Some Ring Theory Class Notes

Class March 12

Conventions regarding 1 (multiplicative unity):

1. Every ring R has a multiplicative unity denoted by 1 or 1_R such that $1 * a = a * 1 \ \forall\ a \in R$. Note: $1 = 0$ in $R \Leftrightarrow R = \{0\}$ because $\forall a \in R$: $a = a * 1 = a * 0 = 0$.
2. Any subring S of R must contain 1_R. For subring, check
   (a) $1_R \in S$
   (b) $a \in S \implies -a \in S$
   (c) $a, b \in S \implies a + b \in S$
   (d) $a, b \in S \implies ab \in S$

   Note: An ideal I of R is a subring if and only if $I = R$ ($1 \in I \implies a = a * 1 \in I\ \forall\ a \in R$).

   Example 0.1. $R \times \{0\} = \{(a, 0) \mid a \in R\}$ is not a subring of $R \times R$ if $R \neq \{0\}$ since $(1, 1) \notin R \times \{0\}$. But $\{(a, a) \mid a \in R\}$ is a subring of $R \times R$.
3. For any ring homomorphism $\varphi : R \to S$ we require $\varphi(1_R) = 1_S$. Note that this is not a consequence of the other ring homomorphism properties:
   (a) $\varphi(a + b) = \varphi(a) + \varphi(b)\ \forall a, b \in R$
   (b) $\varphi(ab) = \varphi(a)\varphi(b)\ \forall\ a, b \in R$

   $\varphi(0) = 0$ is a consequence of (a): $\varphi(0) = \varphi(0+0) = \varphi(0)+\varphi(0) \implies 0 = \varphi(0)$. For multiplication, $\varphi(1) = \varphi(1 * 1) = \varphi(1) * \varphi(1)$ does not necessarily imply $1 = \varphi(1)$ since $\varphi(1)$ need not have a multiplicative inverse in S.

   Example 0.2. $\varphi : R \to R \times R$ which maps $a \to (a, 0)$ is NOT a ring homomorphism since $\varphi(1_R) = (1_R, 0) \neq 1_{R \times R}$ if $R \neq \{0\}$

   Example 0.3. $\psi : R \to R \times R$ which maps $a \to (a, a)$ is a ring homomorphism.
4. For an integral domain R (commutative without zero divisors) we also require $1 \neq 0 \Leftrightarrow R \neq \{0\}$ (neither integral domain nor a field)

   Example 0.4. (a) of fields: $\mathbb{R}, \mathbb{Z}_p$ (p prime), $\mathbb{Q}, \mathbb{C}$. $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ subfield of $\mathbb{R}$. Check: $0 \neq x \in \mathbb{Q}(\sqrt{2}) \implies x^{-1} \in \mathbb{Q}(\sqrt{2})$ (need $\sqrt{2} \notin \mathbb{Q}$).
   (b) of integral domains which are no fields: $\mathbb{Z}$, when n is a prime $\implies \mathbb{Z}_n$ is an integral domain, but also a field. When n is not a prime $\implies \mathbb{Z}_n$ has zero divisors and isn't an integral domain. Specifically $\exists\ l, m \in \mathbb{N},\ 1 < l, m < n$ such that $n = lm \rightsquigarrow$ (modulo n). $[0] = [n] = [lm] = [l][m]$ in $\mathbb{Z}_n$ (such that $[l] \neq [0]$ and $[m] \neq [0]$.
   (c) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ subring of $\mathbb{C}$; $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$.
   (d) commutative rings which are not integral domains. $\mathbb{Z}_n$, n is not prime. $\mathbb{Z} \times \mathbb{Z}$ has zero divisors e.g. $(1, 0) * (0, 1) = (0, 0)$.
   (e) of non-commutative rings:

i. $M(n, R)$, $n \geq 2$ and R any ring $\neq \{0\}$. $\exists A, B \in M(n, R)$ such that $AB \neq BA$

ii. Hamilton's quaternions $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ ($\cong \mathbb{R}^4$ as abelian group). Multiplication is induced by that $\mathbb{Q}$ and distributive laws $\rightsquigarrow$ example of skew field or division ring.

Class March 14

Remark 0.5. Units. $(R* =)\ U(R) := \{a \in R \mid \exists\ b \in R \text{ s.t. } ab = ba = 1\}$

1. There can only be one $b \in R$ with $ab = ba = 1$. In fact, if $ba = 1 = ab = ab'$ for some $b' \in R$ $\implies (ba)b = (ba)b' \implies 1b = 1b' \implies b = b'$. Notation: $a \in U(R)$ $ab = ba = 1 \rightsquigarrow b = a^{-1}$ multiplicative inverse.

2. For non-commutative R, $ab = 1$ usually does not imply $ba = 1$. However, if $\exists c \in R$ with $ca = 1$, then $c = b$ and hence also $ba = 1$. This is seen by $c = c * 1 = c(a * b) = (ca)b = 1 * b = b$.

3. $U(R)$ is closed under multiplication and $(ab)^{-1} = b^{-1}a^{-1}$ for $ab \in U(R)$. Immediately checks that $(U(R), *)$ is a group.

4. $a, b \in R$ are called zero divisors if $a, b \neq 0$ but $ab = 0$. $U(R) \cap \{\text{zero divisors}\} = \emptyset$.

Example 0.6.
1. F field (or skew field) $\implies U(F) = F \setminus \{0\} =: F*$

2. $U(\mathbb{Z}) = \{1, -1\}$. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \implies U(\mathbb{Z}[i]) = \{1, -1, i, -i\} = \{x \in \mathbb{Z}[i] \mid |x| = 1\}$

3. $U(\mathbb{Z}_n) = \{[a] \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$. Notation $U(\mathbb{Z}_n) = U(n)$.

4. $U(R \times S) = U(R) \times U(S)$ (direct product groups). $(a, b) \implies (a, b)^{-1} = (a^{-1}, b^{-1})$.

5. $U(M(n, F)) = GL(n, F) = \{A \in M(n, F) \mid det(A) \neq 0\}$

Remark 0.7. The Center (of a Ring). $Z(R) := \{z \in R \mid za = az\ \forall\ a \in R$. This is a subring of R:

1. $1 \in Z(R)$ since $a * 1 = 1 * a = a\ \forall\ a \in R$

2. $z \in Z(R) \implies -z \in Z(R)$: $-z * a = -(za) = -(az) = a * (-z)\ \forall\ a \in R$.

3. $y, z \in Z(R) \implies y + z \in Z(R)$: $(y + z)a = ya + za = ay + az = a(y + z)\ \forall a \in R$.

4. $y, z \in Z(R) \implies yz \in Z(R)$. $(yz)a = y(za) = y(az) = (ya)z = (ay)z = a(yz)\ \forall\ a \in R$.

Remark 0.8. Integral Multiples (of element of R). For $a \in R$, $n \in \mathbb{Z}$, we define $n * a :=$ if $n > 0, a + ... + a$, if $n = 0$, 0 n-times and if $n < 0$, $(-a) + ... + (-a)$ n-times.
Note: $n > 0$: $a + ... + a = 1_R a + ... + 1_R a$. $a(1_R + ... + 1_R) = (n * 1_R)a$. If $n < 0$, $n * a = (-a) + ... + (-a) = ((-1_R) + ... + (-1_R))a = (n * 1_R)a$. Always, $n * a = (n * 1_R)a\ \forall\ a \in R\ \forall\ n \in \mathbb{Z}$.

Remark 0.9. More rules:

1. $a \in Z(R)$ (e.g. $a = 1_R$), then $n * a \in Z(R)\ \forall\ n \in \mathbb{Z}$ since $Z(R)$ is a subring of R.

2. $(-n) * a = -(n * a)\ \forall\ n \in \mathbb{Z}$, $a \in R$

3. $1 * a = a \ \forall \ a \in R$ by definition

4. $n * (a + b) = n * a + n * b \ \forall \ n \in \mathbb{Z} \ \forall \ a, b \in R$ (follows from $(R, +)$ is an abelian group).

5. $(n + m) * a = n * a + m * a$

6. $(nm) * (ab) = (n * a)(m * b) \ \forall \ n, m \in \mathbb{Z} \ \forall \ a, b \in R$.

7. $(nm) * a = n * (m * a) \ \forall \ n, m \in \mathbb{Z}, \ \forall \ a \in R$.

Definition 0.10. For any ring R, there is a unique ring homomorphism $\varphi = \varphi_R : \mathbb{Z} \to R$ which maps $1 \to 1_R$. Must have $\varphi(1) = 1_R$.
If $n \in \mathbb{Z}$, $n > 0$ then $\varphi(n) = \varphi(1 + ... + 1) = \varphi(1) + ... + \varphi(1) = 1_R + ... + 1_R = n * I_R$. $n \in \mathbb{Z}$, $n < 0$, then $\varphi(n) = -\varphi(-n) = -\varphi(1 + ... + 1) = -(-n * 1_R) = n * I_R$. Therefore, the only possible ring homomorphism is $\varphi_R : \mathbb{Z} \to R$ (which maps $n \to n * 1_R$) $\ni \varphi(n) = n * 1_R \ \forall \ n \in \mathbb{Z}$.
Now, we check $\varphi : \mathbb{Z} \to R$ which maps $n \to n * I_R$ is in fact a ring homomorphism:

1. $\varphi(1) = 1_R$ by definition

2. $\varphi(n + m) = (n + m)1_R = n * 1_R + m * 1_R = \varphi(n) + \varphi(m) \ \forall \ n, m \in \mathbb{Z}$.

