ALGEBRA NOTE 5

JOHNEW ZHANG

1. Polynomials

If $\mathbb{R}$ is a commutative ring, then let $\mathbb{R}[x]$ be the set of polynomials with coefficients in $\mathbb{R}$.

$f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0 = \sum_{i=0}^{d} a_i x^i$, $a_i \in \mathbb{R}$.

Adding and multiplying polynomials.
$\sum_{i=0}^{d} a_i x^i + \sum_{i=0}^{d} b_i x^i = \sum_{i=0}^{d} (a_i + b_i) x^i$.
$\sum_{i=0}^{d} a_i x^i \sum_{i=0}^{d} b_i x^i = \sum (\sum_{j+k=1} a_j b_k) x^i$.

Check that $\mathbb{R}[x]$ is also a commutative ring, with 0 and 1, being the constant polynomials 0 and 1.
The degree of a polynomial $\sum_{i=0}^{m} a_i x^i$ is the largest d such that $a_d \neq 0$.
The zero polynomial has degree $-\infty$
If $\mathbb{F}$ is a field, and $f(x), g(x) \in \mathbb{F}[x]$,
then $deg(fg) = deg(f) + deg(g)$.

Example : of a ring, where that doesn't work.
$\mathbb{R} = \mathbb{Z}_6$,
$f(x) = 3x^2 + 1, g(x) = 2x^5 + x$.
$f(x)g(x) = (3x^2 + 1)(2x^5 + x) = 2x^5 + 3x^3 + x$.
Therefore the degree is 5.

Why does it work in a field?
$(a_j x^d +$ (lower degree terms)$)(b_e x^e +$(lower terms)$) = a_j b_e x^{d+e}$ + lower degree terms.
If the coefficients are in a field $\mathbb{F}$, and $a_j \neq 0$, $b_e \neq 0$, then $a_j b_e \neq 0$, also. (integral domain)

Application:
Let $\mathbb{F}$ be a field, and $f(x) \in \mathbb{F}[x]$ is a unit. Then $f(x)$ is constant.

Proof. If $g(x) \in \mathbb{F}[x]$ with $fg = 1$, then $deg(f) + deg(g) = deg(fg) = 0$.
$f \neq 0, g \neq 0$, so $deg(f), deg(g) \geq 0$,
So $deg(f) + deg(g) = 0$.
$f(x) = \sum_{i=0}^{m} a_i x^i$, $deg(f)$ is the largest d such that $a_d \neq 0$.

So $f(x) = a_0 \in \mathbb{F}.g(x) = b_0 \in \mathbb{F}$. $\square$

AKA: If $\mathbb{F}$ is a field, then algebra in $\mathbb{F}[x]$ is a lot like algebra in $\mathbb{Z}$.
We really need $\mathbb{F}$ to be a field, or things are not like $\mathbb{Z}$.

Example: In $\mathbb{Z}$, if $a^2 = 1$, then $a = \pm 1$.
If $f(x) \in \mathbb{Z}_4[x]$, then $(2f(x)+1)^2 = 4f(x)^2 + 4f(x) + 1 = 1$.

Lemma 1. *Let $\mathbb{F}$ is a field, and $f(x), g(x) \in \mathbb{F}[x]$ (non-zero). Then there are polynomials $q(x)$ and $r(x)$,*
such that, $g(x) = q(x)f(x) + r(x)$ and $deg(r) < deg(f)$. Also, $q(x)$ and $r(x)$ are unique.

