On the level of principal ideal domains

J. K. Arason, R. Baeza*

1. Introduction

Let A be a commutative ring with 1. If -1 can be written as a sum of squares in A then the level $s(A)$ of A is defined as the minimal number of squares needed. Else one says that $s(A) = \infty$.

If A is a field then a well known result due to Pfister says that $s(A)$ is a power of 2 or ∞. On the other hand, in [DLP] (see also [DL]) it is shown that any natural number can be realized as the level of some ring A.

If A is a Dedekind ring then, by [B1], $s(K) \leq s(A) \leq s(K) + 1$, where K is the field of fractions. If $s(K) = 1$ then also $s(A) = 1$ because A is integrally closed. But in [B1] the question remained open, whether $s(A)$ can have the value $s(K) + 1$ if $s(K) > 1$. In this note we answer this question affirmatively. In fact, we shall show that there are examples where A is a principal ideal domain.

At the end we also make some remarks on the sublevel of principal ideal domains. (See [DL] or Section 3 for the definition of the sublevel.)

We shall assume throughout that $2 \neq 0$. We shall use standard notations in the theory of symmetric bilinear forms as, for example, in [L].

2. Levels.

In this section we shall show that any number of the form $2^n + 1$ is the level of some principal ideal domain.

We start with a general result of independent interest.

(2.1) Lemma. Let F be a field and let φ be a Pfister form over F. Let c and d be non-zero elements in F such that d is not represented by φ over F and c is not represented by the pure subform φ' of φ over F. Let $q(x) \in F[x]$ be a polynomial of even positive degree with leading coefficient c. Then d is not represented by φ over the ring $F[x][\sqrt{-q(x)}]$.

*Partially supported by Fondecyt 1090011 and Anillo ACT 56

Proof. Suppose that d is represented by φ over $F[x][\sqrt{-q(x)}]$. This means that there are elements $\vec{u}(x), \vec{v}(x) \in F[x]^{2^n}$ such that

$$\varphi\left(\vec{u}(x) + \vec{v}(x)\sqrt{-q(x)}\right) = d$$

i.e.,

$$\varphi(\vec{u}(x)) - q(x)\varphi(\vec{v}(x)) = d \tag{1}$$

and

$$\varphi_b(\vec{u}(x), \vec{v}(x)) = 0 \tag{2}$$

where φ_b is the symmetric bilinear form with $\varphi(\vec{w}) = \varphi_b(\vec{w}, \vec{w}))$ for every $\vec{w}$.

Note that $\vec{v}(x) \neq 0$ since φ does not represent d over F. Let $2k > 0$ be the degree of $q(x)$ and l the degree of $\vec{v}(x)$, i.e., the maximum of the degrees of its components. From equation (1) it then follows that $\deg \vec{u}(x) = l + k$.

We denote by $\vec{a}$ the leading coefficient of $\vec{u}(x)$ and by $\vec{b}$ that of $\vec{v}(x)$. Looking at the coefficients by x^{2l+2k} in equation (1), we get

$$\varphi(\vec{a}) - c\varphi(\vec{b}) = 0$$

and the coefficients by x^{2l+k} in (2) give

$$\varphi_b(\vec{a}, \vec{b}) = 0$$

Let $e = \varphi(\vec{b})$. As φ does not represent every element in F, φ must be anisotropic over F. Since $\vec{b} \neq 0$ it follows that $e \neq 0$. Then also $\varphi(\vec{a}) = ce \neq 0$. The last equation says that $\vec{a}$ and $\vec{b}$ are orthogonal with respect to φ. Therefore the form φ contains over F the subform $\langle ce, e\rangle \cong \langle e\rangle\langle 1, c\rangle$. But e is represented by φ and φ is multiplicative so $\langle e\rangle\varphi \cong \varphi$. Hence φ also contains $\langle 1, c\rangle$ as a subform, i.e., $\langle 1\rangle \perp \varphi' \cong \langle 1, c\rangle \perp \ldots$. Cancelling $\langle 1\rangle$ we conclude that c is represented by φ', contradicting a hypothesis.

Remark. The lemma also holds for $d = 0$ if 'represented by φ' is understood as 'non-trivially represented by φ'.

With this lemma it is easy to construct Dedekind rings A with field of fractions K such that $s(A) = s(K) + 1$.

(2.2) Proposition. Let $n \geq 1$ be an integer and let F be a field of level $> 2^n$. Assume that there is an element $c \in F$ which is a sum of 2^n squares in F but not fewer.

Choose a square free polynomial $q(x) \in F[x]$ of positive degree and with leading coefficient c such that $q(x)$ is a sum of less than 2^{n+1} squares in $F[x]$.

Let $A = F[x][\sqrt{-q(x)}]$ and $K = F(x)(\sqrt{-q(x)})$. Then A is a Dedekind ring with field of fractions K such that $s(K) = 2^n$ and $s(A) = s(K) + 1$.

