Integral Quadratic Forms

Ajay Prajapati

Indian Institute of Technology, Kanpur

January 31, 2024

Overview

Overview

Classification over finite fields

Let $a \in \mathbb{F}_q^* - (\mathbb{F}_q^*)^2$. Then every nondegenerate quadratic form of rank n over $\mathbb{F}_q$ is equivalent to

$$X_1^2 + \ldots + X_{n-1}^2 + X_n^2 \quad \textbf{or}$$

$$X_1^2 + \ldots + X_{n-1}^2 + aX_n^2$$

depending on whether its discriminant is a square or not.

Classification over finite fields

Let $a \in \mathbb{F}_q^* - (\mathbb{F}_q^*)^2$. Then every nondegenerate quadratic form of rank n over $\mathbb{F}_q$ is equivalent to

$$X_1^2 + \ldots + X_{n-1}^2 + X_n^2 \quad \textbf{or}$$

$$X_1^2 + \ldots + X_{n-1}^2 + aX_n^2$$

depending on whether its discriminant is a square or not.

Theorem

Two quadratic forms over $k = \mathbb{Q}_p$ are equivalent $\iff$ they have the same rank, same discriminant, and same invariant ε.

Classification over finite fields

Let $a \in \mathbb{F}_q^* - (\mathbb{F}_q^*)^2$. Then every nondegenerate quadratic form of rank n over $\mathbb{F}_q$ is equivalent to

$$X_1^2 + \ldots + X_{n-1}^2 + X_n^2 \quad \textbf{or}$$

$$X_1^2 + \ldots + X_{n-1}^2 + aX_n^2$$

depending on whether its discriminant is a square or not.

Theorem

Two quadratic forms over $k = \mathbb{Q}_p$ are equivalent $\iff$ they have the same rank, same discriminant, and same invariant ε.

Theorem

Two quadratic forms over $\mathbb{Q}$ are equivalent $\iff$ they are equivalent over each $\mathbb{Q}_v$.

Classification over finite fields

Let $a \in \mathbb{F}_q^* - (\mathbb{F}_q^*)^2$. Then every nondegenerate quadratic form of rank n over $\mathbb{F}_q$ is equivalent to

$$X_1^2 + \ldots + X_{n-1}^2 + X_n^2 \quad \textbf{or}$$

$$X_1^2 + \ldots + X_{n-1}^2 + aX_n^2$$

depending on whether its discriminant is a square or not.

Theorem

Two quadratic forms over $k = \mathbb{Q}_p$ are equivalent $\iff$ they have the same rank, same discriminant, and same invariant ε.

Theorem

Two quadratic forms over $\mathbb{Q}$ are equivalent $\iff$ they are equivalent over each $\mathbb{Q}_v$.

Want to classify quadratic forms over $\mathbb{Z}$.

Definition

For $n \geq 1$, define a category S_n which consists of

1. **Objects:** Free abelian group E of rank n together with symmetric bilinear form $E \times E \longrightarrow \mathbb{Z}$, $(x, y) \longmapsto x \cdot y$ such that
$$E \longrightarrow \mathrm{Hom}(E, \mathbb{Z}), \quad (x \longmapsto (y \longmapsto x \cdot y))$$
is an isomorphism.

Definition

For $n \geq 1$, define a category S_n which consists of

1. **Objects:** Free abelian group E of rank n together with symmetric bilinear form $E \times E \longrightarrow \mathbb{Z}$, $(x, y) \longmapsto x \cdot y$ such that
$$E \longrightarrow \mathrm{Hom}(E, \mathbb{Z}), \quad (x \longmapsto (y \longmapsto x \cdot y))$$
is an isomorphism.
2. **Morphisms:** Isomorphism of free abelian groups $f : E \longrightarrow E'$ such that the following diagram commutes:
$$\begin{tikzcd} E \times E \arrow[rr, "{(f,f)}"] \arrow[dr, "{(\cdot,\cdot)}"] & & E' \times E' \arrow[dl, "{(\cdot,\cdot)}"] \\ & \mathbb{Z} & \end{tikzcd}$$

We let $S := \cup_n S_n$.

Definition

For $n \geq 1$, define a category S_n which consists of

1. **Objects:** Free abelian group E of rank n together with symmetric bilinear form $E \times E \longrightarrow \mathbb{Z}$, $(x, y) \longmapsto x \cdot y$ such that
$$E \longrightarrow \mathrm{Hom}(E, \mathbb{Z}), \quad (x \longmapsto (y \longmapsto x \cdot y))$$
is an isomorphism.
2. **Morphisms:** Isomorphism of free abelian groups $f : E \longrightarrow E'$ such that the following diagram commutes:
$$\begin{tikzcd} E \times E \arrow[rr, "{(f,f)}"] \arrow[dr, "{(\cdot,\cdot)}"] & & E' \times E' \arrow[dl, "{(\cdot,\cdot)}"] \\ & \mathbb{Z} & \end{tikzcd}$$

We let $S := \cup_n S_n$.

If $E, E' \in S$, then $E \oplus E'$ denotes the direct sum of E and E' together with bilinear form which is direct sum of those on E and E'. i.e. $(x, y) \cdot (x', y') := (x \cdot x', y \cdot y')$.