Proof. We can assume that $deg(g) \leq deg(f)$. Otherwise, $q = 0, r = q$ works.
We are going to proceed by induction on the degree of g.
If $deg(g) = 0$, then either $deg(g) < deg(f)$ (done!) or else.
$f(x)$ and $g(x)$ are both constant.
If $f(x) = a_0, g(x) = b_0$, then $g(x) = \frac{b_0}{a_0} f(x) + 0$
Induction step: Assume that for any $g_2(x) \in \mathbb{F}[x]$ with $deg(g_2) < deg(g)$
we can write
$g_2(x) = q_2(x)f(x) + r_2(x), deg(r_2) < deg(f)$
Write $g(x) = a_d x^d +$ other terms of lower degree.
And $f(x) = b_e x^e +$ lower order terms. $b_e \neq 0$.
Let $g_2(x) = g(x) - \frac{a_d}{b_e} f(x) x^{d-e}$.
Write out the first term
$g_2(x) = (a_d x^d + \ldots) - \frac{a_d}{b_e} f(x) x^{d-e}(b_e x^e + \ldots) = (a_d x^d + \ldots) - (a_d x^d + \ldots) = 0 \cdot x^d + \ldots =$ something of degree less than $d = deg(g)$.
$deg(g_2) < deg(g)$.
By the induction hypothesis, we can write $g_2(x) = q_2(x)f(x) + r(x)$ with $q_2, r \in \mathbb{F}[x]$, $deg(r) < deg(f)$.
Since $g(x) = g_2(x) + \frac{a_d}{b_e} f(x) x^{d-e} f(x)$,
we get
$g(x) = \frac{a_d}{b_e} x^{d-e} f(x) + q_2(x)f(x) + r(x) = (\frac{a_d}{b_e} f(x) x^{d-e} + q_2(x))f(x) + r(x)$. with $deg(r) < deg(f)$,
So take
$q(x) = \frac{a_d}{b_e} f(x) x^{d-e} + q_2(x)$.
By induction, we can do this for all polynomials.
Secondly, for the uniqueness,
Suppose that $g(x) = q_1(x)f(x) + r_1(x)$ and $g(x) = q_2(x)f(x) + r_2(x)$
with $deg(r_1), deg(r_2) < deg(f)$.
Then $0 = (q_1(x)f(x) + r_1(x)) - (q_1(x)f(x) + r_1(x))$
So $r_1 - r_2 = f(q_2 - q_1)$.
Since $\mathbb{F}$ is a field,
$deg(r_1 - r_2) = deg(f) + deg(q_2 - q_1)$

If $q_2 - q_1 \neq 0$, then $deg(r_1 - r_2) \geq deg(f)$
But $deg(r_1), deg(r_2) < deg(f)$.
So $deg(r_1 - r_2) < deg(f)$
Useful fact $deg(f+g) \leq max\{deg(f), deg(g)\}$
So we have a contradiction.
$\therefore, q_1 = q_2, r_1 = r_2$.

□

The proof shows how to do the division algorithm.

Example: Long divide x^2+1 into $x^3 - 2x^2 + 1$ and find the quotient $q(x)$ and remainder $r(x)$.
$x^3 - 2x^2 + 1 = x(x^2+1) + (-2x^2 - x + 1)$
$-2x^2 - x + 1 = 2(x^2+1) + (-x+3)$.
So the remainder is $(-x+3)$.
Therefore $x^3 - 2x^2 + 1 = (x^2+1)(x-2) + (-x+3)$.

Proposition 1. *If $\mathbb{F}$ is a field, $f(x) \in \mathbb{F}[x]$, and $c \in \mathbb{F}$, then $f(c) = 0$, if and only if $(x-c)|f(x)$.*

Proof. By the division algorithm, we can write $f(x) = q(x)(x-c) + r(x)$ where $deg(r(x)) < deg(x-c) = 1$.
Since $deg(r) < 1$, then $r \in \mathbb{F}$ is a constant.
So $f(c) = q(c)(c-c) + r = r$.
In fact, $f(x) = q(x)(x-c) + f(c)$
If $f(c) = 0$, then $f(x) = q(x)(x-c)$, so $x - c|f(x)$.
On the other hand, if $f(x) = (x-c)h(x)$,
then $f(c) = (c-c)h(c) = 0$

□

Definition 1. *For a commutative ring $\mathbb{R}$, we say that a divides b, (for $a, b \in \mathbb{R}$) if and only if $b = ac$ for some $c \in \mathbb{R}, a|b$.*
If $\mathbb{F}$ is a field, and $f(x), g(x) \in \mathbb{F}[x]$, then $f(x)|g(x)$ means $c_1 f(x)|c_2 g(x)$ for any $c_1, c_2 \in \mathbb{F}$, (they are not 0)

For example, $(x-1)|(x^3-1)(in$Q[x])
but also $(2x-2)|(x^3-1)$.

