(1) Let $R$ be unital. The *units* of $R$ are the elements which have a multiplicative inverse. They form a group $U(R)$ under multiplication.

(2) A *left (resp right) ideal* of $R$ is an additive subgroup $I \subseteq (R, +)$ such that $RI \subseteq I$ (resp $IR \subseteq I$). A *two sided ideal* is an additive subgroup with both these properties.

(3) If $I$ is a two sided ideal then the quotient abelian group $R/I$ has a natural ring structure, where $(a+I)(b+I) = ab+I$.

(4) A *ring HM* is a map $\phi : R \rightarrow S$ which preserves both $+$ and $\times$, that is $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$. The *kernel* is $\{ r : \phi(r) = 0 \}$ and the *image* is $\{ \phi(r) : r \in R \}$.

(5) The image of a ring under a HM is a ring, the kernel of a HM is a two sided ideal.

(6) If $\phi : R \rightarrow S$ is a HM then $R/\ker(\phi) \cong \text{im}(\phi)$.

(7) For the rest of this handout $R$ is a commutative ring with $1$.

(8) An ideal $I$ is *prime* iff $I \neq R$ and $ab \in I$ implies $a \in I$ or $b \in I$, and *maximal* if $I \neq R$ and $I$ is maximal under inclusion among proper ideals (that is $I \subseteq J \subseteq R$ implies $J = I$ or $J = R$ for any ideal $J$).

(9) $I$ is prime iff $R/I$ is an ID and *maximal* iff $R/I$ is a field. In particular $R$ is an ID iff the zero ideal is prime, and is a field iff it is maximal.

(10) Two nonzero elements of an ID are *associates* iff each divides the other, equivalently one is a unit times the other. This is an ER.

(11) Let $R$ be an ID. Then $a \in R$ is *irreducible* iff $a$ is a nonzero nonunit and $a = bc$ implies one of $b, c$ is a unit (note that $b$ is a unit iff $c$ is an associate of $a$). $a$ is *prime* iff $a$ is a nonzero nonunit and $Ra$ is a prime ideal, that is $a|bc$ implies that $a|b$ or $a|c$. Prime elements are irreducible.

(12) $R$ is a *unique factorisation domain (UFD)* iff $R$ is an ID and every element has a factorisation into irreducibles, which is unique up to order and associates. In a UFD irreducible elements are prime.

(13) $R$ is a *principal ideal domain (PID)* iff $R$ is an ID and every ideal is principal (that is of form $Ra$ for some $a$). A PID is a UFD. In a PID $Ra$ is maximal for $a$ irreducible, and if $R$ is not a field the converse holds.
(14) $R$ is a **Euclidean domain** iff $R$ is an ID and there is a **Euclidean function** $\phi$ from $R$ to $\mathbb{N}$. That is for all $a$ and all $b \neq 0$ there exist $q, r$ such that $a = bq + r$ and either $r = 0$ or $\phi(r) < \phi(b)$. Euclidean domains are PIDs. $\mathbb{Z}$ is Euclidean, and so is $F[x]$ for $F$ any field.