Invariants quantities associated

If $E \in S$ with $(\cdot, \cdot)$ the bilinear form then (E, f) is a quadratic $\mathbb{Z}$-module with $f(x) = (x, x)$.

Definition

1. If $E \in S_n$ then n is called the rank of E.

Invariants quantities associated

If $E \in S$ with $(\cdot, \cdot)$ the bilinear form then (E, f) is a quadratic $\mathbb{Z}$-module with $f(x) = (x, x)$.

Definition

1. If $E \in S_n$ then n is called the rank of E.
2. Let $E \in S$ and let $V := E \otimes \mathbb{R}$. Then quadratic $\mathbb{R}$-module V has a well-defined signature (r, s). Then
$$\tau(E) := r - s \tag{1}$$
is called the index of E.

Invariants quantities associated

If $E \in S$ with $(\cdot, \cdot)$ the bilinear form then (E, f) is a quadratic $\mathbb{Z}$-module with $f(x) = (x, x)$.

Definition

1. If $E \in S_n$ then n is called the rank of E.
2. Let $E \in S$ and let $V := E \otimes \mathbb{R}$. Then quadratic $\mathbb{R}$-module V has a well-defined signature (r, s). Then
$$\tau(E) := r - s \tag{1}$$
is called the index of E.
3. The discriminant of (E, f), denoted by $d(E)$ is the disc. of f.
4. Let $(E, f) \in S$. Then we say E is even (or of type II) if f only takes even values. Otherwise, it is called odd (or of type I).

Invariants quantities associated

If $E \in S$ with $(\cdot, \cdot)$ the bilinear form then (E, f) is a quadratic $\mathbb{Z}$-module with $f(x) = (x, x)$.

Definition

1. If $E \in S_n$ then n is called the rank of E.
2. Let $E \in S$ and let $V := E \otimes \mathbb{R}$. Then quadratic $\mathbb{R}$-module V has a well-defined signature (r, s). Then
$$\tau(E) := r - s \tag{1}$$
is called the index of E.
3. The discriminant of (E, f), denoted by $d(E)$ is the disc. of f.
4. Let $(E, f) \in S$. Then we say E is even (or of type II) if f only takes even values. Otherwise, it is called odd (or of type I).

I_-- rank 1 $\mathbb{Z}$-module with quadratic form $x \longmapsto -x^2$.
I_+- rank 1 $\mathbb{Z}$-module with quadratic form $x \longmapsto x^2$.
U- rank 2 $\mathbb{Z}$-module with quadratic form $(x, y) \longmapsto 2xy$.
Finally, we defined the group Γ_{8n} for $n \in \mathbb{Z}_{\geq 1}$.

Overview

Theorem

If $E \in S$ is indefinite and of type I, E is isomorphic to $sI_- \oplus tI_+$ where $s, t \in \mathbb{Z}_{\geq 1}$.

Theorem

If $E \in S$ is indefinite of type II, then E is isomorphic to $pU \oplus q\Gamma_8$ where $p, q \in \mathbb{Z}_{\geq 1}$.

Theorem

If $E \in S$ is indefinite and of type I, E is isomorphic to $sI_- \oplus tI_+$ where $s, t \in \mathbb{Z}_{\geq 1}$.

Theorem

If $E \in S$ is indefinite of type II, then E is isomorphic to $pU \oplus q\Gamma_8$ where $p, q \in \mathbb{Z}_{\geq 1}$.

Definition

Let $E \in S$. One says that E represents zero if there exists $x \in E$, $x \neq 0$, such that $x \cdot x = 0$.

Theorem

If $E \in S$ is indefinite and of type I, E is isomorphic to $sI_- \oplus tI_+$ where $s, t \in \mathbb{Z}_{\geq 1}$.

Theorem

If $E \in S$ is indefinite of type II, then E is isomorphic to $pU \oplus q\Gamma_8$ where $p, q \in \mathbb{Z}_{\geq 1}$.

Definition

Let $E \in S$. One says that E represents zero if there exists $x \in E$, $x \neq 0$, such that $x \cdot x = 0$.

Theorem

If $(E, f) \in S$ is indefinite, (E, f) represents zero.

Hasse Minkowski Therorem

Let f be a quadratic form over $\mathbb{Q}$.

Hasse Minkowski Therorem

Then f represents 0 over $\mathbb{Q} \iff f$ represents 0 over $\mathbb{Q}_v$ for each v.

Hasse Minkowski Therorem

Let f be a quadratic form over $\mathbb{Q}$.

Hasse Minkowski Therorem

Then f represents 0 over $\mathbb{Q} \iff f$ represents 0 over $\mathbb{Q}_v$ for each v.

Theorem

For f to represent 0 over $k = \mathbb{Q}_p$ it is necessary and sufficient that:

1. $n = 2$ and $d = -1 \quad$ (in k^*/k^{*2}),
2. $n = 3$ and $(-1, -d) = \varepsilon$,
3. $n = 4$ and either $d \neq 1$ or $d = 1$ and $\varepsilon = (-1, -1)$.
4. $n \geq 5$. In particular, all forms in at least 5 variables represent 0

Hasse Minkowski Therorem

Let f be a quadratic form over $\mathbb{Q}$.