Theorem 1. *(Euclidean Algorithm for Polynomials)*
Let F be a field, $f(x), g(x) \in F[x]$. non-zero, then $f(x), g(x)$ have a greatest common divisor.
I.e., there is a polynomial $d(x)$ so that
(1) $d|f, d|g$.
(2) if $e(x) \in F[x]$ with $e|f, e|g$ then $e|d$.

(3) Bezout's Properties: There exists $s(x), t(x) \in F[x]$, with $d = fs + gt$.

d is not unique, but if d_2 is another polynomial with all the same properties, then $d(x) = cd_2(x)$ for some non-zero $c \in F$.

Observation: If F is a field and $f, g \in F[x]$ then $f|g, g|f$ if and only if $f = cg$ for some $c \in F, c \neq 0$.

Proof. If $f = cg$ then $g|f$, and $g = c^{-1}f$, so $f|g$.
If $g|f, f|g$, $deg(f) = deg(g)$.
So $g = fh$ for some $h \in F[x]$, $deg(h) = 0$.
Then $h = c \in F$. □

If d has those properties in the theorem of the gcd of polynomials, then so does cd for any $c \in F, c \neq Q$.
On the other hand, if d_2 also has all of these properties, then $d|d_2$ and $d_2|d$, so $d_2 = cd$.

Definition 2. *$f(x) \in F[x]$ is monic if $f(x) = x^d$+smaller terms.*
So for $f(x), g(x) \in F[x]$ there is a unique monic d satisfying the condition $d|f, d|g$.
We call that the gcd of $f(x), g(x)$.

Proof of the theorem:

Proof. We can suppose that $deg(f) \geq deg(g)$,
Using the division algorithm, write
$f = q_1 g + r_1$, $deg(r_1) < deg(g)$.
$g = q_2 r_1 + r_2, de(r_2) < deg(r_1)$
Eventually, $r_j = 0$.
$r_{j-3} = q_{j-1} r_{j-2} + r_{j-1}$ $(\star)$
$rj - 2 = q_j r_{j-1} + 0$.
Then take $d = r_{j-1}$.
$d = r_{j-1} | r_{j-2}$
$d | r_{j-3}$
Continuing, $d|f, d|g$.
Then want to show that $d = sf + tg$ for some $s, t \in F[x]$.
By the $\star$, $d = (1)r_{j-3} + (-q_{j-1})r_{j-2}$.
but $r_{j-4} = q_{j-2} r_{j-3} + r_{j-2}$
so $d = (1)r_{j-3} + (-q_{j-1})(r_{j-4} - q_{j-2} r_{r-3}) = (?)f + (?)g$.
Now, if $e|f, e|g$, then $e|sf + tg = d$.
□

Example: Find the gcd of $f(x) = x^4 - 2x^3 + x^2 - 2x, g(x) = x^4 + 3x^3 + 2x^2 + 3x + 1$.
Go through the Euclidean Algorithm and the long division,
you get the gcd is $d = x^2 + 1$. $x^2 + 1 = (\frac{5}{11}x + \frac{14}{11})f(x) + (\frac{-5}{11}x + 1)g(x)$.
GCDs for polynomial over F VS GCDs for integers.

1.1. Unique factorization for polynomials.

Definition 3. *A polynomial $f(x) \in F[x]$ is irreducible if and only if whenever $f(x) = g(x)h(x)$,$g, h \in F[x]$, then g or h is constant.*

Theorem 2. *Any non-zero polynomial $f(x) \in F[x]$ can be written as*
$f = ap_1^{e_1} \dots p_k^{e_k}$
where $a \in F$,
$p_i \in F[x]$ are distinct monic and irreducible, and $e_i \geq 1$.
This representation is unique (up to order).

Lemma 2. *If $p, q, r \in F[x]$, and $gcd(p, q) = 1$ and $p|qr$, then $p|r$*

Proof. Choose $s, t \in F[x]$ so that $sp + tq = 1$.
$r = r \cdot 1 = r(sp + tq) = prs + rqt$
Therefore the whole thing is divisible by p. □

Corollary 1. *If p is irreducible, and $p|q_1q_2 \dots q_r$, then $p|q_i$ for some i.*

