29.17.1 Show that the evaluation map $e_{\sqrt{-1}}\colon \mathbb{Z}[t] \to \mathbb{C}$ defined by $f \mapsto f(\sqrt{-1})$ is a ring homomorphism with kernel (t^2+1) and image the Gaussian integers.

Solution Since we can multiply and add polynomials like we would normally, and because $e_{\sqrt{-1}}(0) = 0$ and $e_{\sqrt{-1}}(1) = 1$, it's clear that $e_{\sqrt{-1}}$ is a ring homomorphism.

Notice $e_{\sqrt{-1}}(t^2+1) = -1+1 = 0$, so $t^2+1 \in \ker e_{\sqrt{-1}} \implies (t^2+1) \subseteq \ker e_{\sqrt{-1}}$.

Now let $f \in \ker e_{\sqrt{-1}}$. We must have $t^2+1 \mid f$. Otherwise, we can write $f = (t^2+1)q + r$, where $r \neq 0$. Then $f(\sqrt{-1}) \neq 0$, which is a contradiction. Thus, $f \in (t^2+1)$.

For $f = a_0 + a_1 t + \cdots + a_n t^n$, we have

$$e_{\sqrt{-1}}(f) = a_0 + a_1\sqrt{-1} + \cdots a_n(\sqrt{-1})^n = (a_0 - a_2 + a_4 - \cdots) + (a_1 - a_3 + a_5 - \cdots)\sqrt{-1} = 0.$$

The result is a Gaussian integer. The map is also onto, since we $e_{\sqrt{-1}}(a+bt) = a + b\sqrt{-1}$ for any $a, b \in \mathbb{Z}$, so the image of $e_{\sqrt{-1}}$ is $\mathbb{Z}[\sqrt{-1}]$.

29.17.2 Let $R = \mathbb{Z}[\sqrt{-1}]$ and $n = p_1^{e_1} \cdots p_r^{e_r}$ be the standard factorization of the integer $n > 1$. Show that the following are equivalent:

a. n is the sum of two squares.

b. $n = N(\alpha)$ for some $\alpha \in R$.

c. If $p_i \equiv 3 \mod 4$, then e_i is even.

Solution (a) $\implies$ (b)

If $n = a^2 + b^2$, then $n = N(a + b\sqrt{-1})$.

(b) $\implies$ (a)

This case is trivial, as $N(\alpha)$ is a sum of to squares.

(a) $\implies$ (c)

We will show by induction that if n is the sum of two squares and $p_i \equiv 3 \mod 4$, then e_i is even.

Base step:

Let $n = 2$. Every odd factor has 0 as its power.

Inductive step:

Write $n = a^2 + b^2$. We know that $p_i \mid a^2 + b^2$, so $\gcd(a, b) \neq 1$. Otherwise, by a lemma, $p_i \equiv 1 \mod p_i$, which is impossible.

Let $d = \gcd(a, b)$, and consider $n' = n/d^2$, which is integer since $d \mid a, b \implies d^2 \mid a^2 + b^2$. Thus, we can write $n' = a^2/d^2 + b^2/d^2$. If $p \nmid n'$, this implies that $p_i^2 \mid d^2$ or $d^2 \mid p_i^2$. In the first case, we have $p_i \mid d \implies p \mid a, b \implies p_i^2 \mid a^2 + b^2 = n$, so $2 \mid e_i$. In the second, because p_i is prime, we get that $d = p_i$, and we can use the same argument once again.

On the other hand, if $p_i \mid n'$, then by induction, $2 \mid e_i'$, where e_i' is the power of p_i in the factorization of n'. Thus, since multiplying by d^2 can only add even powers of primes, it follows that $2 \mid e_i$, so the inductive step holds.

(c) $\implies$ (a)

Notice that for $a, b, c, d \in \mathbb{Z}$,

$$N\big((a + b\sqrt{-1})(c + d\sqrt{-1})\big) = N\big((a + b\sqrt{-1})\big)N\big((c + d\sqrt{-1})\big).$$

Hence, products of sums of squares are sums of two squares.