Proof. A is a Dedekind ring because $q(x)$ is square free. It is clear that K is the field of fractions of A. Since $q(x)$ is a sum of $m < 2^{n+1}$ squares in $F[x]$, we see that -1 is a sum of m squares in K and hence $s(K) < 2^{n+1}$. But $s(K)$ is a power of 2, so it follows that $s(K) \leq 2^n$.

Lemma (2.1) with $\varphi = 2^n \times \langle 1 \rangle$ and $d = -1$ implies that -1 is not a sum of 2^n squares in A, hence $s(A) > 2^n$. As $s(K) \leq s(A) \leq s(K) + 1$ by [B1], it follows that $s(K) = 2^n$ and $s(A) = 2^n + 1 = s(K) + 1$.

Remark. If F is the rational function field $\mathbb{R}(t_1, \ldots, t_{2^n})$ and $c = t_1^2 + \cdots + t_{2^n}^2$ then, by a well known theorem of Cassels, the hypotheses of the theorem are satisfied.

For $q(x)$ one can take $cx^2 + 1$.

By the way, this result gives rise to another algebraic proof of the fact that the ring $\mathbb{Z}[x_1, \ldots, x_{2^n+1}]/(1 + x_1^2 + \cdots + x_{2^n+1}^2)$ has level $2^n + 1$. (For the first algebraic proof see [B2].)

In fact, we even get principal ideal domains A with field of fractions K such that $s(A) = s(K) + 1$.

(2.3) Theorem. For any integer $n \geq 1$ there are principal ideal domains A with field of fractions K such that $s(K) = 2^n$ and $s(A) = s(K) + 1$.

Proof. By [S, Theorem 5.1], the Dedekind ring A in the preceding proof is a principal ideal domain if the polynomial $q(x)$ has degree 2 and if the affine conic given by $y^2 = -q(x)$ has no F-rational points. This is the case if, for example, $q(x) = cx^2 + 1$.

3. Sublevels

Related to the level $s(A)$ of a ring A, there is another invariant, called the sublevel $\sigma(A)$ of A (see [DL]). It is the smallest natural number r such that there is a unimodular vector $(a_1, \ldots, a_{r+1}) \in A^{r+1}$ with $a_1^2 + \cdots + a_{r+1}^2 = 0$. (Recall that a vector $(a_1, \ldots, a_n) \in A^n$ is said to be unimodular if there are $c_1, \ldots, c_n \in A$ with $a_1c_1 + \cdots + a_nc_n = 1$.)

For any ring A we have $\sigma(A) \leq s(A)$ because $a_1^2 + \cdots + a_s^2 = -1$ implies $a_1^2 + \cdots + a_s^2 + 1^2 = 0$.

If A is a field or a local ring then it is easily seen that $\sigma(A) = s(A)$. With some work, it can be shown that this also holds for semi-local rings A. But in general this does not hold. For example the principal ideal domain $A = \mathbb{Q}[x, y]$, $1 + x^2 + 2y^2 = 0$, satisfies $\sigma(A) = s(K) = 2$ but $s(A) = 3$, where

K is the field of fractions of A (see [CLRR], [DL]). We shall later generalize this example.

A natural question to ask is how large the difference $s(A) - \sigma(A)$ can be. The following proposition gives a partial answer.

(3.1) Proposition. In general $s(A) \leq \sigma(A) + 4$. If 2 is invertible in A then even $s(A) \leq \sigma(A) + 1$.

Furthermore, for any ring A we have:

If $\sigma(A) = 1$ then $s(A) = 1$.

If $\sigma(A) = 2$ then $s(A) \leq 3$.

If $\sigma(A) = 3$ then $s(A) = 3$.

Proof. In any ring A the equations

$$x_1^2 + \cdots + x_{r+1}^2 = 0 \quad \text{and} \quad x_1 y_1 + \cdots + x_{r+1} y_{r+1} = 1$$

imply the equation

$$\sum_{i=1}^{r+1} ((1+q)x_i - 2y_i)^2 = -4$$

where $q = y_1^2 + \cdots + y_{r+1}^2$. If 2 is invertible in A we can divide this equation by 2^2 to see that then $s(A) \leq r + 1$. In general we can rewrite the equation as $\sum_{i=1}^{r+1} ((1+q)x_i - 2y_i)^2 + 1^2 + 1^2 + 1^2 = -1$ and get $s(A) \leq r + 4$.

If $r = 1$ then $(x_1 y_2 - x_2 y_1)^2 = -1$ and if $r = 2$ then $(x_2 y_3 - x_3 y_2)^2 + (x_3 y_1 - x_1 y_3)^2 + (x_1 y_2 - x_2 y_1)^2 = -1$. If $r = 3$ we use Euler's four square formula to write $(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4)^2 + w_2^2 + w_3^2 + w_4^2$ with elements $w_2, w_3, w_4 \in A$. It follows that $w_2^2 + w_3^2 + w_4^2 = -1$.

