Chapter 1

Gaussian integers

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 $z = \pm p_1 p_2 \ldots p_n$.

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:

$$\begin{aligned}&\delta(Ar) = \delta(A)(r_0^2 + s_0^2) \leq \left[\delta(A)(1/2^2 + 1/2^2) = \delta(A)(1/4 + 1/4) = \delta(A)/2\right]\\ &\delta(Ar) \leq \delta(A)/2\end{aligned}$$

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. $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

1.4 Ideal of $\mathbb{Z}[i]$

Theorem 5. 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 6. 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.

1.5 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 7. (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:

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

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 $\mathbb{Z}[i]$.

1.6 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 8. 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 9. 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 10. 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.

1.7 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 11. 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 12. *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 13. 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 2

Atiyah MacDonald, Ch1 exercises

2.1 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 $2x = 0$.

2.2 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:

2.2.1 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 $E \xrightarrow{frakp_x} \cdot$ 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.

2.2.2 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 $radical(\mathfrak{a}) \xrightarrow{\mathfrak{p}} 0$.

2.3 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.

2.3.1 $X_f \cap X_g = X_{fg}$

$X_f \cap X_g$ 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.

2.3.2 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.

2.3.3 $X_f = \emptyset \iff f$is nilpotent

($\impliedby$): 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 $\cup Prime^{\mathsf{C}}$. We claim that no nilpotent element belongs to $\cup Prime^{\mathsf{C}}$. Assume it does. Then this nilpotent element n is in the complement of some prime ideal $\mathfrak{p}^{\mathsf{C}}$.

[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

2.3.4 $X_f = X \iff f$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 $\mathfrak{p} \in X$, $f \not\in \mathfrak{p}$. 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 $f \not\in \mathfrak{p}$.

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

2.3.5 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.

2.3.6 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

2.4 Q18

2.4.1 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 $F(\text{all other prime ideals}) \neq 0$. 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 $\{x\}$.

2.4.2 $\overline{\{x\}} = V(\mathfrak{p}_x)$

(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.

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

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

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