Homework 6
Algebra

Joshua Ruiter

April 10, 2018

Proposition 0.1 (Exercise 1, Image of ψ_S)**.** *Let A be a commutative ring and S a multiplicative subset. Let $J(A)$ denote the set of ideals of A and let $J(S^{-1}A)$ denote the set of ideals of $S^{-1}A$. Then define $\psi_S : J(A) \to J(S^{-1}A)$ by*

$$\psi_S(I) = S^{-1}I = \left\{ \frac{a}{s} : a \in I, s \in S \right\}$$

The map $\psi_S : J(A) \to J(S^{-1}A)$ defined above is surjective.

Proof. Let $f : A \to S^{-1}A$ be the canonical homomorphism $a \mapsto \frac{a}{1}$ and let I be an ideal of $S^{-1}A$. We know that $f^{-1}(I)$ is an ideal of A. We claim that $\psi_S(f^{-1}(I)) = I$. (Then I must be in the image of ψ_S, so ψ_S is surjective.) First we show that $\psi_S(f^{-1}(I)) \subset I$. From the definition,

$$\begin{aligned} \psi_S(f^{-1}(I)) &= \left\{ \frac{a}{s} : a \in f^{-1}(I), s \in S \right\} = \left\{ \frac{a}{s} : f(a) = \frac{a}{1} \in I, s \in S \right\} \\ &= \left\{ \left(\frac{a}{1}\right)\left(\frac{1}{s}\right) : \frac{a}{1} \in I, \frac{1}{s} \in S \right\} \subset I \end{aligned}$$

where the last inclusion follows from the fact that I is an ideal of $S^{-1}A$. Now we show that $I \subset \psi_S(f^{-1}(I))$. If $\frac{a}{s} \in I$, then

$$\left(\frac{a}{s}\right)\left(\frac{s}{1}\right) = \frac{a}{1} = f(a) \in I \implies a \in f^{-1}(I) \implies \frac{a}{s} \in \psi_S(f^{-1}(I))$$

Hence $I = \psi_S(f^{-1}(I))$, so ψ_S is surjective. □

Proposition 0.2 (Exercise 1, Kernel of ψ_S)**.** *Let ψ_S be the map defined above. Then its kernel, with respect to the multiplicative homomorphism structure of $J(A)$ is*

$$\ker \psi_S = \{I : I \cap S \neq \emptyset\}$$

Proof. Suppose $I \in \ker \psi_S$. Then

$$\psi_S(I) = \left\{ \frac{a}{s} : a \in I, s \in S \right\} = S^{-1}A$$

If $I \cap S \neq \emptyset$, then $\psi_S(I)$ contains 1 and hence is equal to $S^{-1}A$. If $I \cap S = \emptyset$, then $1 \notin \psi_S(I)$, so $\psi_S(I) \neq S^{-1}A$. Thus an ideal I is in the kernel of ψ if and only if it has nonempty intersection with S. □

Proposition 0.3 (Exercise 2a)**.** *Every Euclidean domain is a principal ideal domain. Consequently, every Euclidean domain is a unique factorization domain.*

Proof. Let R be a Euclidean domain, and $\phi : R \setminus \{0\} \to \mathbb{N}$ a function satisfying $ab \neq 0 \implies \phi(a) < \phi(ab)$ and for $a, b \in R$ with $b \neq 0$, there exist $r, q \in R$ so that $a = qb + r$ with either $r = 0$ or $r \neq 0$ and $\phi(r) < \phi(b)$.

Let I be an ideal of R and choose a nonzero $a \in I$ such that $\phi(a) \leq \phi(b)$ for all $b \in I$. We claim that $I = \langle a \rangle$. If $b \in I$ with $b \neq 0$, then there exist r, q such that $b = aq + r$ where $r = 0$ or $\phi(r) < \phi(a)$. Then since $r = b - aq$, $r \in I$. By choice of a, we have $\phi(a) \geq \phi(r)$, so we must have $r = 0$. Thus $b = aq$ for some $q \in R$, hence $I = \langle a \rangle$.

