Math 361

March 29, 2023

Quiz

1. Let R be a commutative ring with 1.
   (i) What does it mean to say $p \in R$ is *prime*.
   (ii) What does it mean to say an ideal P of R is *prime*?

2. How does the Smith normal form allow us to determine the structure of $\mathfrak{O}_K/\mathfrak{a}$ for an ideal $\mathfrak{a}$ in the number ring $\mathfrak{O}_K$?
   (i) What is the relevant commutative diagram that allows us to turn this question into a question about matrices?
   (ii) What is the size of $\mathfrak{O}_K/\mathfrak{a}$ in terms of this matrix?

Today

- Finish up Monday's work.
- $\mathfrak{O}_K$ is almost a PID always.
- Factoring rational primes in number rings having power bases.

Catch up

See Monday's slides.

gcds and lcms for ideals

Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in $\mathfrak{O}_K$.

gcds and lcms for ideals

Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in $\mathfrak{O}_K$.

Definition. $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$ if

gcds and lcms for ideals

Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in $\mathfrak{O}_K$.

Definition. $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$ if

- $\mathfrak{c}|\mathfrak{a}$ and $\mathfrak{c}|\mathfrak{b}$, and

gcds and lcms for ideals

Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in $\mathfrak{O}_K$.

Definition. $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$ if

- $\mathfrak{c}|\mathfrak{a}$ and $\mathfrak{c}|\mathfrak{b}$, and
- if $\mathfrak{d}$ is any ideal dividing $\mathfrak{a}$ and $\mathfrak{b}$, then $\mathfrak{d}|\mathfrak{c}$

gcds and lcms for ideals

Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in $\mathfrak{O}_K$.

Definition. $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$ if

- $\mathfrak{c}|\mathfrak{a}$ and $\mathfrak{c}|\mathfrak{b}$, and
- if $\mathfrak{d}$ is any ideal dividing $\mathfrak{a}$ and $\mathfrak{b}$, then $\mathfrak{d}|\mathfrak{c}$

$\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$

gcds and lcms for ideals

Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in $\mathfrak{O}_K$.

Definition. $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$ if

- $\mathfrak{c}|\mathfrak{a}$ and $\mathfrak{c}|\mathfrak{b}$, and
- if $\mathfrak{d}$ is any ideal dividing $\mathfrak{a}$ and $\mathfrak{b}$, then $\mathfrak{d}|\mathfrak{c}$

$\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$

Definition. $\mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$ if

gcds and lcms for ideals

Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in $\mathfrak{O}_K$.

Definition. $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$ if

- $\mathfrak{c}|\mathfrak{a}$ and $\mathfrak{c}|\mathfrak{b}$, and
- if $\mathfrak{d}$ is any ideal dividing $\mathfrak{a}$ and $\mathfrak{b}$, then $\mathfrak{d}|\mathfrak{c}$

$\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$

Definition. $\mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$ if

- $\mathfrak{a}|\mathfrak{c}$ and $\mathfrak{b}|\mathfrak{c}$, and

gcds and lcms for ideals

Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in $\mathfrak{O}_K$.

Definition. $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$ if

- $\mathfrak{c}|\mathfrak{a}$ and $\mathfrak{c}|\mathfrak{b}$, and
- if $\mathfrak{d}$ is any ideal dividing $\mathfrak{a}$ and $\mathfrak{b}$, then $\mathfrak{d}|\mathfrak{c}$

$\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$

Definition. $\mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$ if

- $\mathfrak{a}|\mathfrak{c}$ and $\mathfrak{b}|\mathfrak{c}$, and
- if $\mathfrak{d}$ is any ideal divisible by $\mathfrak{a}$ and $\mathfrak{b}$, then $\mathfrak{c}|\mathfrak{d}$

gcds and lcms for ideals

Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in $\mathcal{O}_K$.

Definition. $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$ if

- $\mathfrak{c}|\mathfrak{a}$ and $\mathfrak{c}|\mathfrak{b}$, and
- if $\mathfrak{d}$ is any ideal dividing $\mathfrak{a}$ and $\mathfrak{b}$, then $\mathfrak{d}|\mathfrak{c}$

$\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$

Definition. $\mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{c}$ if

- $\mathfrak{a}|\mathfrak{c}$ and $\mathfrak{b}|\mathfrak{c}$, and
- if $\mathfrak{d}$ is any ideal divisible by $\mathfrak{a}$ and $\mathfrak{b}$, then $\mathfrak{c}|\mathfrak{d}$

$\mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$

gcds and lcms for ideals

If we have factorizations into primes

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \quad \text{and} \quad \mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i},$$

