Aneis

$$Def.: R \text{ é anel} \Leftarrow \forall a,b,c \in R, \begin{cases} a+b \in R \\ a+(b+c)=(a+b)+c \\ a+b=b+a \\ \exists 0_R \in R: a+0=a=0+a \\ \exists x \in R: a+x=0_R \\ ab \in R \\ a(bc)=(ab)c \\ a(b+c)=ab+ac \\ (a+b)c=ac+bc \end{cases}$$

R é comutativo $\Leftarrow ab=ba, \forall a,b \in R$

R tem identidade $\Leftarrow \exists 1_R \in R: a1=a=1a, \forall a \in R$

$$R \in D.I. \Leftrightarrow R \text{ é domínio de integridade} \Leftarrow \begin{cases} R \text{ é comutativo com identidade } 1 \neq 0 \\ a,b \in R; ab=0 \Rightarrow a=0 \vee b=0 \end{cases}$$

$$R \in \Phi \Leftrightarrow R \text{ é corpo} \Leftarrow \begin{cases} R \text{ é comutativo com identidade } 1 \neq 0 \\ \forall a \in R: a \neq 0, \exists x \in R: ax=1 \end{cases}$$

$$(3.1) \left.\begin{array}{l} \text{Sejam } R, S \text{ aneis} \\ (r,s)+(r',s')=(r+r',s+s') \in R \times S \\ (r,s)(r',s')=(rr',ss') \in R \times S \end{array}\right\} \Rightarrow R \times S \text{ é anel.}$$

R,S são comutativos $\Rightarrow R \times S$ é comutativo

R,S têm identidade $\Rightarrow R \times S$ tem identidade

$$(3.2) \left.\begin{array}{l} S \subset R, \text{ que é anel} \\ a,b \in S \Rightarrow a+b \in S \\ a,b \in S \Rightarrow ab \in S \\ 0_R \in S \\ a \in S \Rightarrow \exists x \in S: a+x=0_R \end{array}\right\} \Rightarrow S \text{ é subanel de } R$$

$(3.3)\ \forall a \in R, \exists! x \in R: a+x=0; Def.: x=-a; b-a=b+(-a)$

$(3.4)\ \forall a,b,c \in R; a+b=a+c \Rightarrow b=c$

$$(3.5)\ \forall a,b \in R; \begin{cases} a0=0=0a \\ a(-b)=-(ab)=(-a)b \\ -(-a)=a \\ -(a+b)=(-a)+(-b) \\ -(a-b)=-a+b \\ (-a)(-b)=ab \\ 1 \in R \Rightarrow (-1)a=-a \end{cases}$$

$$(3.6) \left.\begin{array}{l} \varnothing \neq S \subset R, \text{ que é anel} \\ a,b \in S \Rightarrow a-b \in S \\ a,b \in S \Rightarrow ab \in S \end{array}\right\} \Rightarrow S \text{ é subanel de } R$$

$$Def.: a \in R, n \in Z, n \geq 1 \Rightarrow a^n \equiv \prod_{i=1}^{n} a; na \equiv \sum_{i=1}^{n} a; -na \equiv \sum_{i=1}^{n} (-a); 0a \equiv 0_R$$

$$\forall a \in R, \forall m,n \in Z, m,n \geq 1; \begin{cases} a^m a^n = a^{m+n} \\ (a^m)^n = a^{mn} \end{cases} (i)$$

$1_R \in R, a \neq 0, a^0 \equiv 1_R \Rightarrow (i)$ vale para $m,n \in Z_+$

$(3.7)\, \forall a,b \in R; a+x=b \Leftrightarrow x=b-a$

$Def.$: Seja $a,1 \in R$. a é unidade $\Leftarrow \exists u \in R : au = 1 = ua; u \equiv a^{-1}$