Every principal ideal domain is a unique factorization domain, so every Euclidean domain is a unique factorization domain. □

Lemma 0.4 (for Exercise 2b)**.** *Define $\phi : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$ by $\phi(a + bi) = a^2 + b^2$. Then $\phi(xy) = \phi(x)\phi(y)$.*

Proof. Let $x = a + bi, y = c + di \in \mathbb{Z}[i]$.

$$\begin{aligned}\phi(xy) &= \phi((a+bi)(c+di)) = \phi((ac-bd)+(ad+bc)) = (ac-bd)^2 + (ad+bc)^2 \\ &= a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2adbc + b^2c^2 = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= (a^2+b^2)(c^2+d^2) = \phi(a+bi)\phi(c+di) = \phi(x)\phi(y)\end{aligned}$$

□

Proposition 0.5 (Exercise 2b, part one)**.** *The ring $\mathbb{Z}[i]$ is a Euclidean domain. Consequently, it is a principal ideal domain and a unique factorization domain.*

Proof. Define $\phi : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$ by $\phi(a + bi) = a^2 + b^2$. The first property is easy. Suppose $xy \in \mathbb{Z}[i]$ with $xy \neq 0$. As shown above, $\phi(xy) = \phi(x)\phi(y)$, so

$$\phi(x) \leq \phi(x)\phi(y) = \phi(xy)$$

since $\phi(y) \geq 1$. The second property is harder. Suppose that $x, y \in \mathbb{Z}[i]$ with $y \neq 0$. Since $\mathbb{Z}[i]$ is an integral domain, we can form its field of fractions K. Since $y \neq 0$, $xy^{-1} \in K$. We claim that we can write xy^{-1} as $s + ti$ for $s, t \in \mathbb{Q}$, by performing an operation analogous to multiplying by the complex conjugate. If $x = a + bi$ and $y = c + di$, then

$$xy^{-1} = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{(ac+bd)+(ad-bc)i}{c^2-d^2} = \frac{ac+bd}{c^2-d^2} + \frac{ad-bc}{c^2-d^2}i$$

So we have written xy^{-1} in the appropriate form. Then we can choose $m, n \in \mathbb{Z}$ so that $|m - s| \leq \frac{1}{2}$ and $|n - t| \leq \frac{1}{2}$. Then

$$xy^{-1} = s + ti = (m - m + s) + (n - n + t)i = (m + ni) + \big[(s - m) + (t - n)\big]i$$

Then multiplying through by y gives

$$x = (m + ni)y + \big[(s - m) + (t - n)\big]yi$$

Finally, let $q = (m+ni)$ and $r = [(s-m)+(t-n)i]y$. We have $q \in \mathbb{Z}[i]$ and since $r = x - qy$ we also have $r \in \mathbb{Z}[i]$. And

$$\begin{aligned}\phi(r) &= \phi([(s-m)+(t-n)i]y) = \phi([(s-m)+(t-n)i])\phi(y) \\ &= \left((s-m)^2 + (t-n)^2\right)\phi(y) \le \left(\frac{1}{4}+\frac{1}{4}\right)\phi(y) \le \phi(y)\end{aligned}$$

Thus $\mathbb{Z}[i]$ satisfies the division algorithm property. Thus ϕ makes $\mathbb{Z}[i]$ a Euclidean domain, which implies that it is also a principal ideal domain and a unique factorization domain. ☐

Proposition 0.6 (Exercise 2b, part two)**.** *Let $R = \mathbb{Z}[i]$ and define ϕ as above. Then $x \in \mathbb{Z}[i]$ is a unit if and only if $\phi(x) = 1$. Consequently, the only units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.*

Proof. Suppose that x is a unit. Then $\phi(1) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$. Since $\phi(1) = 1$, this implies that $\phi(x) = 1$. Conversely, suppose that $\phi(x) = \phi(a+bi) = a^2+b^2 = 1$. The only integer solutions to this are $(1,0), (0,1), (-1,0)$, and $(0,-1)$. Hence x is one of the units $1, -1, i, -i$. We have shown that if x is a unit, then $\phi(x) = 1$, and if $\phi(x) = 1$, then $x \in \{\pm 1, \pm i\}$. Hence the only units are $\pm 1, \pm i$. ☐

Proposition 0.7 (Chapter 2, Exercise 10a)**.** *Let $D \in \mathbb{N}$ and let*

$$R = \{a + b\sqrt{-D} : a, b \in \mathbb{Z}\}$$

(We denote R by $\mathbb{Z}[\sqrt{-D}]$.) Then define multiplication and addition in R analogously with the ring structure on $\mathbb{C}$:

$$\begin{aligned}(a+b\sqrt{-D}) + (c+d\sqrt{-D}) &= (a+c) + (b+d)\sqrt{-D} \\ (a+b\sqrt{-D})(c+d\sqrt{-D}) &= (ac-bdD) + (ad+bc)\sqrt{-D}\end{aligned}$$

Then R is a ring under these operations.

