and on $\operatorname{Spec}(A)$
$f \mod \mathfrak{p}$	value of function at point $[\mathfrak{p}] : f([\mathfrak{p}])$
$f \in \mathfrak{p}$	f vanishes at $\mathfrak{p}$
f unit ($fg = 1$ for some g)	f vanishes nowhere
f nilpotent ($f^n = 0$ for some $n \in \mathbb{Z}^*$)	f vanishes everywhere
ring map $B \to A$	set map $\operatorname{Spec} A \to \operatorname{Spec} B$
ring map $A \to A/I$	inclusion $\operatorname{Spec} A/I \hookrightarrow \operatorname{Spec} B$
ring map $A \to S^{-}1A$	inclusion $\operatorname{Spec} S^{-}1A \hookrightarrow \operatorname{Spec} A$
ring map $A \to A_f$	inclusion $\mathfrak{m}\operatorname{Spec} A_k \hookrightarrow \mathfrak{m}\operatorname{Spec} A$

As sets, $\operatorname{Spec} A = \operatorname{Spec} A_f \sqcup \operatorname{Spec} A/(f)$ [whether $f \in \mathfrak{p}$ or not]

14.4 New: radicals

$\operatorname{Spec} A/I = \operatorname{Spec} A/\sqrt{I}$ — so nilpotents don't affect Spec as a set.

14.5 Example: picturing $A \equiv \mathbb{C}[x, y, z]/(x^2 + y^2 + z^2 - 1)$

draw a sphere. $\mathfrak{m}\operatorname{Spec}$ corresponds to solving equations.

We have a prime ideal $(x^2 + y^2 + z^2 - 1)$ which is also on the sphere. It's everywhere.

Another prime ideal is $(z, x^2 + y^2 - 1)$. Why is this prime? because the quotient $A/(z, x^2 + y^2 - 1)$ will be $\mathbb{C}[x, y]/(x^2 + y^2 - 1)$. This corresponds to the circle $z = 0, x^2 + y^2 - 1 = 0$.

Also note that the points in Spec is the exact same as $(z^4, (x^2 + y^2 - 1)^5)$, because solving equations don't care whether we are solving $z = 0$ or $z^4 = 0$ (because $\mathbb{C}$ is a field...)

What about $(z - 2)$? There are *complex* solutions to the sphere equation. eg $(x = 0, y = i, z = 2)$ so we do have a generic point for $z = 2$.

14.6 We want a topology on $\operatorname{Spec} A$

The locus where a function vanishes should be closed. The locus where a function does not vanish should be open.

For $f \in A$, define $D(f) \subset \operatorname{Spec} A$ [D for doesn't vanish] be the locus of f where it does not vanish:

$$D(f) \equiv \{[p] \in \operatorname{Spec} A | f \notin \mathfrak{p}\}$$

We declare these to be open, and these are our distinguished open sets. Their complement must be closed. The intersection of any number of closed sets is closed. So the vanishing set of a *collection* of functions is closed. We define the vanishing set of set of function $T \subseteq A$ as $V(T)$:

$$\begin{aligned} V(T) &\equiv \{\mathfrak{p} \in \operatorname{Spec}(A) : f(\mathfrak{p}) = 0 \text{ for all } f \in T\} \\ &= \cap_{f \in T} V(f) \end{aligned}$$

which is the same as asking for prime ideal $p \in \operatorname{Spec}(A)$ which contains every function $f \in T$. So $V(T) = \{\mathfrak{p} \in \operatorname{Spec}(A) : T \subseteq \mathfrak{p}\}$.

14.7 Check that this is a topology

$V(I) \cup V(J) = V(I \cap J)$ or $V(I) \cup V(J) = V(IJ)$? which one is it?

where $IJ \equiv \{\sum fg : f \in I, g \in J\}$. That is, we need to generate the ideal from the elementwise products.

14.8 Distinguished open sets form a base for Zariski

Consider $\mathbb{A}^2_{\mathbb{C}} = \operatorname{Spec} \mathbb{C}[x, y]$ and find how to cut out the points $(0, 0)$ and the line $x = 1$. The equations cutting out the union is $(x(x-1), y(x-1))$. We need to show that the complement is a union of distinguished open sets. The complement of it is $D(x(x-1)) \cup D(y(x-1))$.

