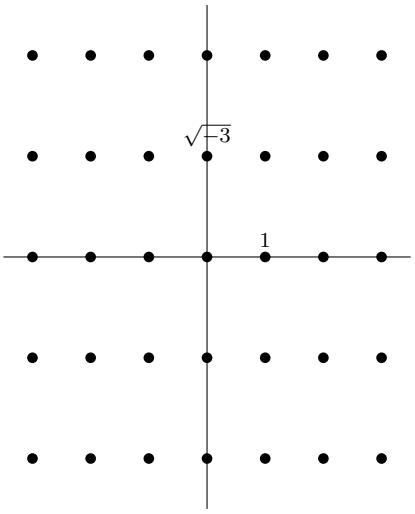
Solutions to Homework 1

1. (a) Let $R = \mathbb{Z}[\sqrt{-3}]$. Sketch the lattice in the complex plane.
Solution:



(b) Prove that R is not integrally closed.
Hint: Think about the minimal polynomial of

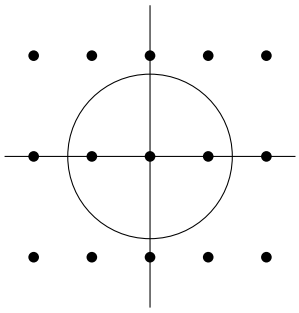
$$\omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}.$$

Solution: The roots of $x^2 + x + 1 = 0$ are ω and $\bar{\omega} = \omega^2$, so we have a monic polynomial with coefficients in R that has a root in $\mathrm{frac}(R)$ but not in R.

(c) Prove that 2 is irreducible in R by reasoning about norms, where $N(a + b\sqrt{-3}) = a^2 + 3b^2$. But prove that 2 is not prime by showing that the quotient ring $R/(2)$ is not an integral domain.

Solution: For any $\alpha \in R$ we have $N(\alpha) = \alpha \cdot \bar{\alpha}$, where $\bar{\alpha}$ is the complex conjugate, so $N(\alpha \cdot \beta) = N(\alpha)N(\beta)$. Moreover, we have $N(\alpha) = 1$ if and only if α is a unit: if $N(\alpha) = 1$ then $\bar{\alpha}$ is the inverse of α, while if α is a unit then $N(\alpha) \cdot N(\alpha^{-1}) = N(\alpha \cdot \alpha^{-1}) = N(1) = 1$, so $N(\alpha)$ is a positive integer that divides 1, so it must equal 1.

Now $N(2) = 4$, so if 2 factors as $\alpha \cdot \beta$ and neither is a unit, then we must have $N(\alpha) = N(\beta) = 2$. But looking at the lattice, we see that the circle of radius $\sqrt{2}$ does not contain any lattice points.



On the other hand, we have $R \cong \mathbb{Z}[x]/(x^2 + 3)$, so

$$\begin{aligned} R/(2) &\cong \mathbb{Z}[x]/(x^2 + 3, 2) \\ &\cong \mathbb{F}_2[x]/(x^2 + 3) \\ &\cong \mathbb{F}_2[x]/(x + 1)^2. \end{aligned}$$

This is not an integral domain because $x + 1$ is a zero-divisor, so (2) is not a prime ideal.

(d) Same for $1 + \sqrt{-3}$.

Solution: We have $N(1 + \sqrt{-3}) = 4$, so the argument that it is irreducible is the same as for 2.

The quotient ring $R/(1 + \sqrt{-3})$ is isomorphic to

$$\mathbb{Z}[x]/(x^2 + 3, x + 1),$$

which is isomorphic to $\mathbb{Z}/4$ by setting $x = -1$. This is not an integral domain because 2 is a zero-divisor, so $(1 + \sqrt{-3})$ is not a prime ideal.

(e) Prove that the ideal $\mathfrak{m} = (2, 1 + \sqrt{-3})$ is maximal by showing that the quotient ring $R/\mathfrak{m}$ is a field. Prove that $\mathfrak{m}$ is the only prime ideal that contains 2 by reasoning about quotient rings. Same for $1 + \sqrt{-3}$.

Solution: The quotient ring $R/\mathfrak{m}$ is isomorphic to

$$\mathbb{Z}[x]/(x^2 + 3, 2, x + 1) \cong \mathbb{Z}/(4, 2) = \mathbb{F}_2,$$

which is a field.