Hasse Minkowski Therorem

Then f represents 0 over $\mathbb{Q} \iff f$ represents 0 over $\mathbb{Q}_v$ for each v.

Theorem

For f to represent 0 over $k = \mathbb{Q}_p$ it is necessary and sufficient that:

1. $n = 2$ and $d = -1$ (in k^*/k^{*2}),
2. $n = 3$ and $(-1, -d) = \varepsilon$,
3. $n = 4$ and either $d \neq 1$ or $d = 1$ and $\varepsilon = (-1, -1)$.
4. $n \geq 5$. In particular, all forms in at least 5 variables represent 0

Let n be the rank of f. Suppose that $n = 3$ or $n = 4$ and $d(f) = 1$. If f represents 0 in all the $\mathbb{Q}_v$ except at most one, then f represents 0.

Hasse Minkowski Therorem

Let f be a quadratic form over $\mathbb{Q}$.

Hasse Minkowski Therorem

Then f represents 0 over $\mathbb{Q} \iff f$ represents 0 over $\mathbb{Q}_v$ for each v.

Theorem

For f to represent 0 over $k = \mathbb{Q}_p$ it is necessary and sufficient that:

1. $n = 2$ and $d = -1$ (in k^*/k^{*2}),
2. $n = 3$ and $(-1, -d) = \varepsilon$,
3. $n = 4$ and either $d \neq 1$ or $d = 1$ and $\varepsilon = (-1, -1)$.
4. $n \geq 5$. In particular, all forms in at least 5 variables represent 0

Let n be the rank of f. Suppose that $n = 3$ or $n = 4$ and $d(f) = 1$. If f represents 0 in all the $\mathbb{Q}_v$ except at most one, then f represents 0.

Corollary (Meyer)

If f is of rank ≥ 5 then f represents 0 over $\mathbb{Q} \iff f$ is indefinite.

General Lemmas

Let $(E, f) \in S$ and let $F \subset E$ be a submodule. Let $F' = \{x \in E : (x, y) = 0 \forall y \in F\}$.

Lemma

$(F, f|_F) \in S \iff E = F \oplus F'$.

General Lemmas

Review

Structure Theorem for the Indefinite Case

Grothendieck Group

Let $(E, f) \in S$ and let $F \subset E$ be a submodule. Let $F' = \{x \in E : (x, y) = 0 \forall y \in F\}$.

Lemma

$(F, f|_F) \in S \iff E = F \oplus F'$.

Proof

1. $(\Longleftarrow)$ If $E = F \oplus F'$, then we have $d(E) = d(F) \cdot d(F')$ from which $d(F') = \pm 1$.

General Lemmas

Let $(E, f) \in S$ and let $F \subset E$ be a submodule. Let $F' = \{x \in E : (x, y) = 0 \forall y \in F\}$.

Lemma

$(F, f|_F) \in S \iff E = F \oplus F'$.

Proof

1. $(\impliedby)$ If $E = F \oplus F'$, then we have $d(E) = d(F) \cdot d(F')$ from which $d(F') = \pm 1$.
2. $(\implies)$ If $d(F) = \pm 1$ then $F \cap F' = \{0\}$. Also we have $F \cong \mathrm{Hom}(F, \mathbb{Z})$. Therefore for $x \in E$, the map
$$F \longrightarrow \mathbb{Z}, \quad y \longmapsto x \cdot y$$
is defined by $x_0 \in F$. Then $x = x_0 + (x - x_0)$ and $E = F \oplus F'$.

General Lemmas

Let $(E, f) \in S$ and let $F \subset E$ be a submodule. Let $F' = \{x \in E : (x, y) = 0 \forall y \in F\}$.

Lemma

$(F, f|_F) \in S \iff E = F \oplus F'$.

Proof

1. $(\Longleftarrow)$ If $E = F \oplus F'$, then we have $d(E) = d(F) \cdot d(F')$ from which $d(F') = \pm 1$.
2. $(\Longrightarrow)$ If $d(F) = \pm 1$ then $F \cap F' = \{0\}$. Also we have $F \cong \mathrm{Hom}(F, \mathbb{Z})$. Therefore for $x \in E$, the map
$$F \longrightarrow \mathbb{Z}, \quad y \longmapsto x \cdot y$$
is defined by $x_0 \in F$. Then $x = x_0 + (x - x_0)$ and $E = F \oplus F'$.

Lemma

Let $x \in E$ be such that $x \cdot x = \pm 1$ and let X be the orthogonal complement of x in E. If $D = \mathbb{Z}x$, one has $E = D \oplus X$.

Definition

An element $x \in E$ is called indivisible if $x \notin nE$ for all $n \geq 2$.

Definition

An element $x \in E$ is called indivisible if $x \notin nE$ for all $n \geq 2$.

Every nonzero element of E can be written in a unique way in the form mx with $m \geq 1$ and x indivisible.

Definition

An element $x \in E$ is called indivisible if $x \notin nE$ for all $n \geq 2$.

Every nonzero element of E can be written in a unique way in the form mx with $m \geq 1$ and x indivisible.