(taking some $e_i = 0$ or $\ell_i = 0$, if necessary),

gcds and lcms for ideals

If we have factorizations into primes

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \quad \text{and} \quad \mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i},$$

(taking some $e_i = 0$ or $\ell_i = 0$, if necessary), then

$$\gcd(\mathfrak{a}, \mathfrak{b}) =$$

gcds and lcms for ideals

If we have factorizations into primes

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \quad \text{and} \quad \mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i},$$

(taking some $e_i = 0$ or $\ell_i = 0$, if necessary), then

$$\gcd(\mathfrak{a}, \mathfrak{b}) = \prod_{i=1}^{k} \mathfrak{p}_i^{\min\{e_i, \ell_i\}}$$

gcds and lcms for ideals

If we have factorizations into primes

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \quad \text{and} \quad \mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i},$$

(taking some $e_i = 0$ or $\ell_i = 0$, if necessary), then

$$\text{gcd}(\mathfrak{a}, \mathfrak{b}) = \prod_{i=1}^{k} \mathfrak{p}_i^{\min\{e_i,\ell_i\}} \quad \text{and} \quad \mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) =$$

gcds and lcms for ideals

If we have factorizations into primes

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \quad \text{and} \quad \mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i},$$

(taking some $e_i = 0$ or $\ell_i = 0$, if necessary), then

$$\gcd(\mathfrak{a}, \mathfrak{b}) = \prod_{i=1}^{k} \mathfrak{p}_i^{\min\{e_i, \ell_i\}} \quad \text{and} \quad \operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \prod_{i=1}^{k} \mathfrak{p}_i^{\max\{e_i, \ell_i\}}.$$

gcds and lcms for ideals

If we have factorizations into primes

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \quad \text{and} \quad \mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i},$$

(taking some $e_i = 0$ or $\ell_i = 0$, if necessary), then

$$\mathsf{gcd}(\mathfrak{a}, \mathfrak{b}) = \prod_{i=1}^{k} \mathfrak{p}_i^{\min\{e_i, \ell_i\}} \quad \text{and} \quad \mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) = \prod_{i=1}^{k} \mathfrak{p}_i^{\max\{e_i, \ell_i\}}.$$

In particular, if $\mathfrak{a}$ and $\mathfrak{b}$ relatively prime,
then $\mathfrak{a} + \mathfrak{b} = \mathsf{gcd}(\mathfrak{a}, \mathfrak{b}) = (1) = \mathfrak{O}_K$.

$\mathfrak{O}_K$ almost a PID

Theorem. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$, and let $0 \neq \beta \in \mathfrak{a}$. Then there exists $\alpha \in \mathfrak{O}_K$ such that

$$\mathfrak{a} = (\alpha, \beta).$$

Proof. We first prove a lemma (see the lecture notes and Lemma 5.19 in the text) saying that if $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero ideals of $\mathfrak{O}_K$, then there exists $\alpha \in \mathfrak{a}$ such that

$$\alpha\mathfrak{a}^{-1} + \mathfrak{b} = \mathfrak{O}_K.$$

$\mathfrak{O}_K$ almost a PID

Theorem. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$, and let $0 \neq \beta \in \mathfrak{a}$. Then there exists $\alpha \in \mathfrak{O}_K$ such that

$$\mathfrak{a} = (\alpha, \beta).$$

Proof. We first prove a lemma (see the lecture notes and Lemma 5.19 in the text) saying that if $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero ideals of $\mathfrak{O}_K$, then there exists $\alpha \in \mathfrak{a}$ such that

$$\alpha\mathfrak{a}^{-1} + \mathfrak{b} = \mathfrak{O}_K.$$

The result then follows by letting $\mathfrak{b} = \beta\mathfrak{a}^{-1}$.

$\mathfrak{O}_K$ almost a PID

Theorem. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$, and let $0 \neq \beta \in \mathfrak{a}$. Then there exists $\alpha \in \mathfrak{O}_K$ such that

$$\mathfrak{a} = (\alpha, \beta).$$

Proof. We first prove a lemma (see the lecture notes and Lemma 5.19 in the text) saying that if $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero ideals of $\mathfrak{O}_K$, then there exists $\alpha \in \mathfrak{a}$ such that

$$\alpha\mathfrak{a}^{-1} + \mathfrak{b} = \mathfrak{O}_K.$$

The result then follows by letting $\mathfrak{b} = \beta\mathfrak{a}^{-1}$. (Note that $\beta\mathfrak{a}^{-1}$ is an ideal since $\beta \in \mathfrak{a}$.)

Factorization of rational integers in number rings

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$. Last time, we saw that there exists a unique rational prime p such that $N(\mathfrak{p}) = p^f$ where $1 \leq f \leq n$. The integer f is called the *inertial degree* of $\mathfrak{p}$.

