Pfister's theorem

Slavko Moconja
slavko@math.rs

Department of Algebra and Logic
Faculty of Mathematics
University of Belgrade, Serbia

Parts

Part I

Classical identities

Sums of one square

In any field F is valid

$$x^2y^2 = (xy)^2.$$

Classical identities

Sums of one square

In any field F is valid

$$x^2y^2 = (xy)^2.$$

Sums of two squares

In any field F is valid

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2.$$

Classical identities

Sums of one square

In any field F is valid

$$x^2y^2 = (xy)^2.$$

Sums of two squares

In any field F is valid

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2.$$

This expresses product of two sums of two squares as another sum of two squares.

Similar identity

Euler in 1748, and later Hamilton in 1843 (in his work on quaternions) discovered:

Similar identity

Euler in 1748, and later Hamilton in 1843 (in his work on quaternions) discovered:

Sums of four squares

In any field F is valid

$$
\begin{aligned}
(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = \\
(x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + \\
(x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 + \\
(x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)^2 + \\
(x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2.
\end{aligned}
$$

Similar identity

Euler in 1748, and later Hamilton in 1843 (in his work on quaternions) discovered:

Sums of four squares

In any field F is valid

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = \\ (x_1y_1-x_2y_2-x_3y_3-x_4y_4)^2+ \\ (x_1y_2+x_2y_1+x_3y_4-x_4y_3)^2+ \\ (x_1y_3+x_3y_1-x_2y_4+x_4y_2)^2+ \\ (x_1y_4+x_4y_1+x_2y_3-x_3y_2)^2.\end{aligned}$$

Product of two sums of four squares is again a sum of four squares.

Further research

- Graves in 1843 and Cayley in 1845 discovered an "eight squares identity, which proves that the product of two sums of eight squares is again a sum of eight squares.

Further research

- Graves in 1843 and Cayley in 1845 discovered an "eight squares identity, which proves that the product of two sums of eight squares is again a sum of eight squares.
- For a long time it was unknown if there is a similar "sixteen squares identity"?

Further research

- Graves in 1843 and Cayley in 1845 discovered an "eight squares identity, which proves that the product of two sums of eight squares is again a sum of eight squares.
- For a long time it was unknown if there is a similar "sixteen squares identity"?
- The answer is no and yes...

Eight squares

Sums of eight squares

$$
\begin{aligned}
&(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2) \cdot \\
&(y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2 + y_7^2 + y_8^2) = \\
&(x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7 - x_8y_8)^2 + \\
&(x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 + x_5y_6 - x_6y_5 - x_7y_8 + x_8y_7)^2 + \\
&(x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 + x_5y_7 + x_6y_8 - x_7y_5 - x_8y_6)^2 + \\
&(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1 + x_5y_8 - x_6y_7 + x_7y_6 - x_8y_5)^2 + \\
&(x_1y_5 - x_2y_6 - x_3y_7 - x_4y_8 + x_5y_1 + x_6y_2 + x_7y_3 + x_8y_4)^2 + \\
&(x_1y_6 + x_2y_5 - x_3y_8 + x_4y_7 - x_5y_2 + x_6y_1 - x_7y_4 + x_8y_3)^2 + \\
&(x_1y_7 + x_2y_8 + x_3y_5 - x_4y_6 - x_5y_3 + x_6y_4 + x_7y_1 - x_8y_2)^2 + \\
&(x_1y_8 - x_2y_7 + x_3y_6 + x_4y_5 - x_5y_4 - x_6y_3 + x_7y_2 + x_8y_1)^2.
\end{aligned}
$$

General question

The general question we ask is:

General question

The general question we ask is:

Sums of n squares

For which n there is an identity:

$$(x_1^2 + x_2^2 + \dots x_n^2)(y_1^2 + y_2^2 + \dots y_n^2) = z_1^2 + z_2^2 + \dots z_n^2,$$

where all $z_k = z_k(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n)$?

General question

The general question we ask is:

Sums of n squares

For which n there is an identity:

$$(x_1^2 + x_2^2 + \dots x_n^2)(y_1^2 + y_2^2 + \dots y_n^2) = z_1^2 + z_2^2 + \dots z_n^2,$$

where all $z_k = z_k(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n)$?

ie, for which n the product of two sums of n squares is a sum of n squares?

The first answer

The first answer is:

The first answer

The first answer is:

Theorem (Hurwitz, 1898)

If there is such identity valid in field of characteristic 0, *where each function* z_k *is bilinear in vectors* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ *and* $\mathbf{y} = (y_1, y_2, \ldots, y_n)$, *then* $n = 1, 2, 4$ *or* 8.

