1.6. $\mathfrak{a} \trianglelefteq R$, $P = R[X_1, \ldots, X_n]$, $\varkappa : R \to R/\mathfrak{a}$.

Define $\psi : P \to R/\mathfrak{a}[X_1, \ldots, X_n]$ by

$$\psi(a) = \varkappa(a), \ a \in R, \ \psi(X_i) = X_i$$

The map is obviously surjective, and the kernel consist of polynomials with coefficients in $\mathfrak{a}$ i.e. $\mathrm{Ker}(\psi) = \mathfrak{a}P$. $\Rightarrow$ iso $P/\mathfrak{a}P \xrightarrow{\sim} R/\mathfrak{a}[X_1, \ldots, X_n]$.

1.9 R, $P = R[X_1, \ldots, X_n]$, $m \leq n$, $a_1, \ldots, a_m \in R$, $\mathfrak{p} = (X_1 - a_1, \ldots, X_m - a_m)$

Define map $\psi : P \to R[X_{m+1}, \ldots, X_n]$ by

$$\psi : X_i \mapsto \begin{cases} a_i & i \leq m \\ X_i & i > m \end{cases}$$

and $\psi(r) = r$, $r \in R$. Then $\mathrm{Ker}\,\psi = \mathfrak{p}$.

Pf. 1) $\mathfrak{p} \subset \mathrm{Ker}(\psi)$: Obvious by construction

2) $\ker \psi \subset \mathfrak{p}$: Let $f(\underline{X}) \in \ker \psi$, i.e. $f(a_1, \ldots, a_m, X_{m+1}, \ldots, X_n) = 0$

By long division we have

$$f(\underline{X}) = q(\underline{X})(X_i - a_i) + r(\underline{X}) \qquad \deg r < \deg f$$

But $f(\underline{a}, \underline{X}) = q(\underline{a}, \underline{X})(a_i - a_i) + r(\underline{a}, \underline{X}) = r(\underline{a}, \underline{X}) = 0$.

The result follows by iteration of this procedure

2.10 $\mathfrak{p} \subset R$ prime

We have $\underset{\text{domain}}{R} \Rightarrow \underset{\text{domain}}{R[X]}$ (AK 2.3 p. 6)

and obviously $\underset{\text{domain}}{R[X]} \Rightarrow \underset{\text{domain}}{R}$

By 1.6 we have $R[X]/\mathfrak{p}R[X] \xrightarrow{\sim} R/\mathfrak{p}[X]$. Thus since $R/\mathfrak{p}$ is a domain, $R/\mathfrak{p}[X]$ is a domain and $R[X]/\mathfrak{p}R[X]$ is a domain $\Rightarrow \mathfrak{p}R[X]$ is a prime.

We have $R[X]/\mathfrak{p}R[X] + (X) \xrightarrow{\sim} R/\mathfrak{p}$, same argument as above

2.11 R domain, $m \leq n$, $\mathfrak{p} = (X_1, \ldots, X_m) \subset R[X_1, \ldots, X_n]$

$$R[X_1, \ldots, X_n]/\mathfrak{p} \xrightarrow{\sim} \underset{\text{domain}}{R[X_{m+1}, \ldots, X_n]}$$

$\Downarrow$

$\mathfrak{p}$ prime.

3.10

$\varphi : R \to R'$ $\qquad$ $\mathfrak{p} \subset R$ ideal $\qquad$ $\mathfrak{q} \subset R'$ ideal

Notation: $\varphi^{-1}(\mathfrak{q}) =: \mathfrak{q}^c$

$R' \cdot \varphi(\mathfrak{p}) =: \mathfrak{p}^e$

1) $(\mathfrak{p}^e)^c = \mathfrak{p} \Leftrightarrow \exists\, \mathfrak{q} \subset R'$ s.t. $\mathfrak{p} = \mathfrak{q}^c$

2) $\mathfrak{p}$ prime s.t. $(\mathfrak{p}^e)^c = \mathfrak{p}$

$\Rightarrow \exists\, \mathfrak{q} \subset R'$ prime s.t. $\mathfrak{q}^c = \mathfrak{p}$.