Proof. (For $r = 2$) Suppose that p is irreducible and $p|q_1q_2$.
$gcd(p, q_1)$ is a divisor of $p(n)$.
So $gcd(p, q_1) = 1$ or cp, for some $c \in F$.
If $gcd(p, q_1) = cp$, then $cp|q_1$, so $p|q_1$.
If $gcd(p, q_1) = 1$, then the previous lemma gives $p|q_2$.
If $r > 2$, just do induction:
$p|q_1q_2 \dots q_r = q_1(q_2 \dots q_r)$.
Then either $p|q_1$ or $p|q_2 \dots q_r$.
□

Theorem 3. *Unique factorization for polynomial:*
If $\mathbb{F}$ is a field and $f(x) \in \mathbb{F}[x]$ is non-zero, then f can be written as
$f(x) = ap_1^{e_1}p_2^{e_2} \dots p_r^{e_r}$ *with $a \in \mathbb{F}$.*
p_i monic irreducible, $e_i \geq 1$.
Uniquely (up to reordering the product).

Proof. If $f(x) = ax^d + \dots$, then $\frac{1}{a}f(x)$ is monic.
So we'll assume that $f(x)$ is monic.
Want to show that $f(x)$ can be written as a product of irreducible monic polynomials.
By induction on the degree.
Base case: $deg(f) = 1$.
Then $f(x) = x + b$ for some $b \in F$.
$f(x)$ is irreducible.
Suppose that the statement is true for polynomials of degree less than degree of f.
If f is irreducible, we are done.
If not, we can write $f(x) = g(x)h(x)$ with $deg(g), deg(h) < deg(f)$. .
Say $g(x)bx^e + \dots, h(x) = cx^e \dots$
$f(x) = bcx^{e+w} + \dots$.

So $bc = 1$.

Then $f(x) = g(x)h(x) = (cg(x))(c_{-1}h(x)) = (x^e + \ldots)(x_w + \ldots)$.

By the induction hypothesis, both $cg(x)$ and $c_{-1}h(x)$ can be written as a product of monic, irreducible polynomials, So $f(x)$ can, too.

By the induction, any monic polynomial can be written as a product of monic irreducible polynomials.

If $f(x) \in \mathbb{F}[x]$ is non-zero (possibly not monic) then $f(x) = ap_1^{e_1}p_2^{e_2}\ldots p_r^{e_r}$ as in the theorem.

For uniqueness, suppose that

$ap_1^{e_1}p_2^{e^2}\ldots p_r^{e_r} = bq_1^{w_1}\ldots q_r^{w_r}$ with $a, b \in F$ non-zero, p_i, q_i monic and irreducible, and $e_i, w_i \geq 1$.

Multiplying out, a is the coefficient of the higher power of x in $ap_1^{e_1}p_2^{e^2}\ldots p_r^{e_r}$. and b is the coefficient of the highest power of x in $bq_1^{w_1}\ldots q_r^{w_r}$.

So $a = b$.

Now we want to show that

$ap_1^{e_1}p_2^{e^2}\ldots p_r^{e_r} = bq_1^{w_1}\ldots q_r^{w_r}$

$\implies p_i$ are the q_j (in some order).

Induction on the number of factors $n = e_1 + e_2 + \ldots + e_r$.

Base case : $n = 1$ $LHS = p = q_1^{w_1}\ldots q_r^{w_r}$

RHS should not be the product of two monic irreducible polynomials. So $RHS = q$, and $p = q$.

So we are done if $n = 1$.

Now suppose that this is true for products of factor than n monic, irreducible polynomials.

If $p_1^{e_1}p_2^{e^2}\ldots p_r^{e_r} = q_1^{w_1}\ldots q_r^{w_r}$ with $n = e_1 + e_2 + \ldots + e_r$, then p_1 is monic, irreducible, and $p_1|q_1^{w_1}\ldots q_r^{w_r}$

By the corollary, $p|q_j$ for some j. But the q_j are irreducible, so $p_1 = cq_j$ for some $c \in \mathbb{F}$.

Since p and q are monic, $c = 1$,

Therefore, $p_1 = q_j$. so $p_1^{e_1-1}p_2^{e^2}\ldots p_r^{e_r} = q_1^{w_1}\ldots q_j^{w_j-1}\ldots q_r^{e_r}$

By the induction hypothesis, the polynomials on the LHS are the same as the polynomials, on the RHS, up to the order.