Our distinguished open sets are awesome, since they obey really nice closure properties:

- $D(f) \cap D(g) = D(fg)$
- $(f) = \operatorname{Spec} A_f$ as a *set*

14.9 Any open cover of $\operatorname{Spec} A$ has a finite subcover. So $\operatorname{Spec} A$ is quasicompact

Devious proof:

We assume that Spec A is a union of open sets $U[i]$. Each of these open sets is a union of distinguished open sets. $U[i] = \cup_j D(f[i][j])$ for some functions $f[i][j]$. So Spec A is the union of $\cup_{i,j} D(f[i][j])$. We'll show that these distinguished open subsets form a finite subcover.

If we have that $\cup_{j,i} D(f[i][j]) = \operatorname{Spec} A$, then the locus where $f[i][j]$ all vanish is the empty set. So we have that:

$$V(\{f[i][j]\}) = \emptyset$$
$$V((\{f[i][j]\})) = \emptyset$$
$$(\{f_[i][j]\}) = A$$

$1 = \sum_{i,j} a[i][j]f[i][j]$for a finite number of i by defn of being an ideal

$$1 = \sum_{k} a_k f_k \text{total number of } k \text{ is finite}$$
$$1 = (f[k])\text{total number of } k \text{ is finite}$$

Hence Spec A is covered by $D(f[k])$.

14.10 Continuing the analogy

- a subset $T \subseteq A$ gives a closed subset $V(T)$
- the ideal $I = (T)$ gives the same closed subset $V(I) = V(T)$
- the ideal $\sqrt{I}$ gives the same closed subset $V(\sqrt{I}) = V(T)$

There's a reverse bijection, which takes subsets of the topology and returns radical ideals. $I(S)$ gives the ideal of functions vanishing at the points of S. This by definition will be $I(S) \equiv \cap_{[\mathfrak{p}]\in S}\mathfrak{p}$.

14.11 Formal claim of inclusion reversing bijections

$$\{\text{radical ideals of } A\} \leftrightarrow \{\text{closed subsets of Spec}(A)\}$$
$$J \to V(J)$$
$$I(S) \leftarrow S$$

We divide the proof into two parts.

Theorem 26. First part: going from ideal to variety and back again: $I(V(J)) = \sqrt{J}$ for *any* ideal J.

Proof.
$$J \mapsto V(J) \mapsto I(V(J)) = \cap_{J\subseteq\mathfrak{p}}\mathfrak{p} = \sqrt{J}$$

Recollect proof that the radical of an ideal J is the intersection of all prime ideals $\mathfrak{p}$ containing J. This is the generalization of the fact that the nilradical is the intersection of all prime ideals. □

Theorem 27. Second part: going from a variety to an ideal and back again: $V(I(S)) = \overline{S}$

Proof. **part 1: $\overline{S} \subseteq V(I(S))$:** For sure V will be a closed subset by definition of Zariski and V as a function. Given a point $\mathfrak{p} \in S \subseteq \text{Spec}(A)$, $I(S)$ will give us all functions that vanish on $\mathfrak{p}$. Then $V(I(S))$ asks "at what points do these" functions vanish? Well, by definition, they vanish on $\mathfrak{p}$. Maybe they vanish on more points. So we must have that $V(I(S))$ contains S. Since V is closed and already contains S, it contains the closure of S: $\overline{(S)} \subseteq V(I(S))$.

part 1: $V(I(S)) \subseteq \overline{S}$: We will show that $\overline{S}^{\complement} \subseteq V(I(S))^{\complement}$.

Let us take $\mathfrak{p} \in \overline{S}^{\complement}$, then there is a closed subset $V(J)$ in $\text{Spec}\, A$ which contains S, but does not contain $\mathfrak{p}$. This is because the closure is the intersection of all closed subsets.

So we have:

- $\overline{S} = V(J)$ since every closed set is the zero set of some ideal.
- $\mathfrak{p} \in \overline{S}^{\complement}$ We will show that this $\mathfrak{p}$ is in $V(I(S))^{\complement}$.
- $[\mathfrak{p}] \notin V(J)$.
- $J \subsetneq \mathfrak{p}$. J does not vanish on $\mathfrak{p}$. So $J \xrightarrow{\mathfrak{p}} \neq 0$. So J is not a subset of $\mathfrak{p}$.
- Since $V(I) = S \subseteq \overline{S} = V(J)$, we have that $J \subseteq I$.
- Since $J \subsetneq \mathfrak{p}$ and $J \subseteq I$, this means that $I \subsetneq \mathfrak{p}$. J itself had elements that $\mathfrak{p}$ did not have. I has all of J's elements, and more. So $\mathfrak{p}$ definitely does not contain I.
- Hence, $\mathfrak{p} \in V(I(S))^{\complement}$. TODO: continue with this proof.

