Elementárna teória deliteľnosti

0. Deliteľnosť: $a|b \Leftrightarrow (\exists c \in A)\ b = c.a$. Reflexívna a tranzitívna relácia.

1. Obor integrity s 1

 a) delitele jednotky

 b) množina $U(A)$ je grupa

2. asociovanosť: $a|b \wedge b|a$. $(a \approx b)$

 $a \approx b \Leftrightarrow \exists\, u \in U(A)\ a = u.b$

 $a = u.b,\ b = v.a \Rightarrow a = (u.v).a \Rightarrow 1.a = (u.v).a \Rightarrow$

 $u.v = 1$, t.j. $u \in U(A)$ (zároveň $v \in U(A)$).

 Naopak, hneď vidíme, že $b|a$. Keďže je $u \in U(A)$, $\exists v \in A$ také, že $u.v = 1$, t.j.

 $a = ub \Rightarrow va = (vu)b = b$, t.j. $a|b$.

3. Nsd (a,b): Nech $a \neq 0$ alebo $b \neq 0$. d je nsd(a,b) ak

 a) $d|a$, $d|b$

 b) $c|a \wedge c|b \Rightarrow c|d$.

 Vo všeobecnosti to nemusí existovať.
 Ak existuje, je určený až na asociovanosť.
 (to je hneď vidieť z podmienky b)).

4. Prienik ideálov je ideál.

5. Nech $X \subseteq A$, $(X) = \bigcap \{I \subseteq A;\ X \subset I,\ I \text{ je ideál}\}$

 je tzv. ideál generovaný mn. X.

6. ak $X = \{x_1, \dots, x_n\}$, $(X) \overset{M=}{=} \{a_1x_1 + \dots + a_nx_n;\ a_i \in A\}$

 odvodíme $X \subseteq M$, lebo $x_i = 0.x_1 + \dots + 1.x_i + 0\,x_{i+1} + \dots 0.x_n$

 Keďže ideál je uzavretý na násobenie prvkami z A, každé $a_ix_i \in (X)$, a keďže ideál je uzavretý na súčty, je $a_1x_1 + \dots + a_nx_n \in (X)$.

 Teda $M \subseteq (X)$. Ľahko overíme, že M je ideál, preto $M = (X)$.

7. Nech $(A,+,\cdot)$ je ~~obor~~ OI s 1 taký, že
$\forall I$ ideál $(\exists a\in A)$, že $I=(a)=a.A\ (=\{r.a;\ r\in A\})$.
Takýto okruh nazývame okruh hlavných ideálov.
~~Veta: $(\{a,b\})=(a,b)=(nsd(a,b))$ v okruhu hl. ideálov.~~
Treba si uvedomiť, že a z predošlej definície je
určené až na asociovanosť, t.j. $(a)=(b)\iff a\approx b$
(Lebo $b\in(b)=(a)$, t.j. $b=ka$, čiže $a|b$. Podobne $b|a \Rightarrow a\approx b$.
Ak $a|b$, tak $(b)\subseteq(a)$. Ak $b|a$, tak $(a)\subseteq(b)$)
Veta: $(\{a,b\})\ (=(a,b))=(d)$, tak $d=nsd(a,b)$.
Totiž $a\in(d)$, $b\in(d)$, preto $d|a$, $d|b$.
Dokazujeme, že $\exists u,v\in A$ také, že $d=ua+bv$
lebo $(d)=(a,b)=\{sa+tb;\ s,t\in A\}$ a $d\in(d)=(a,b)$.
Teda ak $c|a \wedge c|b \Rightarrow c\,|\,ua+bv=d$.

8. Dôsledok: V OHI pre každé a,b, a aspoň $b\neq 0$ existuje $nsd(a,b)$.
Naviac, ak $d=nsd(a,b)$ tak $\exists u,v\in A$ také, že $d=ua+vb$.

9. Euklidovský okruh. Príklad: $(\mathbb{Z},+,\cdot)$; $(F[x],+,\cdot)$ pre pole F.

10. Nech I je ideál v $(E,+,\cdot)$. Potom $\exists a\in E$ také,
že $I=\{r.a;\ r\in E\}$.
Dôkaz: Ak $I=\{0\}$, tak $a=0$.
Nech $I\neq\{0\}$, t.j. $\exists b\in I$, $b\neq 0$. Položme
$M=\{g(b);\ b\in I\setminus\{0\}\}$.
M je neprázdna množina pr. čísel, nech d je jej najmenší
prvok a nech $a\in I\setminus\{0\}$ je taký, že $g(a)=d$.
Dokážeme, že $I=\{r.a;\ r\in A\}$.
Nech $b\in I\setminus\{0\}$, nech $b=qa+r$, $r=0$ al. $g(r)<g(a)$.
Zrejme $r=b-qa\in I$, lebo $b\in I$, $a\in I\Rightarrow b\in I$, $qa\in I$,
ale ak je $r\neq 0$, tak $g(r)\not< g(a)=d$ – spor s definíciou čísla d.
Teda pre každé $b\in I\setminus\{0\}$ $(\exists q\in A)$ také, že $b=qa$, teda
$I=\{r.a;\ r\in A\}$.

11. Dôsledok 1: Ak $(E,+,\cdot)$ je Euklid. okruh, tak má 1.

Dôkaz: E je ideál v $(E,+,\cdot)$, t.j. $\exists\, a \in E$ také, že $E = \{r.a;\ r \in E\}$. Zrejme $a \in E$, t.j. $a \in \{r.a;\ r \in E\}$, nech r je také, že $a = r.a$. Zoberme $b \in E$. Ukážeme, že $b.r = b$. Totiž $\exists$ s také, že $b = s.a$, lebo $b \in \{r.a;\ r \in E\}$.

