1.1. Algebraic number theory. (LC 310)

Question. (Fermat, Euler, Gauss, ...)

Which integers are sums of two squares?

$x = a^2 + b^2$. ~~need, only positive answers~~

$0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 20, \ldots$

Observations.

(1) Only positive numbers.

("Obvious" but significant.)

(2) Must be $0, 1,$ or $2 \bmod 4$.

Why? mod 4,

$$a^2 + b^2 = (0 \text{ or } 1) + (0 \text{ or } 1) = 0, 1, \text{ or } 2.$$

(3) This isn't enough.

Proposition. If x and y are sums of two squares then so is $x \cdot y$.

Proof. $$(a^2 + b^2) \cdot (c^2 + d^2) = (ac - bd)^2 + (bc + ad)^2.$$

FOIL both sides and check it. Q.E.D.!

This proof sucks. Here's a better proof.

$$(a^2 + b^2) = (a + ib)(a - ib)$$

So $$\text{LHS} = (a + ib)(c + id) \cdot (a - ib)(c - id)$$

$$= ([ac - bd] + i[ad + bc]) \cdot \text{conjugate}$$

$$= \text{above}.$$

In other words, $a^2 + b^2$ is the norm form of $\mathbb{Z}[i]/\mathbb{Z}$.

1.2.

Given $x \in \mathbb{Z}$, write $x = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$.

If each p_i is a sum of squares, so is x.

Claim. This is an if and only if.

Why? Use the facts that:

* $\mathbb{Z}[i]$ is a PID (has a Euclidean algorithm) and hence a UFD.
* Being a sum of two squares is equivalent to being a norm from $\mathbb{Z}[i]$.
* Norms are multiplicative

Basically. Write x as a product of primes of $\mathbb{Z}[i]$.

$$x = (a_1 + ib_1)^{f_1} (a_2 + ib_2)^{f_2} \cdots (a_s + ib_s)^{f_3}$$
$$\times (a_1 - ib_1)^{g_1} \cdots\cdots (a_s - ib_s)^{g_s}.$$

Because LHS is invariant under the automorphism $i \to -i$, so is RHS, and RHS is uniquely detemined.

But. Unique factorization is up to the unit group

$$\mathbb{Z}[i]^\times = \{a + bi : a^2 + b^2 = 1\} = \{\pm 1, \pm i\}.$$

HW. Deal with the technicalities.

We can reduce this to the case of primes. There are three possibilities:

(1) $p = (a+bi)(a-bi)$ in $\mathbb{Z}[i]$ where $a \pm bi$ are prime, and have norm p.

Why do we know we can't factor further?

Take norms: $p^2 = p \cdot p$. ("splitting")

1.3.

(2) $p = (a+bi)^2$, same ideal twice.

Here we are really interested in the ideals.

e.g. we have $2 = (1+i)(1-i)$,

but $1+i = i \cdot (1-i)$,

so as a factorization of ideals we have

$$(2) = ((1+i))^2. \qquad (\text{"ramification"})$$

Here all ideals are principal.

units – annoying.

"class group" – also annoying. will appear later.

(3) p remains prime in $\mathbb{Z}[i]$. ("inertia")

In general we will be interested in

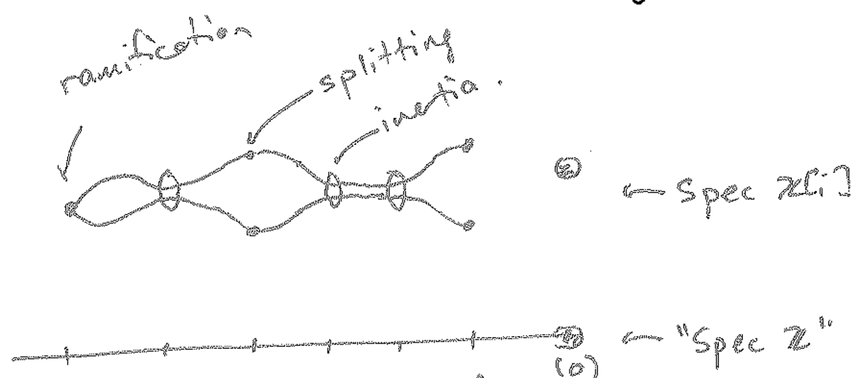
$$\begin{array}{cccl} K & - & \mathcal{O}_K = \text{"ring of integers"} & \text{some product of prime ideals} \\ | & & & \quad | \\ \mathbb{Q} & - & \mathbb{Z} & \quad p \end{array}$$

Will see. $\mathcal{O}_K$ is a Dedekind domain:

It is not a UFD, but ideals have UF into prime ideals.