3. $\varphi(n * m) = (nm)1_R = (nm)(1_R * 1_R) = n1_R * m1_R = \varphi(n)\varphi(m) \ \forall \ n, m \in \mathbb{Z}$.

Note: φ ring hom $\implies \varphi(\mathbb{Z}) = \{n * 1_R \mid n \in \mathbb{Z}\}$ is a subring of R. Moreover, $\varphi(\mathbb{Z}) \subseteq Z(R)$ since $n * 1_R \in Z(R) \ \forall \ n \in \mathbb{Z}$. The kernel of φ_R is an ideal of $\mathbb{Z}$. Hence, $Kern(\varphi_R) = n\mathbb{Z}$ for a unique $n \in \mathbb{N}_0$.

Definition 0.11. The characteristic of R is defined as $char(R) = n \in \mathbb{N}_0$ with $Kern(\varphi_R) = n\mathbb{Z}$. Alternatively, $char(R) = 0 \Leftrightarrow m * 1_R \neq 0 \ \forall \ m > 0$. $char(R) = n > 0 \Leftrightarrow n * 1_R = 0$ and $m * 1_R \neq 0 \ \forall \ 1 \leq m < n$.

Class March 16

Remark 0.12. Some review! For any given ring R with 1, $\exists$ unique ring homomorphism $\varphi_R : \mathbb{Z} \to R$ which maps $m \to m * 1_R$. It is important to note that $\varphi_R(\mathbb{Z})$ is a subring of R, $\varphi_R(\mathbb{Z}) \subseteq Z(R)$, and $Kern(\varphi_R)$ is an ideal of $\mathbb{Z} \implies \exists$ unique $n \in N_0$ with $Kern(\varphi_R) = n\mathbb{Z}$. (For notation purposes, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$)

Definition 0.13. If $Kern(\varphi_R) = n\mathbb{Z}$, $n \in \mathbb{N}_0$, then n is called the characteristic of R, $char(R) = n$. An alternative characterization:

1. $m * 1_R \neq 0 \ \forall \ m \in \mathbb{N} \Leftrightarrow char(R) = 0$

2. n is the smallest natural number with $n * 1_R = 0 \Leftrightarrow char(R) = n$.

Example 0.14. 1. $char(\mathbb{Z}) = 0$ ($\varphi_{\mathbb{Z}} = id_Z$) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fiels of characteristic 0 and $char(\mathbb{Z}[i]) = 0$

2. $char(\mathbb{Z}_n) = n \ \forall \ n \in \mathbb{N}$ and $\varphi_{\mathbb{Z}_n} : \mathbb{Z} \to \mathbb{Z}_n$ which maps $m \to [m]$

3. if p is prime, then $\mathbb{Z}_p$ is a field of characteristic p.

Remark 0.15. If S is a subring of R, then $char(S) = char(R)$

Proof. $1_S = 1_R \implies \varphi_S(m) = \varphi_R(m) = m * 1_R \ \forall \ m \in \mathbb{Z} \implies char(S) = char(R)$ $\square$

Definition 0.16. Any ring R has a unique smallest subring called the prime subring R_0 of R, namely $R_0 = \varphi_R(\mathbb{Z}) = \{m*1_R \mid m \in \mathbb{Z}\}$ and any subring of R must contain 1_R and hence $\{m*1_R \mid m \in \mathbb{Z}\} = R_0$

Theorem 0.17. *1st Isomorphism Theorem for Rings: If $\varphi : R \to S$ is a ring homomorphism, then $Kern(\varphi)$ is an ideal of R and $R/Kern(\varphi) \cong \varphi(R)(\subseteq S)$.*

Proof. On the level of abelian groups, the map $\hat{\varphi} : R/Kern(\varphi) \to \varphi(R)$ which maps $a + Kern(\varphi) \to \varphi(a)$. This map is a well-defined isomorphism (see 1.2.2). We want a ring homomorphism. Therefore, we have to check that $\hat{\varphi}$ is also multiplicative. $\hat{\varphi}((a+K)(b+K)) = \hat{\varphi}(ab+K) = \varphi(ab) = \varphi(a)\varphi(b) = \hat{\varphi}(a+K)\hat{\varphi}(b+K)$ □

Proposition 0.18. *R ring with prime subring R_0. If $char(R) = 0$, then $R_0 \cong \mathbb{Z}$. If $char(R) = n > 0$, then $R_0 \cong \mathbb{Z}_n$*

Proof. $\varphi_R : \mathbb{Z} \to R$ with $Kern(\varphi_R) = n\mathbb{Z}$ for $n \in \mathbb{N}_0$, $n = char(R)$. $R_0 := \varphi_R(\mathbb{Z}) = \mathbb{Z}/Kern(\varphi_R) = \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}$ if $n < 0$ and $\mathbb{Z}_n$ if $n \geq 0$ □

Remark 0.19. R is an integral domain $\to$ By definition, R is commutative (w/ $1 \neq 0$).

Corollary 0.20. *If R is an integral domain, then either $char(R) = 0$ or $char(R)$ is a prime number.*

Proof. R_0, as a subring of an integral domain must be an integral domain itself. But by the previous proposition, $R_0 \cong \mathbb{Z} \implies char(R) = 0$ (integral domain) or $R_0 \cong \mathbb{Z}_n$ with $char(R) = n$, but $\mathbb{Z}_n$ is an integral domain $\Leftrightarrow$ n is prime (implies zero divisors). $a, b \in R$ are zero divisors $\Leftrightarrow a \neq 0$ and $b \neq 0$ and $ab = 0$ $n = ml$, $1 < m, l < n \implies [m], [l]$ are zero divisors in $\mathbb{Z}_n \implies [m][l] = [n] = [0]$. □

Ideals. R ring with 1.

Definition 0.21. Repetition. A subset $I \subseteq R$ is called an ideal of R of (1) $0 \in I$ (2) $a, b \in I \implies a + b \in I$ (3) $r \in R$, $a \in I \implies ra, ar \in I$.

Remark 0.22. $a \in I \implies$ by (3) $(-1)a = -a \in I$. Hence, $(I, +)$ is a subgroup of the abelian group $(R, +)$. Notation: $I \lhd R$ means that I is an ideal of $R \rightsquigarrow$ quotient ring R/I such that $+ : (a+I) + (b+I) := (a+b) + I$ $(a, b \in R)$ and $* : (a+I) * (b+I) := ab + I$. These operations are well-defined and yield a (quotient) ring $(R/I, +, *)$. $0_{R/I} = I = (0+I)$ and $1_{R/I} = 1 + I$.
Why is $*$ well-defined? Assume $a + I = a' + I$, $b + I = b' + I \implies a' = a + x$ for some $x \in I$ and $b' = b + y$ for some $y \in I$. $a'b' = (a+x)(b+y) = ab + (ay + xb + xy) \implies$, by $(ay + xb + xy) \in I$, $a'b' + I = ab + I$.

Lemma 0.23. *$\varphi : R \to S$ is a ring homomorphism.*

1. *if $J \lhd S$, then $\varphi^{-1}(J) \lhd R$*
2. *if $I \lhd R$ and φ is surjective, then $\varphi(I) \lhd S$*

Remark 0.24. (2) is not true without surjectivity e.g. $\varphi : \mathbb{Z} \to \mathbb{Q}$ which maps $m \to m$ and $n\mathbb{Z} \lhd \mathbb{Z}$ but $n\mathbb{Z} \not\lhd \mathbb{Q}$ (unless $n = 0$.

Proof. Proof of (1).

1. $0_S \in J \lhd S$ and $\varphi(0_R) = 0_S \implies 0_R \in \varphi^{-1}(J)$
2. $a, b \in \varphi^{-1}(J) \implies \varphi(A), \varphi(B) \in J \implies \varphi(a+b) = varphi(a) + \varphi(b) \in J \implies a + b \in \varphi^{-1}(J)$

3. $a \in \varphi^{-1}(J)$, $r \in R \implies \varphi(a) \in J \implies varphi(ar) = \varphi(a)\varphi(r) \in J$, $\varphi(ra) = \varphi(r)\varphi(a) \in J \implies ar \in \varphi^{-1}(J)$ and $ra \in \varphi^{-1}(J)$

$\square$

Remark 0.25. In particular, $Kern(\varphi) = \varphi^{-1}(\{0\})$ is an ideal of R.