If $p_i = 2$, then $p_i = 1^2 + 1^2$. Thus p_i is odd modulo 4, so it's either 1 or 3. If $p_i \equiv 1 \mod 4$, then by Fermat, it's a sum of squares. On the other hand, if $p_i \equiv 3 \mod 4$, then by assumption, e_i is even, so $p_i^{e_i}$ is a square. If we distribute that over a sum of squares, the result is still a sum of squares, and we're done.

29.17.4 Determine all prime elements, up to units, in $\mathbb{Z}[\sqrt{-1}]$.

Solution We will show that a Gaussian integer $a + b\sqrt{-1}$ is prime if and only if:

a. $a = 0$ (respectively $b = 0$) and $|b| \equiv 3 \mod 4$ (respectively $|a| \equiv 3 \mod 4$), or

b. if $a, b \neq 0$, then $N(a + b\sqrt{-1})$ is prime.

"$\implies$"

Let $p = a + b\sqrt{-1}$ be a prime Gaussian integer.

Suppose, without loss of generality, that $a = 0$. Then b must be prime in $\mathbb{Z}$, or else we can simply factor it over $\mathbb{Z}$. Moreover, b must be odd, since $2 = (1 - \sqrt{-1})(1 + \sqrt{-1})$.

Now suppose that $b \mid \alpha\beta$, for some $\alpha = c + d\sqrt{-1}, \beta = e + f\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$. By assumption, $b \mid \alpha$ or $b \mid \beta$. In the first case, $b^2 = N(b) \mid N(\alpha) = c^2 + d^2$.

If c and d are not coprime, then there exists $\delta > 1 \in \mathbb{Z}[\sqrt{-1}]$ which divides c and d. But then d divides b, so $\delta = b$, since b was prime in $\mathbb{Z}$. Hence, $b\sqrt{-1} \mid \alpha$, so $b \mid \alpha$.

If c and d are coprime, then by a lemma, we have $b^2 = N(b) \equiv 1 \mod 4$. The only non-trivial solution to this modulo 4 is $|b| \equiv 3 \mod 4$, so this part holds.

Now assume that $a, b \neq 0$, and suppose that $N(p) = a^2 + b^2$ is not a prime in $\mathbb{Z}$. Then we can write $a^2 + b^2 = cd$, for some $c, d \in \mathbb{Z}$ non-unit. Then $cd = (a + b\sqrt{-1})(a - b\sqrt{-1})$.

The Gaussian integers are a UFD, $c \approx a + b\sqrt{-1}$ and $d \approx a - b\sqrt{-1}$, or vice versa. In either case, we have a non-trivial divisor of p, which implies that p is not prime, a contradiction.

Thus, one of the two situations must hold.

"$\impliedby$"

Let $p = a + b\sqrt{-1}$ be prime in $\mathbb{Z}[\sqrt{-1}]$.

a. Suppose $a = 0$ and $N(b) \equiv 3 \mod 4$. Suppose b were not prime in $\mathbb{Z}[\sqrt{-1}]$ so that there exist non-unit $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$ with
$$b^2 = N(b) = N(\alpha)N(\beta).$$
So, we need $N(\alpha) = N(\beta) = b$. But this means that $N(\alpha)^2 \equiv 3 \mod 4$, and there are no solutions to this modulo 4, so b is prime in the Gaussian integers. The same argument holds for when $b = 0$.

b. Now assume that $a^2 + b^2$ is prime in $\mathbb{Z}$, and assume that $a + b\sqrt{-1}$ is not prime, so that $p = \alpha\beta$ for some non-trivial $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$. Then
$$p^2 = N(\alpha)N(\beta),$$
which implies that $p = N(\alpha) = N(\beta)$. Hence, there exist $c, d \in \mathbb{Z}$ so that $p = c^2 + d^2$. But this means
$$a^2 + b^2 = (c^2 + d^2)^2,$$
but $a^2 + b^2$ was prime, a a contradiction. Hence, p must be prime in $\mathbb{Z}[\sqrt{-1}]$.

29.17.5 Show that $\mathbb{Z}[\sqrt{-2}]$ is a (strong) Euclidean domain.

Solution We will show that $N(a+b\sqrt{-2}) = a^2 + 2b^2$ is a Euclidean function.