Will see that the three behaviors described above govern what can happen.

Snobby Highbrow Picture.



1.4. The big theorem.

<u>Theorem.</u> p <u>splits</u> in $\mathbb{Z}[i]$ if $p \equiv 1 \mod 4$

p is <u>inert</u> in $\mathbb{Z}[i]$ if $p \equiv 3 \mod 4$

p <u>ramifies</u> in $\mathbb{Z}[i]$ if $p = 2$.

So nice! So simple! First case of <u>Artin reciprocity</u>.

How do we prove this?

$p = 2$ we already saw.

$p \equiv 3 \pmod 4$ we also already saw.

If p is a norm we would have

$$p = a^2 + b^2 \equiv 3 \mod 4$$

but $a^2, b^2 \equiv 0, 1 \mod 4$.

We say that there is a <u>local obstruction at 2</u>.

$a^2 + b^2$ does <u>not</u> have a solution in $\mathbb{Z}/4$

If it had a solution in $\mathbb{Z}$ it would reduce to a solution in $\mathbb{Z}/4$.

We can also say it does not have a solution in $\mathbb{Z}_2$ (2-adic integers)

or even $\mathbb{Q}_2$ (2-adic numbers)

and we will see

$$\underbrace{\mathbb{Q}(x)/(x^2+1)}_{\text{This is the same as } \mathbb{Q}(i)\text{!!}} \otimes \mathbb{Q}_p = \begin{cases} \text{a } \underline{\text{field}} \text{ if } p \text{ is inert or ramifies} \\ \mathbb{Q}_p \oplus \mathbb{Q}_p \text{ if } p \text{ is split.} \end{cases}$$

<u>Hasse – Minkowski Theorem.</u>

A quadratic form has a solution $/\mathbb{Q}$

$\Longleftrightarrow$ has a solution over $\mathbb{Q}_p$ for every p.

HW. For any n, and any $p \neq 2$, $a^2 + b^2 \equiv n \pmod{p^k}$ has a solution.

1.5. So how do we prove splitting?

Lemma. If $p \equiv 1 \pmod 4$ then the congruence $x^2 + 1 \equiv 0 \pmod p$ has a solution.

This is much easier.

Proof. Wilson's Theorem says that $(p-1)! \equiv -1 \pmod p$
(Ex. prove this)

and so (writing $p = 1 + 4n$)

$$
\begin{aligned}
-1 \equiv (p-1)! &= [1 \cdot 2 \cdot \cdots (2n)][(p-1)(p-2)\cdots(p-2n)] \\
&= (2n)! \cdot (-1)^{2n}(2n)! \\
&= [(2n)!]^2 .
\end{aligned}
$$

Alternate proof. $(\mathbb{Z}/p)^\times$ is a cyclic group.

We have

$$(\mathbb{Z}/p)^\times, \times) \xrightarrow{\sim} (\mathbb{Z}/(p-1), +).$$

$$-1 \longrightarrow \frac{p-1}{2}.$$

So -1 is something squared iff $p \equiv 1 \mod 4$.

Now this says $p \mid n^2 + 1$

$$= (n+i)(n-i).$$

But $\frac{n}{p} \pm \frac{i}{p}$ is not in $\mathbb{Z}[i]$, so p cannot be prime in this ring.

ANT. 2.1. The basic setup.

Def. A *number field* is a finite extension of $\mathbb{Q}$.

Fact. If K is a NF, then $K = \mathbb{Q}(\alpha)$ for some algebraic α.