The maximal ideals of R that contain 2 are in bijection with the maximal ideals of $R/(2) \cong \mathbb{F}_2[x]/(x + 1)^2$, but there is only one of those, namely $(x + 1)$.

The maximal ideals of $\mathbb{R}$ that contain $1 + \sqrt{-3}$ are in bijection with the maximal ideals of $R/(1 + \sqrt{-3}) \cong \mathbb{Z}/4$, but there is only one of those, namely (2).

(f) Prove that $\mathfrak{m}^2 = 2\mathfrak{m}$. Find the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over $R/\mathfrak{m}$. Prove that the principal ideals (2) and $(1+\sqrt{-3})$ are not powers of $\mathfrak{m}$, so they do not factor as products of primes.

Solution: We have

$$\mathfrak{m}^2 = (4, 2 + 2\sqrt{-3}, -2 + 2\sqrt{-3}) = (4, 2 + 2\sqrt{-3}) = 2\mathfrak{m}.$$

Knowing that $\mathfrak{m}/\mathfrak{m}^2$ is a vector space over $R/\mathfrak{m} \cong \mathbb{F}_2$, we can find its dimension by finding its cardinality. Since $\mathfrak{m}$ is isomorphic to $\mathbb{Z}^2$ as an Abelian group, $\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{m}/2\mathfrak{m}$ is isomorpic to $(\mathbb{Z}^2)/(2\mathbb{Z}^2) = \mathbb{F}_2^2$. Thus the dimension is 2.

If (2) factored as a product of primes, then each one would contain 2, so each one would equal $\mathfrak{m}$. But (2) is not equal to $\mathfrak{m}$, or to $\mathfrak{m}^2 = 2\mathfrak{m}$, or to $\mathfrak{m}^3 = 4\mathfrak{m}$, or any higher power of $\mathfrak{m}$: we see that (2) is a subgroup of index 4 in R, while $\mathfrak{m}$ is a subgroup of index 2, $\mathfrak{m}^2 = 2\mathfrak{m}$ is a subgroup of index 8, $\mathfrak{m}^3 = 4\mathfrak{m}$ is a subgroup of index 32, and so on.

The argument for $(1 + \sqrt{-3})$ is the same.

(g) Let $S = \mathbb{Z}[\omega]$. Use the fact that S is a principal ideal domain, and in fact a Euclidean domain (you may use this without proof), to prove that the Krull dimension of R is 1.

Hint: Say "integral extension" and quote your favorite algebra book.

(In the coordinate ring of an affine variety, $\mathfrak{m}/\mathfrak{m}^2$ was the Zariski cotangent space of the variety of the corresponding point. Because this $\mathfrak{m}/\mathfrak{m}^2$ is too big, we want to say that it's like a singular point.)

Solution: We see that S is an integral extension of R, because it was obtained by adjoining a root of x^2+x+1. My favorite algebra book is Dummit and Foote, where exercise 17 from §15.3 states that if S is integral over R then their Krull dimensions agree; but you will probably find a different reference. The Krull dimension of S is 1 because it is a principal ideal domain, or because it is an integral extension of $\mathbb{Z}$.

(h) Let $\mathfrak{n} = \mathfrak{m}S$. Prove that $\mathfrak{n}$ is a principal ideal. Is it still prime? Describe the quotient ring $S/\mathfrak{n}$, which should contain $R/\mathfrak{m}$.

Solution: We have $\mathfrak{m}S = (2, 2\omega) = (2)$. To see that this is prime, write

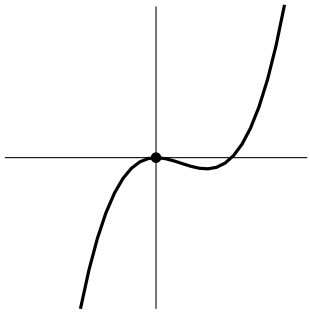
$$S/\mathfrak{n} = S/(2) \cong \mathbb{Z}[x]/(x^2 + x + 1, 2) \cong \mathbb{F}_2[x]/(x^2 + x + 1) \cong \mathbb{F}_4.$$

(i) Find the dimension of $\mathfrak{n}/\mathfrak{n}^2$ as a vector space over $S/\mathfrak{n}$.