Proof. First we check that R is an abelian group with respect to addition. Closure is easy, the identity is $0+0\sqrt{-D}$, and the additive inverse of $a+b\sqrt{-D}$ is $= a-b\sqrt{-D}$. Associativity is inherited from $\mathbb{Z}$. The multiplicative unit is $1+0\sqrt{-D}$, since

$$(a+b\sqrt{-D})(1+0\sqrt{-D}) = (a1 - 0bD) + (a0 + b1\sqrt{-D}) = a + b\sqrt{-D}$$

for $a + b\sqrt{-D} \in \mathbb{Z}[\sqrt{-D}]$. We check associativity with a tedious computation. Note that this computation isn't really necessary, because $\mathbb{Z}[\sqrt{-D}]$ is a subring of $\mathbb{C}$, so associativity is inherited.

$$\begin{aligned}[(a+b\sqrt{-D})(c+d\sqrt{-D})](e+f\sqrt{-D}) &= [(ac-bdD)+(ad+bc)\sqrt{-D}](e+f\sqrt{-D}) \\ &= [(ac-bdD)e - (ad+bc)fD] + [(ac-bdD)f + (ad+bc)e]\sqrt{-D} \\ &= [ace - bdeD - adfD + bcfD] + [acf - bdfD + ade + bce]\sqrt{-D} \\ (a+b\sqrt{-D})[(c+d\sqrt{-D})(e+f\sqrt{-D})] &= (a+b\sqrt{-D})[(ce-dfD)+(cf+ed)\sqrt{-D}] \\ &= [a(ce-dfD) - b(cf+de)D] + [b(ce-dfD) + a(cf+de)]\sqrt{-D} \\ &= [ace - adfD - bdfD - bdeD] + [bce - bdfD + acf + ade]\sqrt{-D}\end{aligned}$$

Thus multiplication is associative. Finally, we check that multiplication distributes over addition with another tedious calculation.

$$\begin{aligned}
(a+b\sqrt{-D})[(c+d\sqrt{-D})+(e+f\sqrt{-D})] &= (a+b\sqrt{-D})[(c+e)+(d+f)\sqrt{-D}] \\
&= [a(c+e)-b(d+f)D]+[b(c+e)+a(d+f)]\sqrt{-D} \\
&= [ac+ae-bdD-bfD]+[bc+be+ad+af]\sqrt{-D} \\
(a+b\sqrt{-D})(c+d\sqrt{-D})+(a+b\sqrt{-D})(e+f\sqrt{-D}) &= \\
&= [(ac-bdD)+(ad+bc)D]+[(ae-bfD)+(af+be)\sqrt{-D}] \\
&= [ac+ae-bdD-bfD]+[ad+bc+af+be]\sqrt{-D}
\end{aligned}$$

Thus multiplication distributes over addition. □

Proposition 0.8 (Chapter 2, Exercise 10b). *Let $D \in \mathbb{N}$ and let $R = \mathbb{Z}[\sqrt{-D}]$. Then the map $R \to R$ given by $(a+b\sqrt{-D}) \mapsto (a-d\sqrt{-D})$ is a ring isomorphism.*

Proof. It is obvious that ϕ is a bijection. It is a homomorphism by the following tedious calculations. Let $a,b,c,d \in \mathbb{Z}$. Addition is preserved, as seen below.

$$\begin{aligned}
\phi[(a+b\sqrt{-D})+(c+d\sqrt{-D})] &= \phi[(a+c)+(b+d)\sqrt{-D}] \\
&= (a+c)-(b+d)\sqrt{-D} \\
&= (a-d\sqrt{-D})+(c-d\sqrt{-D}) \\
&= \phi(a+b\sqrt{-D})+\phi(c+d\sqrt{-D})
\end{aligned}$$

And multiplication is also preserved, by the following calculation.

$$\begin{aligned}
\phi[(a+b\sqrt{-D})(c+d\sqrt{-D})] &= \phi[(ac-bdD)+(bc+ad)\sqrt{-D}] \\
&= (ac-bdD)-(bc+ad)\sqrt{-D} \\
&= (ac-bdD)+(-bc-ad)\sqrt{-D} \\
&= (a-b\sqrt{-D})(c-d\sqrt{-D})
\end{aligned}$$

□

Lemma 0.9 (for Chapter 2, Exercise 10c). *Let $D \in \mathbb{N}$ and let $R = \mathbb{Z}[\sqrt{-D}]$. Define $\phi : R \setminus \{0\} \to \mathbb{N}$ by*

$$\phi(a+b\sqrt{-D}) = a^2+b^2D$$

Then $\phi(xy) = \phi(x)\phi(y)$ for $x,y \in R$.