$U(R) = \{x \in R : xv = 1, \exists v \in R\}$

$F \in \Phi \Rightarrow U(F) = F - \{0\} = F^*$

$(3.8)\, b,1 \in R, a \in U(R) \Rightarrow \begin{cases} ax = b \Leftrightarrow x = a^{-1}b \\ ya = b \Leftrightarrow y = ba^{-1} \end{cases}$

$(3.9)\, \Phi \subset D.I.$

$Ex.$: $Z_6 \notin D.I.; Z_3, Z, Z[x] \in D.I. - \Phi$ (São também $D.E.$); $Q, \Re[x]$ (reais), $C \in \Phi$

$(3.10)\, a,b,c \in R \in D.I., a \neq 0, ab = ac \Rightarrow b = c$

$(3.11)\, R \in D.I., \#R \in Z_+ \Rightarrow R \in \Phi$

$Def.$: $a \in R^*$. a é divisor de 0 $\Leftarrow \exists b \in R^* : ab = 0 \vee ba = 0$

$Def.$: $\varphi : R \mapsto S$ é homomorfismo $\Leftarrow \forall a,b \in R, \begin{cases} \varphi(a+b) = \varphi(a) + \varphi(b) \\ \varphi(ab) = \varphi(a)\varphi(b) \end{cases}$

$Def.$: $\left.\begin{matrix} R \cong S \\ \varphi \text{ é isomorfismo} \end{matrix}\right\} \Leftarrow \exists \varphi : R \mapsto S : \varphi$ é homomorfismo bijetor

$(3.12)\, \varphi : R \mapsto S$ é homomorfismo $\Rightarrow \forall a,b \in R, \begin{cases} \varphi(0_R) = 0_S \\ \varphi(-a) = -\varphi(a) \\ \varphi(a-b) = \varphi(a) - \varphi(b) \end{cases}$

$1_R \in R, \underset{\varphi \text{ é sobrejetor}}{\operatorname{Im}\varphi = S} \Rightarrow \begin{cases} \varphi(1_R) = 1_S \in S \\ u \in U(R) \Rightarrow \varphi(u) \in U(S); [\varphi(u)]^{-1} = \varphi(u^{-1}) \end{cases}$

$(3.13)\, \varphi : R \mapsto S$ é homomorfismo $\Rightarrow S \supset \operatorname{Im}\varphi$ é subanel de S

Aritmética em F[x]

$Def.$: $\sum_{i=0}^{n} a_i x^i \in R[x] \Leftarrow a_i \in R, x \in \tilde{R} \supset R$, que é subanel de $\tilde{R}$

$(4.1)\, \exists P \supset R : \begin{cases} x \in P - R \\ \forall a \in R, xa = ax \\ \forall y \in P, y = \sum_{i=0}^{n} a_i x^i, \exists n \geq 0, \exists a_i \in R \\ \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{m} b_i x^i, n \leq m \Rightarrow \begin{cases} a_i = b_i, \forall i \leq n \\ b_i = 0, \forall i > n \end{cases} \\ p(x) = 0_P \Leftrightarrow a_i = 0, \forall i \end{cases}$

$Def.$: $R = Z, P \equiv Z[x]$

$\nexists \deg 0$

$(4.2)\, R \in D.I.; f,g \in R[x]; f^2 + g^2 \neq 0 \Rightarrow \deg fg = \deg f + \deg g$

$f,g \in R[x] \notin D.I. \Rightarrow \deg fg \leq \deg f + \deg g$

$(4.3)\, R \in D.I. \Rightarrow R[x] \in D.I.$

*Seja $F \in \Phi$

Euclides $(4.4)\, f,g \in F[x], g \neq 0 \Rightarrow \exists!(q,r) : \begin{cases} f = gq + r \\ r = 0 \vee \deg r < \deg g \end{cases} \because 9.1+$