Let $\alpha = a+b\sqrt{-2}, \beta = c+d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ with $\beta \neq 0$, so that $\alpha/\beta = f' + g'\sqrt{-2} \in \mathbb{Q}[\sqrt{-2}]$. Pick $f, g \in \mathbb{Z}$ so that $N(f-f'), N(g-g') \leq 1/4$. Then

$$\begin{aligned} a+b\sqrt{-2} &= (c+d\sqrt{-2})(f'+g'\sqrt{-2}) \\ &= (c+d\sqrt{-2})(f+g\sqrt{-2}+(f'-f)+(g'-g)\sqrt{-2}) \\ &= (c+d\sqrt{-2})(f+g\sqrt{-2}) + (c+d\sqrt{-2})\big[(f'-f)+(g'-g)\sqrt{-2}\big]. \end{aligned}$$

Notice that

$$\begin{aligned} N((c+d\sqrt{-2})\big[(f'-f)+(g'-g)\sqrt{-2}\big]) &= N(c+d\sqrt{-2})N((f'-f)+(g'-g)\sqrt{-2}) \\ &\leq N(c+d\sqrt{-2})\big(N(f'-f)+N((g'-g)\sqrt{-2})\big) \\ &\leq N(c+d\sqrt{-2})\left(\frac{1}{4}+\frac{2}{4}\right) \\ &< N(c+d\sqrt{-2}). \end{aligned}$$

Thus, N is a Euclidean function, and monotonicity also clearly holds, since $N(a+b\sqrt{-2}) = a^2+2b^2 \geq 1$ for any $a, b \in \mathbb{Z}$.

29.17.9 Let $R = \mathbb{Z}[\sqrt{-5}]$. Show the following:

a. The elements $2, 3, 1+\sqrt{-5}$, and $1-\sqrt{-5}$ are all irreducible, but no two are associates.

b. None of the elements $2, 3, 1+\sqrt{-5}$, and $1-\sqrt{-5}$ are prime. In particular, R is not a UFD.

Solution a. If we let $a+b\sqrt{-5}, c+d\sqrt{-5} \in R$, then

$$4 = N(2) = (a^2+5b^2)(c^2+5d^2).$$

To get a non-trivial factorization, we need to have $a^2+5b^2 = 2$, but this is impossible. The same argument works for 3.

For $1+\sqrt{-5}$, we write

$$6 = N(1+\sqrt{-5}) = (a^2+5b^2)(c^2+5d^2).$$

So, we need $a^2+5b^2 \in \{2, 3\}$, but as before, this is impossible.

Thus, all of the given elements are irreducible.

The only units are 1 and -1, and it's clear that no pair of these elements are associates.

b. Notice that

$$2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

but none of these factors divide each other, since they're all irreducible. Hence, none of them are prime.

29.17.10 Let $R = \mathbb{Z}[\sqrt{-5}]$. Let $\mathfrak{P} = (2, 1+\sqrt{-5})$. Show

a. $\mathfrak{P}^2 = (2)$ in R.

b. $\mathfrak{P}$ is a maximal ideal.

c. $\mathfrak{P}$ is not a principal ideal.

Solution a. Let $2a + (1+\sqrt{-5})b, 2c + (1+\sqrt{-5})d \in \mathfrak{P}$. We can write them as

$$(2a+b) + b\sqrt{-5} \quad \text{and} \quad (2c+d) + d\sqrt{-5}.$$

Then their product is

$$(2a+b)(2c+d) + \sqrt{-5}(2ad + bd + 2bc + bd) - 5bd = 4ac + 2ad + 2bc - 4bd + 2\sqrt{-5}(ad + bc + bd) \in (2),$$

so $\mathfrak{P}^2 \subseteq (2)$, since we chose arbitrary elements in $\mathfrak{P}$.