By the induction, the representation is unique.

□

We've been looking at polynomials in $\mathbb{F}[x]$ where $\mathbb{F}$ is a field. What about polynomials in $\mathbb{Z}[x]$.

Irreducible polynomial in $\mathbb{Z}[x]$.

Question : When can $f(x) \in \mathbb{Z}[x]$ be factored (in $\mathbb{Z}[x]$).

A polynomial $f(x) \in \mathbb{Z}[x]$ is primitive if the gcd of the coefficients is 1. I.E. if there is no prime dividing all of the coefficients.

Lemma 3. *If f and $g \in \mathbb{Z}[x]$ are primitive, then so is $f \cdot g$.*

Proof. Let p be a prime, and $f(x) = \sum_{i=0}^{d} a_i x^i, a_i \in \mathbb{Z}$,
$f(x) = \sum_{i=0}^{e} b_i x^i, b_i \in \mathbb{Z}$,
By hypothesis, there is at least one i with $p \nmid b_i$. Let i be the smallest i such that $p \nmid b_i$.
Similarly, let j_0 be the least j such that $p \nmid a_j$.
Now, $fg = (\sum_{i=0}^{d} a_i x^i)(\sum_{i=0}^{d} b_i x^i) = \sum_{i=0}^{d+e}(\sum_{i+j=k} a_j b_i)x^k$.
Then coefficient of $x^{i_0+j_0}$ is $\sum_{i+j=i_0+j_0=k_0} a_j b_i$.
This $= (a_0 b_{k_0} + a_1 b_{k_0-1} + \ldots) + a_{j_0} b_{i_0} + (a_{j_0+1} b_{i_0-1} + \ldots + a_{k_0} b_0)$.
Therefore, this expression is not divisible by p.
So the coefficient of $x^{i_0+j_0}$ in $f \cdot g$ is not divisible by p.
Since p was any prime, $f \cdot g$ is primitive. □

Theorem 4. *Gauss Lemma : if $f(x) \in \mathbb{Z}[x]$ and f(x) is reducible in $\mathbb{Q}[x]$, then f(x) is reducible in $\mathbb{Z}[x]$.*

Proof. Let $f(x) \in \mathbb{Z}[x]$. and suppose that $f = gh$, for $g, h \in \mathbb{Q}[x]$, $deg(g), deg(h) < deg(f)$.
Choose $M, N \in \mathbb{Z}$ such that $Mg(x), Nh(x) \in \mathbb{Z}[x]$.
Also, of , os the gcd of the coefficients of $Mg(x)$, then $Mg(x) = mg_1(x)$,for $g_1(x) \in \mathbb{Z}[x]$ primitive.
Similarly, $Nh(x) = nh_1(x)$ where $h_1(x) \in \mathbb{Z}[x]$ is primitive.
Now, $g_1 h_1 \in \mathbb{Z}[x]$ is primitive, and $mn(g_1 h_1) = (mg_1(x))(nh_1(x)) = Mg(x)Nh(x) = MNf(x)$.
If d is the gcd of the coefficients of f, then $mn = MNd$.
$MNdg_1(x)h_1(x) = MNf(x)$
and so $(dg_1(x))(h_1(x)) = f(x)$. $dg_1(x), h_1(x) \in \mathbb{Z}[x]$.
(degrees haven't changed). □

Corollary 2. *Let $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$.,*
and suppose that
$f(\frac{b}{c}) = 0$, $b, c \in \mathbb{Z}, gcd(b, c) = 1$.
Then $c|a_d, b|a_0$.

Proof. Suppose that $f(\frac{b}{c}) = 0$. Then in $\mathbb{Q}[x]$, $(x - \frac{b}{c})|f(x)$.
So in fact there is some integer N such that if $N(x - \frac{b}{c}) \in \mathbb{Z}[x]$ is primitive and $N(x - \frac{b}{c})|f(x)$
So $(cx - b)|f(x)$ in $\mathbb{Z}[x]$.
That means $(cx - b)(g_e x^e + \ldots + g_0) = (a_d x^d + \ldots + a_0)(cg_e x^{e+1} + \ldots - bg_0) = (a_d x^d + \ldots + a_0)$.
So $a_0 = -bg_0$ Then $b|a_0, c|a_d$. □

Example :
Show that $f(x) = 3x^5 + 2x - 2$ has no rational roots.
Solution : If $f(\frac{b}{c}) = 0$, $\frac{b}{c} \in \mathbb{Q}$ in least terms.
The corollary says that $b|2, c|3$, b= $\pm 1, \pm 2$.
$c = \pm 1, \pm 3$.
Then list it,

None of these is a root.