$Def.$: Sejam $a,b,1\in R$ comutativo. $a|b \Leftarrow b=ak, \exists k\in R$

$x\in R \Rightarrow 1|x$

$u\in U(R)\Rightarrow u\,|\,1$

$f|g \Rightarrow cf|g, \forall c\in F^*$

$f|g \Rightarrow \deg f \le \deg g$

$Def.$: $p(x)\in Mon \Leftrightarrow p(x)=\sum_{i=0}^{n} a_i x^i$ é mônico $\Leftarrow a_n=1$

* Sejam $f,g\in F[x]; f^2+g^2\neq 0.$

$Def.$: $\text{mdc}(f,g)=d\in Mon \Leftarrow \begin{cases} d|f, d|g \\ c|f, c|g \Rightarrow \deg c \le \deg d \end{cases}$

$(4.5)\exists! d=\text{mdc}(f,g)$

$\exists u,v\in F[x]: d=fu+gv \because 9.3$

$(4.6)\Leftrightarrow(9.4)$ p/ $\text{mdc}(f,g)$

$(4.7)\Leftrightarrow(9.5)$ p/ $\text{mdc}(f,g)$

$(4.8) R\in D.I. \Rightarrow U(R[x])=U(R) \qquad \Leftrightarrow \{f(x)\in U(R[x])\Leftrightarrow f(x)=u\in U(R)\}$

$(4.9) U(F[x])=F^* \because 3.7+$

$Def.$: $a,b,1\in R$ comutativo. $a\sim b \Leftrightarrow a$ é associado de $b \Leftarrow a=bu, \exists u\in U(R)$

$Def.$ conjunto dos Associados: $r\in R\Rightarrow \text{Assoc}([r])=\{x\in R: x\sim r\}$

$a\sim b\Rightarrow \text{Assoc}(a)=\text{Assoc}(b)$

$U(R)=\text{Assoc}(1) \qquad \Leftrightarrow [u\in U(R)\Rightarrow u\sim 1]$

$u\in F^* \Rightarrow u\sim 1 \because 4.9$

$a\sim b\neq 0 \Rightarrow b|a \wedge a|b$

$f,g\in F[x]\Rightarrow \begin{cases} f(x)\sim cf(x), \forall c\in F^* \\ f(x)\nsim g(x)\Leftrightarrow g(x)\neq cf(x), \forall c\in F^* \end{cases}$

$Def.$: $p\in \text{Irred}(F[x])\Leftrightarrow p\in \underset{\deg p\ge 1}{F[x]-F}$ é irredutível $\Leftarrow (d|p \Rightarrow d\sim p \vee d\sim 1)$

(4.10) Seja $f\in F[x]^*$. $f\notin \text{Irred}(F[x])\Leftrightarrow f=gh; \deg g, \deg h<\deg f$

(4.11) Sejam $b,c\in F[x]; p\in F[x]-F$. $p\in \text{Irred}(F[x]) \underset{\because 9.6}{\Leftrightarrow} (p|bc \Rightarrow p|b \vee p|c) \underset{\because 9.1}{\Leftrightarrow} (p=bc\Rightarrow b\sim 1 \vee c\sim 1)$

$(4.12)\Leftrightarrow 9.6.ii$

$(4.13)\, 9.7+$ p/ $R=F[x]$

$Ex.$ funções: $f(x)=x^4+x+1; g(x)=x^3+x^2+1; f,g\in Z_3[x]\Rightarrow f=g$

$Def.$: Seja $f(x)\in R[x]$ comutativo; $\tilde{f}: R\mapsto R$. $a\in R$ é raiz de $f(x)\Leftarrow \tilde{f}(a)\equiv f(a)=0$

Teorema do resto $(4.14)\, [f(x)]_{x-a}=[f(a)]_{x-a}\in \dfrac{F[x]}{\langle x-a\rangle} \qquad \Leftrightarrow \left[\left.\begin{matrix} q,r\in F[x] \\ f(x)=(x-a)q+r \\ r=0\vee \deg r=0 \end{matrix}\right\}\Rightarrow r=f(a)\right]$

