1. *Az R egységelemes kommutatív gyűrűben definiáljuk az ideálok közötti oszthatóságot az $A \mid B \Leftrightarrow B \subseteq A$ feltétellel. Mi a legnagyobb közös osztó, a legkisebb közös többszörös, irreducibilis elem, egység, relatív prím elempár erre az oszthatóságra nézve? Mutassuk meg, hogy Dedekind-gyűrűben ez az oszthatóság ekvivalens azzal, hogy $B = AC$ valamilyen C ideálra.*

Megoldás: $l.n.k.o(A, b) = A + B$
$l.k.k.t.(A, b) = A \cap B$
A egység $\Leftrightarrow$ A tartalmaz minden ideált $\Leftrightarrow$ $A = R$
A irreducibilis $\Leftrightarrow$ A-t csak önmaga és R tartalmazza $\Leftrightarrow$ A maximális
A és B relatív prímek $\Leftrightarrow$ $A + B = R$
P prím $\Leftrightarrow$ $(AB \subseteq P \Rightarrow A \subseteq P$ vagy $A \subseteq P)$ $\Leftrightarrow$ P prímideál:
$\Rightarrow$: $ab \in P \Rightarrow (a)(b) \subseteq P \Rightarrow (a) \subseteq P$ vagy $(b) \subseteq P \Rightarrow a \in P$ vagy $b \in P$;
$\Leftarrow$: Tegyük fel, hogy $AB \subseteq P$, de $A \not\subseteq P$. Ekkor van $a \in A \setminus P$, és erre $aB \subseteq AB \subseteq P \Rightarrow ab \in P\ \forall b \in B$, így $b \in P\ \forall b \in B \Rightarrow B \subseteq P$.

2. *Legyen R Dedekind-gyűrű, $A, B, C \triangleleft R$. Bizonyítsuk be, hogy*

a) ha $C \neq (0)$, akkor $AC \subseteq BC \Leftrightarrow A \subseteq B$;
b) $A \cap (B + C) = A \cap B + A \cap C$;
c) $A \cap B + C = (A + C) \cap (B + C)$.

Megoldás: a) $AC \subseteq BC \Leftrightarrow \exists D : AC = BCD \Leftrightarrow \exists D : A = BD$ az egyértelmű prímfelbontás miatt $\Leftrightarrow A \subseteq B$

b),c) Ha $A = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, $B = P_1^{\beta_1} \cdots P_r^{\beta_r}$ és $C = P_1^{\gamma_1} \cdots P_r^{\gamma_r}$ (a valamelyikben nem szereplő prímideált ott 0 kitevővel írva), akkor a két bizonyítandó összefüggés: $\max(\alpha_i, \min(\beta_i, \gamma_i)) = \min(\max(\alpha_i, \beta_i), \max(\alpha_i, \gamma_i))$, és $\min(\alpha_i, \max(\beta_i, \gamma_i)) = \max(\min(\alpha_i, \beta_i), \min(\alpha_i, \gamma_i))$.

3. *Legyen $R = \mathbb{Z}[\sqrt{-5}]$.*

a) Adjuk meg 6-nak két (lényegesen) különböző, irreducibilis elemekre való felbontását R-ben.
b) Adjuk meg a (6) ideálnak a prímideálokra való felbontását R-ben.

Megoldás:

a) $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ (ld. 6./8. feladat)
b) $(2, 1+\sqrt{-5})(2, 1-\sqrt{-5})(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. Ezeknek az elemeit felírva láthatjuk, hogy maximális ideálok. Pl. $I = (2, 1+\sqrt{-5}) = \{\, a+b\sqrt{-5} \mid a, b \in \mathbb{Z},\ a \equiv b \pmod 2 \,\}$, így minden kívül levő elem $1 + a$ alakban írható, ahol $a \in I$, tehát az összes I-t valódi módon tartalmazó ideál tartalmazza 1-et, vagyis azonos R-rel.

4. *Legyen R Dedekind-gyűrű, $A, B \triangleleft R$. Bizonyítsuk be, hogy ha A és B relatív prímek, és $c, d \in R$, akkor van olyan $x \in R$, amire $x \equiv c\ ((\text{mod A}))$ és $x \equiv d\ ((\text{mod B}))$. Mondjuk ki, és lássuk be az állítás megfelelőjét $A_1, A_2, \ldots, A_n$ páronként relatív prím ideálokra (Kínai maradéktétel).*

Megoldás: A és B relatív prímek: $A+B = R$, így van olyan $a \in A$ és $b \in B$, hogy $a+b = 1$. Azt kell belátni, hogy van olyan $x \in R$, amelyre $x - c \in A$ és $x - d \in B$. $a + b = 1 \Rightarrow (c - d)a + (c - d)b = c - d$ implies $x = (d - c)a + c = (c - d)b + d$-re $x - c = (d - c)a \in A$, és $x - d = (c - d)b \in B$.