Theorem 5. *Eisenstein's Criterion :*
Let $f(x)\mathbb{Z}[x]$.
$f(x) = \sum_{i=0}^{d} a_i x^i, a_i \in \mathbb{Z}, a_j \neq 0.$
If there is a prime p such that
1) $p \nmid a_d$.
2) $p|a_i$ *for* $0 \leq i < d$.
3) $p^2 \nmid a_0$.
Then f(x) is irreducible.

Example : $f(x) = 2x^{10} - 10x^3 + 5$
Is irreducible, since $5 \nmid 2, 5|10, 5|5, 5^2|5$.

Proof. Suppose f(x) is reducible and write $f(x) = g(x)h(x) = (\sum_{i=0}^{m} b_i x^i)(\sum_{j=0}^{n} c_j x^d)$.
$deg(g), deg(h) < deg(f), b_i, c_j \in \mathbb{Z}$.
$a_d = b_m c_n$ (assuming $m = deg(g), n = deg(h)$)
So $p \nmid b_m, p \nmid c_n$.
Also $a_0 = b_0 c_0$
So $p|b_0 c_0$ but $p^2 \nmid b_0 c_0$
Thus, exactly one of c_0, b_0 is divisible by p.
We will suppose that $p|b_0, p \nmid c_0$.
Let i_0 be the least value of i such that $p \nmid b_i$.
Look at a_{i_0}. $(i_0 \leq m < d)$.
By the assumption, $p|a_{i_0}$ since $i_0 < d$.
$a_{i_0} = \sum_{j+k=i_0} b_k c_j = b_{i_0} c_0 + b_{i_0 - 1} c_1 + \cdots + b_0 c_{i_0}$.
Divisible by p, since $p|b_i$ for $i < i_0$.
So $p|b_{i_0} c_0$ but $p \nmid b_{i_0}, p \nmid c_0$.
This is a contradiction, so $f(x)$ does not factor in $\mathbb{Q}[x]$.

□

2. Algebraic Numbers

A number $a \in \mathbb{C}$ is algebraic if there is some polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(a) = 0$.

Example : $\sqrt{2}$ is the positive solution to $x^2 - 2 = 0$.
If $f(x) \in \mathbb{Q}[x]$, the roots of f(x) (in $\mathbb{C}$ or in $\mathbb{R}$) are somehow described.
In terms of $\mathbb{Q}$, $f(x) = 10x^7 - 3x - 1$.
$f(a) = 0$.

If $a \in \mathbb{C}$ is not algebraic, then it is transcendental.

Theorem 6. *If* $a \in \mathbb{C}$ *us algebraic, then there is a unique monic polynomial* $f(x) \in \mathbb{Q}$ *such that* $f(a) = 0$ *and* $f(x)|g(x)$ *for any non-zero* $g(x) \in \mathbb{Q}[x]$ *such that* $g(a) = 0$.

Proof. We know that a is the root of some non-zero polynomial. Let f(x) be apolynomial of lowest degree in $\mathbb{Q}[x]$ which is monic, and $f(a) = 0$.

Suppose that $g(a) = 0$, for $g(x) \in \mathbb{Q}[x]$.

Write $g(x) = q(x)f(x) + r(x), q, r \in \mathbb{Q}[x]$ and $deg(r) < deg(f)$.

Then $0 = g(a) = q(a)f(a) + r(a) = r(a)$, since $f(a) = 0$.

If r(x) is not the zero polynomial then dividing by the leading coefficient, give a polynomial $r_2(x) \in \mathbb{Q}[x]$. which is monic, and $r_[2](a) = 0, deg(r_2) < deg(f)$.

It contradicts, so $r(x) = 0, g(x) = q(x)f(x)$.

In other words, $f(x)|g(x)$.

If $f_1(x), f_2(x)$ both have this property.