Class March 19

Before anything else, we'll review a few concepts from last class.

Definition 0.26. $\varphi : R \to S$ ring homomorphism.

1. $J \lhd S \implies \varphi^{-1}(J) \lhd R$
2. $I \lhd R$ and φ surjective $\implies \varphi(I) \lhd S$

Definition 0.27. Ideals of R/I ($I \lhd R$).
$\exists$ surjective ring homomorphism $\pi : R \to R/I$ which maps $a \to a + I$ with $Kern(\pi) = I$ because $a + I = 0 \Leftrightarrow a \in I$.
For any $I' \lhd R$ with $I \subseteq I'$, we define $I'/I := \{a + I \mid a \in I'\} = \pi(I') \lhd R/I$.

Claim: $f : \{I' \lhd R \mid I \subseteq I'\} \to \{J \lhd R/I\}$ (which maps $I'I'/I$) is bijective.

Proof. f is surjective: Let $J \lhd R/I$ be given $\rightsquigarrow$ set $I' := \pi^{-1}(J) \lhd R$ by part (a) of the definition of ring homomorphism. Also, $I' \supseteq \pi^{-1}(0) = Kern(\pi) = I$ such that $f(I') = I'/I = \pi(I') = \pi(\pi^{-1}(J)) = J$ since π is surjective $\implies f$ is surjective.
f is injective: $I_1', I_2' \lhd R$; $I_1', I_2' \supseteq I$ and $f(I_1') = f(I_2')$ to show $I_1' = I_2'$. Specifically, $a \in I_1' \implies a + I \in I_1'/I = f(I_1') = f(I_2') = I_2'/I \implies \exists\, b \in I_2'$ s.t. $a \in b + I$. $a \in b + I \subseteq I_2' + I = I_2'$ (since $I \subseteq I_2'$) $\implies a \in I_2'$ for any $a \in I_1' \implies I_1' \subseteq I_2'$. Similarly, $I_1' \subseteq I_2' \implies I_1' = I_2'$ $\square$

Lemma 0.28. *Let R be a commutative ring with $1 \neq 0$. Then, R is a field $\Leftrightarrow$ R has precisely two ideals, namely $\{0\}$ and R*

Proof. "$\Rightarrow$" Assume $\{0\} \neq I \lhd R$. Want to show $I = R$. $I \neq \{0\} \implies \exists\, 0 \neq x \in I$, R is a field $\implies \exists\, x^{-1} \in R \implies$ for any $a \in R$, we obtain $a = a * 1 = a(x^{-1}x) = (ax^{-1})x \in I \implies I = R$.
"$\Leftarrow$" To show $0 \neq x \in R \implies x \in U(R)$. Consider the principal ideal $I :=< x >:= \{rx \mid r \in R\} \lhd R$. $0 \neq x = 1 * x \in I \implies I \neq \{0\} \implies I = R$ by assumption $\implies 1 \in I =< x > \implies \exists\, r \in R$ with $1 = rx = xr \implies x \in U(R)$. Hence, $U(R) = R \setminus \{0\} \implies R$ is a field. $\square$

From now on, we assume that the ring R with 1 is commutative.

Definition 0.29.
1. A proper ideal $I \lhd R$ (i.e. $I \neq R$) is called a prime ideal of R if the $x, y \in R$, $xy \in I \implies x \in I$ or $y \in I$.
2. A proper ideal $I \lhd R$ is called a maximal ideal of R if: $J \lhd R$ with $I \subseteq J \implies J = I$ or $J = R$.
3. $\{0\}$ is allowed in (1) and (2)

Remark 0.30. One can show using Zorn's Lemma that every proper ideal of R is contained in some maximal ideal.

Proposition 0.31. *Assume $I \lhd R$, $I \neq R \implies R \neq \{0\} \implies 1 \neq 0$. Then, I is a maximal ideal of $R \Leftrightarrow R/I$ is a field.*

Proof. ($\Rightarrow$) By definition of a maximal ideal, $\{I' \lhd R \mid I \subseteq I'\} = \{I, R\} \implies \{J \lhd R/I\} = \{I/I = \{0\}, R/I\} \implies R/I$ is a field.
($\Leftarrow$) Assume R/I is a field $\implies \{0\}$ and R/I are only ideals of $R/I \implies \{I' \lhd R \mid I' \supseteq I\} = \{I, R\}$ $\implies I$ is a maximal ideal of R. $\square$

Proposition 0.32. *$I \lhd R$, $I \neq R$ ($\implies 1 \neq 0$). Then, I is a prime ideal of $R \Leftrightarrow R/I$ is an integral domain.*

Proof. ($\Rightarrow$) R/I is a commutative ring with $1 + I \neq 0 + I$ since $1 \notin I$ ($1 \in I \implies I = R$). To show, R/I has no zero divisors. So assume for $x, y \in R$, we have $(x+I)(y+I) = 0 + I$ in $R/I \Leftrightarrow xy + I = I$ $\implies xy \in I \implies (I is prime)\ x \in I$ or $y \in I \implies x + I = I$ or $y + I = I$ ($= 0$ in R/I) $\implies$ no zero divisors in R/I is an integral domain. Assume $xy \in I$ for $x, y \in R \implies I = xy + I = (x+I)(y+I)$ $\implies$ (R/I has no zero divisors) $x + I = I$ or $y + I = I \implies x \in I$ or $y \in I$ $\square$

Proposition 0.33. *Assume $I \lhd R$, $I \neq R$. I is a maximal ideal of $R \Leftrightarrow R/I$ is a field.*

Corollary 0.34. *$I \lhd R$, $I \neq R$. If I is maximal, then it's also a prime ideal of R.*

Proof. I maximal $\implies R/I$ is a field $\implies R/I$ is an integral domain $\implies I$ is a prime ideal $\square$

Example 0.35.
1. if F is a field, $\{0\}$ is a prime and a maximal ideal of F
2. $\{0\}$ is a prime ideal of $R \Leftrightarrow R/\{0\} \cong R$ is an integral domain.

Class March 23

R commutative ring with $1 \neq 0$, $R \neq I \lhd R$. I is a **prime ideal** of $R \Leftrightarrow x, y \in R$, $xy \in I \to x \in I$ or $y \in I$. I is a **maximal ideal** of $R \Leftrightarrow \{J \mid J \lhd R \text{ and } I \subseteq J\} = \{I, R\}$.

Proposition 0.36. *I maximal $\Leftrightarrow R/I$ is an integral domain.*

Example 0.37.
1. F is a field $\implies \{0\}, F$ are its only ideals $\implies \{0\}$ is the only prime and maximal ideal of F.
2. $\{0\}$ is a prime ideal of $R \Leftrightarrow R$ is an integral domain.

   Remark 0.38. $\{0\}$ is a maximal ideal of $R \Leftrightarrow R$ is a field $\cong R/\{0\}$.

3. $R = \mathbb{Z}$ $\{$ideals of $\mathbb{Z}\} = \{$subgroups of $(\mathbb{Z}, +)\} = \{<n>= n\mathbb{Z} \mid n \in \mathbb{N}_0\}$
   $n = 0$: $n\mathbb{Z} = \{0\}$ is a prime ideal of $\mathbb{Z}$ (not maximal). $n > 0$: $<n>$ is prime $\Leftrightarrow \mathbb{Z}/<n>= \mathbb{Z}_n$ is an integral domain $\Leftrightarrow \mathbb{Z}_n$ is a field $\Leftrightarrow n$ is prime $\Leftrightarrow <n>$ is maximal.
4. $\mathbb{Z} \times \{0\} = \{(a, 0) \mid a \in \mathbb{Z}\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$ since $\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \{0\} \cong \mathbb{Z}$ integral domain but not a field $\implies \mathbb{Z} \times \{0\}$ is not maximal in $\mathbb{Z} \times \mathbb{Z}$ e.g. $\mathbb{Z} \times \{0\} \subsetneq \mathbb{Z} \times <n>$ with $n \geq 2$.

Polynomial Rings. We start with the standard assumption that R is a commutative ring with $1 \neq 0$.

Definition 0.39. A **polynomial** (in one variable x) with coefficients in R is a finite formal sum $f(x) = \sum_{i=1}^{n} a_i x^i$ with $n \in \mathbb{N}_0$ and $a_i \in R \; \forall \; i$. Identify $x^0 = 1$, $1 * x^i = x^i$, $a_0 * x^0 = a_0$. If $f(x) \neq 0$, $f(x) = \sum_{i=0}^{n} a_i x^i$ with $a_n \neq 0$, we define the **degree** of $f(x)$ as $deg(f) := n$ and the **leading coefficient** $l(f) := a_n \neq 0$. $f(x)$ is called **monic** if $l(f(x)) = 1$.

Conventions regarding $deg(0) : deg(0) = -1$, $deg(0) = -\infty$ or $deg(0)$ is not defined. Never $deg(0) = 0 \implies$ Always $deg(0) \neq 0$. Rather $deg(f(x)) = 0 \Leftrightarrow f(x) \in R \setminus \{0\}$.