Lemma

If x is an indivisible element of E there exists $y \in E$ s.t. $x \cdot y = 1$.

Definition

An element $x \in E$ is called indivisible if $x \notin nE$ for all $n \geq 2$.

Every nonzero element of E can be written in a unique way in the form mx with $m \geq 1$ and x indivisible.

Lemma

If x is an indivisible element of E there exists $y \in E$ s.t. $x \cdot y = 1$.

Proof

1. Let $f_x \in \mathrm{Hom}(E, \mathbb{Z})$ be the linear form $y \mapsto x.y$ defined by x.

Definition

An element $x \in E$ is called indivisible if $x \notin nE$ for all $n \geq 2$.

Every nonzero element of E can be written in a unique way in the form mx with $m \geq 1$ and x indivisible.

Lemma

If x is an indivisible element of E there exists $y \in E$ s.t. $x \cdot y = 1$.

Proof

1. Let $f_x \in \mathrm{Hom}(E, \mathbb{Z})$ be the linear form $y \mapsto x.y$ defined by x.
2. f_x is indivisible since x is.

Definition

An element $x \in E$ is called indivisible if $x \notin nE$ for all $n \geq 2$.

Every nonzero element of E can be written in a unique way in the form mx with $m \geq 1$ and x indivisible.

Lemma

If x is an indivisible element of E there exists $y \in E$ s.t. $x \cdot y = 1$.

Proof

1. Let $f_x \in \mathrm{Hom}(E, \mathbb{Z})$ be the linear form $y \mapsto x.y$ defined by x.
2. f_x is indivisible since x is.
3. f_x is surjective.

Indefinite forms of type I

Theorem

If $E \in S$ is indefinite and of type I, E is isomorphic to $sI_- \oplus tI_+$ where $s, t \in \mathbb{Z}_{\geq 1}$.

Indefinite forms of type I

Theorem

If $E \in S$ is indefinite and of type I, E is isomorphic to $sI_- \oplus tI_+$ where $s, t \in \mathbb{Z}_{\geq 1}$.

Corollary

Let E and E' be two elements of S with the same rank and index. Then either $E \oplus I_+ \simeq E' \oplus I_+$ or $E \oplus I_- \simeq E' \oplus I_-$.

Indefinite forms of type I

Theorem

If $E \in S$ is indefinite and of type I, E is isomorphic to $sI_- \oplus tI_+$ where $s, t \in \mathbb{Z}_{\geq 1}$.

Corollary

Let E and E' be two elements of S with the same rank and index. Then either $E \oplus I_+ \simeq E' \oplus I_+$ or $E \oplus I_- \simeq E' \oplus I_-$.

1. This is clear if $E = 0$. Otherwise, one of $E \oplus I_+$ or $E \oplus I_-$ is indefinite and of Type I. Suppose that the first is.

Indefinite forms of type I

Theorem

If $E \in S$ is indefinite and of type I, E is isomorphic to $sI_- \oplus tI_+$ where $s, t \in \mathbb{Z}_{\geq 1}$.

Corollary

Let E and E' be two elements of S with the same rank and index. Then either $E \oplus I_+ \simeq E' \oplus I_+$ or $E \oplus I_- \simeq E' \oplus I_-$.

1. This is clear if $E = 0$. Otherwise, one of $E \oplus I_+$ or $E \oplus I_-$ is indefinite and of Type I. Suppose that the first is.
2. $E' \oplus I_+$ is also indefinite.

Indefinite forms of type I

Theorem

If $E \in S$ is indefinite and of type I, E is isomorphic to $sI_- \oplus tI_+$ where $s, t \in \mathbb{Z}_{\geq 1}$.

Corollary

Let E and E' be two elements of S with the same rank and index. Then either $E \oplus I_+ \simeq E' \oplus I_+$ or $E \oplus I_- \simeq E' \oplus I_-$.

1. This is clear if $E = 0$. Otherwise, one of $E \oplus I_+$ or $E \oplus I_-$ is indefinite and of Type I. Suppose that the first is.
2. $E' \oplus I_+$ is also indefinite.
3. $E \oplus I_+ \cong sI_+ \oplus tI_-$ and $E' \oplus I_+ \cong s'I_+ \oplus t'I_-$.

Indefinite forms of type I

Theorem

If $E \in S$ is indefinite and of type I, E is isomorphic to $sI_- \oplus tI_+$ where $s, t \in \mathbb{Z}_{\geq 1}$.

Corollary

Let E and E' be two elements of S with the same rank and index. Then either $E \oplus I_+ \simeq E' \oplus I_+$ or $E \oplus I_- \simeq E' \oplus I_-$.

1. This is clear if $E = 0$. Otherwise, one of $E \oplus I_+$ or $E \oplus I_-$ is indefinite and of Type I. Suppose that the first is.
2. $E' \oplus I_+$ is also indefinite.
3. $E \oplus I_+ \cong sI_+ \oplus tI_-$ and $E' \oplus I_+ \cong s'I_+ \oplus t'I_-$.

Lemma

Let $E \in S_n$. Suppose E is indefinite and of type I. There exists $F \in S_{n-2}$ such that $E \cong I_+ \oplus I_- \oplus F$.