$f_2(a) = 0$ so

$f_1(x)|f_2)(x)$

$f_1(a) = 0, f_2(x)|f_1(x)$

This means that $f_1(x) = cf_2(x)$ for some non-zero $c \in \mathbb{Q}$.

But both are monic, $c = 1$. □

The polynomial in the theorem is the minimal polynomial for a.

Corollary 3. *If $a \in \mathbb{C}$ is the root of a polynomial $f(x) \in \mathbb{Q}[x]$ which is non-zero and irreducible, then a is irrational. (unless $deg(f) = 1$)*

Proof. If a is rational, then $(x - a)|f(x)$. (given that $f(a) = 0$).

So f(x) is not irreducible. □

Example :

$f(x) = x^n - 2 \in \mathbb{Q}[x]$ is irreducible by the Eisenstein's Criterion .

So if $n > 1$, then $2^{\frac{1}{n}} \notin \mathbb{Q}$.

Example :

$\sqrt{2} + \sqrt{3}$ is algebraic, but what is the minimal polynomial $f(x) \in \mathbb{Q}[x]$. such that $f(\sqrt{2} + \sqrt{3}) = 0$.

Solution 1. *Need some $a_d w^d + a_{d-1} w^{d-1} + \ldots + a_0 = 0, a_d \in \mathbb{Q}$.*

$w = \sqrt{2} + \sqrt{3}$

$w^2 = (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$.

$w^3 = 11\sqrt{2} + 9\sqrt{3}$.

$w^4 = 49 + 20\sqrt{6}$.

$w^4 - 10w^2 = (49 + 20\sqrt{6}) - 10(5 + 2\sqrt{6}) = -1$

$w^4 - 10w^2 + 1 = 0$.

$f(x) = x^4 - 10x^2 + 1$.

$f(w) = 0$.

Done but is f(x) the minimal polynomial?

If not, f(x) factors in $\mathbb{Z}[x]$.

If f(x) factors, then either it has a root in $\mathbb{Q}$, or else if factors as (quadratic)(quadratic).

By Gauss Lemma Corollary, the only possible roots of f(x) in $\mathbb{Q}$ are $x = \pm 1$.

f(x) has no root in $\mathbb{Q}$, so if it is reducible, it factors as $f(x) = x^4 - 10x^3 + 1 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a+c)x^3 + (d+b+ac)x^2 + (ad+bc)x + bd$.

There is no solution for this equation group.

3. Transcendental Numbers

$a \in \mathbb{C}$ is transcendental if and only if it is not algebraic.

Examples (without proof)

e, π ....

How do you show that specific number is transcendental?

Theorem 7. *Liouville : Suppose that $a \in \mathbb{R}$ is a root of the irreducible polynomial $f(x) \in \mathbb{Q}[x]$. Then there is a $\delta > 0$ such that $|a - \frac{p}{q}| > \frac{\delta}{q^d}$ for any rational number $\frac{p}{q} \in \mathbb{Q}$ in lowest terms $d = deg(f) > 1$.*

For any real number a, you can find rational $\frac{p}{q}$ with $|a - \frac{p}{q}|$ as small as you want.

For example, just cut off the decimal expression of a at some point.

$a = 1.362187...$, $\frac{p}{q} = 1.362187$

If I want $|a - \frac{p}{q}| < \varepsilon$, a algebraic and irrational.

$\frac{\delta}{q^d} < \ldots < \varepsilon$.

so $(\delta\varepsilon^{-1})^{\frac{1}{d}} < q$.

Proof. We have $f(x) \in \mathbb{Q}[x]$ of degree $d > 1$, irreducible. $f(a) = 0$.

Without loss of generality, $f(x) \in \mathbb{Z}[x]$.

so $f(x) = a_d x^d + \ldots + a_1 x + a_0, a_i \in \mathbb{Z}$.

What a lower bound on $|x - a|$ for $x \in \mathbb{Q}$.

If x is not in $[a-1, a+1]$, then $|x - a| > 1$.

On the other hand, if x is in $[a-1, a+1]$, then for some c in $[a-1, a+1]$ we have $|f(x)| = |f'(c)||x - a|$.

$|f'(c)| \leq M$ for c on the interval for some M.

$|x - a| \geq \frac{1}{M}|f(x)|$.

