

# Valuations and the Nullstellensatz

[from lectures by Maxwell Rosenlicht]

## 1 Valuations

**Definition 1.1** An ordered abelian group is an abelian group  $\Gamma$  with a subset  $\Gamma_+$  such that

- (i)  $\Gamma_+$  is closed under addition,
- (ii)  $\Gamma_+ \cap -\Gamma_+ = \emptyset$ ,
- (iii)  $\Gamma_+ \cup -\Gamma_+ \cup \{0\} = \Gamma$ .

**Proposition 1.1** If  $\Gamma$  is an ordered abelian group, it is linearly ordered with  $\gamma_1 \leq \gamma_2 \Leftrightarrow \gamma_2 - \gamma_1 \notin \Gamma_+$  for  $\gamma_1, \gamma_2 \in \Gamma$ .

**Proposition 1.2** If  $\Gamma_1$  and  $\Gamma_2$  are ordered abelian groups, then so is the direct sum  $\Gamma_1 \oplus \Gamma_2$  with lexicographic ordering.

**Definition 1.2** If  $k$  is a field, a valuation is a homomorphism  $\nu: k^* \rightarrow \Gamma$ , where  $\Gamma$  is an ordered abelian group and  $k^* = k \setminus \{0\}$  is the multiplicative group of units of  $k$ , such that  $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$  for  $a, b \in k^*$  with  $a+b \in k^*$ .

**Definition 1.3** In the above definition  $\nu(k^*) < \Gamma$  is called the value group of  $\nu$ .

**Example 1.1** Let  $\Omega \subseteq \mathbf{C}$  be a domain and  $z_0 \in \Omega$ . Let  $k = M(\Omega)$  be the field of all meromorphic functions on  $\Omega$ . For  $f \in k$  define  $\nu(f)$  to be the order of  $f$  at  $z_0$ . Then  $\nu: k^* \rightarrow \mathbf{Z}$  is a valuation.

**Example 1.2** Let  $R$  be a unique factorization domain and  $k$  its field of quotients. If  $p \in R$  is prime, we can express each nonzero  $x \in k$  in the form  $x = p^n ab^{-1}$ , where  $a, b \in R$  are not divisible by  $p$ . Clearly  $n$  is unique and  $x \mapsto n$  gives a valuation to  $\mathbf{Z}$ .

**Note 1.1** Any nontrivial valuation on  $\mathbf{Q}$  is as in Example 1.2, for some prime in  $\mathbf{Z}$ .

**Proposition 1.3** Suppose  $\nu: k^* \rightarrow \Gamma$  is a valuation. If  $a, b \in k^*$  and  $\nu(a) \neq \nu(b)$ , then  $a+b \in k^*$  and  $\nu(a+b) = \min\{\nu(a), \nu(b)\}$ .

**Proof:** Suppose  $\nu(a) > \nu(b)$ . Then  $\nu(a+b) \geq \nu(b) = \nu((a+b) - a) \geq \min\{\nu(a+b), \nu(a)\} = \nu(a+b)$ . ■

**Example 1.3** Suppose  $\Gamma$  is an ordered abelian group and  $F$  is a field. Let  $R$  be the free  $F$ -module generated by  $\Gamma$  and let  $i: \Gamma \rightarrow R$  denote the natural inclusion. Define multiplication on  $R$  by  $i(\gamma_1) \cdot i(\gamma_2) = i(\gamma_1 + \gamma_2)$  for  $\gamma_1, \gamma_2 \in \Gamma$ . This makes  $R$  into a domain and suggests the following notation:  $i(\gamma) = t^\gamma$ , where  $t$  is an indeterminate. This way elements of  $R$  are polynomials in  $t$ . Let  $k$  be the field of quotients of  $R$ . For  $x \in k$  let  $\nu(x)$  be the degree of  $x$  in  $t$ . Then  $\nu: k^* \rightarrow \Gamma$  is a valuation.

**Proposition 1.4** If  $k \subseteq K$  are fields and  $\nu: K^* \rightarrow \Gamma$  is a valuation, then  $|\nu(K^*)/\nu(k^*)| \leq [K:k]$ .