Indefinite forms of type I

Proof

1. there exists indivisible $x \in E, x \neq 0$ such that $x \cdot x = 0$. There exists thus $y \in E$ such that $x \cdot y = 1$.

Indefinite forms of type I

Proof

1. there exists indivisible $x \in E, x \neq 0$ such that $x \cdot x = 0$. There exists thus $y \in E$ such that $x \cdot y = 1$.
2. We can choose y such that $y \cdot y$ is odd.
3. Suppose $y \cdot y$ is even. Then choose $t \in E$ such that $t \cdot t$ is odd and Put $y' = t + ky$ with $k = 1 - x \cdot t$.

Indefinite forms of type I

Proof

1. there exists indivisible $x \in E, x \neq 0$ such that $x \cdot x = 0$. There exists thus $y \in E$ such that $x \cdot y = 1$.
2. We can choose y such that $y \cdot y$ is odd.
3. Suppose $y \cdot y$ is even. Then choose $t \in E$ such that $t \cdot t$ is odd and Put $y' = t + ky$ with $k = 1 - x \cdot t$.
4. Let $y \cdot y = 2m + 1$. Put then $e_1 = y - mx$, $e_2 = y - (m+1)x$. We check that $e_1 \cdot e_1 = 1, e_1 \cdot e_2 = 0, e_2 \cdot e_2 = -1$.

Indefinite forms of type I

Review

Structure Theorem for the Indefinite Case

Grothendieck Group

Proof

1. there exists indivisible $x \in E, x \neq 0$ such that $x \cdot x = 0$. There exists thus $y \in E$ such that $x \cdot y = 1$.
2. We can choose y such that $y \cdot y$ is odd.
3. Suppose $y \cdot y$ is even. Then choose $t \in E$ such that $t \cdot t$ is odd and Put $y' = t + ky$ with $k = 1 - x \cdot t$.
4. Let $y \cdot y = 2m + 1$. Put then $e_1 = y - mx$, $e_2 = y - (m+1)x$. We check that $e_1 \cdot e_1 = 1, e_1 \cdot e_2 = 0, e_2 \cdot e_2 = -1$.
5. Thus $\mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \cong I_+ \oplus I_-$.

Proof of Theorem

1. Induction on n. Let $E \in S_n$ with E indefinite and of type I.
2. By lemma $4, E \simeq I_+ \oplus I_- \oplus F$. If $n = 2$, we have $F = 0$ and the theorem is proved.

Indefinite forms of type I

Proof

1. there exists indivisible $x \in E, x \neq 0$ such that $x \cdot x = 0$. There exists thus $y \in E$ such that $x \cdot y = 1$.
2. We can choose y such that $y \cdot y$ is odd.
3. Suppose $y \cdot y$ is even. Then choose $t \in E$ such that $t \cdot t$ is odd and Put $y' = t + ky$ with $k = 1 - x \cdot t$.
4. Let $y \cdot y = 2m + 1$. Put then $e_1 = y - mx$, $e_2 = y - (m+1)x$. We check that $e_1 \cdot e_1 = 1, e_1 \cdot e_2 = 0, e_2 \cdot e_2 = -1$.
5. Thus $\mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \cong I_+ \oplus I_-$.

Proof of Theorem

1. Induction on n. Let $E \in S_n$ with E indefinite and of type I.
2. By lemma $4, E \simeq I_+ \oplus I_- \oplus F$. If $n = 2$, we have $F = 0$ and the theorem is proved.
3. If $n > 2$, we have $F \neq 0$ and one of the modules $I_+ \oplus F$, $I_- \oplus F$, is indefinite.

Indefinite forms of type II

Theorem

If $E \in S$ is indefinite of type II, and if $\tau(E) \geqq 0$, then E is isomorphic to $pU \oplus q\Gamma_8$ where $p, q \in \mathbb{Z}_{\geq 1}$.

Indefinite forms of type II

Theorem

If $E \in S$ is indefinite of type II, and if $\tau(E) \geqq 0$, then E is isomorphic to $pU \oplus q\Gamma_8$ where $p, q \in \mathbb{Z}_{\geq 1}$.

When $\tau(E) \leqq 0$, we get the corresponding result by applying the theorem to the module $-E := (E, -f)$.

Indefinite forms of type II

Theorem

If $E \in S$ is indefinite of type II, and if $\tau(E) \geqq 0$, then E is isomorphic to $pU \oplus q\Gamma_8$ where $p, q \in \mathbb{Z}_{\geq 1}$.

When $\tau(E) \leqq 0$, we get the corresponding result by applying the theorem to the module $-E := (E, -f)$.

Lemma

Let $E \in S$. Suppose E is indefinite and of type II. There exists $F \in S$ such that $E \simeq U \oplus F$.

Indefinite forms of type II

Theorem

If $E \in S$ is indefinite of type II, and if $\tau(E) \geqq 0$, then E is isomorphic to $pU \oplus q\Gamma_8$ where $p, q \in \mathbb{Z}_{\geq 1}$.

When $\tau(E) \leqq 0$, we get the corresponding result by applying the theorem to the module $-E := (E, -f)$.

Lemma

Let $E \in S$. Suppose E is indefinite and of type II. There exists $F \in S$ such that $E \simeq U \oplus F$.

