COURSE 5

Divisibility în integral domains

Let $(R, +, \cdot)$ be an integral domain.

Definition 1. The relation $|$ defined on R by

$$a \mid b \Leftrightarrow \exists\, x \in R,\ b = ax$$

is called **the divisibility relation on** R, and if $a \mid b$ one says that a **divides** b or a **is a divisor of** b or b **is a multiple of** a or b **factorizes through** a.

Theorem 2. (Some properties of the divisibility relation)
Let $a, a', b, b', c \in R$. The following statements hold:
(i) $1 \mid a$, $a \mid a$, $a \mid 0$;
(ii) $0 \mid a$ if and only if $a = 0$;
(iii) if $a \mid b$ and $b \mid c$ then $a \mid c$;
(iv) if $a \mid b$ and $a' \mid b'$ then $aa' \mid bb'$;
(v) if $a \mid b$ then $a \mid bc$;
(vi) for $c \neq 0$, $a \mid b$ if and only if $ac \mid bc$;
(vii) if $a \mid b$ and $a \mid c$ then $a \mid b + c$;
(viii) if $a \mid b + c$ and $a \mid b$ then $a \mid c$; .

Remark 3. The divisibility relation is a reflexive and transitive relation which is not always a partial order. The integral domain $(\mathbb{Z}, +, \cdot)$ is an example in this respect since, as we already saw, $2 \mid -2$, $-2 \mid 2$ and $2 \neq -2$.

Definition 4. One says that the elements $a, b \in R$ are **associates** (or **associated elements**), and we write $a \sim b$, if $a \mid b$ and $b \mid a$.

The previous notion determines a relation $\sim$ on R.

Theorem 5. (Some properties of the relation $\sim$)
Let $a, a', b, b', c \in R$. The following statement hold:
(i) $a \sim a$;
(ii) if $a \sim b$ then $b \sim a$;
(iii) if $a \sim b$ and $b \sim c$ then $a \sim c$;
(iv) $a \sim 0$ if and only if $a = 0$;
(v) if $a \sim b$ and $a' \sim b'$ then $aa' \sim bb'$;
(vi) $a \sim 1 \ \Leftrightarrow\ a \mid 1 \ \Leftrightarrow\ a$ is a unit in R;
(vii) $a \sim b$ if and only if there exists $u \in U(R)$ such that $b = ua$.

Corollary 6. The relation $\sim$ is an equivalence relation on R. If $a \in R$ then the equivalence class of a modulo $\sim$ is

$$[a] = aU(R) = \{ax \mid x \in U(R)\}.$$

Remarks 7. i) In any integral domain R, the class $[0]$ has only one element which is 0.
ii) For any $a \in R$ the units of R and the associates of a are divisors of a. Any other divisor of a is called **non-trivial divisor**.
iii) The divisibility relation on R is a partial order if and only if the only unit of R is 1.

Theorem 8. Let R be an integral domain. The quotient set $R/\sim = \{[a] \mid a \in R\}$ is a partial ordered set (poset) with respect to the relation $\leq$ defined by:

$$[a] \leq [b] \Leftrightarrow a \mid b\,.$$

Remark 9. From theorem 5 one deduces that $[1] = U(R)$, and from theorem 2 it follows that $[1]$ is the smallest element of the poset $(A/\sim, \leq)$.

Examples 10. a) In the integral domain $(\mathbb{Z}, +, \cdot)$, $[1] = U(\mathbb{Z}) = \{-1, 1\}$. So,

$$m \sim n \Leftrightarrow m \in \{-n, n\}$$

and $[n] = \{-n, n\}$ for any $n \in \mathbb{Z}^*$. In the poset $(\mathbb{Z}/\sim, \leq)$, $[0] = \{0\}$ is the greatest element element, and if $m, n \in \mathbb{Z}^*$ then

$$\{-m, m\} \leq \{-n, n\} \Leftrightarrow m \mid n.$$

Since each class from $\mathbb{Z}/\sim$ contains exactly one natural number, studying the divisibility in $\mathbb{Z}$ comes to studying the divisibility in $\mathbb{N}$.
b) If K is a field (for instance, K can be $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ (with p prime)) then K is an integral domain with $U(K) = K^*$. Thus in K, $a \sim b$ for any $a, b \in K^*$, hence $K/\sim$ has only two elements: $\{0\}$ (which is $[0]$ and is the greatest element) and K^* (which is $[1]$ and is the smallest element).
c) If R is an integral domain then $U(R[X]) = U(R)$, hence for any $f, g \in R[X]$,

$$f \sim g \;\Leftrightarrow\; \exists\, a \in R^* \text{ unit in } (R, \cdot) \text{ such that } f = ag.$$

In particular, if $f, g \in \mathbb{Z}[X]^*$ then

$$f \sim g \;\Leftrightarrow\; f = \pm g,$$

and if K is a field, then in the integral domain $K[X]$,

$$f \sim g \;\Leftrightarrow\; \exists\, a \in K^* :\; f = ag.$$

Thus, each class from $K[X]^*/\sim$ contains exacly one polynomial with the leading coefficient 1.
d) We saw in the previous course that $U(\mathbb{Z}[i]) = \{-1, 1, -i, i\}$, so, if $z_1, z_2 \in \mathbb{Z}[i]$ then

$$z_1 \sim z_2 \;\Leftrightarrow\; z_2 \in \{-z_1, z_1, -iz_1, iz_2\}.$$

e) Since $U(\mathbb{Z}[i\sqrt{5}]) = \{-1, 1\}$, $z_1 \sim z_2$ in $\mathbb{Z}[i\sqrt{5}]$ if and only if $z_2 \in \{-z_1, z_1\}$.