$(4.15)\,(x-a)|f(x)\in F[x]\Leftrightarrow f(a)=0$

$(4.16)\, R\in D.I.; f(x)\in R[x]^*; \deg f=n \Rightarrow \#\{a\in R: f(a)=0\}\le n$

(4.17) Seja $f\in F[x]$. $\deg f\ge 2; f\in \text{Irred}(F[x])\Rightarrow \forall a\in F, f(a)\neq 0$

(4.18) Seja $f\in F[x], \deg f\in\{2,3\}$. $f\in \text{Irred}(F[x])\Rightarrow \forall a\in F, f(a)\neq 0$

$(4.19)\, F\in\Phi; \#F\ge \#Z; f(x)=g(x)\in F[x]\Leftrightarrow \tilde{f}=\tilde{g}\in\{\varphi: R\to R\}$

$f\in Q[x]\Rightarrow \exists c\in Z: cf\in Z[x] \because f=\sum_{i=0}^{n}\dfrac{p^i}{q^i}x^i \Rightarrow c=\underset{i}{\text{mmc}}(q_i)$

Raízes Racionais $(4.20)\ f(x)\in Z[x], r,s\in Z^*, f\left(\frac{r}{s}\right)=0\Rightarrow r|a_0 \wedge s|a_n$

(4.21) Sejam $p\in \text{Irred}(Z); f,g,h\in Z[x]; f=\sum_{i=0}^{n+r} a_i x^i = gh, g=\sum_{i=0}^{n} b_i x^i, h=\sum_{i=0}^{r} c_i x^i$

$p|a_i, \forall i\le n+r \Rightarrow p|b_i, \forall i\le n \vee p|c_i, \forall i\le r$

(4.22) Seja $f(x)\in Z[x]. f=gh; \deg g=n; \deg h=r; g,h\in Q[x] \Leftrightarrow f=pq, \deg p=n, \deg q=r; p,q\in Z[x]$

Eisenstein (4.23) Seja $f(x)\in Z[x]. \left.\begin{array}{l}\exists p\in \text{Irred}(Z): p|a_i, \forall i<n=\deg f\\ p\nmid a_n, p^2\nmid a_0\end{array}\right\}\Rightarrow f\in \text{Irred}(Q[x])$

$\forall n\ge 1, \exists f\in \text{Irred}(Q[x]): \deg f=n$

(4.24) Sejam $f=\sum_{i=0}^{n} a_i x^i\in Z[x], p\in \text{Irred}(Z_+), p\nmid a_n. \tilde{f}=\sum_{i=0}^{n}[a_i]_p x^i\in \text{Irred}(Z_p[x])\Rightarrow f\in \text{Irred}(Q[x])$

$(4.25)\ \forall p\in C[x]-C, \exists a\in C: p(a)=0$

$(4.26)\ p\in \text{Irred}(C[x]) \Leftrightarrow \deg p=1$

$(4.27)\ f\in C[x], \deg f=n\ge 1\Rightarrow f(x)=c\prod_{i=1}^{n}(x-a_i), \exists!\{c,a_i\}\subset C$

$(4.28)\ a+bi\in C, f\in \Re[x], f(a+bi)=0\Rightarrow f(a-bi)=0$

$(4.29)\ f\in \text{Irred}(\Re[x]) \Leftrightarrow \deg f=1 \vee f(x)=ax^2+bx+c, \Delta<0$

$(4.30)\ f\in \Re[x], \deg f=2k+1, k\in Z_+ \Rightarrow \exists a\in \Re: f(a)=0$

Ideais

Def.: I é subanel de R. $I\in$ ideais$(R)\Leftrightarrow I$ é ideal de $R \Leftarrow (r\in R, a\in I\Rightarrow ra, ar\in I)$

(6.1) Seja $R\supset I\neq\varnothing$. $I\in$ ideais$(R)\Leftrightarrow \begin{cases} a,b\in I\Rightarrow a-b\in I\\ r\in R, a\in I\Rightarrow ra, ar\in I\end{cases}$