Proof

1. Choose first $x \in E, x \neq 0, x$ indivisible such that $x \cdot x = 0$; choose next $y \in E$ such that $x.y = 1$.

Indefinite forms of type II

Theorem

If $E \in S$ is indefinite of type II, and if $\tau(E) \geqq 0$, then E is isomorphic to $pU \oplus q\Gamma_8$ where $p, q \in \mathbb{Z}_{\geq 1}$.

When $\tau(E) \leqq 0$, we get the corresponding result by applying the theorem to the module $-E := (E, -f)$.

Lemma

Let $E \in S$. Suppose E is indefinite and of type II. There exists $F \in S$ such that $E \simeq U \oplus F$.

Proof

1. Choose first $x \in E, x \neq 0, x$ indivisible such that $x \cdot x = 0$; choose next $y \in E$ such that $x.y = 1$.
2. If $y \cdot y = 2m$, replace y by $y - mx$ to obtain a y s.t. $y \cdot y = 0$.

Lemma

Let $F_1, F_2 \in S$. Suppose that F_1 and F_2 are of type II and that $I_+ \oplus I_- \oplus F_1 \simeq I_+ \oplus I_- \oplus F_2$. Then $U \oplus F_1 \simeq U \oplus F_2$.

Lemma

Let $F_1, F_2 \in S$. Suppose that F_1 and F_2 are of type II and that $I_+ \oplus I_- \oplus F_1 \simeq I_+ \oplus I_- \oplus F_2$. Then $U \oplus F_1 \simeq U \oplus F_2$.

1. To simplify the notations, we put $W = I_+ \oplus I_-$, $E_i = W \oplus F_i$, and $V_i = E_i \otimes \mathbb{Q}$. Let $E_i^0 := \{x \in E : x \cdot x \equiv 0 \pmod 2\}$ and $W^0 := \{x = (x_1, x_2) \in W : x_1 \equiv x_2 \pmod 2\}$

Lemma

Let $F_1, F_2 \in S$. Suppose that F_1 and F_2 are of type II and that $I_+ \oplus I_- \oplus F_1 \simeq I_+ \oplus I_- \oplus F_2$. Then $U \oplus F_1 \simeq U \oplus F_2$.

1. To simplify the notations, we put $W = I_+ \oplus I_-$, $E_i = W \oplus F_i$, and $V_i = E_i \otimes \mathbb{Q}$. Let $E_i^0 := \{x \in E : x \cdot x \equiv 0 \pmod 2\}$ and $W^0 := \{x = (x_1, x_2) \in W : x_1 \equiv x_2 \pmod 2\}$
2. Then E_i^0 is of index 2 in E_i and $E_i^0 = W^0 \oplus F_i$.

Lemma

Let $F_1, F_2 \in S$. Suppose that F_1 and F_2 are of type II and that $I_+ \oplus I_- \oplus F_1 \simeq I_+ \oplus I_- \oplus F_2$. Then $U \oplus F_1 \simeq U \oplus F_2$.

1. To simplify the notations, we put $W = I_+ \oplus I_-$, $E_i = W \oplus F_i$, and $V_i = E_i \otimes \mathbb{Q}$. Let $E_i^0 := \{x \in E : x \cdot x \equiv 0 \pmod 2\}$ and $W^0 := \{x = (x_1, x_2) \in W : x_1 \equiv x_2 \pmod 2\}$
2. Then E_i^0 is of index 2 in E_i and $E_i^0 = W^0 \oplus F_i$.
3. Let E_i^+be the "dual" of E_i^0 in V_i, i.e.

$$E_i^+ := \{y \in V_i : f_x \in \mathrm{Hom}(E_i^0, \mathbb{Z})\} \quad \text{and}$$

$$W^+ := \{(x_1, x_2) \in W : 2x_1 \in \mathbb{Z}, 2x_2 \in \mathbb{Z}, x_1 - x_2 \in \mathbb{Z}\}.$$

Then $E_i^+ = W^+ \oplus F_i$.

Lemma

Let $F_1, F_2 \in S$. Suppose that F_1 and F_2 are of type II and that $I_+ \oplus I_- \oplus F_1 \simeq I_+ \oplus I_- \oplus F_2$. Then $U \oplus F_1 \simeq U \oplus F_2$.

1. To simplify the notations, we put $W = I_+ \oplus I_-$, $E_i = W \oplus F_i$, and $V_i = E_i \otimes \mathbb{Q}$. Let $E_i^0 := \{x \in E : x \cdot x \equiv 0 \pmod 2\}$ and $W^0 := \{x = (x_1, x_2) \in W : x_1 \equiv x_2 \pmod 2\}$
2. Then E_i^0 is of index 2 in E_i and $E_i^0 = W^0 \oplus F_i$.
3. Let E_i^+be the "dual" of E_i^0 in V_i, i.e.
   $$E_i^+ := \{y \in V_i : f_x \in \mathrm{Hom}(E_i^0, \mathbb{Z})\} \quad \text{and}$$
   $$W^+ := \{(x_1, x_2) \in W : 2x_1 \in \mathbb{Z}, 2x_2 \in \mathbb{Z}, x_1 - x_2 \in \mathbb{Z}\}.$$
   Then $E_i^+ = W^+ \oplus F_i$.
4. One has $E_i^0 \subset E_i \subset E_i^+$ and the quotient E_i^+/E_i^0 is isomorphic to W^+/W_0; it is a group of type $(2, 2)$.