Proof. Let $x = a+b\sqrt{-D}$ and $y = c+d\sqrt{-D}$.

$$\begin{aligned}
\phi(xy) &= \phi((a+b\sqrt{-D})(c+d\sqrt{-D})) = \phi((ac-bdD)+(ad+bc)) \\
&= (ac-bdD)^2+(ad+bc)^2D \\
&= a^2c^2-2acbdD+b^2d^2D^2+a^2d^2D+2adbcD+b^2c^2D \\
&= a^2c^2+b^2d^2D^2+a^2d^2D+b^2c^2D = (a^2+b^2D)(c^2+d^2D) \\
&= \phi(a+b\sqrt{-D})\phi(c+d\sqrt{-D}) = \phi(x)\phi(y)
\end{aligned}$$

□

Proposition 0.10 (Chapter 2, Exercise 10c)**.** *Let $D \geq 2$ and define ϕ as above. Then $\phi(x) = 1$ if and only if x is a unit. Consequently, the only units in $\mathbb{Z}[\sqrt{-D}]$ are ± 1.*

Proof. Suppose that $x = a + b\sqrt{-D}$ is a unit in $\mathbb{Z}[\sqrt{-D}]$. Then $\phi(1) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$. Since $\phi(1) = 1$, this implies that $\phi(x) = 1$. Conversely, suppose that $\phi(x) = \phi(a + b\sqrt{-D}) = a^2 + b^2 D = 1$. Then since $D \geq 2$, the only integer solutions for a, b are $a = 1, b = 0$. Hence x is the unit ± 1.

We have shown that if x is a unit, then $\phi(x) = 1$, and if $\phi(x) = 1$, then $x = \pm 1$. Hence the only units are ± 1. □

Proposition 0.11 (Chapter 2, Exercise 10d)**.** *The elements $3, 2 + \sqrt{-5}$, and $2 - \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$.*

Proof. Suppose that any of $3, 2 + \sqrt{-5}$ or $2 - \sqrt{-5}$ is reducible. Then it can be written as a product xy for some non-units $x, y \in \mathbb{Z}[\sqrt{-5}]$. Then

$$9 = \phi(3) = \phi(2 + \sqrt{-5}) = \phi(2 - \sqrt{-5}) = \phi(xy) = \phi(x)\phi(y)$$

Since $\phi(x), \phi(y) \in \mathbb{N} \subset \mathbb{Z}$ and $\mathbb{Z}$ is a unique factorization domain, this implies that $\phi(x) = \phi(y) = 3$ or $\phi(x) = 1$ and $\phi(y) = 9$ (up to switching the labels x, y.) The latter case contradicts the fact that x is not a unit, so we have $\phi(x) = \phi(y) = 3$. Then if $x = a + b\sqrt{-5}$, we have $a^2 + 5b^2 = 3$.

There are no solutions to the above equation for integers a, b. (We must have $b = 0$ since otherwise the sum exceeds 3, but 3 is not the square of any integer.) Thus there is no such $x \in \mathbb{Z}[\sqrt{-5}]$ with $\phi(x) = 3$, so there cannot be such a nontrivial factorization of $3, 2 + \sqrt{-5}$, or $2 - \sqrt{-5}$. Hence all three are irreducible. □

Proposition 0.12 (Chapter 2, Exercise 10e)**.** *The ideal $\langle 3, 2 + \sqrt{-5} \rangle$ is not principal in $\mathbb{Z}[\sqrt{-5}]$.*

Proof. Suppose it is principal. Then we can write 3 and $2 + \sqrt{-5}$ as multiples of some $x \in \mathbb{Z}[\sqrt{-5}]$.

$$3 = \alpha x \qquad 2 + \sqrt{-5} = \beta x$$

where $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Then

$$9 = \phi(3) = \phi(\alpha)\phi(x) \qquad 9 = \phi(2 + \sqrt{-5}) = \phi(\beta)\phi(x)$$