The first answer

The first answer is:

Theorem (Hurwitz, 1898)

If there is such identity valid in field of characteristic 0*, where each function* z_k *is bilinear in vectors* $\mathbf{x} = (x_1, x_2, \dots, x_n)$ *and* $\mathbf{y} = (y_1, y_2, \dots, y_n)$*, then* $n = 1, 2, 4$ *or* 8*.*

Note that identities we saw are bilinear in vectors $\mathbf{x}$ and $\mathbf{y}$.

One sixteen squares identity

- In 1966 Zassenhaus and Eichhorn discovered a sixteen squares identity.

One sixteen squares identity

- In 1966 Zassenhaus and Eichhorn discovered a sixteen squares identity.
- The identity doesn't violate Hurwitz's theorem, since z_k's are not bilinear in vectors $\mathbf{x}$ and $\mathbf{y}$.

One sixteen squares identity

- In 1966 Zassenhaus and Eichhorn discovered a sixteen squares identity.
- The identity doesn't violate Hurwitz's theorem, since z_k's are not bilinear in vectors $\mathbf{x}$ and $\mathbf{y}$.
- Actually, z_k's are rational expressions in x_i's and y_j's.

Pfister

In late 1960's, Albrecht Pfister proved several beautiful theorems considering this question...

Part II

Pfister's theorems

Theorem 1

If F is a field, and $n = 2^m$ is a power of 2, then there is an identity of form

$$(x_1^2 + x_2^2 + \dots x_n^2)(y_1^2 + y_2^2 + \dots y_n^2) = z_1^2 + z_2^2 + \dots z_n^2,$$

with $z_k \in F(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n)$, valid in F.

Pfister's theorems

Theorem 1

If F is a field, and $n = 2^m$ is a power of 2, then there is an identity of form

$$(x_1^2 + x_2^2 + \dots x_n^2)(y_1^2 + y_2^2 + \dots y_n^2) = z_1^2 + z_2^2 + \dots z_n^2,$$

with $z_k \in F(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n)$, valid in F.

And more:

Pfister's theorems

Theorem 1

If F is a field, and $n = 2^m$ is a power of 2, then there is an identity of form

$$(x_1^2 + x_2^2 + \dots x_n^2)(y_1^2 + y_2^2 + \dots y_n^2) = z_1^2 + z_2^2 + \dots z_n^2,$$

with $z_k \in F(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n)$, valid in F.

And more:

Theorem 2

If n is not a power of two, then there exists some field F such that there is no identity

$$(x_1^2 + x_2^2 + \dots x_n^2)(y_1^2 + y_2^2 + \dots y_n^2) = z_1^2 + z_2^2 + \dots z_n^2,$$

with $z_k \in F(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n)$, valid in F.

The proof of Theorem 1

To prove the first theorem, fix a field F, and write $n = 2^m$.

One lemma

First, we prove next lemma.

One lemma

First, we prove next lemma.

Lemma 1

Let $a_1, a_2, \ldots, a_n \in F$ and put $a = a_1^2 + a_2^2 + \ldots + a_n^2$. There is an $n \times n$ matrix A with first row $(a_1, a_2, \ldots, a_n)$ such that $AA^T = A^TA = aE$.

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ * & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \ldots & * \end{pmatrix}$$

Proof of Lemma 1

We prove lemma by induction on m.

Proof of Lemma 1

We prove lemma by induction on m.

- The case $m = 0$ is trivial.

Proof of Lemma 1

We prove lemma by induction on m.

- The case $m = 0$ is trivial.
- For the case $m = 1$ note matrix:

Proof of Lemma 1

We prove lemma by induction on m.

- The case $m = 0$ is trivial.
- For the case $m = 1$ note matrix:

$$A = \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix}.$$

Proof of Lemma 1

We prove lemma by induction on m.

- The case $m = 0$ is trivial.
- For the case $m = 1$ note matrix:

$$A = \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix}.$$

- It is easy to check that $AA^T = A^T A = (a_1^2 + a_2^2)E$.

Proof of Lemma 1

Proof of Lemma 1

- Suppose that the result is true for $2^{m-1} \times 2^{m-1}$ matrices. We prove it for $2^m \times 2^m$ matrices.

Proof of Lemma 1

- Suppose that the result is true for $2^{m-1} \times 2^{m-1}$ matrices. We prove it for $2^m \times 2^m$ matrices.
- First, let $a = a_1^2 + a_2^2 + \ldots + a_n^2 = 0$.

Proof of Lemma 1

- Suppose that the result is true for $2^{m-1} \times 2^{m-1}$ matrices. We prove it for $2^m \times 2^m$ matrices.
- First, let $a = a_1^2 + a_2^2 + \ldots + a_n^2 = 0$.
- If all $a_k = 0$, then we can take $A = 0$.