Lemma 0.40. *Defining addition and multiplication of polynomials:* $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$. $f(x) + g(x) = \sum_{i=0}^{max(m,n)} (a_i + b_i) x^i$ *with the convention that* $a_i = 0 \; \forall \; i > n$ *if* $m > n$ *and* $b_i = 0 \; \forall \; i > m$ *if* $n > m$. $a_i = 0 \; \forall \; i > n$ *if* $m > n$ *and* $b_i = 0 \; \forall \; i > m$ *if* $n > m$.
$f(x)g(x) := \sum_{j=0}^{m+n} c_j x^j$ *with* $c_j := \sum_{i=0}^{i} a_i b_{j-i} = \sum_{i,k \in \mathbb{N}_0, i+k=j} a_i b_k$ *and* $a_i = 0$ *if* $i > n$ *and* $b_{j-i} = 0$ *if* $j - i > m$. *In particular,* $c_0 = a_0 b_0$, $c_{n+m} = a_n b_m$. *Also,* $x^n x^m = (1 * x^n)(1 * x^m) = 1 * x^{n+m} = x^{n+m}$.

Lemma 0.41. *With addition and multiplication as defined above* $R[x] := \{f(x) == \sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}_0$, *all* $a_i \in R\}$ *becomes a commutative ring with* 1_R *called the* ***polynomial ring*** *(in one variable) over* R. *Note:* R *is a subring of* $R[x] \implies 1_{R[x]} = 1_R$, *more generally,* $a(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} (a a_i) x^i$. *Verification of the ring axioms is left as an exercise.*

For commutative law $\implies \sum_{i,k \in \mathbb{N}_0, i+k=j} a_i b_k \rightsquigarrow$ commutativity. For the associative law for multiplication, $(f(x)g(x))h(x) = f(x)(g(x)h(x)) \rightsquigarrow$ coefficients in the product $\sum_{l=0} d_l x^l$. $\sum_{i,j,k \in \mathbb{N}_0, i+j+k=l} (a_i b_j) c_k = \sum_{i,j,k \in \mathbb{N}_0, i+j+k=l} a_i (b_j c_k)$.

Proposition 0.42 ("Universal Property"). *R, S commutative rings with 1,* $\varphi : R \to S$ *is a ring hom and* $s \in S$, *then there exists a unique ring hom* $\tilde{\varphi} = \tilde{\varphi}_S : R[x] \to S$ *with* $\varphi_{1R} = \varphi$ *and* $\tilde{\varphi}(x) = s$.

Proof. Assume $\tilde{\varphi}$ exists and $f(x) = \sum_{i=0}^{n} a_i x^i$. $\tilde{\varphi}(f(x)) = \tilde{\varphi}(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \tilde{\varphi}(a_i x^i) = \sum_{i=1}^{n} \tilde{\varphi}(a_i)\tilde{\varphi}(x^i) = \sum_{i=0}^{n} \varphi(a_i) s^i$. Verify that this yields a ring such that $\varphi_{1R} = \varphi$.
It follows from the fact that $\varphi(a_i + b_i) = \varphi(a_i) + \varphi(b_i)$ that $\tilde{\varphi}(f + g) = \tilde{\varphi}(f) + \tilde{\varphi}(g) \; \forall \; f, g \in R[x]$. Multiplication of $\tilde{\varphi}$: $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i \implies f(x)g(x) = \sum_{j}^{n+m} c_j x^j$ such that $c_j = \sum_{i=0}^{j} a_i b_{j-i}$. $\tilde{\varphi}(f(x)g(x)) = \tilde{\varphi}(f(x)g(x)) = \tilde{\varphi}(\sum_{j=0}^{n+m} (\sum_{i=0}^{j} a_i b + j - i) x^j = \sum_{j=0}^{n+m} \varphi(\sum_{i=0}^{j} a_j b_{j-i}) s^j = (\varphi$ is a ring hom$) = \sum_{j=0}^{n+m} (\sum_{i=0}^{j} \varphi(a_i) s^i \sum_{i=0}^{m} \varphi(b_i) s^i = \tilde{\varphi}(f(x))\tilde{\varphi}(g(x))$. Also, $\tilde{\varphi}(a_0) = \varphi(a_0)$ by definition of $\tilde{\varphi}$ and $\tilde{\varphi}(x) = \tilde{\varphi}(x) = \tilde{\varphi}(1 * x) = \varphi(1_R)s = 1_s * s = s$. ☐

Class March 26

["Universal Property"] R, S commutative rings with 1, $s \in S$, $varphi : R \to S$ ring homomorphism. Then, there exists a unique ring homomorphism $\tilde{\varphi} : R[x] \to S$ such that $\tilde{\varphi}_{1R} = \varphi$ and $\tilde{\varphi}(x) = s$ $(\varphi(a) = a \; \forall \; a \in R)$.

Corollary 0.43 (Special cases of last proposition).

1. *$\varphi : R \to S$ ring homomorphism $\implies \exists$ unique ring homomorphism* $\tilde{\varphi} : R[x] \to S[x]$ *with* $\sum_{i=1}^{n} a_i x^i \to \sum_{i=1}^{n} \varphi(a_i) x^i$. *This follows from 2.3.3 with* $S = S[x]$, $\varphi : RS[x]$ *(S is a subring of $S[x]$).*

2. *With* $S = R$, $\varphi = id_R$. *For any* $r \in R$, *there exists a unique evaluation homomorphism (at r):* $xr \implies \tilde{\varphi} : R[x] \to R$ *such that* $\sum_{i=0}^{n} a_i x^i \to \sum_{i=0}^{n} a_i r^i =: f(r) \implies f(x) \to \tilde{\varphi}(f(x))$. *From this, we know that* $\tilde{\varphi}$ *is a ring homomorphism* $\implies \forall \; f, g \in R[x] : (fg)(r) = f(r)g(r)$, $(f + g)(r) = f(r) + g(r)$. $r \in R$ *is called the root of* $f(x) \in R[x]$ *if* $f(r) = 0$.

3. *R is a subring of S and $\varphi : R \to S$ is the embedding homomorphism $r \to r$. For any given $s \in S$, we obtain a ring homomorphism, $\tilde{\varphi} : R[x] \to S$ which maps $\sum_{i=0}^{n} a_i x^i \to \sum_{i=0}^{n} a_i s^i =: f(s)$. Therefore, $\tilde{\varphi}$ is a ring homomorphism $\implies \tilde{\varphi}(R[x])$ is a subring of S. More explicitly, $\tilde{\varphi}(R[x]) = \{\sum_{i=0}^{n} a_i s^i \mid n \in \mathbb{N}_0,$ all $a_i \in R\}$ wich is the smallest subring of S containing R and s. Notation $\tilde{\varphi}(R[x]) = R[s] \subseteq S$. We say that $R[s]$ is obtained from R by adjoining s.*

Example 0.44. $R = \mathbb{Z}, S = \mathbb{C}, s = i, \mathbb{Z}[i] = \{\sum_{j=0}^{n} a_j i^i \mid n \in \mathbb{N}_0, \forall a_i \in \mathbb{Z}\} = \{a_0 + a_1 i \mid a_0, a_1 \in \mathbb{Z}\}$ which is the smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and i.
Similarly, $\mathbb{Z}[\sqrt{2}] \in \mathbb{R}$ and $\mathbb{Z}[\sqrt{2}] = \{a + b^2 \mid a, b \in \mathbb{Z}\}$.

Remark 0.45. Using the evaluation homomorphism in 2.3.4(b) every polynomial $f(x) \in R[x]$ defines a function $R \to R$ such that $r \to f(r)$. One has to distinguish between the polynomial and the corresponding function since different polynomials induce the same function $R \to R$.

Example 0.46. R $\mathbb{Z}_3$, $f(x) = x^3 - x$, $g(x) = 0$, $f(x) = 0 = g(r)\ \forall\ r \in \mathbb{Z}_3$

Lemma 0.47. *$f(x), g(x) \in R[x] \setminus \{0\}$.*

1. *If $l(f(x))$ or $l(g(x))$ is <u>not</u> a zero divisor (automatically satisfied if R is an integral domain), then $deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$ and $l(f(x)g(x)) = l(f(x))l(g(x))$.*

2. *R is an integral domain $\implies$ $R[x]$ is an integral domain and $U(R[x]) = U(R)$.*

Proof. $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$ and $a_n \neq 0 \neq b_m \implies deg(f(x)) = n$, $l(f(x)) = a_n$ and $deg(g(x)) = m$, $l(g(x)) = b_m$.

1. Assumption $\implies a_n b_m \neq 0$. $f(x)g(x) = \sum_{j=0}^{m+n} c_j x^j$, $c_{n+m} = a_n b_n \neq 0 \implies deg(f(x)g(x)) = n + m = deg(f(x)) + deg(g(x))$, $l(f(x)g(x)) = c_{n+m} = a_n b_m = l(f(x))l(g(x))$.