Def. ideal principal gerado finitamente: Seja $c_i\in R. \langle c_1,c_2,\ldots,c_n\rangle_{R^n}\equiv\{\vec{\mathbf{c}}\cdot\vec{\mathbf{t}}:\vec{\mathbf{t}}\in R^n\}$

$(6.2)\ 1\in R$ comutativo $\Rightarrow \langle c\rangle\in$ ideais$(R), \forall c\in R$

$(6.3)\ 1\in R$ comutativo $\Rightarrow \langle c_1,c_2,\ldots,c_n\rangle\in$ ideais$(R), \forall c_i\in R, \forall n\ge 1$

* Seja $I\in$ ideais(R).

Def. congruência módulo $I: a,b\in R. a\equiv b(\text{mod } I)\Leftarrow a-b\in I$

Def. classe de congruência: $[a]=[a]_I=\{x\in R: x\equiv a(\text{mod } I)\}=\{a+i: i\in I\}$

$(6.6)\ [a]=[b]\Leftrightarrow a\equiv b(\text{mod } I)$

$(6.7)\ x,y\in R\Rightarrow [x]\cap[y]=\varnothing \vee ([x]=[y]\Leftrightarrow [x]\subset[y]\subset[x])$

$(6.4)\ a,b,c\in R\Rightarrow \begin{cases}[a]=[a]\\ [a]=[b]\Rightarrow[b]=[a]\\ [a]=[b]=[c]\Rightarrow[a]=[c]\end{cases}$

$\begin{pmatrix}6.5\ \text{módulo}\\ 6.8\ \text{classes}\end{pmatrix} a,b,c,d\in R; [a]=[b], [c]=[d]\Rightarrow \begin{cases}[a+c]=[b+d]\\ [ac]=[bd]\end{cases}$

Aneis Quociente

$Def.: \frac{R}{I} = \{[x]_I : x \in R\}$

$(6.9)\, S = \frac{R}{I} \text{ é anel}: \begin{cases} [a+b]=[a]+[b] \in S, [ab]=[a][b] \in S \\ R \text{ é comutativo} \Rightarrow S \text{ é comutativo} \\ \exists 1_R \Rightarrow \exists 1_S \end{cases}$

$(6.10)\, \varphi : R \mapsto S \text{ é homomorfismo} \Rightarrow \ker\varphi = \{r \in R : \varphi(r) = 0_S\} \in \text{ideais}(R)$

$(6.11)\, \varphi : R \mapsto S \text{ é homomorfismo}; \ker\varphi = \{0_R\} \Leftrightarrow \varphi \text{ é injetor}$

$(6.12)\, \varphi : R \mapsto \frac{R}{I}; \varphi(r) = [r]_I \Rightarrow \begin{cases} \varphi \text{ é homomorfismo, chamado natural; } \operatorname{Im}\varphi \underset{\varphi \text{ é sobrejetor}}{=} \frac{R}{I} \\ \ker\varphi = I \end{cases}$

1o Teorema do Isomorfismo $(6.13)\, \varphi : R \mapsto S = \operatorname{Im}\varphi \text{ é homomorfismo} \Rightarrow \frac{R}{\ker\varphi} \cong \operatorname{Im}\varphi$

$Def.: R \text{ é comutativo. } I \text{ é ideal primo} \Leftarrow \begin{cases} I \neq R \\ bc \in I \Rightarrow b \in I \vee c \in I \end{cases}$

$(6.14)\, 1 \in R \text{ é comutativo} \Rightarrow \left(I \text{ é ideal primo} \Leftrightarrow \frac{R}{I} \in D.I. \right)$

$Def.: I \text{ é ideal maximal} \Leftarrow \begin{cases} I \neq R \\ I \subset \tilde{M} \subset R \Rightarrow \tilde{M} = I \vee \tilde{M} = R \end{cases}$

$(6.15)\, 1 \in R \text{ é comutativo} \Rightarrow \left(I \text{ é ideal maximal} \Leftrightarrow \frac{R}{I} \in \Phi \right)$