Proof of Lemma 1

- Suppose that the result is true for $2^{m-1} \times 2^{m-1}$ matrices. We prove it for $2^m \times 2^m$ matrices.
- First, let $a = a_1^2 + a_2^2 + \ldots + a_n^2 = 0$.
- If all $a_k = 0$, then we can take $A = 0$.
- So assume that $a_1 \neq 0$.

Proof of Lemma 1

- Suppose that the result is true for $2^{m-1} \times 2^{m-1}$ matrices. We prove it for $2^m \times 2^m$ matrices.
- First, let $a = a_1^2 + a_2^2 + \ldots + a_n^2 = 0$.
- If all $a_k = 0$, then we can take $A = 0$.
- So assume that $a_1 \neq 0$.
- Take row $R = (a_1, a_2, \ldots, a_{2^m})$ and $A = \frac{1}{a_1} R^T R$.

Proof of Lemma 1

- Suppose that the result is true for $2^{m-1} \times 2^{m-1}$ matrices. We prove it for $2^m \times 2^m$ matrices.
- First, let $a = a_1^2 + a_2^2 + \ldots + a_n^2 = 0$.
- If all $a_k = 0$, then we can take $A = 0$.
- So assume that $a_1 \neq 0$.
- Take row $R = (a_1, a_2, \ldots, a_{2^m})$ and $A = \frac{1}{a_1} R^T R$.
- Its first raw is R, as required, and

Proof of Lemma 1

- Suppose that the result is true for $2^{m-1} \times 2^{m-1}$ matrices. We prove it for $2^m \times 2^m$ matrices.
- First, let $a = a_1^2 + a_2^2 + \ldots + a_n^2 = 0$.
- If all $a_k = 0$, then we can take $A = 0$.
- So assume that $a_1 \neq 0$.
- Take row $R = (a_1, a_2, \ldots, a_{2^m})$ and $A = \frac{1}{a_1} R^T R$.
- Its first raw is R, as required, and $AA^T = \frac{1}{a_1^2} R^T R R^T R = 0$ (since $RR^T = a_1^2 + \ldots + a_{2^m}^2 = a = 0$), and

Proof of Lemma 1

- Suppose that the result is true for $2^{m-1} \times 2^{m-1}$ matrices. We prove it for $2^m \times 2^m$ matrices.
- First, let $a = a_1^2 + a_2^2 + \ldots + a_n^2 = 0$.
- If all $a_k = 0$, then we can take $A = 0$.
- So assume that $a_1 \neq 0$.
- Take row $R = (a_1, a_2, \ldots, a_{2^m})$ and $A = \frac{1}{a_1} R^T R$.
- Its first raw is R, as required, and $AA^T = \frac{1}{a_1^2} R^T R R^T R = 0$ (since $RR^T = a_1^2 + \ldots + a_{2^m}^2 = a = 0$), and $A^T A = \frac{1}{a_1^2} R^T R R^T R = 0$.

Proof of Lemma 1

Proof of Lemma 1

- Let now $a \neq 0$.

Proof of Lemma 1

- Let now $a \neq 0$.
- Put $b = a_1^2 + \ldots + a_{2^{m-1}}^2$ and $c = a_{2^{m-1}+1}^2 + \ldots + a_{2^m}^2$, $a = b + c$.

Proof of Lemma 1

- Let now $a \neq 0$.
- Put $b = a_1^2 + \ldots + a_{2^{m-1}}^2$ and $c = a_{2^{m-1}+1}^2 + \ldots + a_{2^m}^2$, $a = b + c$.
- We can assume that $b \neq 0$.

Proof of Lemma 1

- Let now $a \neq 0$.
- Put $b = a_1^2 + \ldots + a_{2^{m-1}}^2$ and $c = a_{2^{m-1}+1}^2 + \ldots + a_{2^m}^2$, $a = b + c$.
- We can assume that $b \neq 0$.
- Let B and C be $2^{m-1} \times 2^{m-1}$ matrices with first rows $(a_1, \ldots, a_{2^{m-1}})$ and $(a_{2^{m-1}+1}, \ldots, a_{2^m})$ such that $BB^T = B^T B = bE$ and $CC^T = C^T C = cE$.

Proof of Lemma 1

Proof of Lemma 1

- Let's try to find matrix A in form $A = \begin{pmatrix} B & C \\ X & Y \end{pmatrix}$.