We can also write $K = \mathbb{Q}(x)/(f(x))$ where $f(x)$ is the min. poly. of α.

Note. This is not obvious.

For example, there is a primitive element for $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

This is a *biquadratic* field with $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2)^2$ and, e.g. $\sqrt{2} + \sqrt{3}$ generates it over $\mathbb{Q}$.

Def. Let $K/\mathbb{Q}$ be a number field. The *ring of integers* $\mathcal{O}_K$ of K is

$$\mathcal{O}_K := \{ \alpha \in K : \alpha \text{ satisfies a monic polynomial in } \mathbb{Z}[x] \}.$$

Proposition. $\mathcal{O}_K$ is indeed a ring.

Proofs.

Proof 1. Symmetric functions: (Milne, Filaseta)

We will give a different proof. (Dedekind)

Def. Given an extension of rings $A \subseteq B$. An element of B is *integral over* A if it satisfies a monic polynomial w/ coeffs in A. B is integral$/A$ if all its elements are. ~~[illegible]~~

Proposition. Given an extension of rings B/A, and $b \in B$.

TFAE. (1) b is integral over A.

(2) The ring $A[b]$ is contained in a ring R which is finitely generated as an A-module.

i.e., $A[b] = A \cdot x_1 + A \cdot x_2 + \cdots + A \cdot x_n$ for some n and $\{x_i\} \subset B$

2.2.

Let's figure out what this means.

* Prove (1) $\to$ (2) (and a little bit more)
* Prove $\mathcal{O}_K$ is a ring
* Prove (2) $\to$ (1).

(1) $\to$ (2). In fact, we have:

If $b \in B$ is integral over A, then $A[b]$ is f.g. over A.

Proof? b satisfies $b^n + a_{n-1} b^{n-1} + a_{n-2} b^{n-2} + \cdots + a_0 = 0$

An arbitrary element $x \in A[b]$ can be written

$$x = c_0 + c_1 \cdot b + c_2 \cdot b^2 + \cdots + c_m b^m \quad \text{where } c_i \in A.$$

We don't know m is small, but use above to rewrite

$$b^m = -a_{n-1} b^{m-1} - a_{n-2} b^{m-2} - \cdots - a_0 b^{m-n}$$

if $m \geq n$.

By doing this repeatedly we can rewrite x as a linear combination of $1, b, b^2, \ldots, b^{n-1}$.

So, $A[b]$ is gen by $1, b, \ldots, b^{n-1}$ as an A-module.

careful! gen. as a ring / as a module > different.

OK. Now proving $\mathcal{O}_K$ is a ring is the easy part!

Given $\alpha, \beta \in \mathcal{O}_K$. Then $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are f.g. over $\mathbb{Z}$.

This means that $\mathbb{Z}[\alpha, \beta]$ is also f.g. $/ \mathbb{Z}$.

("obvious", but worth checking.)

Clearly $\mathbb{Z}[\alpha + \beta] \subseteq \mathbb{Z}[\alpha, \beta]$.

So by (2) $\to$ (1), $\alpha + \beta$ is integral over $\mathbb{Z}$.

Same for $\alpha \cdot \beta$.

2.3. This leaves us $(2) \to (1)$.

<u>Linear algebra fact.</u>

Given an $s \times s$ matrix $M = (m_{ij})$ with entries in a ring A.

Define the <u>adjoint matrix</u> M^* by (m_{ij}^*), where

$$m_{ij}^* = (-1)^{i+j} \det(\underbrace{M_{ij}}_{\text{matrix with } i\text{th row and } j\text{th col. deleted}})$$

Then $M \cdot M^* = M^* \cdot M = (\det M) \cdot \underbrace{I_s}_{I_s = s \times s \text{ id}}$.

Basically, think of $M^* = \frac{1}{\det M} \cdot M^{-1}$, <u>but</u>

* this does not depend on M being invertible
* all entries of M^* will be in A (no fractions)
* The ring A can be arbitrarily bad.

Proof of $(2) \to (1)$.

We have $A[b]$ is contained in R, a f.g. A-module.

Write $R = r_1 A + r_2 A + \cdots + r_n A$.