$(6.16)\, 1 \in R \text{ é comutativo}; I \text{ é ideal maximal} \Rightarrow I \text{ é ideal primo}$

Aritmética em Domínios de Integridade

$*\text{Seja } R \in D.I.$

$Def.\text{ generaliza 4.9+} : \text{Irred}(R) = \{p \in R^* - U(R) : x|p \Rightarrow x \sim p \vee x \sim 1\}$

$(9.1)\; p \in \text{Irred}(R) \Leftrightarrow (p = rs \Leftrightarrow r \sim 1 \vee s \sim 1)$

$Def.: R \in D.E. \Leftrightarrow R \text{ é Domínio Euclideano} \Leftarrow \exists N : R^* \mapsto Z_+ : \begin{cases} a,b \in R^* \Rightarrow N(a) \leq N(ab) \\ a,b \in R; b \neq 0 \Rightarrow \exists q,r \in R : \begin{cases} a = bq + r \\ r = 0_R \vee N(r) < N(b) \end{cases} \end{cases}$

$*\text{Sejam } a,b \in R \in D.E.$

$(9.2)\, u \in R^* \Rightarrow [u \sim 1 \Leftrightarrow N(u) = N(1_R) \Leftrightarrow \exists c \in R^* : N(c) = N(uc)]$

$Def.\text{ conjunto dos máximos divisores comuns} : d \in \underset{\text{generaliza 4.7+}}{\text{MDC}(a,b)} \subset R \Leftarrow \begin{cases} a^2 + b^2 \neq 0 \\ d|a, d|b \\ c|a, c|b \Rightarrow N(c) \leq N(d) \end{cases}$

$(9.3)\, d \in \text{MDC}(a,b) \Rightarrow \begin{cases} \text{Assoc}(d) = \text{MDC}(a,b) \quad \Leftrightarrow \begin{cases} r \sim d \in \text{MDC}(a,b) \Rightarrow r \in \text{MDC}(a,b) \\ \{x,y\} \subset \text{MDC}(a,b) \Rightarrow x \sim y \end{cases} \\ \exists u,v \in R : d = au + bv \end{cases}$

$(9.4)\, d \in \text{MDC}(a,b) \Leftrightarrow \begin{cases} d|a, d|b \\ c|a, c|b \Rightarrow c|d \end{cases}$

$(9.5) \left. \begin{matrix} a|bc \\ \text{MDC}(a,b) = U(R) \ni 1 \end{matrix} \right\} \Rightarrow a|c$

(9.6) Seja $p \in \text{Irred}(R)$. $p|ab \underset{(i)}{\Rightarrow} p|a \vee p|b$

$$p\left|\prod_{n=1}^{M} a_n \underset{(ii)}{\Rightarrow} \exists n_0 < M : p\right|a_{n_0}$$

$D.E. \underset{9.8}{\subset} D.I.P. \underset{9.12}{\subset} D.F.U. \quad \underset{9.14}{\subset} A.C.C.$

$D.E. \quad \underset{9.7}{\subset} D.F.U.$

$D.I.P. \quad \underset{9.10}{\subset} A.C.C.$

$$Def.: R \in D.F.U. \Leftrightarrow R \text{ é Domínio de Fatoração Única} \Leftarrow \begin{cases} r \in R^* - U(R) \Rightarrow r = \prod_{i=1}^{n} p_i, \exists n \geq 1, \exists p_i \in \text{Irred}(R) \\ \text{Unicidade}: r = \prod_{i=1}^{n} p_i = \prod_{j=1}^{s} q_j \Rightarrow \begin{cases} n = s \\ \forall i \leq n, \exists j \leq n : p_i \sim q_j \end{cases} \end{cases}$$