Factorization of rational integers in number rings

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$. Last time, we saw that there exists a unique rational prime p such that $N(\mathfrak{p}) = p^f$ where $1 \leq f \leq n$. The integer f is called the *inertial degree* of $\mathfrak{p}$.

Theorem (e_i-f_i theorem) Let p be a rational prime, and say $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ is the prime factorization of the ideal (p) in $\mathfrak{O}_K$. Then

$$\sum_{i=1}^{k} e_i f_i = n.$$

were f_i is the inertial degree of $\mathfrak{p}_i$ for each i and $n = [K : \mathbb{Q}]$.

Factorization of rational integers in number rings

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$. Last time, we saw that there exists a unique rational prime p such that $N(\mathfrak{p}) = p^f$ where $1 \leq f \leq n$. The integer f is called the *inertial degree* of $\mathfrak{p}$.

Theorem (e_i-f_i theorem) Let p be a rational prime, and say $(p) = \prod_{i=1}^k \mathfrak{p}_i^{e_i}$ is the prime factorization of the ideal (p) in $\mathfrak{O}_K$. Then

$$\sum_{i=1}^{k} e_i f_i = n.$$

were f_i is the inertial degree of $\mathfrak{p}_i$ for each i and $n = [K : \mathbb{Q}]$.

Proof.

$$p^n = N((p)) =$$

Factorization of rational integers in number rings

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$. Last time, we saw that there exists a unique rational prime p such that $N(\mathfrak{p}) = p^f$ where $1 \leq f \leq n$. The integer f is called the *inertial degree* of $\mathfrak{p}$.

Theorem (e_i-f_i theorem) Let p be a rational prime, and say $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ is the prime factorization of the ideal (p) in $\mathfrak{O}_K$. Then

$$\sum_{i=1}^{k} e_i f_i = n.$$

were f_i is the inertial degree of $\mathfrak{p}_i$ for each i and $n = [K : \mathbb{Q}]$.

Proof.

$$p^n = N((p)) = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{e_i} =$$

Factorization of rational integers in number rings

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$. Last time, we saw that there exists a unique rational prime p such that $N(\mathfrak{p}) = p^f$ where $1 \leq f \leq n$. The integer f is called the *inertial degree* of $\mathfrak{p}$.

Theorem (e_i-f_i theorem) Let p be a rational prime, and say $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ is the prime factorization of the ideal (p) in $\mathfrak{O}_K$. Then

$$\sum_{i=1}^{k} e_i f_i = n.$$

were f_i is the inertial degree of $\mathfrak{p}_i$ for each i and $n = [K : \mathbb{Q}]$.

Proof.

$$p^n = N((p)) = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{e_i} = \prod_{i=1}^{k} p^{f_i e_i} = p^{\sum_{i=1}^{k} e_i f_i}.$$

Factorization of rational integers in number rings

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$. Last time, we saw that there exists a unique rational prime p such that $N(\mathfrak{p}) = p^f$ where $1 \leq f \leq n$. The integer f is called the *inertial degree* of $\mathfrak{p}$.

Theorem (e_i-f_i theorem) Let p be a rational prime, and say $(p) = \prod_{i=1}^k \mathfrak{p}_i^{e_i}$ is the prime factorization of the ideal (p) in $\mathfrak{O}_K$. Then

$$\sum_{i=1}^{k} e_i f_i = n.$$

were f_i is the inertial degree of $\mathfrak{p}_i$ for each i and $n = [K : \mathbb{Q}]$.

Proof.

$$p^n = N((p)) = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{e_i} = \prod_{i=1}^{k} p^{f_i e_i} = p^{\sum_{i=1}^{k} e_i f_i}.$$

Equate coefficients. $\square$

Factorization of rational integers in number rings

Say $K = \mathbb{Q}(\theta)$ and $\mathfrak{O}_K = \mathbb{Z}[\theta]$.

Factorization of rational integers in number rings

Say $K = \mathbb{Q}(\theta)$ and $\mathfrak{O}_K = \mathbb{Z}[\theta]$. Suppose that p is a rational prime, and let f be the minimal polynomial for θ over $\mathbb{Q}$.

Factorization of rational integers in number rings

Say $K = \mathbb{Q}(\theta)$ and $\mathfrak{O}_K = \mathbb{Z}[\theta]$. Suppose that p is a rational prime, and let f be the minimal polynomial for θ over $\mathbb{Q}$.
Suppose that

$$\overline{f} = \prod_{i=1}^{k} \overline{f}_i^{e_i}$$

is the factorization of f as an element of $\mathbb{F}_p[x]$ into monic irreducibles $\overline{f}_i$ (where $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$).