Theorem 11. Let R be an integral domain and $a, b \in R$. Then:
i) $a \mid b \;\Leftrightarrow\; (b) \subseteq (a) \;\Leftrightarrow\; bR \subseteq aR$;
ii) $a \sim b \;\Leftrightarrow\; (a) = (b) \;\Leftrightarrow\; aR = bR$.

From the previous theorem one immediately deduce the following:

Corollary 12. For any elements $a, b \in R$ of an integral domain R we have:
$[a] \leq [b] \;\Leftrightarrow\; bR \subseteq aR\,$;
$[a] = [b] \;\Leftrightarrow\; aR = bR\,$.

The greatest common divisor and the least common multiple

Let $(R,+,\cdot)$ be an integral domain.

Definition 13. Let $a_1,\dots,a_n\in R$. We say that $d\in R$ is **a greatest common divisor** (abreviated **gcd**) of $a_1,\dots,a_n\in R$ if in the poset $(R/\sim,\le)$

$$\exists\inf([a_1],\dots,[a_n])\in R/\sim \ \text{ and } [d]=\inf([a_1],\dots,[a_n]).$$

If $a,b\in R$ and $\inf([a],[b])=[1]$, i.e. 1 is a gcd of a and b, we say that a and b are **coprime**.

We identify each class from $R/\sim$ by a representantive and, this way, the fact that d a gcd of $a_1,\dots,a_n$ is denoted, as for integers, by $d=(a_1,\dots,a_n)$.

Remarks 14. a) If $d=(a_1,\dots,a_n)$ then

$$d'=(a_1,\dots,a_n)\ \Leftrightarrow\ d'\sim d.$$

b) Since $[a]\le[b]$ in $R/\sim$ means $a|b$ in R, one can rewrite the gcd definition as follows:

$$d=(a_1,\dots,a_n)\Leftrightarrow\begin{cases} d\mid a_1,\ \dots,\ d\mid a_n\\ d'\in R,\quad d'\mid a_1,\dots,d'\mid a_n\Rightarrow d'\mid d\end{cases}.$$

c) For $a,b\in R$,

$$a\mid b\ \Leftrightarrow\ (a,b)=a.$$

d) If any two elements from R have a gcd, then for any $a_1,a_2,a_3\in R$ there exists a gcd (a_1,a_2,a_3) and $((a_1,a_2),a_3)=(a_1,a_2,a_3)=(a_1,(a_2,a_3))$.
e) If any two elements from R have a gcd, then, for any $n\in\mathbb{N}^*$ and any $a_1,\dots,a_n\in R$, there exists $(a_1,\dots,a_n)$.

Theorem 15. If any two elements from R have a gcd and $a,b,c\in R$ then:
(1) $(a,b)c=(ac,bc)$;
(2) $(a,b)=1$ and $(a,c)=1\Rightarrow(a,bc)=1$;
(3) $a\mid bc$ and $(a,b)=1\Rightarrow a\mid c$.

Corollary 16. If $d=(a,b)$ and $a=da'$, $b=db'$ then $(a',b')=1$.

Definition 17. Let $a_1,\dots,a_n\in R$. One says that $m\in R$ is a **least** (or **lowest**) **common multiple** (abreviated **lcm**) of $a_1,\dots,a_n$ if in the poset $(R/\sim,\le)$

$$\exists\sup([a_1],\dots,[a_n])\in R/\sim \ \text{ and } [m]=\sup([a_1],\dots,[a_n]).$$

We identify each class from $R/\sim$ by a reprezentantive and, this way, the fact that m is a lcm of $a_1,\dots,a_n$ is denoted by $m=[a_1,\dots,a_n]$.

Remarks 18. a) If $m=[a_1,\dots,a_n]$ then

$$m'=[a_1,\dots,a_n]\ \Leftrightarrow\ m'\sim m.$$

b) One can rewrite the lcm definition by means of divisibility relation as follows:

$$m=[a_1,\dots,a_n]\Leftrightarrow\begin{cases} a_1\mid m,\ \dots,\ a_n\mid m\\ m'\in R,\quad a_1\mid m',\dots,a_n\mid m'\Rightarrow m\mid m'.\end{cases}$$

c) For $a, b \in R$,

$$a \mid b \Leftrightarrow [a, b] = b.$$

d) If any two elements of R have a lcm, then for any $a_1, a_2, a_3 \in R$ there exists a lcm $[a_1, a_2, a_3]$ and $[[a_1, a_2], a_3] = [a_1, a_2, a_3] = [a_1, [a_2, a_3]]$. e) If any two elements of R have a lcm, then for any $n \in \mathbb{N}^*$ and any $a_1, \ldots, a_n \in R$ there exists $[a_1, \ldots, a_n]$.

Theorem 19. If for any $a, b \in R$ there exists (a, b) then there also exists a lcm for a and b and we can choose it such that $ab = (a, b)[a, b]$.

Theorem 20. If R is a principal ideal domain (PID) then:
1) For any $a, b \in R$ there exist a gcd and a lcm.
2) $d = (a, b) \Leftrightarrow dR = aR + bR$.
3) $m = [a, b] \Leftrightarrow mR = aR \cap bR$.

Corollary 21. If R is a PID and $a, b, d \in R$ then
a) $d = (a, b) \Rightarrow \exists\, u, v \in R;\ d = au + bv$;
b) $(a, b) = 1 \Leftrightarrow \exists\, u, v \in R;\ au + bv = 1$.

Remark 22. Since $\mathbb{Z}$ is a PID the Bézout representation of the gcd of two integers is a particular case of the previous corollary.