11. *Hilbert rings and the Nullstellensatz*

$***$ *Goldman-Krull proof of Hilbert's Nullstellensatz* $***$

If P is an ideal of a commutative ring R, we know that

$$P \text{ is prime} \iff R/P \text{ is an integral domain}$$
$$P \text{ is maximal} \iff R/P \text{ is a field.}$$

We are now going to see a similar characterization for a concept that falls in between prime and maximal.

P is a prime ideal that is not an intersection of strictly larger prime ideals.	$\iff$	R/P is an integral domain whose quotient field is generated (as a ring over R/P) by a single element.

11.1 Definition. An ideal P is a **G-ideal** (or **Goldman-ideal**) if P is a prime ideal which is not an intersection of prime ideals strictly containing P.

Note that P is a G-ideal iff R/P is an integral domain in which the intersection of all non-zero prime ideals is not (0).

11.2 Definition. A domain D with quotient field K is a **G-domain** if K is generated by a single element as a ring over D, i.e., $\exists z \in K$ such that $K = D[z]$.

Some equivalent characterizations of G-domains:

11.3 Lemma. Let D be a domain and K its quotient field. The following are equivalent:

(1) There exists $u \in D \setminus \{0\}$ such that $K = D[u^{-1}]$.

(2) K is generated by a single element as a ring over D.

(3) K is finitely generated as a ring over D.

Proof. $(3 \Rightarrow 1)$ If $K = D[\frac{a_1}{b_1}, \dots, \frac{a_n}{b_n}]$ and $u = b_1 \cdot \ldots \cdot b_n$ then $K = D[u^{-1}]$. $\square$

11.4 Lemma. Let D be a domain, K its quotient field, and $0 \neq u \in D$. Then $K = D[u^{-1}]$ iff u is in the intersection of all prime ideals $P \neq (0)$ of D.

Proof. Suppose $K = D[u^{-1}]$ and let P be a non-zero prime ideal. Pick $b \in P \setminus \{0\}$. Then $b^{-1} = cu^{-n}$ for some $c \in D$ and $n \in \mathbb{N}$. Now $bc = u^n$, therefore $u^n \in P$ and finally $u \in P$.

Conversely, suppose $u \in P$ for every prime ideal $P \neq (0)$. Let $0 \neq b \in D$. Then $u \in \sqrt{Rb}$, meaning there exists $n \in \mathbb{N}$ with $u^n = cb$ for some $c \in D$. Rewritten as $b^{-1} = cu^{-n}$ this shows $b^{-1} \in D[u^{-1}]$. As b was arbitrary, $K = D[u^{-1}]$. $\square$

As a consequence of the previous two lemmata:

11.5 Theorem. Let D be a domain. The intersection of all non-zero prime ideals of D is not (0) iff the quotient field of D is generated by a single element as a ring over D.

Applying this to residue class rings we get:

11.6 Corollary. Let $P \trianglelefteq R$. Then P is a G-ideal iff R/P is a G-domain.

Note that a commutative ring R is a G-domain if and only if (0) is a G-ideal of R.

11.7 Lemma. Let I be an ideal in a commutative ring R. Then

$$\sqrt{I} = \bigcap_{\substack{P \text{ G-ideal} \\ I \subseteq P}} P.$$

Proof. Clearly, $\sqrt{I}$ is contained in every prime ideal containing I. Conversely, if $u \notin \sqrt{I}$ then there exists a G-ideal P containing I with $u \notin P$: As in the proof of $\sqrt{I} = \bigcap_{I \subseteq P \text{ prime}} P$ (10.8), let P be maximal among the ideals containing I and disjoint with $S = \{u^n \mid n \in \mathbb{N}\}$. Then P is prime. Also, P is a G-ideal, because every prime ideal strictly containing P intersects S and therefore contains u, but $u \notin P$. □

11.8 Lemma and Definition. Let R be a commutative ring. Then the following are equivalent

1) Every G-ideal of R is maximal.
2) For every ideal I of R, $\sqrt{I}$ is an intersection of maximal ideals.

A commutative ring satisfying one (and hence both) of the above conditions is called **Hilbert ring** (or **Jacobson ring**).