□

14.12 Topological notions: Finitely many pieces

Empirical fact: If we have a bunch of equations in a bunch of variables, we will always have finitely many pieces. This only seems to happen with polynomial equations. $\sin(x) = 0$ has infinitely many pieces, to show what happens in the non-polynomial world.

14.12.1 Definition: Irreducible

A topological space is *irreducible* if for all Z_1, Z_2 closed, we have $X = Z_1 \cup Z_2$ then $X = Z_1 \vee X = Z_2$. **TODO: interpret irreducible in terms of continuous map**

14.12.2 Definition: Irreducible component

the maximal irreducible subsets are called as irreducible components. that is, "the pieces".

14.12.3 Connected/Disconnected

A space is disconnected if we can write it as the union of two disjoint open subsets. A space that is not disconnected is connected.

14.13 Why do zariski closed subsets of $\operatorname{Spec} \mathbb{C}[x_1, \ldots, x_n]$ have finitely many irreducible components?

Definition 28. Noetherian topological space: X satisfies the descending chain condition for closed subsets: $Z_1 \supset Z_2 \supset Z_3 \ldots$ [ie, $\cdots \subseteq Z_3 \subseteq Z_2 \subseteq Z_1$]then there exists an n such that $Z_n = Z_{n+1} = Z_{n+2} = \ldots$. The sequence stabilizes. This is the same as having an ascending chain condition for open subsets.

Theorem 29. Any Noetherian topological space has finitely many pieces

Proof. If it's irreducible, we win. If it's reducible, then it's the union of two closed subsets. Recurse. on the two closed subsets. It should eventually become irreducible because of the descending chain condition. □

Definition 30. Noetherian ring: Ideals satisfy ascending chain condition

Theorem 31. $\operatorname{Spec} A$ is a Noetherian topological space, if A is a Noetherian ring.

Proof. If we have a descending chain of subsets $\ldots Z_3 \subseteq Z_2 \subseteq Z_1$, then set $I_j = V(Z_j)$. This gives us an ascending chain of ideals since V is order reversing. So we have $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$. Since A is Noetherian, eventually the ideals stabilize: $I_n = I_{n+1} = \ldots$. Hence the zero sets stabilize at $Z_n = Z_{n+1} = \ldots$. □

14.14 Noetherian rings

This is an example of a condition which is a priori unimportant, but is actually super duper important.

- Fields are noetherian since they have only two ideals
- Integers are noetherian because of being a PID and having the euclidian algorithm: $(a_1) \subseteq (a_2)$ implies $a_2 | a_1$, hence $a_2 \leq a_1$. We can always take the generators to live in $\mathbb{N}$. This gives us a sequence of numbers $0 \leq \cdots \leq a_3 \leq a_2 \leq a_1$ which must eventually stabilize because it's well founded / has a minimal element.

- If A is Noetherian, then A/I and $S^{-}1A$ are Noetherian, because the ideals of these procedures are a subset of the ideals of A.
- Not quite immediate: Noetherian is the same as every ideal A is finitely generated. Start with an ideal I we wish to finitely generate. The idea is that we can keep building ideals as $(f_1) \subsetneq (f_1, f_2) \subsetneq (f_1, f_2, f_3) \dots$ by repeatedly taking elements $f_1 \in I$, $f_2 \in I - (f_1)$, $f_3 \in I - (f_1, f_2), \dots$. Such a chain must eventually stabilize since the ring A is Noetherian. This will give us $I = (f_1, f_2, \dots)$.
- Clever: **Hilbert basis theorem** — $A[x]$ is Noetherian if A is Noetherian.

14.15 Last few things about topology

In Spec(A), not every point is closed. For example, the generic point is not a closed subset. The closed points of Spec A, ie, points such that $\overline{\mathfrak{p}} = \mathfrak{p}$ correspond to maximal ideals of A. So all the points of $\mathfrak{m}\operatorname{Spec} A$ are closed.

We have a bijection between points of Spec(A) and irreducible closed subsets of Spec(A) by taking $\mathfrak{p} \to \overline{\mathfrak{p}}$. The point that corresponds to the irreducible closed subset is called the **generic point** of that subset.