$Def.: R \in D.I.P. \Leftrightarrow R$ é Domínio Ideal Principal $\Leftarrow [I \in \text{ideais}(R) \Rightarrow I = \langle c \rangle, \exists c \in R]$

$$(9.9)\, a,b \in R \in D.I. \Rightarrow \begin{cases} \langle a \rangle \subseteq \langle b \rangle \Leftrightarrow b|a \\ \langle a \rangle = \langle b \rangle \Leftrightarrow a \sim b \neq 0_R \\ \langle a \rangle \subset \langle b \rangle \neq \langle a \rangle \Leftrightarrow b|a \wedge b \nmid a \end{cases}$$

$Def.: R \in A.C.C. \Leftrightarrow \underset{\text{"condição de cadeia ascendente"}}{R \text{ satisfaz } A.C.C.}$ em ideais principais $\Leftarrow [\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq ... \Rightarrow \exists n_0 \in Z_+ : \forall n \geq n_0, \langle a_n \rangle = \langle a_{n_0} \rangle]$

(9.11) Em um $D.I.P.$, vale $9.6.i$

Fatores comuns (9.13) Sejam $a,b \in R^*; R \in D.F.U.$

$$\exists u,v \in U(R); \exists n \geq 1; \exists \alpha_i, \beta_i \geq 0; \exists p_i \in \text{Irred}(R): \begin{cases} \forall i,j \leq n, i \neq j \Rightarrow p_i \nmid p_j \\ a = u\prod_{i=1}^{n} p_i^{\alpha_i} \\ b = v\prod_{i=1}^{n} p_i^{\beta_i} \end{cases}$$

$$a|b \Leftrightarrow \alpha_i \leq \beta_i, \forall i \leq n$$

$$\text{MDC}(a,b) = \text{Assoc}\left(\prod_{i=1}^{n} p_i^{m_i}\right), m_i = \min\{\alpha_i, \beta_i\}$$

$$\text{MMC}(a,b) \ni uv\prod_{i=1}^{n} p_i^{M_i}, M_i = \max\{\alpha_i, \beta_i\}$$

(9.15) Em um $D.F.U.$, vale $9.6.i$

$$(9.16) \left.\begin{matrix} R \in A.C.C. \\ \text{Vale } 9.6.i \end{matrix}\right\} \Rightarrow R \in D.F.U.$$

Generalização de 9.3: $(9.17)\, R \in D.I.; d \in \text{MDC}(a_1, a_2, ..., a_n) \Rightarrow \text{MDC}(a_i) = \text{Assoc}(d)$

Generalização de 9.13: (9.18) Sejam $t \geq 2; a_k \in R \in D.F.U.$

$$\sum_{k=1}^{t} a_k^2 \neq 0 \Rightarrow \begin{cases} a_k = u_k\prod_{i=1}^{n} p_i^{\alpha_{k,i}} \\ \text{MDC}(a_k) = \text{Assoc}\left(\prod_{i=1}^{n} p_i^{m_i}\right), m_i = \min\{\alpha_{1,i}, \alpha_{2,i}, ..., \alpha_{n,i}\} \\ \text{MMC}(a_k) \ni \prod_{k=1}^{t}\prod_{i=1}^{n} u_k p_i^{M_i}, M_i = \max\{\alpha_{1,i}, \alpha_{2,i}, ..., \alpha_{n,i}\} \end{cases}$$

$Def.: N : Z[\sqrt{d}] \mapsto Z; N(a + b\sqrt{d}) = a^2 - db^2$

$d < 0 \Rightarrow N(x) \geq 0, \forall x \in Z[\sqrt{d}]$

$$Def.: Z[\sim p^2] = \left\{ x \in Z - \{1\} : \left. x = \prod_{\substack{i=1 \\ \exists n \geq 1; \exists p_i \in Z; \exists \alpha_i \geq 1}}^{n} p_i^{\alpha_i} \right| \Rightarrow \alpha_i \neq 2, \forall i \leq n \right\}$$

$*$Seja $d \in Z[\sim p^2]$

$(9.19)\, \forall a,b \in Z[\sqrt{d}], \begin{cases} N(a)=0 \Leftrightarrow a=0 \\ N(ab)=N(a)N(b) \end{cases}$