Proof of Lemma 1

- Let's try to find matrix A in form $A = \begin{pmatrix} B & C \\ X & Y \end{pmatrix}$.
- $AA^T = \begin{pmatrix} B & C \\ X & Y \end{pmatrix} \begin{pmatrix} B^T & X^T \\ C^T & Y^T \end{pmatrix}$

Proof of Lemma 1

- Let's try to find matrix A in form $A = \begin{pmatrix} B & C \\ X & Y \end{pmatrix}$.
- $AA^T = \begin{pmatrix} B & C \\ X & Y \end{pmatrix} \begin{pmatrix} B^T & X^T \\ C^T & Y^T \end{pmatrix}$
  $= \begin{pmatrix} BB^T + CC^T & BX^T + CY^T \\ XB^T + YC^T & XX^T + YY^T \end{pmatrix}$

Proof of Lemma 1

- Let's try to find matrix A in form $A = \begin{pmatrix} B & C \\ X & Y \end{pmatrix}$.
- $$AA^T = \begin{pmatrix} B & C \\ X & Y \end{pmatrix} \begin{pmatrix} B^T & X^T \\ C^T & Y^T \end{pmatrix}$$
$$= \begin{pmatrix} BB^T + CC^T & BX^T + CY^T \\ XB^T + YC^T & XX^T + YY^T \end{pmatrix}$$
$$= \begin{pmatrix} aE & BX^T + CY^T \\ XB^T + YC^T & XX^T + YY^T \end{pmatrix}.$$

Proof of Lemma 1

- Let's try to find matrix A in form $A = \begin{pmatrix} B & C \\ X & Y \end{pmatrix}$.
- $$AA^T = \begin{pmatrix} B & C \\ X & Y \end{pmatrix} \begin{pmatrix} B^T & X^T \\ C^T & Y^T \end{pmatrix}$$
  $$= \begin{pmatrix} BB^T + CC^T & BX^T + CY^T \\ XB^T + YC^T & XX^T + YY^T \end{pmatrix}$$
  $$= \begin{pmatrix} aE & BX^T + CY^T \\ XB^T + YC^T & XX^T + YY^T \end{pmatrix}.$$
- We want that $BX^T + CY^T = O$ and $XX^T + YY^T = aE$.

Proof of Lemma 1

- Let's try to find matrix A in form $A = \begin{pmatrix} B & C \\ X & Y \end{pmatrix}$.
- $$AA^T = \begin{pmatrix} B & C \\ X & Y \end{pmatrix} \begin{pmatrix} B^T & X^T \\ C^T & Y^T \end{pmatrix}$$
$$= \begin{pmatrix} BB^T + CC^T & BX^T + CY^T \\ XB^T + YC^T & XX^T + YY^T \end{pmatrix}$$
$$= \begin{pmatrix} aE & BX^T + CY^T \\ XB^T + YC^T & XX^T + YY^T \end{pmatrix}.$$
- We want that $BX^T + CY^T = O$ and $XX^T + YY^T = aE$.
- Inspired by case $m = 1$, let's try to take $Y = B$.

Proof of Lemma 1

Proof of Lemma 1

- Note that B is invertible iff $b \neq 0$, since $BB^T = bE$ (therefore $B^{-1} = \frac{1}{b}B^T$).

Proof of Lemma 1

- Note that B is invertible iff $b \neq 0$, since $BB^T = bE$ (therefore $B^{-1} = \frac{1}{b}B^T$).
- Hence, B is invertible.

Proof of Lemma 1

- Note that B is invertible iff $b \neq 0$, since $BB^T = bE$ (therefore $B^{-1} = \frac{1}{b}B^T$).
- Hence, B is invertible.
- Therefore, take $Y = B$.

Proof of Lemma 1

- Note that B is invertible iff $b \neq 0$, since $BB^T = bE$ (therefore $B^{-1} = \frac{1}{b}B^T$).
- Hence, B is invertible.
- Therefore, take $Y = B$.
- And from $BX^T + CY^T = O$, we find $X = -BC^T(B^{-1})^T = -\frac{1}{b}BC^TB$.