Proof. $(2 \Rightarrow 1)$ Let P be a G-ideal. Then $\sqrt{P} = P$, because P is prime. By 2), P is an intersection of maximal ideals, but, as a G-ideal, P is no intersection of prime ideals strictly containing P, therefore P must be maximal. □

11.9 Lemma. Let R be a commutative ring. Then $R[x]$ is not a G-domain.

Proof. If R is not a domain, then $R[x]$ is not a domain, let alone a G-domain. Now let R be a domain with quotient field K. We must show that the intersection of all non-zero prime ideals of $R[x]$ is (0).

Since $P \cap R[x]$ is a non-zero prime ideal of $R[x]$ for every non-zero prime ideal P of $K[x]$, it suffices to show that the intersection of all non-zero prime ideals of $K[x]$ is (0).

This is the case because there are infinitely many monic irreducible polynomials in $K[x]$: If there were only finitely many, $p_1 = x, p_2, \dots, p_n$, then $p_1 \cdot \ldots \cdot p_n + 1$ (which is not a unit because its degree is not zero), would not be divisible by any monic irreducible polynomial, a contradiction to $K[x]$ being a unique factorization domain. □

11.10 Corollary. Let K be a field. Then $K[x]$ is a Hilbert ring.

Proof. $K[x]$ is a principal ideal domain, so the only non-maximal prime ideal is (0), which is not a G-ideal by 11.9. Therefore every G-ideal of $K[x]$ is maximal. □

11.11 Lemma. Let $S \subseteq T$ be domains, $T = S[t]$ with t algebraic over S. Then T is a G-domain if and only if S is a G-domain.

Proof. Let K and L be the quotient fields of S and T respectively. Then $L = K[t]$ is algebraic over K (and hence over S). Suppose T is a G-domain. Then $L = T[c^{-1}] = S[t, c^{-1}]$ for some $c \in T$. Both c^{-1} and t are algebraic over S. Let a and b be the leading coefficients of non-zero polynomials f and g in $S[x]$ with $f(c^{-1}) = 0$ and $g(t) = 0$ and let $\tilde{S} = S[a^{-1}, b^{-1}]$. Then c^{-1} and t are integral over $\tilde{S}$. Hence L is integral over $\tilde{S}$, which makes $\tilde{S}$ a field (4.17). Clearly, $\tilde{S} = K$. Therefore K is finitely generated as a ring over S, and S is a G-domain.

The converse is easy. If S is a G-domain then $K = S[s^{-1}]$ for some $s \in S$ and the quotient field of $T = S[t]$ (with t algebraic over S) is $K(t) = K[t] = S[s^{-1}, t] = T[s^{-1}]$. □

11.12 Lemma. Let R be a commutative ring. If Q is a G-ideal of $R[x]$ then $P = Q \cap R$ is a G-ideal of R.

Proof. Let Q be a G-ideal of $R[x]$ and $P = Q \cap R$. Then Q contains $P[x]$ and this containment is strict, because $R[x]/Q$ is a G-domain by hypothesis and $R[x]/P[x] \simeq (R/P)[x]$ is not a G-domain by Lemma 11.9.

Let $S = R/P$ and $T = R[x]/Q$. We know that T is a G-domain and want to show that S is a G-domain.

S is contained in T via $r + P \mapsto r + Q$, which is injective, because $P = Q \cap R$. Also, $T = S[t]$ for $t = x + Q$.

We show that t is algebraic over S: Clearly, $t = x + Q \in T$ is a root of f for any $f \in Q$, and there exists some $f \in Q$ which is not the zero polynomial in $(R/P)[x]$, because $Q \supsetneqq PR[x]$. We can now apply Lemma 11.11. $\square$

11.13 Lemma. Let R be a commutative ring and P a G-ideal of R. Then there exists a maximal ideal M of $R[x]$ with $M \cap R = P$.

Proof. Let $S = R/P$ and K the quotient field of S. As S is a G-domain, $K = S[b]$ for some $b \in K$. Let $\pi\colon S[x] \to S[b]$ be the substitution homomorphism with $\pi(x) = b$, $\pi\big|_S = \mathrm{id}_S$. Since the image of π, $S[b]$, is a field, the $\mathrm{Ker}(\pi) = M$ is a maximal ideal of $S[x]$, and clearly $\mathrm{Ker}(\pi) \cap S = (0)$.