Pf. General facts: $\mathfrak{p} \subseteq (\mathfrak{p}^e)^c$, $(\mathfrak{q}^c)^e \subseteq \mathfrak{q}$

1) Let $x \in (\mathfrak{p}^e)^c$, i.e. $\varphi(x) \in \mathfrak{p}^e = \varphi(\mathfrak{p}) \cdot R'$. Suppose $\exists\, \mathfrak{q} \subseteq R'$ s.t. $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$. Then $\varphi(\mathfrak{p}) = \varphi(\varphi^{-1}(\mathfrak{q})) \subset \mathfrak{q}$ and $\varphi(x) \in \mathfrak{q} \cdot R' = \mathfrak{q}$. Thus $x \in \varphi^{-1}(\mathfrak{q}) = \mathfrak{q}^c = \mathfrak{p}$. On the other hand, if $\mathfrak{p} = (\mathfrak{p}^e)^c$, then put $\mathfrak{q} = \mathfrak{p}^e$.

2) Let $\mathfrak{p}$, prime, s.t. $(\mathfrak{p}^e)^c = \mathfrak{p}$, and put $S = R - \mathfrak{p}$. Then $(\mathfrak{p}^e)^c \cap S = \emptyset$. Suppose $y \in \mathfrak{p}^e \cap \varphi(S) \neq \emptyset$. Then $\exists\, x \in S$ s.t. $\varphi(x) = y$. But then $x \in \varphi^{-1}(\mathfrak{p}^e) = (\mathfrak{p}^e)^c = \mathfrak{p}$, i.e. $x \in S = R - \mathfrak{p}$ and $x \in \mathfrak{p}$, contradiction. Thus $\mathfrak{p}^e \cap \varphi(S) = \emptyset$. The set $\varphi(S)$ is multiplicatively closed, and put $\mathfrak{q} = R' - \varphi(S)$, a prime. We claim that $\mathfrak{q}^c = \mathfrak{p}$. Since $\mathfrak{p}^e \cap \varphi(S) = \emptyset$ we have $\mathfrak{p}^e \subset \mathfrak{q}$. But then $(\mathfrak{p}^e)^c \subset \mathfrak{q}^c$, and $\mathfrak{p} \subset \mathfrak{q}^c$. On the other hand $\mathfrak{q}^c \subset \mathfrak{p}$ since $x \in \mathfrak{q}^c$ implies $\varphi(x) \in \mathfrak{q} = R' - \varphi(S)$, i.e. $\varphi(x) \notin \varphi(S)$, or $x \notin S$ i.e. $x \in \mathfrak{p}$.

3.19 Let $n = n_1^{r_1} \cdots n_l^{r_l}$. Then $\sqrt{0} = \langle n_1^{s_1} \cdots n_l^{s_l} \rangle$ where $0 < s_i \leq r_i$.

For $n = 12 = 2^2 \cdot 3$ we have $\sqrt{(12)} = \langle 2 \cdot 3 \rangle = (6)$ i.e. $\bar{6}$ is only nilpotent element in $\mathbb{Z}/(12)$

3.20

$\varphi : R \to R'$, $\mathfrak{b} \subseteq R'$ subset

Then $\varphi^{-1}(\sqrt{\mathfrak{b}}) = \sqrt{\varphi^{-1}(\mathfrak{b})}$

Pf. $\subseteq$: Let $x \in \varphi^{-1}(\sqrt{\mathfrak{b}})$. Then $\varphi(x) \in \sqrt{\mathfrak{b}}$. Thus $\exists\, n > 0$ s.t. $\varphi(x^n) = \varphi(x)^n \in \mathfrak{b} \Rightarrow x^n \in \varphi^{-1}(\mathfrak{b})$ and $x \in \sqrt{\varphi^{-1}(\mathfrak{b})}$