Proof of Lemma 1

- Note that B is invertible iff $b \neq 0$, since $BB^T = bE$ (therefore $B^{-1} = \frac{1}{b}B^T$).
- Hence, B is invertible.
- Therefore, take $Y = B$.
- And from $BX^T + CY^T = O$, we find $X = -BC^T(B^{-1})^T = -\frac{1}{b}BC^TB$.
- Finally, $XX^T + YY^T =$

Proof of Lemma 1

- Note that B is invertible iff $b \neq 0$, since $BB^T = bE$ (therefore $B^{-1} = \frac{1}{b}B^T$).
- Hence, B is invertible.
- Therefore, take $Y = B$.
- And from $BX^T + CY^T = O$, we find $X = -BC^T(B^{-1})^T = -\frac{1}{b}BC^TB$.
- Finally, $XX^T + YY^T =$
  $= (-\frac{1}{b}BC^TB)(-\frac{1}{b}BC^TB)^T + BB^T$

Proof of Lemma 1

- Note that B is invertible iff $b \neq 0$, since $BB^T = bE$ (therefore $B^{-1} = \frac{1}{b}B^T$).
- Hence, B is invertible.
- Therefore, take $Y = B$.
- And from $BX^T + CY^T = O$, we find $X = -BC^T(B^{-1})^T = -\frac{1}{b}BC^TB$.
- Finally, $XX^T + YY^T =$
  $= (-\frac{1}{b}BC^TB)(-\frac{1}{b}BC^TB)^T + BB^T$
  $= \frac{1}{b^2}BC^TBB^TCB^T + bE$

Proof of Lemma 1

- Note that B is invertible iff $b \neq 0$, since $BB^T = bE$ (therefore $B^{-1} = \frac{1}{b}B^T$).
- Hence, B is invertible.
- Therefore, take $Y = B$.
- And from $BX^T + CY^T = O$, we find $X = -BC^T(B^{-1})^T = -\frac{1}{b}BC^TB$.
- Finally, $XX^T + YY^T =$
  $= (-\frac{1}{b}BC^TB)(-\frac{1}{b}BC^TB)^T + BB^T$
  $= \frac{1}{b^2}BC^TBB^TCB^T + bE$
  $= \frac{1}{b}BC^TCB^T + bE$

Proof of Lemma 1

- Note that B is invertible iff $b \neq 0$, since $BB^T = bE$ (therefore $B^{-1} = \frac{1}{b}B^T$).
- Hence, B is invertible.
- Therefore, take $Y = B$.
- And from $BX^T + CY^T = O$, we find $X = -BC^T(B^{-1})^T = -\frac{1}{b}BC^TB$.
- Finally, $XX^T + YY^T =$

$$= (-\tfrac{1}{b}BC^TB)(-\tfrac{1}{b}BC^TB)^T + BB^T$$
$$= \tfrac{1}{b^2}BC^TBB^TCB^T + bE$$
$$= \tfrac{1}{b}BC^TCB^T + bE$$
$$= \tfrac{c}{b}BB^T + bE$$

Proof of Lemma 1

- Note that B is invertible iff $b \neq 0$, since $BB^T = bE$ (therefore $B^{-1} = \frac{1}{b}B^T$).
- Hence, B is invertible.
- Therefore, take $Y = B$.
- And from $BX^T + CY^T = O$, we find $X = -BC^T(B^{-1})^T = -\frac{1}{b}BC^TB$.
- Finally, $XX^T + YY^T =$

$$= (-\tfrac{1}{b}BC^TB)(-\tfrac{1}{b}BC^TB)^T + BB^T$$
$$= \tfrac{1}{b^2}BC^TBB^TCB^T + bE$$
$$= \tfrac{1}{b}BC^TCB^T + bE$$
$$= \tfrac{c}{b}BB^T + bE$$

$= cE + bE = aE$, and we are finished.

Corollaries

Corollary 1

In any field F, the set of sums of n squares is closed under multiplication when $n = 2^m$. Further, the set of all nonzero sums of n squares is a group under multiplication.

Corollaries

Proof.

Corollaries

Proof.

- Let $u = u_1^2 + \ldots + u_n^2$ and $v = v_1^2 + \ldots + v_n^2$.

Corollaries

Proof.

- Let $u = u_1^2 + \ldots + u_n^2$ and $v = v_1^2 + \ldots + v_n^2$.
- Take U and V to be matrices with first rows $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$, such that $UU^T = U^T U = uE$ and $VV^T = V^T V = vE$.

Corollaries

Proof.

- Let $u = u_1^2 + \ldots + u_n^2$ and $v = v_1^2 + \ldots + v_n^2$.
- Take U and V to be matrices with first rows $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$, such that $UU^T = U^T U = uE$ and $VV^T = V^T V = vE$.
- Take $W = UV^T$ and let first row of W to be $(w_1, \ldots, w_n)$.

Corollaries

Proof.

- Let $u = u_1^2 + \ldots + u_n^2$ and $v = v_1^2 + \ldots + v_n^2$.
- Take U and V to be matrices with first rows $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$, such that $UU^T = U^T U = uE$ and $VV^T = V^T V = vE$.
- Take $W = UV^T$ and let first row of W to be $(w_1, \ldots, w_n)$.
- Then, $WW^T = UV^T VU^T = uvE$, and taking $(1, 1)$ entry of this matrix we get

Corollaries

Proof.

