3. FACTORIZATION IN COMMUTATION RINGS

We always assume that R is commutative.

Definition.

1. $a|b$ if $b = ac$ for some $c \in$ R.
2. a, b are associates, if $a|b$ and $b|a$.
3. a is a unit if $a|1$.
4. a is irreducible if
   a. $a \neq 0$, unit;
   b. $a = bc \Rightarrow$ b is a unit or c is a unit.
5. a is prime if
   a. $a \neq 0$, unit;
   b. $a|bc \Rightarrow a|b$ or $a|c$.

Lemma. Let R be an integral domain and $a \in$ R is a prime, then a is irreducible.

Proof. Suppose $a|bc$, then $a|b$ or $a|c$, say $a|b$. Then $b = ad$ for some $d \in$ R. Thus $a = bc = adc$, hence $a \cdot (1 - dc) = 0 \because$ R is an integral domain $\Rightarrow dc = 1$ (c is a unit). □

Example. R=$\mathbb{Z}_{12}, \bar{3} = \bar{3} \times \bar{9}$ is not irreducible(reducible), suppose $\bar{3}|\bar{a}\bar{b}$ for $a, b \in \mathbb{Z}$. Then $3|ab + 12k$ hence $3|ab$. So $3|a$ or $3|b$. And we have $\bar{3}|\bar{a}$ or $\bar{3}|\bar{b}$. Thus $\bar{3}$ is a prime.

Definition. An integral domain R is a unique factorization domain(UFD) if

1. for any nonzero nonunit element $a \in$ R$, a = c_1c_2 \cdots c_n$ for some irreducible elements $c_i \in$ R.
2. if $c_1c_2 \cdots c_n = d_1d_2 \cdots d_m$ for c_i, d_j irreducible, then $n = m$ and there exists a bijection σ such that $d_i, c_{\sigma(i)}$ are associates.

Example. $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5}|a, b \in \mathbb{Z}\}$. We have $4 = 2 \times 2 = (\sqrt{5}+1)(\sqrt{5}-1)$. Since $2, \sqrt{5}+1, \sqrt{5}-1$ are irreducible $\Rightarrow \mathbb{Z}[\sqrt{5}]$ is not UFD. Note $2, \sqrt{5}+1, \sqrt{5}-1$ are not primes in $\mathbb{Z}[\sqrt{5}]$.

Lemma. Let R be UFD. Then an irreducible element is a prime.

Proof. Let $a \in \mathrm{R}$ be irreducible. Suppose that $a|bc$ and $a \nmid b$. Then $ad = bc$ for some d. Since a is not associated any irreducible factors of $b \Rightarrow a|c$. $\square$