Review

Structure Theorem for the Indefinite Case

Grothendieck Group

Lemma

Let $F_1, F_2 \in S$. Suppose that F_1 and F_2 are of type II and that $I_+ \oplus I_- \oplus F_1 \simeq I_+ \oplus I_- \oplus F_2$. Then $U \oplus F_1 \simeq U \oplus F_2$.

1. To simplify the notations, we put $W = I_+ \oplus I_-$, $E_i = W \oplus F_i$, and $V_i = E_i \otimes \mathbb{Q}$. Let $E_i^0 := \{x \in E : x \cdot x \equiv 0 \pmod 2\}$ and $W^0 := \{x = (x_1, x_2) \in W : x_1 \equiv x_2 \pmod 2\}$
2. Then E_i^0 is of index 2 in E_i and $E_i^0 = W^0 \oplus F_i$.
3. Let E_i^+be the "dual" of E_i^0 in V_i, i.e.
$$E_i^+ := \{y \in V_i : f_x \in \mathrm{Hom}(E_i^0, \mathbb{Z})\} \quad \text{and}$$
$$W^+ := \{(x_1, x_2) \in W : 2x_1 \in \mathbb{Z}, 2x_2 \in \mathbb{Z}, x_1 - x_2 \in \mathbb{Z}\}.$$
Then $E_i^+ = W^+ \oplus F_i$.
4. One has $E_i^0 \subset E_i \subset E_i^+$ and the quotient E_i^+/E_i^0 is isomorphic to W^+/W_0; it is a group of type $(2,2)$.
5. Let E_i' and E_i''. be the two others subgroups strictly between E_1^0 and E_i^+. Here again we have:
$$E_i' = W' \oplus F_i \quad \text{and} \quad E_i'' = W'' \oplus F_i$$
One checks that W' and W'' are isomorphic to U.

1. Let then $f : W \oplus F_1 \to W \oplus F_2$ be an isomorphism. It extends to an isomorphism of V_1 onto V_2, which carries E_1 onto E_2, thus also E_1^0 onto E_2^0 and E_1^+onto E_2^+.

1. Let then $f : W \oplus F_1 \to W \oplus F_2$ be an isomorphism. It extends to an isomorphism of V_1 onto V_2, which carries E_1 onto E_2, thus also E_1^0 onto E_2^0 and E_1^+onto E_2^+.
2. Thus it carries also (E_1', E_1'') onto either (E_2', E_2'') or (E_2'', E_2') .

1. Let then $f : W \oplus F_1 \to W \oplus F_2$ be an isomorphism. It extends to an isomorphism of V_1 onto V_2, which carries E_1 onto E_2, thus also E_1^0 onto E_2^0 and E_1^+onto E_2^+.
2. Thus it carries also (E_1', E_1'') onto either (E_2', E_2'') or (E_2'', E_2') .

Proof of Theorem

1. We first prove that if $E_1, E_2 \in S$ are indefinite of type II and have the same rank and same index, they are isomorphic.
2. We have $E_1 = U \oplus F_1, E_2 = U \oplus F_2$; And F_1 and F_2 are of type II and same rank and same index.

1. Let then $f : W \oplus F_1 \to W \oplus F_2$ be an isomorphism. It extends to an isomorphism of V_1 onto V_2, which carries E_1 onto E_2, thus also E_1^0 onto E_2^0 and E_1^+onto E_2^+.
2. Thus it carries also (E_1', E_1'') onto either (E_2', E_2'') or (E_2'', E_2') .

Proof of Theorem

1. We first prove that if $E_1, E_2 \in S$ are indefinite of type II and have the same rank and same index, they are isomorphic.
2. We have $E_1 = U \oplus F_1, E_2 = U \oplus F_2$; And F_1 and F_2 are of type II and same rank and same index.
3. The modules $I_+ \oplus I_- \oplus F_1$ and $I_+ \oplus I_- \oplus F_2$ are indefinite, of type I, of same rank and index.

1. Let then $f : W \oplus F_1 \to W \oplus F_2$ be an isomorphism. It extends to an isomorphism of V_1 onto V_2, which carries E_1 onto E_2, thus also E_1^0 onto E_2^0 and E_1^+onto E_2^+.
2. Thus it carries also (E_1', E_1'') onto either (E_2', E_2'') or (E_2'', E_2') .

Proof of Theorem

1. We first prove that if $E_1, E_2 \in S$ are indefinite of type II and have the same rank and same index, they are isomorphic.
2. We have $E_1 = U \oplus F_1, E_2 = U \oplus F_2$; And F_1 and F_2 are of type II and same rank and same index.
3. The modules $I_+ \oplus I_- \oplus F_1$ and $I_+ \oplus I_- \oplus F_2$ are indefinite, of type I, of same rank and index.
4. Theorem 5 is now clear: if E is indefinite, of type II, and if $\tau(E) \geq 0$, let $p = \frac{1}{2}(r(E) - \tau(E))$ and $q = \frac{1}{8}\tau(E)$ be the integers. Apply above to E and $pU \oplus q\Gamma + 8$.