Now we want a lower bound on $|f(x)|$ for $x \in \mathbb{Q}$.

Write $x = \frac{p}{q}, p, q \in \mathbb{Z}$.

$f(\frac{p}{q}) = a_d \frac{p_d}{q_d} + \ldots + a_0$.

$q^d f(\frac{p}{q}) = a_d p^d + \ldots + a_{d-1} q p^{d-1} + \ldots + a_1 p q^{d-1} + a_0 q^d$.

So $q^d f(\frac{p}{q}) \in \mathbb{Z}$.

and it is not 0, so $|q^d f(\frac{p}{q})| \geq 1$.

$|f(\frac{p}{q})| \geq \frac{1}{q^d}$.

$|\frac{p}{q} - a| \geq \frac{1}{M} \cdot \frac{1}{q^d}$.

So if $\frac{p}{q}$ is not in $[a-1, a+1]$, $|a - \frac{p}{q}| > 1 \geq \frac{1}{q^d}$ and of $\frac{p}{q}$ is in $[a-1, a+1]$.

$|a - \frac{p}{q}| \geq \frac{M^{-1}}{q^d}$
So $|a - \frac{p}{q}| \geq \frac{min\{1,M^{-1}\}}{q^d} > \frac{min\{1,M^{-1}\}}{2q^d}$

□

Construction transcendental construct $a \in \mathbb{R}$ with very good approximation in $\mathbb{Q}$.

For $\frac{p}{q} \in \mathbb{Q}$, $|\sqrt{2} - \frac{p}{q}| > \frac{\delta}{q^2}$ for some $\delta > 0$.
Want to use this to show that certain numbers are transcendental.

Example : Let
$a = \sum_{m=1}^{\infty} 10^{-10!}$.
Then a is transcendental.

Proof. First of all, $a = \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^6} + \frac{1}{10^{24}} + \frac{1}{10^{120}} + \frac{1}{10^{720}} \ldots = 0.11000100...010...010....$
Point : the partial sums are rational numbers that are extremely close to a.
Let $\frac{p_n}{q_n} = \sum_{m=1}^{n} 10^{-10!} \in \mathbb{Q}$.
$q_n = 10^{n!}$
$p_n = \sum_{m=1}^{n} 10^{n!-m!} = 1 + 10^? + 10^? + \ldots.$
$\frac{p_1}{q_1} = \sum_{m=1}^{1} 10^{-m!} = \frac{1}{10}$.
$\frac{p_2}{q_2} = \sum_{m=1}^{2} 10^{-m!} = \frac{11}{100}$.
$\frac{p_3}{q_3} = \sum_{m=1}^{3} 10^{-m!} = \frac{110001}{1000000}$.
$|a - \frac{p_n}{q_n}| = |\sum_{m=1}^{\infty} 10^{-m!} - \sum_{m=1}^{n} 10^{-m!}| = \sum_{m=n+1}^{\infty} 10^{-m!} = 10^{-(n+1)!} + 10^{-(n+2)!} + \ldots < 2 \cdot 10^{-(n+1)!}$
$|a - \frac{p_n}{q_n}| < 2 \cdot 10^{-(n+1)!} = 2(10^{n! - (n+1)} = 2 \cdot q_n^{-(n+1)}$, for all n.
Now, suppose that a is algebraic. So
$f(a) = 0$. for some irreducible $f(x) \in \mathbb{Q}[x]$. of degree $d \geq 2$.
By Liouville's Theorem, there is a $\delta > 0$ such that $|a - \frac{p}{q}| > \frac{\delta}{q^d}$, for all $\frac{p}{q} \in \mathbb{Q}$.
So $\frac{\delta}{q_n^d} < |a - \frac{p_n}{q_n}| < \frac{2}{q_n^{n+1}}$.
So $\delta q_n^{n+1} < 2q_n^d$.
As soon as $n \geq d$, we get
$10^{-n!} = q_n \leq q_n^{n+1-d} < \frac{2}{\delta}$, for all $n \geq d$.
$\frac{2}{\delta}$ is some real numbers.
This is impossible. So a is not algebraic. □

Can use this to show that $\sum_{m=1}^{\infty} b^{-m!}$ is transcendental for any integer $b \geq 2$.
Lots of transcendental numbers.
e is transcendental.