Now $S[x] = (R/P)[x] \simeq R[x]/P[x]$, and every maximal ideal M of $R[x]/P[x]$ corresponds to a maximal ideal Q of $R[x]$ containing $P[x]$ (the inverse image of M under the canonical projection of $R[x]$ onto $(R/P)[x]$, and $M \cap S = (0)$ translates to $Q \cap R = P$. $\square$

Lemma 11.13 and Lemma 11.12 combined yield:

11.14 Theorem. Let R be a commutative ring and P an ideal of R. The following are equivalent:

(1) P is a G-ideal of R.

(2) There exists a maximal ideal M of $R[x]$ with $M \cap R = P$.

(3) There exists a G-ideal Q of $R[x]$ with $Q \cap R = P$.

11.15 Proposition. Let R be a commutative ring.

(1) $R[x]$ is a Hilbert ring if and only if R is a Hilbert ring.

(2) If R is a Hilbert ring, then every maximal ideal Q of $R[x]$ is generated by $P = Q \cap R$ together with some $f \in R[x]$, which represents an irreducible polynomial in $(R/P)[x]$.

Proof. Suppose R is a Hilbert ring, Q a G-ideal of $R[x]$, and $P = Q \cap R$.

$P = Q \cap R$ is a G-ideal of R by 11.12, and hence maximal by hypothesis. Q is the inverse image of some G-ideal $\bar{Q}$ of $R[x]/PR[x] \simeq (R/P)[x]$ under the canonical projection $\pi : R[x] \to R[x]/PR[x]$. As $(R/P)[x]$ is the polynomial ring over a field, $\bar{Q}$ is maximal by 11.10, and therefore Q is a maximal ideal of $R[x]$.

Furthermore, $\bar{Q}$ is generated by a single irreducible polynomial in $\bar{f} \in (R/P)[x]$, so Q is generated by P and f, a representative in $R[x]$ of $\bar{f}$.

We have shown (2), and the "if" direction of (1). The "only if" direction of (1) is easy: R is a homomorphic image of $R[x]$ and the Hilbert ring property clearly carries over to homomorphic images. $\square$

11.16 Theorem. Let K be an algebraically closed field and $n \in \mathbb{N}$. Then

(1) $K[x_1, \ldots, x_n]$ is a Hilbert ring.

(2) Every maximal ideal of $K[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$, for some $a_1, \ldots, a_n \in K$.

Proof. (1) follows from 11.15 by induction. (Note that a field is trivially a Hilbert ring: every prime ideal is maximal.)

Similarly, we show (2) by induction, using 11.15: $n = 1$: if K is algebraically closed, every maximal ideal of $K[x]$ is generated by a monic linear polynomial.

Now let M be a maximal ideal of $K[x_1, \ldots, x_n]$ and $P = M \cap K[x_1, \ldots, x_{n-1}]$. P is a G-ideal by 11.12, and hence maximal by (1). $P = (x_1 - a_1, \ldots, x_{n-1} - a_{n-1})$, by induction hypothesis, therefore $K[x_1, \ldots, x_{n-1}]/P \simeq K$, and every irreducible polynomial of $(K[x_1, \ldots, x_{n-1}]/P)[x_n]$ has the form $x_n - (a_n + P)$, for some $a_n \in K$.

Applying part (2) of 11.15 to $R = K[x_1, \ldots, x_{n-1}]$, M is generated by $x_1 - a_1, \ldots, x_{n-1} - a_{n-1}$ and $x_n - a_n$. □

11.17 Corollary (Version of Hilbert's Nullstellensatz). Let K be an algebraically closed field and $I \trianglelefteq K[x_1, \ldots, x_n]$. Then $\sqrt{I}$ is the intersection of all ideals of the form $M_a = \{f \in K[x_1, \ldots, x_n] \mid f(a) = 0\}$ (with $a \in K^n$) containing I.

11.18 Corollary (Hilbert's Nullstellensatz). Let K be an algebraically closed field and $n \in \mathbb{N}$. If $f_1, \ldots, f_m, g$ are polynomials in $K[x_1, \ldots, x_n]$ such that $g(a) = 0$ for all $a \in K^n$ for which $f_i(a) = 0$ for $1 \leq i \leq m$ then $g \in \sqrt{(f_1, \ldots, f_m)}$.