1. Let then $f : W \oplus F_1 \to W \oplus F_2$ be an isomorphism. It extends to an isomorphism of V_1 onto V_2, which carries E_1 onto E_2, thus also E_1^0 onto E_2^0 and E_1^+onto E_2^+.
2. Thus it carries also (E_1', E_1'') onto either (E_2', E_2'') or (E_2'', E_2') .

Proof of Theorem

1. We first prove that if $E_1, E_2 \in S$ are indefinite of type II and have the same rank and same index, they are isomorphic.
2. We have $E_1 = U \oplus F_1, E_2 = U \oplus F_2$; And F_1 and F_2 are of type II and same rank and same index.
3. The modules $I_+ \oplus I_- \oplus F_1$ and $I_+ \oplus I_- \oplus F_2$ are indefinite, of type I, of same rank and index.
4. Theorem 5 is now clear: if E is indefinite, of type II, and if $\tau(E) \geq 0$, let $p = \frac{1}{2}(r(E) - \tau(E))$ and $q = \frac{1}{8}\tau(E)$ be the integers. Apply above to E and $pU \oplus q\Gamma + 8$.

Overview

Theorem

If $E, E' \in S$ are indefinite, and have same rank, index, and type, they are isomorphic.

Definition

Let $E, E' \in S$. We say that E and E' are stably isomorphic if there exists $F \in S$ such that $E \oplus F \simeq E' \oplus F$.

We denote by $K_+(S)$ the quotient of S by this relation and if $E \in S$, we denote by (E) the class of E in $K_+(S)$.
The operation $\oplus$ defines a composition law $+$ on $K_+(S)$. This law is commutative, associative, and has an identity element. We have

$$(E \oplus E') = (E) + (E') \tag{2}$$

This forms a cancellative monoid. Thus we can define a group $K(S)$ from the semi-group $K_+(S)$
$K(S) = \{(x, y) : x, y \in K_+(S)$ with $(x, y) = (x', y') \iff x+y' = y+x'$
The composition law of $K(S)$ is defined by

$$(x, y) + (x', y') := (x + x', y + y') \tag{3}$$

It makes $K(S)$ into a commutative group with neutral element $(0, 0)$

Determination of the Grothendieck Group

Universal property of $K(S)$

Let A be a commutative group and let $f : S \to A$ be a function s.t. $f(E) = f(E_1) + f(E_2)$ if $E \simeq E_1 \oplus E_2$. Then there exists a unique group homomorphism $g : K(S) \to A$ such that following diagram commutes:

$$\begin{tikzcd} S \arrow[r, hook] \arrow[dr, "f"] & K(S) \arrow[d, "g"] \\ & A \end{tikzcd}$$

The invariants r, τ, d, σ define homomorphisms
$r : K(S) \to \mathbb{Z}, \quad \tau : K(S) \to \mathbb{Z}, \quad d : K(S) \to \{\pm 1\}, \sigma : K(S) \to \mathbb{Z}/8\mathbb{Z}$
We have again $\tau \equiv r \bmod 2$ and $d = (-1)^{(r-t)/2}$

Theorem

The group $K(S)$ is a free abelian group with basis $(I_+)$and (I_-).

One has $r(f) = s + t, \tau(f) = s - t$, which shows that s and t re determined by r and τ. From this follows:

Corollary

The pair (r, τ) defines an isomorphism of $K(S)$ onto the subgroup of $\mathbf{Z} \times \mathbf{Z}$ formed of elements (a, b) such that $a \equiv b(\mathrm{mod} 2)$.

Corollary

For two elements E and E' of S to be stably isomorphic is necessary and sufficient that they have same rank and same index.

Note that this does not imply $E \simeq E'$.

Let $E \in S, E \neq 0$. Then $E \oplus I_+$or $E \oplus I_-$is indefinite and of type 1 . Applying theorem 4 , we see that the image of E in $K(S)$ is a linear combination of $(I_+)$and of (I_-). This implies that $(I_+)$and (I_-)generate $K(S)$. Since their images by the homomorphism

$$(r, \tau) : K(S) \to \mathbb{Z} \times \mathbb{Z} \tag{4}$$

are linearly independent, $(I_+)$and (I_-)form a basis of $K(S)$.

Theorem

One has $\sigma(E) \equiv \tau(E) \pmod 8$ for every $E \in S$. Indeed τ reduced $\mathrm{mod} 8$, and σ, are homomorphisms of $K(S)$ in $\mathbb{Z}/8\mathbb{Z}$ /hich are equal on the generators $I_+$and $I_-$of $K(S);$ hence they coincide.

Corollary

If E is of type II, one has $\tau(E) \equiv 0(\mathrm{mod} 8)$.

1. Indeed $\sigma(E) = 0$ Note that this implies that $r(E) \equiv 0(\mathrm{mod} 2)$ and $d(E) = (-1)^{r(E)/2})$

Corollary

If E is definite and of type II, one has $r(E) \equiv 0(\mathrm{mod} 8)$. Indeed we