Potom $b.r = s.a.r = s.(r.a) = s.a = b$. Teda r je jednotka v $(E,+,\cdot)$ (lebo je to kom. okruh).

12. Dôsledok 2: Euklid. okruh je OHI. Existujú v ňom nsd(a,b).

13. Definícia: Nech $p \neq 0$, $p \notin U(A)$, $(A,+,\cdot)$ je obor integrity s 1. Hovoríme, že p je ireducibilný prvok okruhu A, ak $p = a.b \Rightarrow a \approx 1$ alebo $a \approx p$ (t.j. aj $b \approx 1$ alebo $b \approx p$).

~~Veta: Ak $(A,+,\cdot)$ je OHI, p je ireducibilný, $p \mid a.b$. Potom $p \mid a$ alebo $p \mid b$.~~

Nech

14. Veta: Ak $(A,+,\cdot)$ je OHI, nech nsd$(p,a) = 1$. Nech $p \mid a.b$. Potom $p \mid b$.

Dôkaz: $(\exists\, u,v \in A)$ $1 = up + va$. Potom

$b = b.1 = b(up + va) = bup + vab$. Keďže $p \mid ab$, tak $p \mid bup + vab = b$.

15. Dôsledok: Ak $(A,+,\cdot)$ je OHI, p je ireducibilný, $p \mid a.b$. Potom $p \mid a$ alebo $p \mid b$.

Dôkaz: ak $p \nmid a$, tak nsd$(p,a) = 1$, lebo nsd$(p,a) \mid p$ a preto je nsd$(p,a) \approx 1$ alebo $\approx p$. Keďže $p \nmid a$, druhá možnosť nenastáva. Teda nsd$(p,a) = 1$ a teda $p \mid b$.

?

Odtiaľto až do konca je E euklidovský obor.

16. Nech $0 \neq a = u.v$, $u, v \notin U(E)$, E je eukl. obor.

Potom $g(u), g(v) < g(a)$.

Z definície vieme, že $g(u), g(v) \leq g(a)$.

Nech $u = qa + r$, $r = 0$ alebo $g(r) < g(a)$.

Potom $r = u - qa = u - quv = u(1 - qv)$. Preto

$g(u) \leq g(r) < g(a)$, t.j. $g(u) < g(a)$.

$r = 0$ je neprípustné, lebo to by znamenalo, že $a | u$, čo spolu s $a = u.v$ dáva $a \approx u$, t.j. $v \approx 1$.

17. ~~Nech~~ Podľa dôkazu vety v 10 vidíme, že

$E = (1) = (a) \Leftrightarrow a \in U(E) \Leftrightarrow g(a) = d = \min\{k;\ k = g(r);\ r \in E \setminus \{0\}\}$

lebo ideál I bol generovaný ktorýmkoľvek prvkom s touto vlastnosťou.

18. Nech $a \neq 0$. Potom $a \in U(E)$ alebo $\exists p_1, \dots, p_k$ také, že $p_1 \cdots p_k$ sú ireducibilné a $a = p_1 \cdots p_k$.

Dôkaz: indukciou podľa $g(a)$. Nech tvrdenie platí pre všetky prvky $b \neq 0$ také, že $g(b) < g(a)$.

Nech ~~$\exists$~~ $\exists u, v \notin U(E)$ také, že $a = u.v$.

Podľa 16 je $g(u), g(v) < g(a)$, podľa IP $\exists p_1, \dots, p_k$, $p_{k+1}, \dots, p_{k+l}$ také, že $u = p_1 \dots p_k$, $v = p_{k+1} \dots p_{k+l}$, p_j sú ireduc.

Ak $u, v \in U(E)$ kedykoľvek $a = uv$, tak je a prvočíslo, t.j. $a = p_1$.

Štart indukcie zabezpečuje 17.

19. Nech $a \neq 0$, $a \notin U(E)$. Potom je rozklad $a = p_1 \cdots p_k$ jednoznačný až na asociovanosť a poradie činiteľov.

$p_1 \cdots p_k = q_1 \dots q_l \Rightarrow p_1 | q_1 \dots q_l \Rightarrow \exists j$ také, že

$p_1 | q_j$. Keďže q_j je prvočíslo, $p_1 \approx q_j$, t.j. $p_1 = u.q_j$, $u \in U(E)$.

Potom $p_2 \cdots p_k = (u q_1) q_2 \dots q_{j-1} q_{j+1} \dots q_l$ indukciou dostaneme výsledok. Podľa 16, 17 nemôže byť súčin ~~[illegible]~~ ireduc. prvkov prvok z $U(A)$ ← "štart indukcie"

20. Nech $(A,+,\cdot)$ je OHI, $\{0\} \neq I \neq A$ je prvoideál.

Potom I je maximálny ideál.

Nech $I = (a)$, $I \subseteq J \subseteq A$, $J = (d)$.

Teda $d \mid a$, $a = d.u$.

Keďže I je prvoideál, je $d \in I$ alebo $u \in I$.

1. $d \in I \Rightarrow d = v.a \Rightarrow d = v.(d.u) = (v.u).d \Rightarrow v, u \in U(A)$,

$\quad$ t.j. $d \approx a$ a $I = J$

2. $u \in I \Rightarrow u = v.a \Rightarrow a = (d.v)a \Rightarrow 1 = d.v \Rightarrow d \approx 1 \Rightarrow (d) = (1) = A$.

21. Dôsledok: Nech $(A,+,\cdot)$ je OHI, $p \neq 0$, $p \notin U(A)$.

Potom (p) je prvoideál $\Leftrightarrow$ p je ireducibilný v $(A,+,\cdot)$