For the other direction, notice that $(1+\sqrt{-5})^2 = -4 + 2\sqrt{-5}$, $(1-\sqrt{-5})^2 = -4 - 2\sqrt{-5}$, and $2^2 = 4$. Each of these elements is in $\mathfrak{P}^2$, so

$$3 \cdot 4 + \sqrt{-5}\big[4 + \big(-4 + 2\sqrt{-5}\big)\big] = 12 - 10 = 2 \in \mathfrak{P}^2.$$

Since products of ideals are ideals, $(2) \subseteq \mathfrak{P}^2$.

b. Let $\mathfrak{A} > \mathfrak{P}$ and let $x = a + b\sqrt{-5} \in \mathfrak{A} \setminus \mathfrak{P}$.

Notice that we can't have $2 \mid a + b\sqrt{-5}$ or else $x \in \mathfrak{P}$, so 2 must not divide at least one of them.

If $2 \mid a$, then $b\sqrt{-5} \in \mathfrak{A} \implies -b \in \mathfrak{A} \implies b \in \mathfrak{A}$. Since $2 \nmid b$, then $\gcd(2, a) = 1 \implies 1 \in \mathfrak{A} \implies \mathfrak{A} = R$.

If $2 \mid b$, then $a \in \mathfrak{A}$. Since $2 \nmid b$, as before, this implies that $\mathfrak{A} = R$ also.

Now if 2 does not divide either of them, we have that $1 + bc\sqrt{-5} \in \mathfrak{A}$, for some $c \in \mathbb{Z}$. If c is even, then $1 \in \mathfrak{A}$. Otherwise, subtracting by $bc\big(1+\sqrt{-5}\big)$, we get $-bc \in \mathfrak{A}$, and it must be odd. Thus, $\gcd(2, -bc) = 1$, and this implies that $1 \in \mathfrak{A}$.

In any case, $\mathfrak{A} = R$, so R is maximal.

c. Suppose $\mathfrak{P}$ were principal, and that $\mathfrak{P} = (a)$ for some $a \in R$. Then there exist $x, y \in R$ so that $ax = 2$ and $ay = 1 + \sqrt{-5}$. In particular, $a \mid 2$ and $a \mid (1+\sqrt{-5})$.

Suppose $2 = (\alpha + \beta\sqrt{-5})(\gamma + \delta\sqrt{-5})$ for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Then

$$N(2) = N(c)N(d) \implies 4 = (\alpha^2 + 5\beta^2)(\gamma^2 + 5\delta^2).$$

To get a non-trivial factorization, we need (without loss of generality) that $\alpha^2 + 5\beta^2 = 2$, which isn't possible, so 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Hence, $a = 1$ or $a = 2$. If $a = 1$, then $\mathfrak{P} = R$, which can't happen. But if $a = 2$,

$$N(a) = 4 \nmid 6 = N(1+\sqrt{-5}) \implies a \nmid \big(1+\sqrt{-5}\big),$$

a contradiction. Thus, $\mathfrak{P}$ is not principal.

31.19.1 Let R be a commutative ring. Show that a polynomial $f = a_0 + a_1 t + \cdots + a_n t^n$ in $R[t]$ is a unit in $R[t]$ if and only if a_0 is a unit in R and a_i is nilpotent for every $i > 0$.

Solution "$\implies$"

Let $f = a_0 + \cdots + a_n t^n$ be a unit, and let $g = b_0 + \cdots + b_m t^m$ be its inverse.

We have
$$fg = \sum_{i=0}^{n+m} \sum_{j=0}^{i} a_{i-j} b_j t^i = 1.$$

When $i = 0$, we have $a_0 b_0 = 1$, so a_0 must be a unit.

For $i = n + m$, we have
$$a_n b_m = 0.$$

For $i = n + m - 1$,
$$a_n b_{m-1} + a_{n-1} b_m = 0 \implies a_n^2 b_{m-1} + a_{n-1} a_n b_m = a_n^2 b_{m-1} = 0.$$

We proceed by induction on the power of a_n:

Suppose we have $a_n b_m = a_n^2 b_{m-1} = \ldots = a_n^k b_{m-k+1} = 0$. If we look at the $i = n + m - k$ term, we have
$$\sum_{i+j=n+m-k} a_i b_j = 0.$$

If we multiply through by a_n^k, all the terms drop out except for $a_n^{k+1} b_{m-k}$, since all the other terms have b_ℓ where $\ell \geq m - k + 1$, so we get $a_n^{k+1} b_{m-k} = 0$, which shows that the inductive step holds.