$(9.20)\, u \in U(Z[\sqrt{d}]) \Leftrightarrow |N(u)|=1$

$(9.21)\, d>1 \Rightarrow \#U(Z[\sqrt{d}]) \geq \#Z$

$U(Z[i]) = \{\pm 1, \pm i\}$

$d<-1 \Rightarrow U(Z[\sqrt{d}]) = \{\pm 1\}$

$(9.22)\, N(p) \in \text{Irred}(Z) \Rightarrow p \in \text{Irred}(Z[\sqrt{d}])$

(9.23) 9.7+, sem unicidade, p/ $R = Z[\sqrt{d}]$

$Def.: r \in C$ é nro. algébrico $\Leftarrow \exists f(x) \in Q[x] \cap Mon : f(r)=0$

r é algébrico; $\deg f = n \Rightarrow \begin{cases} C \supset Q(r) = \left\langle r, r^2, \ldots, r^{n-1} \right\rangle_{Q^{n-1}} \in \Phi \\ x \in Q(r) \Rightarrow x \text{ é algébrico} \end{cases}$

(9.24) r é algébrico; $R = Q(r) \cap Z \Rightarrow [I \in \text{ideais}(R) - R; I \neq \{0\} \Rightarrow I \in D.F.U.]$

$*$Seja $R \in D.I.$

$Def.: \text{Frac}(R) \equiv \left\{ \frac{a}{b} : a \in R, b \in R^* \right\}$

$*$Sejam $\frac{a}{b}, \frac{c}{d}, \frac{a'}{b'}, \frac{c'}{d'} \in \text{Frac}(R)$

$(9.25)\, ad = bc \Rightarrow \frac{a}{b} = \frac{c}{d}$

$Def.: \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}; \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

$(9.26)\, \frac{a}{b} = \frac{a'}{b'}; \frac{c}{d} = \frac{c'}{d'} \Rightarrow \begin{cases} \frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'} \\ \frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'} \end{cases}$

$(9.27)\, \frac{0}{b} = \frac{0}{d}$

$\frac{a}{b} = \frac{ad}{bd}$

$\frac{b}{b} = \frac{d}{d}$

$(9.28)\, \text{Frac}(R) \in \Phi$

$(9.29)\, \text{Frac}(R) \supset \tilde{R} = \left\{ \frac{a}{1} : a \in R \right\} \cong R$

$(9.30)\, \exists \text{Frac}(R)$ com 9.25,28,29

$(9.31)\, D \in D.I.; D \subset F \in \Phi \Rightarrow \exists X \in \Phi : D \subseteq X \cong \text{Frac}(D) \subseteq F$

$*$Seja $R \in D.F.U.$

(9.32) Vale 9.7+, sem unicidade, em $R[x]$

Análogo a 9.6.i $(9.33)\, f, g \in R[x]; p \in \text{Irred}(R); p | f(x)g(x) \Rightarrow p | f(x) \vee p | g(x)$

$Def.: f \in R[x]$ é primitivo $\Leftarrow [c|f(x) \Rightarrow c \in U(R)]$

(9.34) $f, g \in R[x]$ são primitivos $\Rightarrow fg$ é primitivo

$*$ Sejam $f, g \in R[x]$, primitivos.

(9.35) Sejam $r, s \in R^*.\ rf(x) = sg(x) \Rightarrow r \sim s, f \sim g$

(9.36) $\dfrac{f(x)}{1} \sim \dfrac{g(x)}{1} \in \text{Frac}(R)[x] \Rightarrow f(x) \sim g(x)$

(9.37) $\text{Irred}(R[x]) \subset \text{Irred}(\text{Frac}(R)[x])$

(9.38) $R \in D.F.U. \Rightarrow R[x] \in D.F.U.$

(9.39) $Z[x] \in D.F.U. - D.I.P.$