Factorization of rational integers in number rings

Say $K = \mathbb{Q}(\theta)$ and $\mathfrak{O}_K = \mathbb{Z}[\theta]$. Suppose that p is a rational prime, and let f be the minimal polynomial for θ over $\mathbb{Q}$.
Suppose that

$$\overline{f} = \prod_{i=1}^{k} \overline{f}_i^{e_i}$$

is the factorization of f as an element of $\mathbb{F}_p[x]$ into monic irreducibles $\overline{f}_i$ (where $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$). Let $\mathfrak{p}_i = (p, f_i(\theta))$ for $i = 1, \ldots, k$.

Factorization of rational integers in number rings

Say $K = \mathbb{Q}(\theta)$ and $\mathfrak{O}_K = \mathbb{Z}[\theta]$. Suppose that p is a rational prime, and let f be the minimal polynomial for θ over $\mathbb{Q}$.
Suppose that

$$\overline{f} = \prod_{i=1}^{k} \overline{f}_i^{e_i}$$

is the factorization of f as an element of $\mathbb{F}_p[x]$ into monic irreducibles $\overline{f}_i$ (where $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$). Let $\mathfrak{p}_i = (p, f_i(\theta))$ for $i = 1, \ldots, k$. Then each $\mathfrak{p}_i$ is prime

Factorization of rational integers in number rings

Say $K = \mathbb{Q}(\theta)$ and $\mathfrak{O}_K = \mathbb{Z}[\theta]$. Suppose that p is a rational prime, and let f be the minimal polynomial for θ over $\mathbb{Q}$.
Suppose that

$$\overline{f} = \prod_{i=1}^{k} \overline{f}_i^{e_i}$$

is the factorization of f as an element of $\mathbb{F}_p[x]$ into monic irreducibles $\overline{f}_i$ (where $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$). Let $\mathfrak{p}_i = (p, f_i(\theta))$ for $i = 1, \ldots, k$. Then each $\mathfrak{p}_i$ is prime and

$$(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}$$

is the prime factorization of (p) in $\mathfrak{O}_K$.

Examples

Consider the case $K = \mathbb{Q}(\sqrt{-6})$.

Examples

Consider the case $K = \mathbb{Q}(\sqrt{-6})$.

How do (2), (5), (10), and (7) factor into primes in $\mathfrak{O}_K$?

Proof of theorem

Proof of Theorem.

Proof of theorem

Proof of Theorem. We have the surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x]$$

Proof of theorem

Proof of Theorem. We have the surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_i)$$

Proof of theorem

Proof of Theorem. We have the surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$$

Proof of theorem

Proof of Theorem. We have the surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$$

and f is in the kernel.

Proof of theorem

Proof of Theorem. We have the surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$$

and f is in the kernel. So we get a well-defined surjection

$$\mathbb{Z}[x]/(f) \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i).$$

.

Proof of theorem

Proof of Theorem. We have the surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$$

and f is in the kernel. So we get a well-defined surjection

$$\phi_i \colon \mathbb{Z}[\theta] \simeq \mathbb{Z}[x]/(f) \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i).$$

.

Proof of theorem

Proof of Theorem. We have the surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$$

and f is in the kernel. So we get a well-defined surjection

$$\phi_i \colon \mathbb{Z}[\theta] \simeq \mathbb{Z}[x]/(f) \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i).$$

Hence, $\mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$.

.

Proof of theorem

Proof of Theorem. We have the surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$$

and f is in the kernel. So we get a well-defined surjection

$$\phi_i \colon \mathbb{Z}[\theta] \simeq \mathbb{Z}[x]/(f) \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i).$$

Hence, $\mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$. Now f_i irreducible $\Rightarrow (f_i)$ maximal in $\mathbb{F}_p[x]$

.

Proof of theorem

Proof of Theorem. We have the surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$$

and f is in the kernel. So we get a well-defined surjection

$$\phi_i \colon \mathbb{Z}[\theta] \simeq \mathbb{Z}[x]/(f) \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i).$$

Hence, $\mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$. Now f_i irreducible $\Rightarrow (f_i)$ maximal in $\mathbb{F}_p[x] \Rightarrow \mathbb{F}_p[x]/(f_i)$ is a field

.

Proof of theorem

Proof of Theorem. We have the surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$$

and f is in the kernel. So we get a well-defined surjection

$$\phi_i \colon \mathbb{Z}[\theta] \simeq \mathbb{Z}[x]/(f) \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i).$$

Hence, $\mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$. Now f_i irreducible $\Rightarrow (f_i)$ maximal in $\mathbb{F}_p[x] \Rightarrow \mathbb{F}_p[x]/(f_i)$ is a field $\Rightarrow \ker(\phi_i)$ maximal.