Thus, after finitely many steps, we see that $a_n^{1+m} b_0 = 0$. Multiplying by a_0, we get a_n^{1+m}, so a_n is nilpotent.

By a previous homework assignment, if u is a unit and x and nilpotent element, then $u + x$ is still a unit. Thus, $f - a_n t^n$ is a unit, and we can run the same argument finitely many times. Thus, $a_1, \ldots, a_n$ are units.

"$\impliedby$"

By a previous homework problem, if x is nilpotent and u is unit, then $u + x$ is a unit. We proceed by induction:

Base step:

Suppose a_0 is a unit. Because a_1 is nilpotent, so is $a_1 t$, so $a_0 + a_1 t$ is a unit.

Inductive step:

Now suppose $a_0 + \cdots + a_n t^n$ is a unit, and suppose a_{n+1} is nilpotent. Then $a_{n+1} t^{n+1}$ is also nilpotent, so $a_0 + \cdots + a_n t^n + a_{n+1} t^{n+1}$ is a unit, which completes the inductive step.

By induction, f is a unit,

31.19.3 Let R be a nontrivial commutative ring. If $f = a_0 + a_1 t + \cdots + a_n t^n$ is a polynomial in $R[t]$, define the *formal derivative* f' of f to be $f = a_1 + 2a_2 t + \cdots + na_n t^{n-1}$.

a. Show the usual rules of differentiation hold.

b. Suppose R is a field of characteristic zero. Show that a polynomial $f \in R[t]$ is divisible by the square of a non-constant polynomial in $R[t]$ if and only if f and f' are not relatively prime.

Solution a. We will show that linearity and the product rule hold.

Linearity:

Write $f = a_0 + \cdots + a_n t^n$, $g = b_0 + \cdots + b_m t^m$, and assume without loss of generality that $n \le m$. Then

$$\begin{aligned}
(f+g)' &= \big[(a_0+b_0) + (a_1+b_1)t + \cdots + (a_n+b_n)t^n + b_{n+1}t^{n+1} + \cdots + b_m t^m\big]' \\
&= (a_1+b_1) + 2(a_2+b_2)t + \cdots + n(a_n+b_n)t^{n-1} + (n+1)b_{n+1}t^n + \cdots + mb_m t^{m-1} \\
&= f' + g'.
\end{aligned}$$

If $c \in R$, then

$$(cf)' = [ca_0 + ca_1 t + \cdots + ca_n t^n]' = ca_1 + 2ca_2 t + \cdots + nca_n t^{n-1} = cf'.$$

Thus, linearity holds.

Product rule:

Let f and g be as before.

$$(fg)' = \left[\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i} a_{i-j}b_j\right)t^i\right]' = \sum_{i=1}^{n+m} i\left(\sum_{j=0}^{i} a_{i-j}b_j\right)t^{i-1}$$

On the other hand,

$$\begin{aligned}
f'g + fg' &= \left[\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i}(i-j+1)a_{i-j+1}\cdot b_j\right)t^i\right] + \left[\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i} a_{i-j}\cdot(j+1)b_{j+1}\right)t^i\right] \\
&= \sum_{i=1}^{n+m}\left(\sum_{j=0}^{i} a_{i-j}b_j\right)t^i,
\end{aligned}$$

by reindexing, so the product rule holds.

b. Let $f \in R[t]$.

"$\implies$"

Let f be divisible by g^2, where g is a non-constant polynomial. Then we can write $f = hg^2$, where $h \in R[t]$. By the product rule (we use induction to extend it to any finite number of polynomials), we have

$$f' = h'g^2 + hgg' + hg'g = h'g^2 + 2hgg' = g(h'g + 2hg').$$

Thus, g divides both f and f', so they are not relatively prime.

"$\impliedby$"

We proceed by induction on the degree of f. Throughout the proof, we assume that $f \not\equiv 0$. Moreover, f must have degree at least 2, or else only constant factors can divide f'.

