Algebra I

Nicholas Schwab

Sommersemester 2017

1 The Hilbert Basis- and Nullstellensatz

1.1 Noetherian Rings

Definition 1.1.1. Let R be a ring, and $f_1, \dots, f_n \in R$, then

$$\langle f_1, \dots, f_n \rangle_R = \left\{ \sum_{i=1}^{n} \lambda_i f_i \middle| \lambda_i \in R \right\} = \bigcap_{\substack{I \subseteq R, \\ I \text{ ideal}, \\ f_i \in I \forall i}} I.$$

This is called the *ideal* generated by the f_i and the f_i are called a *basis* or *generators* of I.

Remark. If I is not necessarily finite,

$$\langle f_i \mid i \in I \rangle_R = \left\{ \sum_{i \in I} \lambda_i f_i \middle| \lambda_i = 0 \text{ for all but finitely many } i \right\} = \bigcap_{\substack{I \subseteq R, \\ I \text{ ideal}, \\ f_i \in I \forall i}} I.$$

Definition 1.1.2. Let k be a field, $I \subseteq k[T_1, \dots, T_n]$ an ideal, l a field extension of k. $x \in l^n$ is a zero of I iff $f(x_1, \dots, x_n) = 0$ for all $f \in I$.

Remark. x is a common zero of the $f_i \in k[X_1, \dots, X_n]$ iff is a zero of the ideal generated by the f_i.

Proposition 1.1.1. *For a ring R the following conditions are equivalent:*

a) Every ideal has a finite set of generators (i.e. is finitely generated).

b) Every ascending chain $I_0 \subseteq I_1 \subseteq \dots$ of ideals in R terminates after finitely many steps, i.e. there is some $n \in \mathbb{N}$ such that $I_k = I_n$ for all $k \geq n$.

c) Every non-empty set $\mathfrak{M}$ of ideals in R has an $\subseteq$-maximal element I.

Definition 1.1.3. A ring with these properties is called *Noetherian.*

Example. Fields and principal ideal domains are Noetherian.

Theorem 1.1.1 (Hilbert's Basissatz)**.** *If R is Noetherian, $R[T_1, \dots, T_n]$ (with finite n!) is Noetherian.*

Proof. The proof is recapitulated later on. □

Corollary 1.1.1 (of the Basissatz). *Every polynomial system of equations in finitely many variables over a field has finite subsystem with the same set of solutions.*

Theorem 1.1.2 (Hilbert's Nullstellensatz). *Let k be a algebraically closed field and $I \subsetneq k[X_1, \ldots, X_n]$ a proper ideal. Then I has a zero $x \in k^n$.*

Proof. This will be proofed in a few days. □

1.2 Modules over rings

Definition 1.2.1. An R-Module (where R is a ring) is an abelian group $(M, +)$ with an operation

$$\begin{aligned} \cdot : R \times M &\longrightarrow M \\ (r, m) &\longmapsto r \cdot m \end{aligned}$$

such that

$$\begin{aligned} r \cdot (s \cdot m) &= (r \cdot s) \cdot m \\ (r + s) \cdot m &= r \cdot m + s \cdot m \\ r \cdot (m + n) &= r \cdot m + r \cdot n \\ 1 \cdot m &= m. \end{aligned}$$

A morphism of R-Modules is a map $M \xrightarrow{f} N$ which is a homomorphism of abelian groups compatible with $\cdot$. A submodule of M is a subgroup $X \subseteq M$ of $(M, +)$ such that $R \cdot X \subseteq X$.

Example. The R-submodules of R are the ideals in R.

Proposition 1.2.1. *If $N \subseteq M$ is a R-submodule of the R-module M the quotient group M/N has a unique structure of an R-submodule such that the projection $M \xrightarrow{\pi} M/N$ is a morphism of R-modules, and for arbitrary R-modules T the map*

$$\begin{aligned} \mathrm{Hom}_R(M/N, T) &\longrightarrow \{\tau \in \mathrm{Hom}_R(M, T) | \tau|_N = 0\} \\ t &\longmapsto \tau = t \circ \pi \end{aligned}$$

is bijective, where t is surjective iff τ is and t is injective iff $\ker(\tau)$ equals N.

Remark. Two important corollaries are:

$$(M/L)/(N/L) \xleftarrow{\simeq} M/N$$

for $M \supseteq N \supseteq L$ and, for submodules N and L of M

$$(N + L)/N \xleftarrow{\simeq} L/(N \cap L)$$

where $N + L$ denotes the submodule $\{l + n | l \in L, n \in N\}$ of M.

Definition 1.2.2. If M and N are R-modules, $M \oplus N = \{(m, n), | m \in M, n \in N\} = M \times N$ equipped with component-by-component addition and scalar multiplication. This can be generalized to finitely many summands.

Example. $R^n = \{(r_i)_{i=1}^n | r_i \in R\}$ is an R-module.

Definition 1.2.3. If M is an R-module and $m_1, \ldots, m_k \in M$, then the submodule generated by $\{m_i | 1 \le i \le k\}$ is

$$\left\{ \sum_{i=1}^{k} r_i \cdot m_i \middle| r_i \in R \right\} = \bigcap_{\substack{X \subseteq M \\ X \text{ module} \\ \text{all } m_i \in X}} X$$

As was the case for Definition 1.1.1, this can be generalized to infinitely many generators. M is finitely generated iff there are $(m_i)_{i=1}^{k}$, $k \in \mathbb{N}$, $m_i \in M$ such that the submodules of M generated by the m_i equals M.

Proposition 1.2.2. *Let $N \subseteq M$ be an R-submodule*

a) If M is finitely generated, M/N is finitely generated.

b) If N and M/N are finitely generated, M is finitely generated.

Corollary 1.2.1. *$M \oplus N$ is finitely generated iff M and N are. (Note that: $M \simeq M \oplus \{0\}$ and $(M \oplus N)/M \simeq N$)*

Proposition 1.2.3. *Let M be an R-module. The following properties are equivalent:*

a) Every submodule $N \subseteq M$ of M is finitely generated.

b) Every ascending sequence $N_0 \subseteq N_1 \subseteq \ldots$ of submodules of N terminates.

c) Every non-empty set $\mathfrak{M}$ of R-submodules of M has a $\subseteq$-maximal element.

Proof. **a)** $\to$ **b)** Let $N_\infty = \bigcup_{i=0}^{\infty} N_i$, then this is a submodule, hence finitely generated by a). Let $n_1, \ldots, n_k$, $k \in \mathbb{N}$, generate N_∞ and let j_i, for $1 \le i \le k$, be chosen such that $n_i \in N_{j_i}$ and let $l = \max\{j_i | 1 \le i \le k\}$, then $n_l = N_\infty$.

b) $\to$ **c)** From b) we conclude, that in the $\subseteq$-ordered set $\mathfrak{M}$ every ascending chain has an upper bound in $\mathfrak{M}$, namely the ideal, that terminates the chain. Therefore by Zorn's Lemma there is $\subseteq$-maximal element in $\mathfrak{M}$.

c) $\to$ **a)** Let $\mathfrak{M}$ be the set of finitely generated submodules of N. Since $\{0\} \subseteq N$ is a module, this set is not empty. Therefore there is a $\subseteq$-maximal submodule P in $\mathfrak{M}$ generated by $p_1, \ldots, p_n$. Therefore there is no $f \in N \setminus P$ such that $\langle p_1, \ldots, p_n, f \rangle_R$ is a submodule of N since this would be a superset of P. Hence we have $N = P$ is finitely generated.

□