14.16 What is the sheaf of rings on $\operatorname{Spec}(A)$

Let's start with $\mathbb{A}^1_{\mathbb{C}} \equiv \mathfrak{m}\operatorname{Spec}\mathbb{C}[X]$. We have $\mathbb{C}[X]$ are the functions. On the points $\mathbb{A}^1_{\mathbb{C}} - \{1\} \simeq \mathbb{A}^1_{\mathbb{C}} - [(x-1)]$, the function $3x/(x-1)$ should be an algebraic function. Similarly, on $\mathbb{A}^1_{\mathbb{C}} - \{1, 2, 3\}$ The function $x^1 2/(x-2)(x-3)$ should be an algebraic function.

So, we ought to allow some poles. That is, we ought to allow localizations.

14.16.1 Thought experiment

If we have $\mathbb{A}^2_{\mathbb{C}}$ $(0, 0)$, what should the functions be? is $1/(x^2 + y^2)$ an algebraic function? [hint, maybe not, because $x = i, y = 1$ is a pole.]

Name-drop: Hartog's lemma

14.17 The idea of the ring data(that does not work)

We want $\mathcal{O}(\operatorname{Spec}(A)) = A$, and $\mathcal{O}((f)) = A_f$. Why is this well-defined? because we can have $D(f) = D(g)$ so we need to check that uniqueness works. We also need to check that this is a sheaf

Definition 32. define $\mathcal{O}(D(f))$ to the localization of A at the multiplicative subset of all functions which vanish nowhere over $D(f)$. That is, we are allowed

to divide by elements as long as they vanish on a subset of $V(f)$: They vanish "less than" f itself.

For example, at $\mathcal{O}(xy)$, we can divide by x^7, but not by things like $x+y$. This depends on $D(f)$ and not f itself!

TODO: Show that $\mathcal{O}(D(f)) = A_f$.

14.18 Next week

We will show that it's a sheaf, by showing identity and gluing. We will also use quasicoherent sheafs. Then we will do many many examples. After that, we can do a wide variety of things.

14.19 Questions

14.19.1 Question: $I \cap J$ v/s IJ

We have that $V(I \cap J) = V(IJ)$, but $I \cap J$ need not be equal to IJ.

$$(I \cap J)^2 \subseteq IJ \subseteq I \cap J$$

We have not talked about how to visualize not just the set, but also the nilpotents. The nilpotent picture is supposedly "right" at $I \cap J$, and not at IJ.

Pick $I = J = (x)$. If we then consider $V(IJ) = V((x^2))$. On the other hand, we have $V(I \cap J) = V(x)$. So the nilpotents comes into play here.

Note that $[\mathfrak{p}] \in V(I)$ is asking $I \subseteq \mathfrak{p}$. So if we consider the circle x^2+y^2-5, us asking if it has the generic zero point, $(0) \in V(x^2+y^2-5)$ is the same as asking $(x^2+y^2-5) \subseteq (0)$? the answer is **NO!**. So the generic point (0) does not lie on the circle. The only points the circle contains is all the "usual points", plus the "bonus point" (x^2+y^2-5). No other points.

Also, if we have the equation $xy = 0$, then we have two generic points, corresponding to the irreducible subsets $x = 0$, $y = 0$.

Algebra	Geometry
Minimal prime ideals [generic point?]	Irreducible components (maximal closed subsets)
prime ideals	Irreducible closed subsets
maximal ideals	closed points (minimal closed subsets)

14.19.2 Question: radical ideal, eludicate

$\sqrt{I} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p}$: The intersection of all prime ideals that contain it

14.19.3 Observation: The sphere intersect with the cylinder

If we take $x^2+y^2+z^2-1=0$, and then cylinder $x^2+y^2-1=0$ and quotient out the circle by the cylinder, we are left with $z^2 = 0$. This is telling us that the sphere is tangent to the cylinder at the equator by virtue of the nilpotent z^2.

When we intersect the sphere and cylinder as a scheme, we need to consider $\mathbb{C}[x,y,z]/(x^2+y^2+z^2-1, x^2+y^2-1)$. We have that $z \neq 0$, $z^2 = 0$ in this, which tells us that sphere and cylinder are tangent.