By the same arguments as in part (d), there is no $x \in \mathbb{Z}[\sqrt{-5}]$ with $\phi(x) = 3$, so these equations imply that $\phi(x) \in \{\pm 1, \pm 9\}$. If $\phi(x) = \pm 9$, then $\phi(\alpha) = \phi(\beta) = 1$, so α, β are units, which mean they are equal to $\pm 1, \pm i$. (Note that $\pm i \notin \mathbb{Z}[\sqrt{-5}]$.) But this would imply that $3 = \beta\alpha^{-1}(2 + \sqrt{-5})$ for $\alpha, \beta \in \{\pm 1, \pm i\}$, which is false. Thus $\phi(x) = \pm 1$, which implies that x is unit. Then $\langle x \rangle = R$, so in particular, $2 - \sqrt{-5}$ can be written as

$$\begin{aligned} 2 - \sqrt{-5} &= 3(a + b\sqrt{-5}) + (2 + \sqrt{-5})(c + d\sqrt{-5}) \\ &= 3a + 3b\sqrt{-5} + 2c - 5d + 2d\sqrt{-5} + c\sqrt{-5} \\ &= (3a + 2c - 5d) + (3b + 2d + c)\sqrt{-5} \end{aligned}$$

which implies $c = -1 - 3b - 2d$ so

$$(3a + 2c - 5d) = (3a + 2(-1 - 3b - 2d) - 5d) = (3a - 2 - 6b - 9d)$$

Then equating the "real" parts gives

$$2 = (3a - 6b - 9d - 2) \implies 4 = 3a - 6b - 9d = 3(a - 2b - 3d)$$

But 4 is not divisible by 3, so this is impossible for $a, b, d \in \mathbb{Z}$. Hence $2-\sqrt{-5} \notin \langle 3, 2+\sqrt{-5}\rangle$, so $\langle 3, 2 + \sqrt{-5}\rangle \neq \langle x\rangle$. Thus it is not a principal ideal. □

Proposition 0.13 (Chapter 4, Exercise 1)**.** *Let k be a field and $f(x) \in k[x]$. The following are equivalent:*

1. *The ideal $\langle f(x)\rangle$ is prime.*
2. *The ideal $\langle f(x)\rangle$ is maximal.*
3. *$f(x)$ is irreducible.*

Proof. We already know that (2) $\implies$ (1) since every maximal ideal is prime. First we show (1) $\implies$ (3). Suppose that $\langle f(x)\rangle$ is prime and $f(x)$ is reducible. Then there exist $h, g \in k[x]$ so that $f = gh$ and g, h both have degree ≥ 1. Then $gh \in \langle f(x)\rangle$, but neither of g, h is in $\langle f(x)\rangle$ since both have degree strictly less than $\deg f$. This contradicts $\langle f(x)\rangle$ being prime, so f is irreducible. Thus (1) $\implies$ (3).

Now we show that (3) $\implies$ (2). Suppose that $f(x)$ is irreducible, and $\langle f(x)\rangle$ is not maximal. Then there is a proper ideal $I \subset k[x]$ with $\langle f(x)\rangle \subset I$. Since $k[x]$ is a principal ideal domain, $I = \langle g(x)\rangle$ for some $g \in k[x]$. Then $f \in \langle g\rangle$ so $f(x) = g(x)h(x)$ for some $h \in k[x]$. Since f is irreducible, one of g, h is constant. If h is constant, then $\langle f\rangle = \langle g\rangle = I$, and if g is constant then $\langle g\rangle = k[x]$. Thus $I = k[x]$ of $I = \langle f\rangle$. Thus $\langle f\rangle$ is maximal. □

Proposition 0.14 (Chapter 4, Exercise 5a)**.** *$f(x) = x^4 + 1$ and $g(x) = x^6 + x^3 + 1$ are irreducible over $\mathbb{Q}$.*

Proof. First we compute

$$f(x + 1) = (x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$$

Now we can apply Eisenstein's criterion, with $p = 2$. Thus $f(x+1)$ is irreducible over $\mathbb{Q}$, so $f(x)$ is also irreducible over $\mathbb{Q}$. Similarly,

$$g(x + 1) = (x + 1)^6 + (x + 1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$$

so $g(x + 1)$ satisfies Eisenstein's criterion for $p = 3$. Thus $g(x + 1)$ is irreducible over $\mathbb{Q}$, so $g(x)$ is irreducible over $\mathbb{Q}$. □

Proposition 0.15 (Chapter 4, Exercise 5b, part one)**.** *Let K be a field. A polynomial $f \in k[x]$ with degree 3 is either irreducible or has a root in K.*