.

Proof of theorem

Proof of Theorem. We have the surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$$

and f is in the kernel. So we get a well-defined surjection

$$\phi_i \colon \mathbb{Z}[\theta] \simeq \mathbb{Z}[x]/(f) \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i).$$

Hence, $\mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$. Now f_i irreducible $\Rightarrow (f_i)$ maximal in $\mathbb{F}_p[x] \Rightarrow \mathbb{F}_p[x]/(f_i)$ is a field $\Rightarrow \ker(\phi_i)$ maximal. However, $\ker(\phi_i) = (p, f_i(\theta))$.

Proof of theorem

Proof of Theorem. We have the surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$$

and f is in the kernel. So we get a well-defined surjection

$$\phi_i \colon \mathbb{Z}[\theta] \simeq \mathbb{Z}[x]/(f) \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i).$$

Hence, $\mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$. Now f_i irreducible $\Rightarrow (f_i)$ maximal in $\mathbb{F}_p[x] \Rightarrow \mathbb{F}_p[x]/(f_i)$ is a field $\Rightarrow \ker(\phi_i)$ maximal. However, $\ker(\phi_i) = (p, f_i(\theta))$. Therefore, $(p, f_i(\theta))$ is prime in $\mathbb{Z}[\theta]$.

Proof of theorem

We claim the $\mathfrak{p}_i := (p, f_i(\theta))$ for $i = 1, \ldots, k$ are distinct.

Proof of theorem

We claim the $\mathfrak{p}_i := (p, f_i(\theta))$ for $i = 1, \ldots, k$ are distinct.

If $(p, f_i(\theta)) = (p, f_j(\theta))$, then

Proof of theorem

We claim the $\mathfrak{p}_i := (p, f_i(\theta))$ for $i = 1, \ldots, k$ are distinct.

If $(p, f_i(\theta)) = (p, f_j(\theta))$, then

$$f_j(\theta) \in (p, f_i(\theta)) \in \ker(\phi_i)$$

Proof of theorem

We claim the $\mathfrak{p}_i := (p, f_i(\theta))$ for $i = 1, \ldots, k$ are distinct.

If $(p, f_i(\theta)) = (p, f_j(\theta))$, then

$$f_j(\theta) \in (p, f_i(\theta)) \in \ker(\phi_i) \Rightarrow \phi_i(f_j) = 0$$

Proof of theorem

We claim the $\mathfrak{p}_i := (p, f_i(\theta))$ for $i = 1, \ldots, k$ are distinct.

If $(p, f_i(\theta)) = (p, f_j(\theta))$, then

$$f_j(\theta) \in (p, f_i(\theta)) \in \ker(\phi_i) \Rightarrow \phi_i(f_j) = 0 \Rightarrow f_j(x) \in (p, f_i).$$

Proof of theorem

We claim the $\mathfrak{p}_i := (p, f_i(\theta))$ for $i = 1, \ldots, k$ are distinct.

If $(p, f_i(\theta)) = (p, f_j(\theta))$, then

$$f_j(\theta) \in (p, f_i(\theta)) \in \ker(\phi_i) \Rightarrow \phi_i(f_j) = 0 \Rightarrow f_j(x) \in (p, f_i).$$

So $f_j = hf_i \bmod p$,

Proof of theorem

We claim the $\mathfrak{p}_i := (p, f_i(\theta))$ for $i = 1, \ldots, k$ are distinct.

If $(p, f_i(\theta)) = (p, f_j(\theta))$, then

$$f_j(\theta) \in (p, f_i(\theta)) \in \ker(\phi_i) \Rightarrow \phi_i(f_j) = 0 \Rightarrow f_j(x) \in (p, f_i).$$

So $f_j = hf_i \bmod p$, i.e., $f_j = hf_i$ in $\mathbb{F}_p[x]$.

Proof of theorem

We claim the $\mathfrak{p}_i := (p, f_i(\theta))$ for $i = 1, \ldots, k$ are distinct.

If $(p, f_i(\theta)) = (p, f_j(\theta))$, then

$$f_j(\theta) \in (p, f_i(\theta)) \in \ker(\phi_i) \Rightarrow \phi_i(f_j) = 0 \Rightarrow f_j(x) \in (p, f_i).$$

So $f_j = hf_i \bmod p$, i.e., $f_j = hf_i$ in $\mathbb{F}_p[x]$. However, f_j is irreducible.