14.19.4 How do draw $\mathbb{C}[x,y,z]/(x^2+y^2+z^2)$?

Draw 3-space with a single point $(0,0,0)$. But we've lost all the interesting complex points, and are thus sad. What we can do is to replace $z = iw$. This makes the equation $\mathbb{C}[x,y,w]/(x^2+y^2-w^2)$. This gives us a cone. This cone has a bunch of lines on it through the origin. This tells us something about complex lines. [brilliant!]

This surface is 2D, it's not smooth at the origin, but is smooth everywhere else.

14.19.5 Why is the affine line called the affine line and not the affine plane?

The complex numbers look as 2D reals. But we are thinking about complex numbers in terms of complex numbers, so it stays as $1D$.

14.19.6 What makes a picture good? how do we know what to draw?

A picture is good if it tells us something we didn't immediately know. How to draw a good picture: it's art. The best way to learn how to draw pictures is to see lots of examples.

14.19.7 What is so generic about a generic point?

Let us live on $\mathbb{C}[a,b,c,d,e,f]$ [space of all plane conics]. $ax^2+bxy+cy^2+dx+cy+f=0$. Most of the conics are irreducible. Any time we say "most of", it will be true of the generic point.

14.19.8 How to draw specialization?

Take a surface. We have a generic point of the surface s. Now take a curve on the surface. The curve has a generic point c. Now take a point on the curve p. We can specialize $s \to c \to p$. Generalization would just go the other way

14.19.9 Proper maps

Image of closed set is closed set.

14.19.10 Define Haussdorf in terms of maps: Separated

What is a Haussdorf map of topological spaces? This leads to the notion of *separated*.

14.19.11 Hilbert basis theorem and Chomp

Chomp

We have cookies on the table in a rectangular grid. The bottom left cookie is poisoned, so we don't want to eat the cookie. When it is your turn, your pick a cookie, and eat everything that is north or east (or both) of it. At some point, someone eats a poisoned cookie and dies. To die is to lose the game.

The hilbert basis theorem tells us that the first person has a winning strategy.

Let us eat the top right most cookie. If from here on out, we have a winning strategy, we are done and we win.

Let us say it's not a winning strategy, and we would lose if we did this. Then the other player would play some devastating move to make us lose. In which case, I can simply play the other players' move.

TODO: Why doesn't this work for all games?

infinitely many cookies

We have infinitely many cookies: all the cookies in the first quadrant at integer points. Now we play the same game.

The problem is:

> Why is someone still forced to eat the poisoned cookie, even if you and your friend are cooperating?

The relation to noetherian

If we are on $\mathbb{C}[x, y]$, to every point $\vec{p} = (p_x, p_y)$ we can associate a monominal $x_x^p y_y^p$.

We start with the zero ideal (0). We then pick a monomial, say x^2y^3. So everything that is "north east of this point", ie, is of the form $x^{(2+\delta_x)}y^{(3+\delta_y)}$ is eaten. This represents the ideal $I = (0, x^2y^3)$.

So maybe the next cookie that is eaten is at $\vec{p} = (9, 0)$. Now the ideal becomes $I = (0, x^2y^3, x^9)$. If we could play the game forever, we would then have an infinite increasing sequence of ideals.

But we know that $\mathbb{C}[x, y]$ ought not have such a thing, because the ring is Noetherian.

Very high brow, we are using something called as "groebner degeneration" which allows us to reduce the more complicated case of non-monomial ideals into monomial ideals.

14.19.12 Why does defining $\mathcal{O}(U)$ fail?

We have Spec(A). We are going to try to define functions on $\mathcal{O}(U)$ for the sheaf. This definition **does not work**. We need to understand why.

Take the open set U. We want $\mathcal{O}(U) = A_S$ where S is the set of functions which do not vanish over U. We are assuming something about stuff being an integral domain for this to work, but let's say this work.

This definition does work for distinguished open sets $\mathcal{O}(D(f))$. Why does this not work for general open sets?

14.19.13 Draw $\mathbb{C}[x]/(x^2)$ and $\mathbb{C}[x]/(x^3)$ in a way that is distinguishable

14.19.14 Minimal prime

maximal irreducible closed subsets? The fuzz doesn't change the topology.

14.19.15 drawing things over a non algebraically closed field

We view points on $\mathbb{C}$ as "containing topology" which can be broken up like a hadron to recover quarks over $\mathbb{R}$.

$\operatorname{Spec}\mathbb{Z}$ is a curve. There are points on on $\operatorname{Spec}\mathbb{Z}$ which contain topology.