Base step:

Consider $f = a_0 + a_1 t + a_2 t^2$, where $a_2 \neq 0$. Since f has characteristic 0, $f' = a_1 + 2a_2 t \not\equiv 0$.

Assume that $b_0 + b_1 t$ divide both f and f'. Then we can write $f = (b_0 + b_1 t)(c_0 + c_1 t)$ for some $c_0, c_1 \in R$. By the product rule,

$$f' = b_1(c_0 + c_1 t) + c_0(b_0 + b_1 t).$$

Since $b_0 + b_1 t$ divides f', this implies that it divides $c_0 + c_1 t$ also, which is non-zero since f has characteristic 0. Hence, $(b_0 + b_1 t)^2$ divides f, and the base step holds.

Inductive step:

Assume that g divides f and f', so that we can write $f = gh$ and $f' = gu$.

Then $f' = g'h + gh' = gu \implies g'h = g(u - h')$, so $g \mid g'h$.

If g and g' are coprime, then $g \mid h \implies h = pg$, so $f = g^2 p$. On the other hand, if they have a common factor, then by induction, there is a polynomial so that $p^2 \mid g$. Then $p^2 \mid f$.

31.19.5 Let F be a subfield of the complex numbers $\mathbb{C}$. Let $f \in F[t]$ be an irreducible polynomial. Show that f has no *multiple root* in $\mathbb{C}$, i.e., a root α of f satisfying $(t-\alpha)^n \mid f$ in $F[t]$ with $n > 1$.

Solution Notice that $\gcd_{\mathbb{C}}(f,g) = \gcd_F(f,g)$. It's clear that $\gcd_F(f,g) \mid \gcd_{\mathbb{C}}(f,g)$.

On the other hand, since $F[t]$ is a PID (because of the Euclidean algorithm), so there exist u, v so that $fu + gv = \gcd_F(f,g)$. By definition, $\gcd_{\mathbb{C}}(f,g) \mid f$, $\gcd_{\mathbb{C}}(f,g) \mid g$, so $\gcd_{\mathbb{C}}(f,g) \mid \gcd_F(f,g)$.

It follows that $f \mid g$ in $\mathbb{C}[t]$ implies that $f \mid g$ in $F[t]$. Indeed, if $f \mid g$ in $\mathbb{C}[t]$, then $f = \gcd_{\mathbb{C}}(f,g) = \gcd_F(f,g)$.

Thus, if f is irreducible in $F[t]$ in $F(t)$, then it is irreducible in $\mathbb{C}[t]$, so we may treat as if it were in $\mathbb{C}[t]$.

If f had a multiple root, then it is reducible: $f = (t-\alpha)\cdot(t-\alpha)^{n-1}g$, which are both non-trivial, a contradiction.

31.19.9 Show that over any field F, there exist infinitely many monic irreducible polynomials in $F[t]$. Also show that if F is algebraically closed, then F must have infinitely many elements.

Solution Assume F is not algebraically closed, so that there exists $f_1 \in F[t]$ which is irreducible. Since F is a field, we may scale f_1 so that it is monic and remain irreducible.

Then $f_1 + 1$ is monic. If it is irreducible, then take $f_2 = f_1 + 1$. Otherwise, it may be written as a product $f_2 g_2$, where f_2 is monic (by scaling) and irreducible. $f_1 \not\equiv f_2$, since f_1 does not divide $f_1 + 1$.

Now $f_1 f_2 + 1$ is monic. If it is irreducible, then take $f_3 = f_1 f_2 + 1$. Otherwise, take a monic irreducible factor of it to be f_3, which cannot be f_1 or f_2.

Continuing by induction, we find countably many monic irreducible polynomials in $F[t]$.

Now assume F is algebraically closed and suppose that $F = \{a_1, \ldots, a_n\}$ is finite. Consider $a_1 \cdots a_n + 1$. Since F is algebraically closed, there exists a_{n+1} which divides it. But $a_{n+1} \neq a_i$ for any $1 \leq i \leq n$, a contradiction. Hence, F must be infinite.