$\supseteq$: Let $x \in \sqrt{\varphi^{-1}(\mathfrak{b})}$. Then $\exists\, m > 0$ s.t. $x^m \in \varphi^{-1}(\mathfrak{b})$. Thus $\varphi(x^m) = \varphi(x)^m \in \mathfrak{b}$, i.e. $\varphi(x) \in \sqrt{\mathfrak{b}}$ and $x \in \varphi^{-1}(\sqrt{\mathfrak{b}})$.

4.12. $R \ni x \neq 0$ domain, $M \subset R_{(0)}$ $\quad M$ fin. gen. $\Rightarrow M = \langle 1, x^{-1}, \ldots, x^{-m} \rangle$ and $x^{-n} = \sum_{i=0}^{m} r_i x^{-i}$, $r_i \in R$, $n > m$

M fin. gen., $R_{(0)} = \langle 1, x^{-1}, x^{-2}, \ldots \rangle$ fin. gen.

Thus $x^{-1} = x^{-n} \cdot x^{n-1} = \sum_{i=0}^{m} r_i \cdot x^{-i} \cdot x^{n-1} = \sum_{i=0}^{m} r_i x^{n-1-i}$

But $n-1-i \geq m-i \geq 0$, i.e. $x^{n-1-i} \in R$, and $x^{-1} \in R$.

$\Rightarrow M = \langle 1 \rangle = R$.

5.5 $N \subset M'$, M'' modules, $M = M' \oplus M''$

We have $0 \to N \to M' \to M'/N \to 0$ exact and

$0 \to 0 \to M'' \to M'' \to 0$ exact

But then

$0 \to N \to M' \oplus M'' \to M'/N \oplus M'' \to 0$ is exact,

$\Rightarrow \quad 0 \to N \to M \to M'/N \oplus M'' \to 0$ exact

Consequently $M/N \simeq M'/N \oplus M''$.

5.6 $(*)$: $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$, $\quad M' = \langle x_1, \ldots, x_n \rangle$, $M'' = \langle y_1, \ldots, y_k \rangle$

Then $M = \langle \alpha(x_1), \ldots, \alpha(x_n), z_1, \ldots, z_k \rangle$ where $z_i \in \beta^{-1}(y_i)$

Pf. Let $m \in M$ and suppose $\beta(m) = \sum_{i=1}^{k} r_i y_i$

Then $\beta(m - \sum r_i z_i) = \beta(m) - \sum r_i \beta(z_i)$

$= \sum r_i y_i - \sum r_i y_i = 0$

By exactness of $(*)$ $\ker \beta = \operatorname{im} \alpha$, thus

$m - \sum r_i z_i = \alpha(\sum s_j x_j) = \sum s_j \alpha(x_j) \quad s_j \in R$.

$\Rightarrow \quad m = \sum r_i z_i + \sum s_j \alpha(x_j)$

5.14

$$\begin{tikzcd} M_4 \arrow[r, "\alpha_4"] \arrow[d, "\gamma_4"] & M_3 \arrow[r, "\alpha_3"] \arrow[d, "\gamma_3"] & M_2 \arrow[r, "\alpha_2"] \arrow[d, "\gamma_2"] & M_1 \arrow[r, "\alpha_1"] \arrow[d, "\gamma_1"] & M_0 \arrow[d, "\gamma_0"] \\ N_4 \arrow[r, "\beta_4"] & N_3 \arrow[r, "\beta_3"] & N_2 \arrow[r, "\beta_2"] & N_1 \arrow[r, "\beta_1"] & N_0 \end{tikzcd}$$

exact rows

1) γ_3, γ_1 surjective, γ_0 injective $\Rightarrow$ γ_2 surjective

Pf. Let $y \in N_2$. Then $\exists x_1 \in M_1$ s.t. $\gamma_1(x_1) = \beta_2(y)$. We have