Proof of theorem

We claim the $\mathfrak{p}_i := (p, f_i(\theta))$ for $i = 1, \ldots, k$ are distinct.

If $(p, f_i(\theta)) = (p, f_j(\theta))$, then

$$f_j(\theta) \in (p, f_i(\theta)) \in \ker(\phi_i) \Rightarrow \phi_i(f_j) = 0 \Rightarrow f_j(x) \in (p, f_i).$$

So $f_j = hf_i \bmod p$, i.e., $f_j = hf_i$ in $\mathbb{F}_p[x]$. However, f_j is irreducible. So h is a unit, i.e., a constant in $\mathbb{F}_p$.

Proof of theorem

We claim the $\mathfrak{p}_i := (p, f_i(\theta))$ for $i = 1, \ldots, k$ are distinct.

If $(p, f_i(\theta)) = (p, f_j(\theta))$, then

$$f_j(\theta) \in (p, f_i(\theta)) \in \ker(\phi_i) \Rightarrow \phi_i(f_j) = 0 \Rightarrow f_j(x) \in (p, f_i).$$

So $f_j = hf_i \bmod p$, i.e., $f_j = hf_i$ in $\mathbb{F}_p[x]$. However, f_j is irreducible. So h is a unit, i.e., a constant in $\mathbb{F}_p$. Since f_i and f_j are monic, $h = 1$.

Proof of theorem

We claim the $\mathfrak{p}_i := (p, f_i(\theta))$ for $i = 1, \ldots, k$ are distinct.

If $(p, f_i(\theta)) = (p, f_j(\theta))$, then

$$f_j(\theta) \in (p, f_i(\theta)) \in \ker(\phi_i) \Rightarrow \phi_i(f_j) = 0 \Rightarrow f_j(x) \in (p, f_i).$$

So $f_j = hf_i \bmod p$, i.e., $f_j = hf_i$ in $\mathbb{F}_p[x]$. However, f_j is irreducible. So h is a unit, i.e., a constant in $\mathbb{F}_p$. Since f_i and f_j are monic, $h = 1$. Done.

Proof of theorem

We now show that

$$(p) = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}.$$

Proof of theorem

We now show that

$$(p) = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}.$$

We use the fact that for ideals in $\mathfrak{O}_K$,

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{bc}.$$

Proof of theorem

We now show that

$$(p) = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}.$$

We use the fact that for ideals in $\mathfrak{O}_K$,

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{b}\mathfrak{c}.$$

$\prod_{i=1}^{k} (p, f_i(\theta))^{e_i} =$

Proof of theorem

We now show that

$$(p) = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}.$$

We use the fact that for ideals in $\mathfrak{O}_K$,

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{b}\mathfrak{c}.$$

$\prod_{i=1}^{k} (p, f_i(\theta))^{e_i} = \prod_{i=1}^{k} \left((p) + (f_i(\theta))\right)^{e_i}$

Proof of theorem

We now show that

$$(p) = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}.$$

We use the fact that for ideals in $\mathfrak{O}_K$,

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{b}\mathfrak{c}.$$

$\prod_{i=1}^{k}(p, f_i(\theta))^{e_i} = \prod_{i=1}^{k}\left((p) + (f_i(\theta))\right)^{e_i} \subseteq \prod_{i=1}^{k}((p) + (f_i(\theta)^{e_i}))$

Proof of theorem

We now show that

$$(p) = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}.$$

We use the fact that for ideals in $\mathfrak{O}_K$,

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{b}\mathfrak{c}.$$

$$\prod_{i=1}^{k} (p, f_i(\theta))^{e_i} = \prod_{i=1}^{k} \left((p) + (f_i(\theta))\right)^{e_i} \subseteq \prod_{i=1}^{k} ((p) + (f_i(\theta)^{e_i}))$$
$$\subseteq (p) + \left(\prod_{i=1}^{k} f_i(\theta)^{e_i}\right) =$$

Proof of theorem

We now show that

$$(p) = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}.$$

We use the fact that for ideals in $\mathfrak{O}_K$,

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{b}\mathfrak{c}.$$

$$\textstyle\prod_{i=1}^{k}(p, f_i(\theta))^{e_i} = \prod_{i=1}^{k} \left((p) + (f_i(\theta))\right)^{e_i} \subseteq \prod_{i=1}^{k}((p) + (f_i(\theta)^{e_i}))$$
$$\subseteq (p) + \left(\textstyle\prod_{i=1}^{k} f_i(\theta)^{e_i}\right) = (p) + (f(\theta)) =$$