$* * *$ *classical proof of Hilbert's Nullstellensatz* $* * *$

11.19 Lemma. Let $K \subseteq F$ be fields. If $F = K[z_1, \ldots, z_n]$ (F is generated by $z_1, \ldots, z_n$ as a ring over K) then $z_1, \ldots, z_n$ are algebraic over K.

Proof. Induction on n. If x is transcendental over K then the polynomial ring $K[x]$ is not a field (every polynomial of positive degree is a non-unit).

Now let $F = K[z_1, \ldots, z_n]$, $n > 1$. $F = K(z_1)[z_2, \ldots, z_n]$, so by induction hypothesis $z_2, \ldots, z_n$ are algebraic over $K(z_1)$. There exists an element $r \in K[z_1]$ ($r = g(z_1)$ for some $g \in K[x]$) such that $rz_2, \ldots, rz_n$ are integral over $K[z_1]$. Therefore, for every $f \in K[z_1, \ldots, z_n]$ there exists $m \in \mathbb{N}$ such that $r^m f$ is integral over $K[z_1]$. In particular, this holds for every $f \in K(z_1) \subseteq K[z_1, \ldots, z_n]$.

Suppose z_1 is transcendental over K. Then $K[z_1]$ is a unique factorization domain with infinitely many irreducibles. $K[z_1]$ is integrally closed in its quotient field $K(z_1)$. By the previous paragraph, every element of $K(z_1)$ has a representation as a fraction whose denominator is a power of a fixed polynomial $g(z_1)$. This is false. Therefore, z_1 is algebraic over K. $\square$

11.20 Theorem (weak Nullstellensatz). Let K be an algebraically closed field. Then every maximal ideal of $K[x_1,\dots,x_n]$ is of the form $(x_1-a_1,\dots,x_n-a_n)$ for some $a_1,\dots,a_n\in K$.

Proof. Let M be a maximal ideal of $K[x_1,\dots,x_n]$, and $F=K[x_1,\dots,x_n]/M$ the residue field. The canonical projection $\pi\colon K[x_1,\dots,x_n]\longrightarrow K[x_1,\dots,x_n]/M$, restricted to K is injective, so the elements $k+M$ (with $k\in K$) form an isomorphic copy of K in F, and F is generated as a ring over K by the images of the x_i under π, $F=K[y_1,\dots,y_n]$, with $y_i=x_i+M$.

By 11.19, $y_1,\dots,y_n$ are algebraic over K. As K is algebraically closed, the only monic irreducible polynomials in $K[x]$ are linear, so each y_i is a zero of $x-a_i$ for some $a_i\in K$, i.e., $(x_i+M)-(a_i+M)=0+M$. This implies $x_i-a_i\in M$ for $1\le i\le n$. Since the ideal generated by x_1-a_1, $\dots$, x_n-a_n is maximal, it must be M. $\square$

A really neat argument by Rabinowitsch shows that the Nullstellensatz for n variables follows from the weak Nullstellensatz for $n+1$ variables:

11.21 Theorem. Let K be an algebraically closed field, and $f_1,\dots,f_m,f$ polynomials in $K[x_1,\dots,x_n]$ such that $f(a)=0$ for every common zero $a\in K^n$ of $f_1,\dots,f_m$. Then $f\in\sqrt{(f_1,\dots,f_m)}$.

Proof. Let $f_1,\dots,f_m,f\in K[x_1,\dots,x_n]$ as in the theorem. The polynomials $f_1,\dots,f_m$ and $g=1-x_{n+1}f$ in $K[x_1,\dots,x_{n+1}]$ have no common zero in K^{n+1}. By the weak Nullstellensatz they are not contained in any maximal ideal of $K[x_1,\dots,x_{n+1}]$, so there exist $h_1,\dots,h_m,h\in K[x_1,\dots,x_{n+1}]$ such that

$$f_1h_1+\ldots+f_mh_m+(1-x_{n+1}f)h=1.$$

We now substitute $1/f$ for x_{n+1} and multiply both sides by f^r, where r is the maximal degree in x_{n+1} of any h_i. This gives $f_1g_1+\ldots+f_mg_m=f^r$, where $g_1,\dots,g_m\in R[x_1,\dots,x_n]$, so f is in the radical of the ideal generated by $f_1,\dots,f_m$ in $K[x_1,\dots,x_n]$. $\square$