**Proof:** Suppose  $A \subseteq \nu(K^*)$  and  $|A| > [K:k]$ . For each  $\alpha \in A$  choose  $x_\alpha \in K^*$  such that  $\nu(x_\alpha) = \alpha$ . Let  $X = \{x_\alpha: \alpha \in A\}$ . Since  $|X| = |A| > [K:k]$ ,  $X$  is linearly dependent over  $k$ . In other words there exists a finite set  $B \subset A$  such that for each  $\alpha \in B$  there is  $c_\alpha \in k^*$  with  $\sum_{\alpha \in B} c_\alpha x_\alpha = 0$ . By Proposition 1.3, there exist  $\alpha \neq \beta \in B$  such that  $\nu(c_\alpha x_\alpha) = \nu(c_\beta x_\beta)$ . Then  $\alpha - \beta = \nu(c_\alpha/c_\beta) \in \nu(k^*)$ . ■

**Corollary 1.4.1** If  $[K:k] < \infty$ , then

- (a)  $\nu(k^*) = 0 \Rightarrow \nu(K^*) = 0$ ,
- (b)  $\nu(k^*) \cong \mathbf{Z} \Rightarrow \nu(K^*) \cong \mathbf{Z}$ ,

**Proof:** Let  $n = |\nu(K^*)/\nu(k^*)|$ . Multiplication by  $n$  is a monomorphism  $\nu(K^*) \rightarrow \nu(k^*)$ . ■

**Corollary 1.4.2** Any nontrivial valuation on an algebraic number field (a finite algebraic extension of  $\mathbf{Q}$ ) has value group  $\cong \mathbf{Z}$ .

## 2 Valuation rings

**Definition 2.1** If  $k$  is a field, a subring  $R \subseteq k$  is a valuation ring means  $x \in k^* \Rightarrow x \in R$  or  $x^{-1} \in R$ .

**Proposition 2.1** Valuation rings are local.

**Proof:** Suppose  $k$  is a field and  $R \subseteq k$  is a valuation ring. Let  $M = \{x \in k: x^{-1} \notin R\}$ . Then  $M \subseteq R$  and is the set of nonunits of  $R$ . To show that  $M$  is the unique maximal ideal of  $R$  it suffices to prove that  $M$  is closed under addition. Let  $x, y \in M$ . Since  $R$  is a valuation ring,  $xy^{-1} \in R$  or  $yx^{-1} \in R$ . Suppose  $xy^{-1} \in R$ . Then  $x + y$  factors in  $R$  as  $x + y = y(xy^{-1} + 1)$  and so is a nonunit of  $R$ . ■

**Note 2.1**  $R \setminus M < k^*$  is the multiplicative group of units of  $R$ .

**Proposition 2.2** Suppose  $\nu: k^* \rightarrow \Gamma$  is a valuation. Then  $R_\nu = \{x \in k: x = 0 \text{ or } \nu(x) \geq 0\}$  is a valuation subring of  $k$  with maximal ideal  $M_\nu = \{x \in k: x = 0 \text{ or } \nu(x) > 0\}$ .

**Proof:** Let  $x \in k^*$ . Then  $\nu(x) \geq 0$  or  $\nu(x^{-1}) = -\nu(x) \geq 0$ . ■

**Proposition 2.3** Suppose  $k$  is a field and  $R \subseteq k$  a valuation subring. Then  $\Gamma = k^*/(R \setminus M)$  is an ordered abelian group with  $\Gamma_+ = M^*/(R \setminus M)$  and the natural projection  $k^* \rightarrow \Gamma$  is a valuation.

**Note 2.2** There is a 1-1 correspondence between valuation rings and isomorphism classes of valuations (order isomorphism classes of value groups).

## 3 Places

**Definition 3.1** Given a field  $K$ , define the extended field  $\overline{K} = K \cup \{\infty\}$  with algebraic operations partially extended so that

- (i)  $x \in K \Rightarrow x + \infty = \infty$ ,
- (ii)  $x \in K^* \Rightarrow x\infty = \infty$ ,
- (iii)  $\infty\infty = \infty$ ,
- (iv)  $\infty^{-1} = 0$

**Definition 3.2** A place is a homomorphism  $\tau: k \rightarrow \overline{K}$  such that  $K \subseteq \tau(k)$ .

**Proposition 3.1** Suppose  $\nu: k^* \rightarrow \Gamma$  is a valuation. Let  $K = R_\nu/M_\nu$  and define  $\tau: k \rightarrow \overline{K}$  to be the natural projection on  $R_\nu$  and  $\infty$  on the complement  $k \setminus R_\nu$ . Then  $\tau$  is a place.

**Proposition 3.2** Suppose  $\tau: k \rightarrow \overline{K}$  is a place. Then  $\tau^{-1}(K)$  is a valuation subring of  $k$ .