Általánosan n-re vonatkozó teljes indukcióval bizonyítjuk. $A_1, \dots, A_n$ páronként relatív prímekre és c_i-kre az indukciós feltevés miatt van c, amelyre $c \equiv c_i \pmod{\mathrm{A_i}}$ Ehhez elég találni egy x-et, hogy $x \equiv c \pmod{\mathrm{A_1 \cap \ldots \cap A_{n-1}}}$, és $x \equiv c_n \pmod{\mathrm{A_n}}$. A 2.c) feladat miatt $A_1 \cap \ldots \cap A_{n-1} + A_n = (A_1 + A_n) \cap \ldots \cap (A_{n-1} + A_n) = R \cap \ldots \cap R = R$, tehát $A_1 \cap \ldots \cap A_{n-1}$ és A_n relatív prímek, és így létezik ilyen x az első eset miatt.

5. *Legyen R Dedekind-gyűrű, $A, B \lhd R$, $(0) \neq B \subseteq A$, és $A = P_1^{n_1} \cdots P_k^{n_k}$, $B = P_1^{m_1} \cdots P_k^{m_k}$ az A és B prímtényezős felbontása. Mutassuk meg, hogy van olyan a eleme A-nak, amelyre $a \notin P_i^{n_i+1}$ minden i-re, és hogy ezzel az a elemmel $A = B + (a)$.*

Megoldás: Létezik $c_i \in P_i^{n_i} \setminus P_i^{n_i+1}$ minden i-re az egyértelmű prímfelbontás miatt,és így a kínai maradéktétel miatt van olyan $x \in R$, hogy $x \equiv c_i \pmod{\mathrm{P_i^{n_i+1}}}$ minden i-re. Ebből következik, hogy $x \in P_1^{n_1} \cap \ldots \cap P_k^{n_k} = P_1^{n_1} \cdots P_k^{n_k} = A$ (ugyanis $P_1^{n_1}, \dots, P_k^{n_k}$ páronként relatív prímek, ld. 6/Hf2.), és $x \notin P_i^{n_i+1}$, mert $c_i \notin P_i^{n_i+1}$. Legyen $a = x$. Erre $B \subseteq B + (a) \subseteq A$. Ha $B + (a) \neq A$, akkor $B + (a) = P_1^{\ell_1} \cdots P_k^{\ell_k}$ valamely $n_i \leq \ell_i \leq m_i$ kitevőkkel, és van olyan j, amelyre $\ell_j > n_j$. Így $a \in P_j^{\ell_j} \subseteq P_j^{n_j+1}$ ellentmondás. Tehát $B + (a) = A$.

6. *Bizonyítsuk be, hogy Dedekind-gyűrűben minden ideál generálható legfeljebb két elemmel.*

Megoldás: Legyen $0 \neq A \lhd R$, $0 \neq b \in A$ és $B = (b)$. Ekkor az 5. feladat szerint van olyan $a \in A$, hogy $A = B + (a)$, és így $A = (a, b)$

7. *Legyen $R = K^{n \times n}$ egy K (ferde)test fölötti mátrixgyűrű. Csupán R gyűrűműveleteinek ismeretében hogyan határozhatjuk meg n-et és K-t, ha*
  a) K (kommutatív) test;
  b) K ferdetest?

Megoldás: a) Ebben az esetben $Z(R) \cong K$ és R mint K-vektortér dimenziója n^2 (az R vektortérszerkezetet úgy látjuk, hogy a $Z(R)$ elemeivel való szorzást nézzük). A $Z(R) = \{\, \lambda I \mid \lambda \in K \,\} \cong K$ bizonyítása: A skalármátrixok nyilván felcserélhetők mindennel. Ha pedig egy A mátrix mindennel felcserélhető, akkor $a_{jk} E_{i\ell} = E_{ij} A E_{k\ell} = A E_{ij} E_{k\ell} = 0$, ha $j \neq k$, így A diagonális mátrix: $\sum a_{ii} E_{ii}$, és így $a_{jj} E_{ij} = E_{ij} A = A E_{ij} = a_{ii} E_{ij}$ miatt A skalármátrix.

b) R-ben az idempotens ($e^2 = e$ egyenletet kielégítő) elemek mint lineáris transzformációk egy-egy altérre való vetítések: $V = V_1 \oplus V_2$ esetén $v_1 + v_2 \mapsto v_1$ nyilván idempotens, és fordítva, ha φ idempotens, akkor $V = \operatorname{Ker} \varphi \oplus \operatorname{Im} \varphi$: diszjunktak, mert ha $\mathbf{v}\varphi \in \operatorname{Ker} \varphi$, akkor $\mathbf{v}\varphi = \mathbf{v}\varphi^2 = 0$, és kigenerálják az egész V-t, mert $v \in V$-re $(\mathbf{v} - \mathbf{v}\varphi)\varphi = \mathbf{v}\varphi - \mathbf{v}\varphi^2 = 0$, tehát $\mathbf{v} - \mathbf{v}\varphi \in \operatorname{Ker} \varphi$, és ebből $\mathbf{v} \in \operatorname{Im} \varphi + \operatorname{Ker} \varphi$. Az idempotensek közül is kiválaszthatjuk azokat, amelyeknek nincs olyan $e = e_1 + e_2$ idempotensekre való bontása, amelyekre $e_1 e_2 = e_2 e_1 = 0$; ezek lesznek az egydimenziós alterekre való vetítések. Végül ha e egy ilyen idempotens, akkor $eRe \cong \operatorname{Hom}(K, K) \cong K$, így meghatározhatjuk K-t. n pedig az egységelem ortogonális (azaz páronként 0 szorzatú) idempotensekre való maximális felbontásában a tagok száma.