Proof of theorem

We now show that

$$(p) = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}.$$

We use the fact that for ideals in $\mathfrak{O}_K$,

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{b}\mathfrak{c}.$$

$$\begin{aligned}\textstyle\prod_{i=1}^{k}(p, f_i(\theta))^{e_i} = \prod_{i=1}^{k} \left((p) + (f_i(\theta))\right)^{e_i} &\subseteq \textstyle\prod_{i=1}^{k}((p) + (f_i(\theta)^{e_i})) \\ \subseteq (p) + \left(\textstyle\prod_{i=1}^{k} f_i(\theta)^{e_i}\right) = (p) + (f(\theta)) = (p).\end{aligned}$$

Proof of theorem

We now show that

$$(p) = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}.$$

We use the fact that for ideals in $\mathfrak{O}_K$,

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{b}\mathfrak{c}.$$

$$\prod_{i=1}^{k}(p, f_i(\theta))^{e_i} = \prod_{i=1}^{k} \left((p) + (f_i(\theta))\right)^{e_i} \subseteq \prod_{i=1}^{k}((p) + (f_i(\theta)^{e_i}))$$
$$\subseteq (p) + \left(\prod_{i=1}^{k} f_i(\theta)^{e_i}\right) = (p) + (f(\theta)) = (p).$$

So (p) divides $\prod_{i=1}^{k}(p, f_i(\theta))^{e_i} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$.

Proof of theorem

We now show that

$$(p) = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}.$$

We use the fact that for ideals in $\mathfrak{O}_K$,

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{b}\mathfrak{c}.$$

$$\begin{aligned} \textstyle\prod_{i=1}^{k}(p, f_i(\theta))^{e_i} &= \textstyle\prod_{i=1}^{k} \left((p) + (f_i(\theta))\right)^{e_i} \subseteq \prod_{i=1}^{k}((p) + (f_i(\theta)^{e_i})) \\ &\subseteq (p) + \left(\textstyle\prod_{i=1}^{k} f_i(\theta)^{e_i}\right) = (p) + (f(\theta)) = (p). \end{aligned}$$

So (p) divides $\prod_{i=1}^{k}(p, f_i(\theta))^{e_i} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$.

Hence, $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$ for some $0 \le \ell_i \le e_i$.

Proof of theorem

We have $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$ for some $0 \leq \ell_i \leq e_i$.

Proof of theorem

We have $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$ for some $0 \leq \ell_i \leq e_i$. Take norms:

Proof of theorem

We have $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$ for some $0 \le \ell_i \le e_i$. Take norms:

$$N(\mathfrak{p}_i) = |\mathbb{Z}[\theta]/\mathfrak{p}_i|$$

Proof of theorem

We have $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$ for some $0 \leq \ell_i \leq e_i$. Take norms:

$$N(\mathfrak{p}_i) = |\mathbb{Z}[\theta]/\mathfrak{p}_i|$$

and

$$\mathbb{Z}[\theta]/\mathfrak{p}_i = \mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i).$$

Proof of theorem

We have $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$ for some $0 \leq \ell_i \leq e_i$. Take norms:

$$N(\mathfrak{p}_i) = |\mathbb{Z}[\theta]/\mathfrak{p}_i|$$

and

$$\mathbb{Z}[\theta]/\mathfrak{p}_i = \mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i).$$

The elements of $\mathbb{F}_p[x]/(f_i)$ are exactly $a_0 + a_1 x + \cdots + a_{d_i-1}x^{d_i-1}$ where the a_i are $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $d_i = \deg(f_i)$.

Proof of theorem

We have $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$ for some $0 \leq \ell_i \leq e_i$. Take norms:

$$N(\mathfrak{p}_i) = |\mathbb{Z}[\theta]/\mathfrak{p}_i|$$

and

$$\mathbb{Z}[\theta]/\mathfrak{p}_i = \mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i).$$

The elements of $\mathbb{F}_p[x]/(f_i)$ are exactly $a_0 + a_1x + \cdots + a_{d_i-1}x^{d_i-1}$ where the a_i are $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $d_i = \deg(f_i)$. Therefore, $|\mathbb{F}_p[x]/(f_i)| = p^{\deg(f_i)}$.