Proof. Suppose f is reducible. Then we can write it as $f(x) = g(x)h(x)$ where g, h both have degree greater than or equal to 1. Then since $\deg f = 3 = \deg g + \deg h$, one of g, h must have degree 1. WLOG, assume $\deg g = 1$. Then $g(x) = ax + b$ for some $a, b \in k$. Then $g(-a^{-1}b) = 0$, so $-a^{-1}b$ is a root of g, and hence a root of f. □

Proposition 0.16 (Chapter 4, Exercise 5b, part two). *$f(x) = x^3 - 5x^2 + 1$ is irreducible over $\mathbb{Q}$.*

Proof. By the integral root test, a rational root b/d of f must satisfy $b|1$ and $d|1$. Thus ± 1 are the only possible rational roots. Since $f(1) = -3$ and $f(-1) = -5$, f has no rational roots. By the above proposition, f is irreducible over $\mathbb{Q}$. □

Lemma 0.17 (for Chapter 4, Exercise 5c). *Let R be a unique factorization domain and let $f \in R[x_1, \ldots, x_n]$ be nonzero. Let A be a unique factorization domain containing R. If f is irreducible in $A[x_1, \ldots, x_n]$, then f is irreducible in $R[x_1, \ldots, x_n]$.*

Proof. Let $\phi : R \to A$ be the inclusion homomorphism. Then $\phi f \neq 0$ and $\deg \phi f = \deg f$. By hypothesis, ϕf is irreducible in $A[x_1, \ldots, x_n]$, so by Theorem 3.2 (Reduction Criterion, page 185 of Lang), f is irreducible in $R[x_1, \ldots, x_n]$. □

Proposition 0.18 (Chapter 4, Exercise 5c). *$f(x, y) = x^2 + y^2 - 1$ is irreducible in $\mathbb{C}[x, y]$.*

Proof. Note that $\mathbb{C}[y]$ is a unique factorization domain and $(y - 1)$ is a prime. Then $f \in (\mathbb{C}[y])[x] = \mathbb{C}[x, y]$, and we can rewrite f as

$$f(x, y) = x^2 + y^2 - 1 = x^2 + (y - 1)(y + 1)$$

So we can see that f satisfies Eisenstein's criterion for the prime $(y-1)$. Thus f is irreducible in $K[x]$, where K is the quotient field of $\mathbb{C}[y]$. Then because $\mathbb{C}[y] \subset K$, we also have $\mathbb{C}[y][x] = \mathbb{C}[x, y] \subset K[x]$. By the above lemma, since f is irreducible in $K[x]$, it is irreducible in $\mathbb{C}[x, y]$. □

Corollary 0.19 (Chapter 4, Exercise 5c). *$f(x, y) = x^2 + y^2 - 1$ is irreducible over $\mathbb{Q}$.*

Proof. The unique factorization domain $\mathbb{Q}[x, y]$ is a subset of the unique factorization domain $\mathbb{C}[x, y]$, and f is irreducible in $\mathbb{C}[x, y]$. By the above lemma, this implies that f is irreducible in $\mathbb{Q}[x, y]$. □

Lemma 0.20 (for Exercise 4, Chapter 6). *Let A be a unique factorization domain. For $a, b \in A$,*

$$a|b \iff b \equiv 0 \bmod a$$

Proof.

$$b \equiv 0 \bmod a \iff b - 0 = b \in (a) \iff b = ac \iff a|b$$

□

Proposition 0.21 (Chapter 4, Exercise 6, The Integral Root Test). *Let A be a unique factorization domain and K is quotient field. Let*

$$f(x) = a_n x^n + \ldots + a_0 \in A[x]$$

and let $\alpha \in K$ be a root of f, with $\alpha = b/d$ where b, d are relatively prime. Then $b|a_0$ and $d|a_n$. In particular, if $a_n = 1$, then $\alpha \in A$ and $\alpha|a_0$.

Proof. If $\alpha = b/d$ is a root of f, then

$$f(\alpha) = f(b/d) = 0 \implies a_n(b/d)^n + \ldots + a_1(b/d) + a_0 = 0$$

Multiplying by d^n gives

$$a_n b^n + a_{n-1}b^{n-1}d + \ldots + a_1 b d^{n-1} + a_0 d^n = 0$$

Thus $a_n b^n \equiv 0 \bmod d$ and $a_0 \equiv 0 \bmod b$. Thus $d | a_n b^n$ and $b | a_0 b^n$. Since b, d are relatively prime, $d \nmid b^n$ and $b \nmid d^n$. Thus $d | a_n$ and $b | a_0$. If $a_n = 1$, then d must be a unit, so $\alpha = b/d \in A$. □