- Let $u = u_1^2 + \ldots + u_n^2$ and $v = v_1^2 + \ldots + v_n^2$.
- Take U and V to be matrices with first rows $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$, such that $UU^T = U^T U = uE$ and $VV^T = V^T V = vE$.
- Take $W = UV^T$ and let first row of W to be $(w_1, \ldots, w_n)$.
- Then, $WW^T = UV^T VU^T = uvE$, and taking $(1,1)$ entry of this matrix we get
- $w_1^2 + \ldots + w_n^2 = uv$, ie. the product of two sums of n squares is a sum of n squares.

Corollaries

Proof.

- Let $u = u_1^2 + \ldots + u_n^2$ and $v = v_1^2 + \ldots + v_n^2$.
- Take U and V to be matrices with first rows $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$, such that $UU^T = U^T U = uE$ and $VV^T = V^T V = vE$.
- Take $W = UV^T$ and let first row of W to be $(w_1, \ldots, w_n)$.
- Then, $WW^T = UV^T VU^T = uvE$, and taking $(1, 1)$ entry of this matrix we get
- $w_1^2 + \ldots + w_n^2 = uv$, ie. the product of two sums of n squares is a sum of n squares.
- If $u \neq 0$, then $\frac{1}{u} = \frac{u}{u^2} = \left(\frac{u_1}{u}\right)^2 + \ldots + \left(\frac{u_n}{u}\right)^2$.

Corollaries

Theorem 1

If F is a field, and $n = 2^m$ is a power of 2, then there is an identity of form

$$(x_1^2 + x_2^2 + \dots x_n^2)(y_1^2 + y_2^2 + \dots y_n^2) = z_1^2 + z_2^2 + \dots z_n^2,$$

with $z_k \in F(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n)$, valid in F.

Corollaries

Proof.

Corollaries

Proof.

- Apply Corollary 1 on field $F(x_1, \ldots, x_n, y_1, \ldots, y_n)$.

Corollaries

Proof.

- Apply Corollary 1 on field $F(x_1, \ldots, x_n, y_1, \ldots, y_n)$.
- The sum of squares of x_i's times sum of squares of y_j's is again a sum of squares of n rational expressions in x_i's and y_j's.

Corollaries

Proof.

- Apply Corollary 1 on field $F(x_1, \ldots, x_n, y_1, \ldots, y_n)$.
- The sum of squares of x_i's times sum of squares of y_j's is again a sum of squares of n rational expressions in x_i's and y_j's.
- Thus, that identity is valid in field F.

Part III

Die Stufe

Definition

The smallest positive integer s such that -1 is sum of s squares in a field F

$$-1 = a_1^2 + a_2^2 + \ldots + a_s^2, \; a_k \in F$$

is called the Stufe of field F. We denote it $s(F)$. If such S doesn't exist then we put $s(F) = \infty$ and call F formally real.

Pfister's theorems

Theorem 3

If $s(F) < \infty$ then it is a power of 2.

Pfister's theorems

Theorem 3

If $s(F) < \infty$ then it is a power of 2.

Theorem 4

For every power of 2, n, there is a field F with Stufe $s(F) = n$.

Proof of Theorem 3

- Let $n = 2^m \leq s = s(F) < s^{m+1}$.

Proof of Theorem 3

- Let $n = 2^m \leq s = s(F) < s^{m+1}$.
- Write $0 = a_1^2 + a_2^2 + \ldots a_n^2 + a_{n+1}^2 + \ldots + a_s^2 + 1$.

Proof of Theorem 3

- Let $n = 2^m \leq s = s(F) < s^{m+1}$.
- Write $0 = a_1^2 + a_2^2 + \ldots a_n^2 + a_{n+1}^2 + \ldots + a_s^2 + 1$.
- Take $u = a_1^2 + a_2^2 + \ldots a_n^2$ and $v = a_{n+1}^2 + \ldots + a_s^2 + 1 + 0 + \ldots + 0$.

Proof of Theorem 3

- Let $n = 2^m \leq s = s(F) < s^{m+1}$.
- Write $0 = a_1^2 + a_2^2 + \dots a_n^2 + a_{n+1}^2 + \dots + a_s^2 + 1$.
- Take $u = a_1^2 + a_2^2 + \dots a_n^2$ and $v = a_{n+1}^2 + \dots + a_s^2 + 1 + 0 + \dots + 0$.
- $u, v \neq 0$, otherwise $s(F) < s$.