Remark. By a private communication, Detlev Hoffmann also has a proof of the general inequality $s(A) \leq \sigma(A) + 4$. Furthermore, David Leep has announced a stronger general inequality. In [DL] there is a different proof of the inequality $s(A) \leq \sigma(A) + 1$ in the case that 2 is invertible in A.

We know no ring A with $s(A) > \sigma(A) + 1$. By the next proposition this is at least impossible for a Dedekind ring A.

(3.2) Proposition. If A is a Dedekind ring then there is an integer $n \geq 0$ such that $2^n \leq \sigma(A) \leq s(A) \leq 2^n + 1$.

Proof. Let A be a Dedekind ring and let K be is field of fractions. Writing $s(K) = 2^n$ we then get the statement from the inequalities $s(K) = \sigma(K) \leq \sigma(A) \leq s(A) \leq s(K) + 1$.

The next proposition says that there are examples of $s(A) = \sigma(A) + 1$, where A is even a principal ideal domain.

(3.3) Proposition. For any integer $n \geq 1$ there is a principal ideal domain A such that $\sigma(A) = 2^n$ and $s(A) = 2^n + 1$.

Proof. Choose a field F of level $> 2^n$ with an element c that is a sum of 2^n squares but not fewer. Write c as the sum $c_1^2 + \cdots + c_{2^n}^2$ of squares in F. Let $q(x) = cx^2 + 2c_1x + 1$. Then, $q(x) = (c_1x+1)^2 + c_2^2x^2 + \cdots + c_{2^n}^2x^2$ is sum of $2^n < 2^{n+1}$ squares in $F[x]$. Let $A = F[x][\sqrt{-q(x)}]$ and $K = F(x)(\sqrt{-q(x)})$. By Proposition (2.2), then A is a Dedekind ring with field of fractions K such that $s(K) = 2^n$ and $s(A) = s(K) + 1$. But $\sigma(A) \leq 2^n$ because $\sqrt{-q(x)}^2 + (c_1x+1)^2 + c_2^2x^2 + \cdots + c_{2^n}^2x^2 = 0$ and a vector over A having c_1x+1 and c_2x among its components is unimodular. As in the proof of Theorem (2.3) we see that A is a principal ideal domain.

One can show that the algebraic number ring $\mathbf{Z}[\sqrt{-6}]$ is a Dedekind ring A with field of fractions K such that $\sigma(A) = s(A) = s(K) + 1$. Another example, but more difficult to verify, is the ring $A = \mathbb{R}(t)[x][\sqrt{-q(x)}]$, where $q(x) = (1+t^2)x^4 + 2tx^3 + x^2 + 1$.

For a principal ideal domain A this cannot happen. Indeed, in [DL] it is shown that if A is a principal ideal domain with field of fractions K such that 2 is invertible in A then $\sigma(A) = s(K)$. Their proof of this, however, does not use that 2 is invertible. Hence we have the following.

(3.3) Proposition. Let A be a principal ideal domain with field of fractions K. Then $\sigma(A) = s(K)$.

In fact, the argument can be used to prove the following more general proposition.

(3.5) Proposition. Let A be a principal ideal domain with field of fractions K. Let (M, β) be a non singular symmetric bilinear form over A. If the extension of (M, β) to K is isotropic then M contains a unimodular element u such that $\beta(u, u) = 0$.

Proof. As A is a principal ideal domain, M is free. We therefore may assume that $M = A^m$ for some natural number m. The hypothesis then says that there is a non-zero vector $u \in K^m$ with $\beta(e, e) = 0$. Clearing denominators, we may assume that $u \in A^m$. We write $u = (u_1, \ldots, u_m)$. Dividing by the greatest common factor of $u_1, \ldots, u_m$, we then may assume that $u_1, \ldots, u_m$ are relatively prime. But then $(u_1, \ldots, u_m)$ is unimodular.

Literature

[B1] Baeza, R.: Über die Stufe von Dedekind Ringen. Archiv der Math. 33, 226-231, 1979.

[B2] Baeza, R.: Quadratic forms over semi-local rings. LNM vol. 655, Springer Verlag, Berlin-Heidelberg-New York, 1978.

[CLRR] Choi, M.D.; Lam, T.Y.; Reznick, B.; Rosenberg, A.: Sums of squares in some integral domains. Journal of Algebra, 65, 234-256, 1980.

[DL] Dai, Z.D.; Lam, T.Y.: Levels in algebra and topology. Com. Math. Helv. 59, 376-429, 1984.

[DLP] Dai, Z.D.; Lam, T.Y.; Peng, C.K.: Levels in algebra and topology. Bull. Amer. Math. Soc. (N.S.) 3, 845-848, 1980.

[L] Lam, T.Y.: Introduction to quadratic forms over fields. GSM vol. 67, AMS, 2005.

[S] Samuel, P.: On unique factorization domains. Illinois J. Math. 5, 1-17, 1961.

Faculty of Physical Sciences
University of Iceland
Reykjavik, Iceland

Instituto de Matemáticas,
Universidad de Talca
Talca, Chile