2. $R[x]$ is a commutative ring with $1 \neq 0$. $R[x]$ has no zero divisors: $f(x), g(x) \in R[x] \setminus \{0\} \implies$ (1) $\implies deg(f(x)g(x)) = deg(f(x)) + deg(g(x)) \geq 0 \implies f(x)g(x) \neq 0$.
$U(R) \subseteq U(R[x])$: $a \in U(R) \implies \exists\ a^{-1} \in R \in R[x] \implies a \in U(R[x])$ and $a * a^{-1} = 1$. **More generally, if R is a subring of S, then $U(R) \subseteq U(S)$).** $U(R[x]) \subseteq U(R)$. $f \in R[x] \implies \exists$ $g \in R[x] : fg = 1 (= gf) \implies 0 = deg(1) = deg(fg) = deg(f) + deg(g) \implies deg(f) = deg(g)$ $\implies f, g in R \setminus \{0\}, fg = 1 \implies f \in U(R)$.

□

Theorem 0.48 (Division Algorithm)**.** *Assume $f(x), g(x) \in R[x]$, $g(x) \neq 0$ and $l(g(x)) \in U(R)$. Then there exist uniquely determined $g(x), r(x) \in R[x]$ such that $f(x) = q(x)g(x) + r(x)$ <u>and</u> $r(x)$ or $deg(r(x)) < deg(g(x))$.*
<u>Special cases:</u>

1. *$R = F$, a field, $g(x) \in F[x]$ any polynomial $\neq 0$ ($F \setminus \{0\} = U(F)$.*

2. *$g(x)$ is monic (i.e. $l(g(x)) = 1$).*

Proof. $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$, $deg(g(x)) = m$, $b_m = l(g(x)) \in U(R)$. Proof by induction on $deg(f(x))$: we may assume $f(x) \neq 0$, $n = deg(f(x))$. If $n < m$, then $f(x) = 0 * g(x) + f(x)$ satisfies the requirements with $q(x) = 0$, $r(x) = f(x)$. If $n \geq m$: we consider $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x) = (a_n - a_n b_m^{-1} b_m) x^n$ + lower terms $\implies deg(f_1(x) < n = deg(f(x)) \implies$ I.H¿ $\exists\ g_1(x), r_1(x)$ with $f_1(x) = q_1(x)g(x) + r_1(x)$ and $r_1(x) = 0$ or $deg(r_1(x)) < deg(g(x)) \implies f(x) = f_1(x) + a_n b_m^{-1} x^{n-m} g(x)$ $= (q_1(x) + a_n b_m^{-1} x^{n-m}) g(x) + r_1(x) = q(x) + r(x)$ □

Class March 28

More arguments in the existence proof from last class: $f(x) = \sum_{i=1}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$, $l(g(x)) = b_m \in U(R)$. $n = deg(f) \geq m = deg(g)$; $b_m \in U(R) \rightsquigarrow$ Consider $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x) \implies deg(f_1) < n$.
<u>Uniqueness</u>: Assume $f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$ and $r(x)r'(x)$ are 0 or of degree $< deg(g(x)) \implies (q(x) - q'(x))g(x) = r'(x) - r(x)$ and apply 2.3.6(a).

Example 0.49. $R = \mathbb{Z}_3$, $f(x) = [3]x^3 + [4]x^2 + [2], g(x) = [5]x^2 + [1] \in \mathbb{Z}_{12}[x]$. $[5]^{-1} = [5]$ (since $[5] * [5] = [1]$ in $\mathbb{Z}_{12}$). $([3]x^3 + [4]x^2 + [2]) \div ([5]x^2 + [1]) = [3] * [5]x + [4] * [5] = [3]x + [8] = q(x)$.
$([3]x^3+[4]x^2+[2])-([3]x^3+[3]x) = (f_1 =)[4]x^2-[3]x+[2]-([4]x^2+[8]) = (-[3]x-[6]) = [9]x+[6] = r(x)$.
<u>Check</u>: $q(x)g(x) + r(x) = f(x)$

Corollary 0.50. *If $a \in R$ is a root of $0 \neq f(x) \in R[x]$, then $x - a \mid f(x)$ in $R[x]$.*

Proof. $l(x-a) = 1 \in U(R)$ so 2.3.7 applies $\implies \exists\ q(x), r(x) \in R[x]$ with $f(x) = q(x)(x-a) + r(x)$ <u>and</u> $r(x) = 0$ or $deg(r(x)) < 1$, i.e. $r(x) \in R$ a root of $f(x) \implies 0 = f(a) = q(a)(a-a) + r = r \implies r = 0 \implies f(x) = q(x)g(x) \implies x - a \mid f(x)$ in $R[x]$. □

Proposition 0.51. *If R is an <u>integral domain</u> and $0 \neq f(x) \in R[x]$, then $f(x)$ has at most $deg(f(x))$ many roots.*

Proof. By induction on $deg(f(x)) = n$.
$n = 0 \implies f(x) \in R \setminus \{0\}$, 0 roots
$n \geq 1$: Assume the claim is true for polynomials degree $< n$. If $f(x)$ has no root $\rightsquigarrow$ done! Assume $a \in R$ is a root of $f(x)$, i.e. $f(a) = 0 \implies$ (2.3.9) $(x-a) \mid f(x) \implies f(x) = (x-a)q(x)$ with $q(x) \in R[x]$. 2.3.6 $\implies n = deg(f(x)) = deg(x-a) + deg(q(x)) = 1 + deg(q(x)) \implies deg(q(x)) = n - 1 < n \implies$ I.H. $q(x)$ has at most $n-1$ roots. For any root $b \in R$ of $f(x)$, we obtain $0 = f(b) = (b-a)q(b) \Leftrightarrow b - a = 0$ or $q(b) = 0$. <u>Conclusion</u>: $\{\text{roots of f}\} = \{\text{roots of q}\} \cup \{a\} \implies f$ has at most n roots. □

Theorem 0.52. *If R is an integral domain, then any <u>finite</u> subgroup $G \subseteq U(R)$ is cyclic.*

Proof. R commutative $\implies U(R)$ is abelian $\implies G$ is abelian, finite. Set $n = |G| = \prod_{i=1}^{k} p_i^{e_i}$, $p_1, ..., p_k$ are distinct primes $e_i \in \mathbb{N}$. (Wlog $G \neq \{0\}$). $P_i \in Syl_{p_i}(G)$, $1 \leq i \leq k$ i.e. $|P_i| = p_i^{e_i} = n_i$. G abelian $\implies P_i \lhd G$, $n_{p_i} = 1 \implies G = P_1 \times ... \times P_k$ (1.5.12). Now assume, by way of contradiction, that P_i <u>is not cyclic</u> $\implies |a| < |P_i| = p_i^{e_i}$ for some i and $\forall\ a \in P_i$. But also, $|a| \mid |P_i| \implies |a| \mid p_i^{e_i - 1} = m_i < n_i$ $\forall\ a \in P_i \implies a^{m_i} = 1\ \forall\ a \in P_i \implies$ the polynomial $x^{m_i} - 1 \in R[x]$ of degree $m_i \geq 1$ has $\geq |P_i| = n_i > m_i$ many roots, which contradicts 2.3.10. Hence, $\implies P_i$ is cyclic, $P_i \cong \mathbb{Z}_{n_i} (n_i = p_i^{e_i})$ $\implies G = P_1 \times ... \times P_k \cong \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k} \cong \mathbb{Z}_{n_1 * ... * n_k} = \mathbb{Z}_n$. This follows from the fact that $gcd(n_i, n_j) = 1$ $\forall\ i \neq j$. □

Corollary 0.53. *For any prime number p, $U(p) = U(\mathbb{Z}_p)$ is cyclic.*

Proof. $\mathbb{Z}_p$ is a field $\implies$ integral domain $\implies U(\mathbb{Z}_p)$ is cyclic, i.e. $U(p) \cong \mathbb{Z}_{p-1}$ □

Example 0.54. (Counterexample)

1. $R = \mathbb{Z}_{12}$, $U(R) = U(12) = \{[1], [5], [7], [11]\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

2. $R = H$, division ring (no zero divisors but not commutative). $U(R) = H^*$ contains the finite subgroup Q_8, which is not cyclic.

Class March 30

Definition 0.55. $n \in \mathbb{N}$, R commutative ring with 1 $\rightsquigarrow$ $R[x_1,...,x_n] := R[x_1,...,x_{n-1}][x_n]$. Direct definition: $R[x_1,...,x_n] := \{\sum_{i_1,..,i_n=0}^{m} x_1^{i_{i1}} * ... * x_b^{i_n} \mid m \in \mathbb{N}_0, \text{ all } i_1,...i_n \in R\}$ such that we define $+$:component wise, $*$: $x_{1}^{i}{}_1 * ... * x_n^{i_n} * x_1^{j_1} * ... * x_n^{j_n} = x_1^{i_1+j_1} * ... * x_n^{i_n+j_n}$ and Distributive Law.