Proof of Theorem 3

- Let $n = 2^m \leq s = s(F) < s^{m+1}$.
- Write $0 = a_1^2 + a_2^2 + \dots a_n^2 + a_{n+1}^2 + \dots + a_s^2 + 1$.
- Take $u = a_1^2 + a_2^2 + \dots a_n^2$ and $v = a_{n+1}^2 + \dots + a_s^2 + 1 + 0 + \dots + 0$.
- $u, v \neq 0$, otherwise $s(F) < s$.
- $u + v = 0$, hence $u = -v$, and therefore $-1 = v/u$.

Proof of Theorem 3

- Let $n = 2^m \leq s = s(F) < s^{m+1}$.
- Write $0 = a_1^2 + a_2^2 + \dots a_n^2 + a_{n+1}^2 + \dots + a_s^2 + 1$.
- Take $u = a_1^2 + a_2^2 + \dots a_n^2$ and $v = a_{n+1}^2 + \dots + a_s^2 + 1 + 0 + \dots + 0$.
- $u, v \neq 0$, otherwise $s(F) < s$.
- $u + v = 0$, hence $u = -v$, and therefore $-1 = v/u$.
- By Corollary 1, -1 is a sum of n squares.

Proof of Theorem 3

- Let $n = 2^m \leq s = s(F) < s^{m+1}$.
- Write $0 = a_1^2 + a_2^2 + \ldots a_n^2 + a_{n+1}^2 + \ldots + a_s^2 + 1$.
- Take $u = a_1^2 + a_2^2 + \ldots a_n^2$ and $v = a_{n+1}^2 + \ldots + a_s^2 + 1 + 0 + \ldots + 0$.
- $u, v \neq 0$, otherwise $s(F) < s$.
- $u + v = 0$, hence $u = -v$, and therefore $-1 = v/u$.
- By Corollary 1, -1 is a sum of n squares.
- Hence, $s(F) = n = 2^m$.

Part IV

Some fact

Lemma

Let $\mathbb{R}$ be the field of real numbers. Then $x_1^2 + x_2^2 + \ldots + x_n^2$ is not a sum of $n-1$ squares in field $\mathbb{R}(x_1, x_2, \ldots, x_n)$.

Proof of Theorem 4

Theorem 4

For every power of 2, n, there is a field F with Stufe $s(F) = n$.

Proof of Theorem 4

- Let $n = 2^m$, and let $F = \mathbb{R}(x_1, x_2, \ldots, x_{n+1}, y)$ where $y^2 + x_1^2 + \ldots x_{n+1}^2 = 0$.

Proof of Theorem 4

- Let $n = 2^m$, and let $F = \mathbb{R}(x_1, x_2, \dots, x_{n+1}, y)$ where $y^2 + x_1^2 + \dots x_{n+1}^2 = 0$.
- We claim that $s(F) = n = 2^m$.

Proof of Theorem 4

- Let $n = 2^m$, and let $F = \mathbb{R}(x_1, x_2, \ldots, x_{n+1}, y)$ where $y^2 + x_1^2 + \ldots x_{n+1}^2 = 0$.
- We claim that $s(F) = n = 2^m$.
- $s(F) \leq n + 1$, since $-1 = (\frac{x_1}{y})^2 + \ldots + (\frac{x_{n+1}}{y})^2$, and therefore $s(F) \leq n$ (since it has to be power of 2).

Proof of Theorem 4

- Assume that $s = s(F) < n$.

Proof of Theorem 4

- Assume that $s = s(F) < n$.
- Write $0 = t_1^2 + \ldots + t_n^2$, not all t_k's are zero,

Proof of Theorem 4

- Assume that $s = s(F) < n$.
- Write $0 = t_1^2 + \ldots + t_n^2$, not all t_k's are zero, and $t_k = a_k + b_k y$, $a_k, b_k \in \mathbb{R}(x_1, \ldots, x_{n+1})$.

Proof of Theorem 4

- Assume that $s = s(F) < n$.
- Write $0 = t_1^2 + \ldots + t_n^2$, not all t_k's are zero, and $t_k = a_k + b_k y$, $a_k, b_k \in \mathbb{R}(x_1, \ldots, x_{n+1})$.
- Now we have $0 = \sum (a_k + b_k y)^2 = \sum a_k^2 + 2y \sum a_k b_k + y^2 \sum b_k^2$.

Proof of Theorem 4

- Assume that $s = s(F) < n$.
- Write $0 = t_1^2 + \ldots + t_n^2$, not all t_k's are zero, and $t_k = a_k + b_k y$, $a_k, b_k \in \mathbb{R}(x_1, \ldots, x_{n+1})$.
- Now we have $0 = \sum (a_k + b_k y)^2 = \sum a_k^2 + 2y \sum a_k b_k + y^2 \sum b_k^2$.
- And from there $0 = \sum a_k^2 + y^2 \sum b_k^2$ and $0 = \sum a_k b_k$.