Proof of theorem

We have $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$ for some $0 \leq \ell_i \leq e_i$. Take norms:

$$N(\mathfrak{p}_i) = |\mathbb{Z}[\theta]/\mathfrak{p}_i|$$

and

$$\mathbb{Z}[\theta]/\mathfrak{p}_i = \mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i).$$

The elements of $\mathbb{F}_p[x]/(f_i)$ are exactly $a_0 + a_1 x + \cdots + a_{d_i-1}x^{d_i-1}$ where the a_i are $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $d_i = \deg(f_i)$. Therefore, $|\mathbb{F}_p[x]/(f_i)| = p^{\deg(f_i)}$. It follows that

$$p^n = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{\ell_i} = \prod_{i=1}^{k} p^{\deg(f_i)\ell_i} = p^{\sum_{i=1}^{k} \deg(f_i)\ell_i},$$

Proof of theorem

We have $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$ for some $0 \leq \ell_i \leq e_i$. Take norms:

$$N(\mathfrak{p}_i) = |\mathbb{Z}[\theta]/\mathfrak{p}_i|$$

and

$$\mathbb{Z}[\theta]/\mathfrak{p}_i = \mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i).$$

The elements of $\mathbb{F}_p[x]/(f_i)$ are exactly $a_0 + a_1 x + \cdots + a_{d_i-1}x^{d_i-1}$ where the a_i are $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $d_i = \deg(f_i)$. Therefore, $|\mathbb{F}_p[x]/(f_i)| = p^{\deg(f_i)}$. It follows that

$$p^n = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{\ell_i} = \prod_{i=1}^{k} p^{\deg(f_i)\ell_i} = p^{\sum_{i=1}^{k}\deg(f_i)\ell_i},$$

and hence $n = \sum_{i=1}^{k} \deg(f_i)\ell_i$.

Proof of theorem

We have $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$ for some $0 \leq \ell_i \leq e_i$. Take norms:

$$N(\mathfrak{p}_i) = |\mathbb{Z}[\theta]/\mathfrak{p}_i|$$

and

$$\mathbb{Z}[\theta]/\mathfrak{p}_i = \mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i).$$

The elements of $\mathbb{F}_p[x]/(f_i)$ are exactly $a_0 + a_1 x + \cdots + a_{d_i-1}x^{d_i-1}$ where the a_i are $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $d_i = \deg(f_i)$. Therefore, $|\mathbb{F}_p[x]/(f_i)| = p^{\deg(f_i)}$. It follows that

$$p^n = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{\ell_i} = \prod_{i=1}^{k} p^{\deg(f_i)\ell_i} = p^{\sum_{i=1}^{k} \deg(f_i)\ell_i},$$

and hence $n = \sum_{i=1}^{k} \deg(f_i)\ell_i$. On the other hand, $f = \prod_{i=1}^{k} f_i^{e_i}$ implies $n = \deg(f) =$

Proof of theorem

We have $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$ for some $0 \leq \ell_i \leq e_i$. Take norms:

$$N(\mathfrak{p}_i) = |\mathbb{Z}[\theta]/\mathfrak{p}_i|$$

and

$$\mathbb{Z}[\theta]/\mathfrak{p}_i = \mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i).$$

The elements of $\mathbb{F}_p[x]/(f_i)$ are exactly $a_0 + a_1 x + \cdots + a_{d_i-1}x^{d_i-1}$ where the a_i are $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $d_i = \deg(f_i)$. Therefore, $|\mathbb{F}_p[x]/(f_i)| = p^{\deg(f_i)}$. It follows that

$$p^n = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{\ell_i} = \prod_{i=1}^{k} p^{\deg(f_i)\ell_i} = p^{\sum_{i=1}^{k} \deg(f_i)\ell_i},$$

and hence $n = \sum_{i=1}^{k} \deg(f_i)\ell_i$. On the other hand, $f = \prod_{i=1}^{k} f_i^{e_i}$ implies $n = \deg(f) = \sum_{i=1}^{k} \deg(f_i)e_i$.

Proof of theorem

We have $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$ for some $0 \leq \ell_i \leq e_i$. Take norms:

$$N(\mathfrak{p}_i) = |\mathbb{Z}[\theta]/\mathfrak{p}_i|$$

and

$$\mathbb{Z}[\theta]/\mathfrak{p}_i = \mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i).$$

The elements of $\mathbb{F}_p[x]/(f_i)$ are exactly $a_0 + a_1 x + \cdots + a_{d_i-1}x^{d_i-1}$ where the a_i are $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $d_i = \deg(f_i)$. Therefore, $|\mathbb{F}_p[x]/(f_i)| = p^{\deg(f_i)}$. It follows that

$$p^n = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{\ell_i} = \prod_{i=1}^{k} p^{\deg(f_i)\ell_i} = p^{\sum_{i=1}^{k} \deg(f_i)\ell_i},$$

and hence $n = \sum_{i=1}^{k} \deg(f_i)\ell_i$. On the other hand, $f = \prod_{i=1}^{k} f_i^{e_i}$ implies $n = \deg(f) = \sum_{i=1}^{k} \deg(f_i)e_i$. Since $0 \leq \ell_i \leq e_i$, we must have $\ell_i = e_i$ for all i. $\square$