$\gamma_0 \alpha_1(x_1) = \beta_1 \gamma_1(x_1) = \beta_1 \beta_2(y) = 0$. But γ_0 is injective $\Rightarrow$ $\alpha_1(x_1) = 0$

Thus $\exists x_2 \in M_2$ with $\alpha_2(x_2) = x_1$. Furthermore, $\beta_2 \gamma_2(x_2) = \gamma_1 \alpha_2(x_2) = \gamma_1(x_1) = \beta_2(y)$

Thus $\beta_2(y - \gamma_2(x_2)) = 0$ and $\exists y_3 \in N_3$ s.t. $\beta_3(y_3) = y - \gamma_2(x_2)$

The map γ_3 is surjective, and $\exists\, x_3 \in M_3$ s.t. $\gamma_3(x_3) = y_3$.

Put $x = \alpha_3(x_3) + x_2$. Then $\gamma_2(x) = \gamma_2\alpha_3(x_3) + \gamma_2(x_2) = \beta_3\gamma_3(x_3) + \gamma_2(x_2)$

$$= \beta_3(y_3) + \gamma_2(x_2) = y - \gamma_2(x_2) + \gamma_2(x_2) = y$$

2) γ_3, γ_1 injective, γ_4 surjective $\Rightarrow$ γ_2 injective

Pf. Let $x \in M_2$ s.t. $\gamma_2(x) = 0$. Then $\gamma_1(\alpha_2(x)) = \beta_2\gamma_2(x) = 0$ and $\alpha_2(x) = 0$ by assumption. Thus $\exists\, x_3 \in M_3$ s.t. $\alpha_3(x_3) = x$. We have $\beta_3\gamma_3(x_3) = \gamma_2\alpha_3(x_3) = \gamma_2(x) = 0$. Thus $\exists\, y_4 \in N_4$ s.t. $\beta_4(y_4) = \gamma_3(x_3)$. By surjectivity of γ_4, $\exists\, x_4 \in M_4$ s.t. $\gamma_4(x_4) = y_4$. But we have $\gamma_3\alpha_4(x_4) = \beta_4\gamma_4(x_4) = \beta_4(y_4) = \gamma_3(x_3)$, and injectivity of γ_3 gives $\alpha_4(x_4) = x_3$. Thus $0 = \alpha_3\alpha_4(x_4) = \alpha_3(x_3) = x$, and γ_2 is injective

8.8 R' R-algebra, M, N R'-modules $\Rightarrow \exists\, \tau : M \otimes_R N \longrightarrow M \otimes_{R'} N$

canonical, R-linear

Pf$_1$ We use $M \otimes_R N \cong R^{\oplus(M\times N)}/\sim$ (see 8.2.1)

The structure morphism $\gamma: R \to R'$ induces map

$$\tau : R^{\oplus(M\times N)} \longrightarrow R'^{\oplus(M\times N)}$$

M and N are R-modules via γ, thus for $x \in R$, $xm := \gamma(x)\cdot m$

$$\Rightarrow \quad \tau\big((xm, n) - x(m,n)\big) = (\gamma(x)m, n) - \gamma(x)(m,n)$$

and

$$\tau\big((m, xn) - x(m,n)\big) = \big((m, \gamma(x)n) - \gamma(x)(m,n)\big)$$

Thus τ descents down to

$$\tau : M \otimes_R N \longrightarrow M \otimes_{R'} N$$

Pf$_2$ Let $P = M \otimes_{R'} N$ in Thm 8.3. P is a R-module by

$$r\cdot(m \otimes n) = \gamma(r)\cdot(m \otimes n)$$

Now let $\tau' \in \mathrm{Bil}_R(M,N;P)$ be the map $\tau'(m,n) = m\otimes n$.

and put $\tau = \theta^{-1}(\tau')$.