Euclidean Domains. In this section, R is an integral domain.

Definition 0.56. R is a Euclidean domain if there exists a function $\Upsilon : R\backslash\{0\} \to \mathbb{N}_0$ s.t. (*) $\forall\, a, b \in R$ with $b \neq 0$ $\exists\, q, r \in R$ s.t. $a = bq + r$ and $r = 0$ or $\Upsilon(r) < \Upsilon(b)$

Remark 0.57.

1. if $\Upsilon(0)$ is defined and $\Upsilon(0) < \Upsilon(b)\ \forall\, b \in R \setminus \{0\}$, then we can drop "$r = 0$" in (*) and simply write $\Upsilon(r) < \Upsilon(b)$.
2. We will not require (though it's satisfied in many examples) that $\Upsilon(x) \leq \Upsilon(xy)\ \forall\, R \setminus \{0\}$.
3. We do not require that q and r are uniquely determined.

Example 0.58.

1. $R = \mathbb{Z}$, $\Upsilon : \mathbb{Z} \to \mathbb{N}_0$, $\Upsilon(a) = |a|$ (here $\Upsilon(0) = 0 < \Upsilon(b)\ \forall\, b \in \mathbb{Z} \setminus \{0\}$). (*) $\forall\, a, b \in \mathbb{Z}$ with $b \neq 0$ $\exists\, q, r \in \mathbb{Z}$ with $a = qb + r$ and $|r| < |b|$ (see 0.3.11 in the Pure Applied Algebra textbook).
2. F field, $R = F[x]$, $\Upsilon = deg : F[x] \setminus \{0\} \to \mathbb{N}_0$ then (*) is satisfied by Division Algorithm $f, g \in F[x]$, $g \neq 0 \implies \exists\, q, r \in F[x] : f = qg + r$ and $r = 0$ or $deg(r) < deg(g)$.

Definition 0.59. R (integral domain) is called a principal ideal domain (PID) if every ideal I of R is principal (generated by one element) i.e. $I =< a >= \{ra \mid r \in R\}$ for some $a \in I$.

Example 0.60. $\mathbb{Z}$ is a PID. Every ideal of $\mathbb{Z}$ is of the form $< n >= n\mathbb{Z}$ for some $n \in \mathbb{N}_0$.

Theorem 0.61. *Every Euclidean domain R is a PID. (Note: use this to prove something is a PID, we can prove that it is a Euclidean domain)*

Proof. Let $I \lhd R$ be given. We may assume $I \neq \{0\} =< 0 >$. Set $n := min\{\Upsilon(a) \mid 0 \neq a \in I\}$. Pick $0 \neq b \in I$ with $\Upsilon(b) = n$. Claim: $I =< b >$. Note: $b \in I \implies < b > \leq I$. Let $a \neq 0$ be any element of $I \setminus \{0\}$. (*) $\implies \exists\, q, r \in R$: $a = qb + r$ and $r = 0$ or $\Upsilon(r) < \Upsilon(b)$. Here only $r = 0$ is possible. $a, b \in I \implies a, qb \in I \implies r = a - qb \in I$. If we had $r \neq 0$, $r \in I \implies \Upsilon(r) \geq n$ by definition of n. But also $\Upsilon(r) < \Upsilon(b) = n$, contradiction! Hence, $r = 0 \implies a = qb \in < b >$. This shows $I \subseteq < b > \subseteq I \implies I =< b >$ (principal ideal by defn) □

Example 0.62. $< 2, x >= \{2f + xg \mid f, g \in \mathbb{Z}[x]\}$ is not a principal ideal. Notation: $a_1, ..., a_n \in R \rightsquigarrow < a_1, ..., a_n >= \{\sum_{i=0}^{n} r_i a_i \mid r_i \in R\, \forall\, i\} \lhd R$. This is the smallest ideal of R containing $a_1, ..., a_n$. $d \in \mathbb{Z}$, not a square $\implies \sqrt{d} \in \mathbb{Q}$. Consider $R = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$. If $a + b\sqrt{d} \in F^* = F \setminus \{0\}$ $\implies (a, b) \neq (0, 0)$ and subfield $a, b \in \mathbb{Q} \implies (a + b\sqrt{d})^{-1} = \frac{a - b\sqrt{d}}{a^2 - db^2} \in F$.

Question: When is R a Euclidean domain? Candidate for $\Upsilon : R \to \mathbb{N}_0$ which maps $a + b\sqrt{d} \to |a^2 - db^2|$ $(a, b \in \mathbb{Z})$.

Extension: $\tilde{\Upsilon} : F \to \mathbb{Q}$ which maps $a + b\sqrt{d} \to |a^2 - db^2|$ for $a, b \in \mathbb{Q}$.

Proposition 0.63. *Assume that for any $\alpha \in F$ there exists $r \in R$ with $\tilde{\Upsilon}(\alpha - q) < 1'$. Then R is a Euclidean domain satisfying (*) with Υ as above.*

Corollary 0.64. *$\mathbb{Z}[\sqrt{d}]$ is a Euclidean domain for $d=-2,-1,2,3$ e.g. $d=-1$ i.e. $R=\mathbb{Z}[i]$. Let $\alpha=a+bi\in\mathbb{Q}(i)$ be given $(a,b\in\mathbb{Q})$. Choose $m,n\in\mathbb{Z}$ with $|a-m|$, $|n-b|\leq\frac{1}{2}$. Set $r=m+ni\in\mathbb{Z}_[i]$ $\implies$ $\tilde{\Upsilon}((\alpha-m)+(b-n)i)=(\alpha-m)^2+(b-n)^2\leq\frac{1}{4}+\frac{1}{4}=\frac{1}{2}<1\implies\mathbb{Z}[i]$ is Euclidean $\implies$ PID.*

Class April 2

$d\in\mathbb{Z}$ not a square $\implies\sqrt{d}\notin\mathbb{Q}$.
$R=\mathbb{Z}[\sqrt{d}]=\{a+b\sqrt{d}\mid a,b\in\mathbb{Z}\}$, $F=\mathbb{Q}(\sqrt{d})=\{a+b\sqrt{d}\mid a,b\in\mathbb{Z}\}$.
$\tilde{\Upsilon}:F\to\mathbb{Q}^{\geq 0}$ which maps $a+b\sqrt{d}\to|a^2-db^2|$ $(=a^2-db^2$ if $d<0)$.
$\Upsilon=\tilde{\Upsilon}_{1R}:R\to\mathbb{N}_0$ $(\Upsilon(x)=0\longleftarrow x=0)$
Check $\tilde{\Upsilon}$ is multiplicative i.e. $\tilde{\Upsilon}(\alpha\beta)=\tilde{\Upsilon}(\alpha)\tilde{\Upsilon}(\beta)\ \forall\ \alpha,\beta\in F$.

Proposition 0.65. *Assume that for any $\alpha\in F\ \exists\ q\in R$ s.t. $\underline{\tilde{\Upsilon}(\alpha-q)<1}$. Then R is a Euclidean domain with respect to Υ.*

Proof. Given $x,y\in R$, $y\neq 0\implies$ consider $\alpha=\frac{x}{y}\in F\implies\exists\ q\in R$: $\tilde{\Upsilon}(\alpha-q)<1$ and moreover $1*\tilde{\Upsilon}(y)=\Upsilon(y)\implies\tilde{\Upsilon}(\alpha-q)\tilde{\Upsilon}(y)<\Upsilon(y)\implies\tilde{\Upsilon}(\alpha y-qy)=\tilde{\Upsilon}(x-qy)=:r\in R\implies x=qy+r$ <u>and</u> $\underline{\Upsilon(r)<\Upsilon(y)}$ by definition of r $(q,r\in R)$. ∎

Corollary 0.66. *$\mathbb{Z}[\sqrt{d}]$ is a Euclidean domain for $d=-2,1,2,3$.*

Remark 0.67. One can show that $\mathbb{Z}[\sqrt{-3}]$ is <u>not</u> a PID (hence not Euclidean) but the condition of the proposition can be satisfied with $\tilde{\Upsilon}(\alpha-q)<1$.

If R is Euclidean $\implies$ R is a PID. Hence, if $a,b\in R$ are given, $\exists c\in R$ such that $<a.b>=<c>$ $(<a,b>=\{\lambda*a+\mu*b\ |,\mu\in R\}\lhd R)$. **Question**: How do we <u>compute</u> c? **Answer**: Euclidean Algorithm.