We have $b \cdot r_i = \sum_{j=1}^{n} a_{ji} r_j$ for some $a_{ji} \in A$.

Now let $M = b \cdot I_n - (a_{ji})$ $\quad \vec{r} = \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$.

Look at $M\vec{r} = \begin{pmatrix} b-a_{11} & -a_{21} & -a_{31} & \cdots & -a_{n1} \\ \vdots & b-a_{22} & & & \\ \vdots & & \ddots & & \\ -a_{1n} & & & & b-a_{nn} \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ \vdots \\ r_n \end{pmatrix} = b\vec{r} - b\vec{r} = 0.$

2.4. We have $M\vec{r} = 0$, so $M^{\#} M \vec{r} = 0$, so $\det M = 0$.

Therefore, b is a root of
$$\det\left(X I_n - (a_{ji}) \right) = 0,$$
which is a monic polynomial in A.

Corollary. Given ring extensions $A \subseteq B \subseteq C$.
If C is integral $/B$, and B is integral $/A$,
then C is integral $/A$.

Proof. Formalism ("obvious"), HW.

Def. Given a ring extension B/A,
$$\bar{A} := \{ b \in B : b \text{ is integral over } A \}$$ is
called the integral closure of A in B.

Example. Given the ring extension $K/\mathbb{Z}$, where K is a NF,
$$\bar{\mathbb{Z}} = \{ b \in K : b \text{ is integral over } \mathbb{Z} \} = \mathcal{O}_K$$
so $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K.

(This is a tautology, nothing to prove.)

Prop. Integral closures are integrally closed.
That is, if B/A is a ring extension, and $\bar{A}$ is the integral closure of A in B, then
$$\{ b \in B : b \text{ is integral over } \bar{A} \} = \bar{A}.$$
Follows from our corollary (transitivity of integrality).

2.5. So we have the following picture.

$$\begin{array}{ccl} K & \text{---} & \mathcal{O}_K = \{\alpha \in K : \alpha \text{ is integral over } \mathbb{Z}\}. \\ & & \quad \text{the ring of integers of } K. \\ | & & \\ \mathbb{Q} & \text{---} & \mathbb{Z} \end{array}$$

One more fact.

Prop. If $\mathcal{O}_K$ is the ring of integers of K then K is the field of fractions of $\mathcal{O}_K$. (M. F., Thm 6)

Indeed, any element of K can be written as $\frac{\alpha}{d}$, with $\alpha \in \mathcal{O}_K$, $d \in \mathbb{Z}$.

Proof. If $\beta \in \mathcal{O}_K$, then

$$x_n \beta^n + x_{n-1} \beta^{n-1} + x_{n-2} \beta^{n-2} + \dots + x_0 = 0$$

where $x_i \in \mathbb{Z}$, $x_n \neq 0$.

Maybe x_n is not 1.

But we have also

$$x_n^n \beta^n + x_n^n x_{n-1} \beta^{n-1} + \dots + x_n^n x_0 = 0$$

$$(x_n \beta)^n + x_n x_{n-1} (x_n \beta)^{n-1} + \dots + x_n^n \cdot x_0 = 0$$

and we see that $x_n \beta$ satisfies a monic polynomial.

In general, we say a ring is integrally closed if it is integrally closed in its field of fractions, and this is what we get.

3.1. Recall.

$$\begin{array}{ccc} K & \text{---} & \mathcal{O}_K \\ | & & \\ \mathbb{Q} & \text{---} & \mathbb{Z} \end{array}$$

$\mathcal{O}_K$ is the ring of integers of K.
It forms a ring.
It is integrally closed in its field of fractions (which is K).

Def. A basis for $\mathcal{O}_K$ as a $\mathbb{Z}$-module is called an integral basis of K.
(i.e. $\{\alpha_1, \dots, \alpha_n\}$ is an integral basis if LI and
$$\mathcal{O}_K = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n.\ )$$

Theorem. Integral bases exist, of the same size as $[K:\mathbb{Q}]$.