Proof of Theorem 4

- Not all a_k's are zero, otherwise $\sum b_k^2 = 0$, hence all b_k's are zero (since $\mathbb{R}(x_1, \dots x_{n+1})$ is formally real).

Proof of Theorem 4

- Not all a_k's are zero, otherwise $\sum b_k^2 = 0$, hence all b_k's are zero (since $\mathbb{R}(x_1, \dots x_{n+1})$ is formally real).
- Not all b_k's are zero, because of the same reason.

Proof of Theorem 4

- Not all a_k's are zero, otherwise $\sum b_k^2 = 0$, hence all b_k's are zero (since $\mathbb{R}(x_1, \ldots x_{n+1})$ is formally real).
- Not all b_k's are zero, because of the same reason.
- Hence $x_1^2 + \ldots + x_{n+1}^2 = -y^2 = \sum a^k / \sum b^k = c_1^2 + \ldots + c_n^2$.

Proof of Theorem 4

- Not all a_k's are zero, otherwise $\sum b_k^2 = 0$, hence all b_k's are zero (since $\mathbb{R}(x_1, \ldots x_{n+1})$ is formally real).
- Not all b_k's are zero, because of the same reason.
- Hence $x_1^2 + \ldots + x_{n+1}^2 = -y^2 = \sum a^k / \sum b^k = c_1^2 + \ldots + c_n^2$.
- This contradiction shows us that $s(F) = n = 2^m$.

Proof of Theorem 2

Theorem 2

If n is not a power of two, then there exists some field F such that there is no identity with $z_k \in F(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n)$, valid in F.

Proof of Theorem 2

- Let $2^{m-1} < n < 2^m = s$, and let F be a field having Stufe 2^m.

Proof of Theorem 2

- Let $2^{m-1} < n < 2^m = s$, and let F be a field having Stufe 2^m.
- Then $a_1^2 + \ldots + a_n^2 + a_{n+1}^2 + \ldots + a_s^2 + 1 = 0$.

Proof of Theorem 2

- Let $2^{m-1} < n < 2^m = s$, and let F be a field having Stufe 2^m.
- Then $a_1^2 + \ldots + a_n^2 + a_{n+1}^2 + \ldots + a_s^2 + 1 = 0$.
- Let $u = a_1^2 + \ldots + a_n^2$ and $v = a_{n+1}^2 + \ldots + a_s^2 + 1$.

Proof of Theorem 2

- Let $2^{m-1} < n < 2^m = s$, and let F be a field having Stufe 2^m.
- Then $a_1^2 + \ldots + a_n^2 + a_{n+1}^2 + \ldots + a_s^2 + 1 = 0$.
- Let $u = a_1^2 + \ldots + a_n^2$ and $v = a_{n+1}^2 + \ldots + a_s^2 + 1$.
- u, v are non-zero sums of n squares.

Proof of Theorem 2

- Let $2^{m-1} < n < 2^m = s$, and let F be a field having Stufe 2^m.
- Then $a_1^2 + \ldots + a_n^2 + a_{n+1}^2 + \ldots + a_s^2 + 1 = 0$.
- Let $u = a_1^2 + \ldots + a_n^2$ and $v = a_{n+1}^2 + \ldots + a_s^2 + 1$.
- u, v are non-zero sums of n squares.
- If there is identity

$$(x_1^2 + x_2^2 + \ldots x_n^2)(y_1^2 + y_2^2 + \ldots y_n^2) = z_1^2 + z_2^2 + \ldots z_n^2,$$

valid in F, we would have $-1 = v/u = b_1^2 + \ldots + b_n^2$.

Proof of Theorem 2

- Let $2^{m-1} < n < 2^m = s$, and let F be a field having Stufe 2^m.
- Then $a_1^2 + \ldots + a_n^2 + a_{n+1}^2 + \ldots + a_s^2 + 1 = 0$.
- Let $u = a_1^2 + \ldots + a_n^2$ and $v = a_{n+1}^2 + \ldots + a_s^2 + 1$.
- u, v are non-zero sums of n squares.
- If there is identity

$$(x_1^2 + x_2^2 + \ldots x_n^2)(y_1^2 + y_2^2 + \ldots y_n^2) = z_1^2 + z_2^2 + \ldots z_n^2,$$

  valid in F, we would have $-1 = v/u = b_1^2 + \ldots + b_n^2$.
- Therefore, $s(F) \leq n < s$, which is contradiction.

Thanks for your attention...