Proposition 0.68 (Euclidean Algorithm)**.** *R (Euclidean domain); $a,b\in R\setminus\{0\}$.*
Then $\exists\ q_1,r_1\in R$: $a=q_1b+r$ and if $r_1\neq 0$, then $\Upsilon(r_1)<\Upsilon(b)$
$q_2r_2\in R:b=q_2r_1+r_2$ and if $r_2\neq 0$, then $\Upsilon(r_2)<\Upsilon(r_1)$
...
$\exists\ q_{i+1},r_{i+1}\in R:r_{i-1}=q_{i+1}r_i+r_{i+1}$ and if $r_{i+1}\neq 0$, then $\Upsilon(r_{i+1})<\Upsilon(r_i)$
$\exists\ n$ s.t. $r_{n+1}=0$ for the first time $r_n\neq 0$. $r_{n-2}=q_nr_{n-1}+r_n$ and $\Upsilon(r_n)<\Upsilon(r_{n-1})$
$r_{n-1}=q_{n+1}r_n+0=r_{n+1}$
Then, $<a,b>=<r_i,r_{i+1}>=<r_n>\ \forall\ 0\leq i\leq n$ (because $r_{n+1}=0$ in the last step). Furthermore, coefficients with $r_n=c_{i+1}r_{j-1}+c_ir_i$ can be computed recursively: $c_{n+1}=0$, $c_n=1$, $c_{i-1}=c_{i+1}=+q_ic_i$ $\forall\ n\geq i\geq 0\rightsquigarrow r_n=c_1r_{-1}+c_0r_0=c_1a+c_0b$

Remark 0.69. $r_n=gcd(a,b)$ (clear for $R=\mathbb{Z}$ (has to be defined for general R).

Proof. $a=q_1b+r_1\in<b,r_1>\implies<a,b>\subseteq<b,r_1>$
$r_1=a-q_1b\in<a,b>\implies<b,r_1>\subseteq<a,b>\implies<a,b>=<b,r_1>\implies<r_{-1},r_1>=<r_0,r_1>$
Therefore, we WTS $<a,b>=<r_{i-1},r_i>=<r_i,r_{i+1}>$
$r_{i-1}=q_{i+1}r_i+r_{i+1}\in<r_i,r_{i+1}>\implies<r_{i-1},r_i>\subseteq<r_i,r_{i+1}>$
$r_{i+1}=r_{i-1}+q_{i+1}r_i\in<r_{i-1},r_i>\implies<r_i,r_{i+1}>\subseteq<r_{i-1},r_i>\implies<r_{i-1},r_i>=<r_i,r_{i+1}>$
Recall $r_{n+1}=0$, so for $i=n:<a,b>=<r_n>$. We prove $r_n=c_{i+1}r_{i-1}+c_ir_i$ for $n\geq i\geq 0$ by (reverse) induction on i:
$\underline{i=n}$: $c_{n+1}r_{n-1}+c_nr_n=0*r_{n-1}+1*r_n=r_n$
$i\to i-1$: $r_n=c_{i+1}r_{i-1}+c_ir_i$, $r_{i-2}=q_ir_{i-1}+r_i\iff r_i=r_{i-2}-q_ir_{i-1}$. Moreover, $r_n=c_{i+1}r_{i-1}+c_i(r_{i-2}-q_ir_{i-1})=(c_{i+1}-q_ic_i)r_{i-1}+c_ir_{i-2}=c_{(i-1)+1}r_{(i-1)-1}+c_{i-1}r_{i-1}$ ∎

Example 0.70. $R = \mathbb{Z}[i]$, $a = 4 + 7i$, $b = 8 - i$, $a = q_1 b + r_1$
$\alpha_1 = \frac{a}{b} = \frac{4+7i}{8-i} = \frac{(4+7i)(8+i)}{(8-i)(8+i)} = \frac{25+60i}{65}$ approximate by $m + ni \in \mathbb{Z}[i]$ (e.g. $m = 0, n = i$) $\rightsquigarrow q_1 = m + ni = i$, $r_i = a - q_1 b = 3 - i \implies a = q_1 b + r_1 \iff 4 + 7i = i(8 - i) + (3 - i)$
$\alpha_2 = \frac{b}{r_1} = \frac{8-i}{3-i} = \frac{(8-i)(3+i)}{(3-i)(3+i)} = \frac{25+5i}{10} = \frac{5}{2} + \frac{1}{2}i$, $q_2 = 3 \rightsquigarrow r_2 = b - q_2 r_1 = -1 + 2i$
$\therefore 8 - i = 3(3 - i) + (-1 + 2i) \implies 3 - i = (-1 - i)(-1 + 2i) + 0 \rightsquigarrow n = 2$ and our first result is that $< 4 + 7i, 8 - i > = < -1 + 2i >$.
$r_2 = (8-i)-3(3-i) = (8-i)-3(4+7i)-i(8-i) = (1+3i)(8-i)-3(4+7i) = -3a+(1+3i)b = c_1 a+c_0 b$.
Check that $c_0 = 1 + 3i$, $c_1 = -3$

Miscellaneous Notes from Textbook

Theorem 0.71. *If R is an integral domain, then $R[x]$ is an integral domain, and the product of any two nonzero polynomials $f(x), g(x) \in R[x]$ such that $deg(f(x)) = m$ and $deg(g(x)) = n$, is a nonzero polynomial $f(x) * g(x)$ of degree $m + n$.*

Proof. if $f(x) = a_n x^n + ... + a_0$ and $g(x) = b_m x^m + ... + b_0 \implies f(x) * g(x) = a_n b_m x^{m+n} + ... + a_0 b_0$ $\implies$ because R is an integral domain, $a_n b_m \neq 0 \implies$ the product has degree $m + n$ and it is also clear that $R[x]$ is an integral domain. □

Proposition 0.72. *Let D be an integral domain. Then the units in $D[x]$ are precisely the units in D.*

Corollary 0.73. *If F is a field, then $F[x]$ is an integral domain but not a field.*

Proof. F is a field $\implies$ F is an integral domain $\implies$ $F[x]$ is an integral domain, but all nonzero polynomials in $F[x]$ are nonzero elements that are not units (because all units in $F[x]$ are precisely the units of F). Therefore $F[x]$ is not a field. □

Definition 0.74 (Characteristic)**.** The characteristic of a polynomial ring $R[x]$ is the least integer $n > 0$ such that $nf(x) = 0 \; \forall \; f(x) \in R[x]$ (and is zero if no such n exists).

Proposition 0.75. *Let R be a ring. Then $R[x]$ has the same characteristic as R.*

Proof. Since R is contained in $R[x]$, it is obvious that if $a * f(x) \; \forall \; f(x) \in R[x] \implies a * r = 0 \; \forall \; r \in R$ (because $r \in R[x]$).
Let $f(x) = a_n x^n + ... + a_0$. Then if $a * r = 0 \; \forall \; r \in R \implies a * f(x) = a * a_n x^n + ... + a * a_0$ and because the coefficients are in R, all the new coefficients equal $0 \implies f(x) = 0$ □

Definition 0.76. Let F be a subfield of a field E and $\alpha \in E$. The **evaluation homomorphism** is defined as $\phi_\alpha : F[x] \to E$ such that $f(x) = a_n x^n + ... + a_1 x + a_0 \in F[x]$ and $\phi_\alpha(f(x)) = a_n \alpha^n + ... a_1 \alpha + a_0 \in E$.

Division Algorithm and Proof are worth reviewing

Proposition 0.77. *Let F be a field such that $f(x), g(x) \in F[x]$. Then,*

1. *$g(x) \mid f(x) \implies eg(x) \mid f(x)$ for any element $0 \neq e \in F$.*
2. *$g(x) \mid f(x)$ and $f(x) \mid g(x) \implies f(x) = eg(x)$ for some element $0 \neq e \in F$.*

1. *Proof.* $g(x) \mid f(x) \implies f(x) = q(x) * g(x) \implies f(x) = (e^{-1} * q(x)) * (e * g(x)) \implies e * g(x) \mid f(x)$. □

2. *Proof.* $g(x) \mid f(x) \implies f(x) = q(x) * g(x)$; $f(x) \mid g(x) \implies g(x) = p(x) * f(x)$. Hence, $f(x) = q(x)*p(x)*f(x) \implies q(x)*p(x) = 1 \implies q(x), p(x)$ have degree 0 and are both constant because their product is constant $\implies q(x) = e$ and $p(x) = e^{-1}$ for some element $0 \neq e \in F$. □

Remark 0.78. If the leading coefficient is 1, then the polynomial is called **monic**

Definition 0.79. For $f(x)$ and $g(x)$ in $F[x]$ where F is a field, a **common divisor** of $f(x), g(x)$ is any polynomial $c(x) \in F[x]$ such that $c(x) \mid f(x)$ and $c(x) \mid g(x)$. A **greatest common divisor** of $f(x)$ and $g(x)$ is a common divisor $d(x)$ such that for any other common divisor $c(x)$, $c(x) \mid d(x)$. If the only common divisors and therefore the only greatest common divisors of $f(x)$ and $g(x)$ are constants, then $f(x)$ and $g(x)$ are called **relatively prime**.

Remark 0.80. If $d_1(x), d_2(x)$ are both greatest common divisors, then $d_1(x) = e * d_2(x)$ for some $0 \neq e \in F \implies$ there can only be one *monic* greatest common divisor, denoted $gcd(f(x), g(x))$.