Idea of proof.
Choose any basis $x_1, \dots, x_n$ of K.
Showed last time: there exists a constant c s.t.
$cx_1, \dots, cx_n$ are all in $\mathcal{O}_K$.
The $cx_1, \dots, cx_n$ are all independent, so
$$\mathcal{O}_K \supseteq \mathbb{Z}\cdot(cx_1) + \mathbb{Z}\cdot(cx_2) + \dots + \mathbb{Z}\cdot(cx_n)$$
contains a ~~integral basis~~ free $\mathbb{Z}$-module.

Find some d:
$$\circledast \quad \mathcal{O}_K \subseteq \frac{1}{d}\left[\mathbb{Z}\cdot(cx_1) + \mathbb{Z}\cdot(cx_2) + \dots + \mathbb{Z}\cdot(cx_n)\right]$$
contained in a free $\mathbb{Z}$-module.

It follows that $\mathcal{O}_K$ is itself a free $\mathbb{Z}$-module.
(i.e. $\mathcal{O}_K \cong \mathbb{Z}^n$ as abelian groups)
Structure theorem for finite abelian groups.

How to do $\circledast$? Seems hard.

3.2. The more general theorem:

Given A : an integral domain, integrally closed.
K : field of fractions
$L|K$ finite field extension. (separable)
B : integral closure of A in L.

$$\begin{tikzcd} L \arrow[r, dash] \arrow[d, dash] & B \\ K \arrow[r, dash] & A \end{tikzcd}$$

Thm. (N, 2.10 ; M, 2.29)
If A is a PID then B is a free A-module of rank $[L:K]$.

Ex. $K = \mathbb{Q}$ and $A = \mathbb{Z}$.
Ex. (function fields) $K = \mathbb{F}_q(t)$ and $A = \mathbb{F}_q[t]$.

$$\begin{tikzcd} L \arrow[r, dash] \arrow[d, dash] & \mathcal{O}_L \\ \mathbb{F}_q(t) \arrow[r, dash] & \mathbb{F}_q[t] \end{tikzcd}$$

finite extension
(corr. to a curve with a deg. $[L:\mathbb{F}_q(t)]$ map to $\mathbb{P}^1(\mathbb{F}_q)$.

Ex. Let $K = \mathbb{Q}(\sqrt{5})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{5}]$.
which is not a PID. $h(\mathcal{O}_K) = 2$.

Let L/K be cubic.
Then it is not necessarily true that
$$\mathcal{O}_L = \mathcal{O}_K \oplus \mathcal{O}_K \oplus \mathcal{O}_K \text{ as } \mathcal{O}_K\text{-modules.}$$
We could have
$$\mathcal{O}_L = \mathcal{O}_K \oplus \mathcal{O}_K \oplus \underline{a}$$ where $\underline{a}$ is a nonprincipal ideal of $\mathcal{O}_K$.
It is determined up to multiplication in the class group.
$[\underline{a}] \in Cl(\mathcal{O}_K)$ is called the Steinitz class of L/K.

3.3. We need discriminants to get a proof.

Given an extension * (finite, separable) L/K, basis $\alpha_1, \dots, \alpha_n$.

Def. 1. The discriminant $\mathrm{Disc}(\alpha_1, \dots, \alpha_n)$ (or Δ) is

$$\det \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}^2 .$$

What are the σ's?

(1) This is the same as Michael's def.

(2) If L/K is Galois then $\mathrm{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$.

(3) $\sigma_1, \dots, \sigma_n$ are all the embeddings $~~K~~\ L \hookrightarrow \mathbb{C}$. (if number fields) $\bar{K}$ in general.

(4) If α_1 generates L/K then its min poly is $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$.

Def. 2. $\mathrm{Disc}(\alpha_1, \dots, \alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))$.

What does this mean?

The trace of an element $\alpha \in ~~K~~\ L$ is:

(1) The sum of all the conjugates.