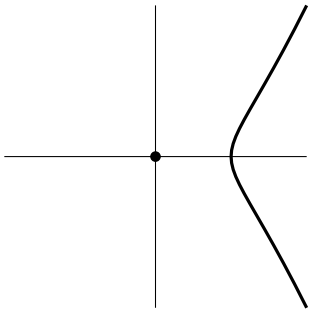
Solution: Again we can find the dimension of $\mathfrak{n}/\mathfrak{n}^2$ by finding its cardinality. We have $\mathfrak{n} = (2)$, so $\mathfrak{n}^2 = 2\mathfrak{n}$ as before, so $\mathfrak{n}/\mathfrak{n}^2$ again has four elements; but since $S/\mathfrak{n} = \mathbb{F}_4$, this now says that $\mathfrak{n}/\mathfrak{n}^2$ is 1-dimensional over $S/\mathfrak{n}$.

2. (a) Let $R = \mathbb{R}[x, y]/(y^2 + x^2 - x^3)$. Sketch the curve in $\mathbb{R}^2$.

Solution: If you first sketch $y = x^3 - x^2$



Then you see that $y = \pm\sqrt{x^3 - x^2}$ looks like this:



(b) Prove that R is not integrally closed.
Hint: Let $z = y/x$ in $\mathrm{frac}(R)$, and prove that $z^2 \in R$.
Solution: If $z = y/x$ then

$$z^2 = \frac{y^2}{x^2} = \frac{x^3 - x^2}{x^2} = x - 1.$$

Thus $z^2 - (x - 1)$ is a monic polynomial with coefficients in R that has a root in $\mathrm{frac}(R)$ but not in R.

(c) Prove that x is irreducible in R by reasoning about degrees. But prove that x is not prime by showing that the quotient ring $R/(x)$ is not an integral.
Solution: As I suggested by email, it's painful to reason about degrees, and better is to consider a norm map from R to $\mathbb{R}[x]$ given by

$$N(f(x,y)) = f(x,y)f(x,-y)$$

or

$$N(g(x) + yh(x)) = g(x)^2 + (x^2 - x^3)h(x)^2.$$

From the first description we see that N is multiplicative, and thus that $f(x,y)$ is a unit in R if and only if $N(f)$ is a unit in $\mathbb{R}[x]$, that is, a constant. Now $N(x) = x^2$, so if x factors as a product of two non-units f_1 and f_2 then $N(f_1) = cx$ and $N(f_2) = c^{-1}x$ for some $c \in \mathbb{R} \setminus 0$. But from the second description of N we see that this is impossible: if $g^2 + (x^2 - x^3)h^2 = x$ then x divides g^2, so x divides g, which gives a contradiction.

We have $R/(x) = \mathbb{R}[x,y]/(y^2 + x^2 - x^3, x) \cong \mathbb{R}[y]/(y^2)$, which is not an integral domain because y is a zero-divisor.

(d) Same for y.

Solution: We have $N(y) = x^2 - x^3 = x^2(1-x)$, so if y factors as a product of two non-units f_1 and f_2 then up to scalars we either have $N(f_1) = x$ and $N(f_2) = x - x^2$, or $N(f_1) = x^2$ and $N(f_2) = 1 - x$. We have already seen that $N(f_1) = x$ is impossible, and by a similar argument we see that $N(f_2) = 1 - x$ is impossible.

We have $R/(y) = \mathbb{R}[x,y]/(y^2 + x^2 - x^3, y) \cong \mathbb{R}[x]/(x^2 - x^3)$, which is not an integral domain because x is a zero-divisor.

(e) Prove that the ideal $\mathfrak{m} = (x, y)$ is maximal by showing that the quotient ring $R/\mathfrak{m}$ is a field. Prove that $\mathfrak{m}$ is the only prime ideal that contains x by reasoning about quotient rings. (But don't bother with y: it is contained in another maximal ideal, as you can see from the picture.)

Solution: We have

$$R/\mathfrak{m} = \mathbb{R}[x,y]/(y^2 + x^2 - x^3, x, y) = \mathbb{R}[x,y]/(x,y) \cong \mathbb{R},$$

which is a field. The maximal ideals of $\mathbb{R}$ that contain x are in bijection with the maximal ideals of $R/(x) \cong \mathbb{R}[y]/(y^2)$, but there is only one of those, namley (y).