**Note 3.1** There is a 1-1 correspondence between order isomorphism classes of valuations and places.

**Theorem 3.1** Suppose  $k$  is a field,  $R \subseteq k$  a subring,  $K$  an algebraically closed field and  $\tau: R \rightarrow K$  a ring homomorphism. Then  $\tau$  can be extended to

- (a) a ring homomorphism  $U \rightarrow K$ , where  $R \subseteq U \subseteq k$  and  $U$  is valuation ring,
- (b) a place  $k \rightarrow \overline{K}$ .

**Proof:** Consider the collection of ring homomorphism extensions of  $\tau$  to subrings  $U$  of  $k$  containing  $R$ , i.e. let

$$\mathcal{R} = \{(U, \sigma): R \subseteq U \subseteq k, \sigma: U \rightarrow K, \sigma|_R = \tau\}.$$

Since  $(R, \tau) \in \mathcal{R}$ ,  $\mathcal{R} \neq \emptyset$ . Inclusion of subrings of  $k$  gives a partial order on  $\mathcal{R}$ . Let  $(U, \sigma)$  be a maximal element of  $\mathcal{R}$ , whose existence is guaranteed by Zorn's lemma. Let  $M = \ker \sigma$ . Since  $U/M \subseteq K$ ,  $M$  is a prime ideal of  $U$ , so  $S = U \setminus M$  is closed under multiplication. Localizing at  $M$  we obtain  $U \subseteq U_M = S^{-1}U$  and extend  $\sigma$  to  $U_M$  by  $s^{-1}u \mapsto \sigma(s)^{-1}\sigma(u)$  for  $s \in S, u \in U$ . Note that  $s \notin M$ , so  $\sigma(s) \neq 0$ . Since  $(U, \sigma)$  is maximal in  $\mathcal{R}$ ,  $U = U_M$ ,  $M$  is the unique maximal ideal of  $U$ , and  $U/M \cong \sigma(U) \subseteq K$  is a field.



## 5 Hilbert's Nullstellensatz

Given a set of polynomials  $I \subseteq k[X_1, \dots, X_n]$  and  $k \subseteq K$ , we denote the zero set (variety) of  $I$  in  $K^n$  by

$$V_K(I) = \{(a_1, \dots, a_n) \in K^n : p \in I \Rightarrow p(a_1, \dots, a_n) = 0\}.$$

Given  $V \subseteq K^n$ , define  $I(V) = \{f \in k[X_1, \dots, X_n] : V \subseteq V(\{f\})\}$ . The set  $I(V)$  is a radical ideal.

**Proposition 5.1** *Suppose  $k$  is a field,  $I \subseteq k[X_1, \dots, X_n] \setminus \{0\}$  is finite, and  $S \subseteq k$  is infinite. Then  $S^n \not\subseteq V(I)$ .*

**Proof:** By taking the product of  $p \in I$  we may assume that  $I = \{p\}$ . Since  $k[X_1, \dots, X_n] \subseteq k(X_1, \dots, X_{n-1})[X_n]$  we may assume  $n = 1$ . Now the result is clear since a polynomial has only finitely many zeros. ■

**Lemma 5.1** *If  $I \subseteq k[X_1, \dots, X_n]$  is an ideal and  $k \subseteq K$  with  $K$  algebraically closed, then  $V_K(I) \neq \emptyset$ .*

**Proof:** Since  $I \subseteq J \Rightarrow V(I) \supseteq V(J)$ , we may assume that  $I$  is maximal. Then  $h = k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/I$  is a field extension of  $k$ . Let  $\{y_1, \dots, y_r\}$  be a transcendence basis for  $h$  over  $k$ . Choose  $f_i \in k(y_i)[X_i] \setminus \{0\}$  such that  $f_i(x_i) = 0$ . Let  $F_i \in k[y_i]$  be the top coefficient of  $f_i$  and choose  $(c_1, \dots, c_n) \in K^n \setminus V(\{F_i\})$ . Extend the  $k$ -algebra homomorphism  $k[y_i] \rightarrow K$  taking  $y_i$  to  $c_i$  to a place  $\tau : h \rightarrow K \cup \{\infty\}$ . Then  $\tau(x_i) \neq \infty$ . ■

**Theorem 5.2** *If  $I$  is an ideal of  $k[X_1, \dots, X_n]$ , then  $I(V(I)) = \sqrt{I}$ .*