So that the min poly of α is (if α generates L/K)

$$x^n - (\mathrm{Tr}\,\alpha)\, x^{n-1} \cdots \pm (N(\alpha)).$$

(2) The trace of the linear transformation

$$L \longrightarrow L$$
$$x \longrightarrow \alpha \cdot x.$$

3.4. Why are these the same?

Nice special case. Assume α generates L

Then a basis of L/K is $1, \alpha, \alpha^2, \dots$

and mult. by α has matrix

say α satisfies $X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \dots + a_0 = 0.$

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & & \ddots & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \cdots & & 0 & 1 \\ -a_0 & -a_1 & \cdots & & -a_{n-1} \end{pmatrix}.$$

Has trace $-a_{n-1}$.

General case.

Write $m = [K(\alpha) : K]$ and $d = [L : K(\alpha)]$.
(and $n = m \cdot d$.)

Then a basis of L/K is

$$\begin{matrix} \beta_1, & \beta_1 \cdot \alpha, & \dots & \beta_1 \alpha^{m-1} \\ \beta_2, & \beta_2 \cdot \alpha, & \dots & \beta_2 \cdot \alpha^{m-1} \\ & \vdots & & \\ \beta_d, & & \dots & \beta_d \cdot \alpha^{m-1} \end{matrix}$$

where $\beta_1 \cdots \beta_d$ is a basis of $L/K(\alpha)$.
(Ex. Prove this.)

The matrix is d copies of the above matrix.
(So that the characteristic polynomial of $L \xrightarrow{\times \alpha} L$
is $X^n - (\mathrm{Tr}\, \alpha) X^{n-1} \dots \pm N(\alpha)$.)

Proposition. These definitions agree.

Proof. By def. 2,

$$\begin{aligned} \mathrm{Disc} &= \det\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right) \\ &= \det\left(\sum_k \sigma_k(\alpha_i \alpha_j)\right) \\ &= \det\left(\sum_k \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) \\ &= \det\left[(\sigma_k(\alpha_i))(\sigma_k(\alpha_j))^T\right] \\ &= \det(\sigma_k(\alpha_i))^2. \end{aligned}$$

3.5.

Special case. If $L = K(\theta)$ of degree n, then $\{1, \theta, \theta^2, \dots \theta^{n-1}\}$ is a basis for L/K.

It may be an integral basis, but it may not be.

Example. If $K/\mathbb{Q}$ is generated by a root θ of $x^3 - x - 4$, then an integral basis is
$$\left\{1, \theta, \frac{\theta + \theta^2}{2}\right\}.$$
Here $\{1, \theta, \theta^2\}$ is an order of index 2.

Dedekind's original example: $x^3 - x^2 - 2x - 8$
(1878) $\left\{1, \theta, \frac{\theta(\theta+1)}{2}\right\}$.

Proposition. $\mathrm{Disc}(1, \theta, \theta^2, \dots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2$

where the θ_i are the conjugates of θ.

Proof. By def. we have
$$\mathrm{Disc}(1, \theta, \dots, \theta^{n-1}) = \det \begin{bmatrix} 1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\ \vdots & \theta_2 & & & \\ \vdots & \vdots & & & \\ 1 & \theta_n & \theta_n^2 & \cdots & \theta_n^{n-1} \end{bmatrix},$$
a van der Monde determinant. Compute! (MF, Lemma on p. 37)

Cor. For any basis $\alpha_1, \dots, \alpha_n$ of L/K (such as an integral basis),
$$\mathrm{Disc}(\alpha_1, \dots, \alpha_n) \neq 0.$$

Proof. We have $L = K(\theta)$ for some θ (primitive elt. theorem)

And we know $\mathrm{Disc}(1, \theta, \theta^2, \dots, \theta^{n-1}) = \prod(\theta_i - \theta_j)^2 \neq 0$.

Exercise. If $A \cdot \begin{bmatrix} 1 \\ \vdots \\ \theta^{n-1} \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$ then $\left(\mathrm{Tr}(\alpha_i \alpha_j)\right) = A \cdot \mathrm{Tr}(\theta^{r-1}\theta^{s-1}) A^T$

and so, taking determinants,
$$\mathrm{Disc}(\{\alpha_1, \dots, \alpha_n\}) = (\det A)^2 \cdot \mathrm{Disc}(\{1, \theta, \dots, \theta^{n-1}\}),$$
and det A ≠ 0