(f) Find the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over $R/\mathfrak{m}$. Prove that the principal ideal (x) is not a power of $\mathfrak{m}$, so it does not factor as a product of primes.

Solution: I claim that $\mathfrak{m}/\mathfrak{m}^2$ is 2-dimensional. To see this clearly, note that every element of R can be written uniquely as $g(x) + yg(x)$, so a basis for $\mathfrak{m}$ as an $\mathbb{R}$-vector space is given by $x, y, x^2, xy, x^3, x^2y, x^4, x^3y, \ldots$, while a basis for

$$m^2 = (x^2, xy, y^2) = (x^2, xy, -x^2 + x^3) = (x^2, xy)$$

is given by $x^2, xy, x^3, x^2y, x^4, x^3y, \ldots$. Thus a basis for $\mathfrak{m}/\mathfrak{m}^2$ is given by x and y.

To see that (x) is not a power of $\mathfrak{m}$, note that the dimension of $R/(x)$ as an $\mathbb{R}$-vector space is 2, while thinking about the bases above we find that the dimension of $R/\mathfrak{m}^k$ is $2k - 1$.

(g) Let $S = \mathbb{R}[z]$. Describe the normalization map $\varphi\colon R \to S$ that sends y/x to z: where does it send x and y? Prove that the Krull dimension of R is 1.

Solution: If $z = y/x$ then $z^2 = y^2/x^2 = x - 1$, so φ should send x to z^2+1. Then it should send $y = x \cdot y/x$ to $(z^2+1)\cdot z = z^3+z$. Now S is an integral extension of R, obtained by adjoining a root of the monic polynomial $z^2-(x-1)$, so they have the same Krull dimension. And the Krull dimension of $\mathbb{R}[z]$ is 1 because it's a principal ideal domain.

(h) Let $\mathfrak{n} = \varphi(\mathfrak{m})S$. Prove that $\mathfrak{n}$ is a principal ideal. Is it still prime? Describe the quotient ring $S/\mathfrak{n}$, which should contain $R/\mathfrak{m}$.

Solution: We have $\mathfrak{n} = (z^2+1, z^3+z) = (z^2+1)$, which is prime because $S/\mathfrak{n} \cong \mathbb{C}$ is a field.

(i) Find the dimension of $\mathfrak{n}/\mathfrak{n}^2$ as a vector space over $S/\mathfrak{n}$.

Solution: We can find the dimension of $\mathfrak{n}/\mathfrak{n}^2$ over $S/\mathfrak{n} \cong \mathbb{C}$ by finding its dimension as a real vector space and dividing by 2. By the third isomorphism theorem,

$$\frac{S/\mathfrak{n}^2}{\mathfrak{n}/\mathfrak{n}^2} \cong S/\mathfrak{n}.$$

Now $S/\mathfrak{n} = \mathbb{R}[z]/(z^2+1)$ is 2-dimensional, with a basis given by 1 and z; and $S/\mathfrak{n}^2 = \mathbb{R}[z]/(z^4+2z^2+1)$ is 4-dimensional, with a basis given by 1, z, z^2, and z^3; so $\mathfrak{n}/\mathfrak{n}^2$ is 2-dimensional as a real vector space, hence 1-dimensional as a complex vector space.

3. Optional: I might have preferred to work with $\mathbb{R}[x,y]/(y^2-x^2-x^3)$ because the picture is prettier, but then the ideal $\mathfrak{m} = (x,y)$ splits in the normalization rather than being inert, so the analogy with $\mathbb{Z}[\sqrt{-3}]$ is not as good...

Can you find a square-free integer D with $D \equiv 1 \pmod 4$ such that the maximal ideal $\mathfrak{m} = (2, 1+\sqrt{D})$ in $R = \mathbb{Z}[\sqrt{D}]$ splits when you extend to $S = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$?

Solution: It works with $D = -7$. Then $\mathfrak{m}$ is prime in R, because $R/\mathfrak{m} \cong \mathbb{F}_2$ as before. But in S, if we let

$$\alpha = \frac{1+\sqrt{-7}}{2}$$

then we find that $\alpha^2 - \alpha + 2 = 0$, so $2 = \alpha(1-\alpha)$, and we can check that $S/\alpha \cong S/(1-\alpha) \cong \mathbb{F}_2$ and $(\alpha, 1-\alpha) = 1$.