Theorem 0.81. *Let F be a field and $f(x), g(x) \in F[x]$ (not both 0). Then there exists a greatest common divisor $d(x)$ of $f(x)$ and $g(x)$ that can be written as a linear combination of $f(x)$ and $g(x)$. Therefore, $\exists\ u(x).v(x) \in F[x]$ such that $d(x) = u(x) * f(x) + v(x) * g(x)$ is a greatest common divisor of $f(x)$ and $g(x)$.*

Proof. Define the set $S = \{m(x)f(x) + n(x)g(x) \mid m(x), n(x) \in F[x]\}$. Note that $f(x), g(x) \in S$. Therefore, S has elements other than 0. Let $d(x) \in S$ of minimum degree. We may take $d(x)$ to be monic because if it isn't then, we can take $a^{-1}d(x)$ which is monic if a was the leading coefficient of $d(x)$. Because, $d(x) \in S \implies d(x) = u(x)f(x) + v(x)g(x)$ for some $u(x), v(x) \in F[x]$.
Now we must show that $d(x)$ is a common divisor of $f(x)$ and $g(x)$. According to the division algorithm, $f(x) = q(x)d(x) + r(x)$ such that $r(x) = 0$ or $deg(r(x)) < deg(d(x))$. Solving for $r(x)$, we obtain $r(x) = f(x) - q(x)d(x) = f(x) - q(x)(u(x)f(x) + v(x)g(x)) = [1 - u(x)q(x)]f(x) - [q(x)v(x)]g(x) \implies r(x) \in S$ by definition. Since $d(x)$ was chosen to be of minimum degree (in S), $\implies deg(r(x)) < deg(d(x))$ is not true and therefore $r(x) = 0 \implies d(x) \mid f(x)$. Wlog this argument also applies to $g(x)$.
To complete the proof, we need to show that $d(x)$ is the greatest common divisor (so any other common divisor $c(x) \mid d(x)$). If $\exists$ common divisor $c(x) \implies f(x) = q(x)c(x)$ and $g(x) = p(x)c(x)$ by definition. Therefore, $d(x) = u(x)f(x) + v(x)g(x) = [u(x)q(x) + v(x)p(x)]c(x) \implies c(x) \mid d(x) \implies d(x)$ is the $gcd(f(x).g(x)$ by construction. □

Practice using the Euclidean Algorithm

Theorem 0.82 (Factor Theorem)**.** *Let F be a field, $f(x) \in F[x]$ and $a \in F$. Then, a is a zero of $f(x)$ $\iff (x - a)$ is a divisor of $f(x)$ in $F[x]$.*

Proof. ($\Rightarrow$) Assume a is a zero of $f(x)$. Applying the division algorithm, we can write $f(x) = q(x)(x - a) + r(x)$ such that $r(x) = 0$ or $deg(r(x)) < deg(x - a)$. Suppose $deg(r(x)) < deg(x - a)$. This implies that $deg(r(x)) = 0$ and $r(x) = c \in F$ (a constant). By definition, $0 = f(a) = q(a)(a - a) + c = 0 + c$ $\implies r(x) = 0 \implies (x - a) \mid f(x)$
($\Leftarrow$) $(x - a) \mid f(x) \implies f(x) = q(x)(x - a) \implies f(a) = q(a)(a - a) = 0 \implies a$ is a zero of $f(x)$. □

Irreducible Polynomials not covered on the exam but seem pretty important

Definition 0.83. Let F be a field and $f(x)$ a nonconstant polynomial in $F[x]$. Then $f(x)$ is **irreducible** over F if $f(x)$ <u>cannot</u> be expressed as a product $f(x) = g(x)h(x)$ of polynomials $g(x)$ and $h(x)$ in $F[x]$ both of lower degree than $f(x)$. $f(x)$ is **reducible** over F if it is not irreducible.

Theorem 0.84. *Let F be a field, $f(x)$ a polynomial in $F[x]$ of degree 2 or 3. Then, $f(x)$ is reducible over $F \iff f(x)$ has a zero in F.*

Ideals in $F[x]$

Definition 0.85. If $a \in R$, then the **principal ideal** $< a >$ generated by a is the ideal $\{ra \mid r \in R\}$ consisting of all multiples by a. Therefore, if F is a field, then the principal ideal $< x >$ in $F[x]$ generated by x is the set of all multiples of x, which is to say, the set of all polynomials in $F[x]$ with constant term 0.

Definition 0.86. Let D be an integral domain. Then D is called a **principal ideal domain (PID)** if every ideal in D is a principal ideal.

Example 0.87. $\mathbb{Z}$ is a PID, since as we know every ideal I in $\mathbb{Z}$ is generated by a fixed element $n \in I$, so $I = n\mathbb{Z} =< n >$.

Theorem 0.88. *Let F be a field. Then $F[x]$ is a PID.*

Proof. $F[x]$ is an integral domain because F is an integral domain. Now, we need to show that for any ideal I in $F[x]$ $\exists$ $f(x) \in I$ such that $I =< f(x) >$. If I is the zero ideal $\{0\}$, then $I =< 0 >$. If I is not the zero ideal, let $g(x)$ be a nonzero element of I of minimal degree. We show that $g(x)$ generates I ($I =< g(x) >$) by showing that if $f(x) \in I \setminus \{g(x)\}$, then $g(x) \mid f(x)$. To show this we apply the division algorithm to write $f(x) = q(x)g(x) + r(x)$ such that $r(x) = 0$ or $deg(r(x)) < deg(g(x))$. Since $r(x) = f(x) - q(x)g(x) \in I$ and $g(x)$ is chosen to have minimal degree, $deg(r(x)) < deg(g(x))$ cannot hold $\implies r(x) = 0 \implies f(x) = q(x)g(x)$ which is a multiple of $g(x)$ by definition. □

Theorem 0.89. *Let F be a field. A nontrivial ideal $I =< p(x) >$ is a maximal ideal in $F[x] \iff p(x)$ is irreducible over F.*

Proof. ($\Rightarrow$) Suppose $I =< p(x) >$ is a maximal ideal in $F[x]$. I is neither $\{0\} =< 0 >$ nor $F[x] =< 1 >$, so $p(x)$ is neither the zero polynomial nor a unit of $F[x]$ (a constant polynomial).If $p(x) = g(x)h(x)$, then $p(x) \in< g(x) >$ and, therefore, $I =< p(x) >\subseteq< g(x) >\subseteq F[x]$. We assume I is maximal $\implies$ either $< p(x) >=< g(x) >$ or $< g(x) >= F[x]$. $< p(x) >=< g(x) > \implies deg(g(x)) = deg(p(x))$. Conversely, $< g(x) >= F[x] \implies deg(g(x)) = 0$ and $deg(h(x)) = deg(p(x))$. This shows that $p(x)$ is irreducible over F.
($\Leftarrow$) Suppose $p(x)$ is irreducible over F and let $J =< f(x) >$ be an ideal with $< p(x) >\subseteq J =< f(x) >\subseteq F[x]$. Then, $p(x) \in< f(x) > \implies p(x) = q(x)f(x)$ for some $q(x) \in F[x]$. By our assumption that $p(x)$ is irreducible, we must either have $deg(f(x)) = deg(p(x)) \implies q(x)$ is a nonzero constant, or $deg(q(x)) = deg(p(x)) \implies f(x)$ is a nonzero constant. In the former case, $< p(x) >=< f(x) >$ and in the latter, $< f(x) >= F[x]$. Either way, this shows that $I =< p(x) >$ is a maximal ideal. □

Practice proof techniques from the last few proofs and return to Page 267 in [P]

Chapter 9: Euclidean Domains

Definition 0.90 (Euclidean Domain)**.** Informally, a **Euclidean Domain** is an integral domain in which a division algorithm holds.
More formally, an integral domain D is called a Euclidean domain if $\exists$ $\curlyvee : D \setminus \{0\} \to \mathbb{Z} \cup \{0\}$ from the set of nonzero elements of D to the set of non negative integers such that

1. For $x \neq 0$, $y \neq 0$ in D, $\curlyvee(x) \leq \curlyvee(xy)$
2. Given a and $b \neq 0$ in D, $\exists$ $q, r \in D$ such that $a = qb + r$ such that $r = 0$ or $\curlyvee(r) < \curlyvee(b)$

Theorem 0.91. *Every Euclidean domain is a PID.*

Proof. Let I be an ideal in a Euclidean domain D. If $I = \{0\}$, then $I =< 0 >$. If $I \neq \{0\}$, let $0 \neq a \in I$ be an element of I such that $\Upsilon(a) \leq \Upsilon(x)$ for all $0 \neq x \in I$. We will show that $I =< a >$. Let $b \in I$. Then $\exists\ q, r \in D$ such that $b = qa + r$ with $r = 0$ or $\Upsilon(r) < \Upsilon(a)$. $r = b - qa \implies r \in I$. By the minimality of $\Upsilon(a)$, we have that $r = 0 \implies b = qa \in< a >$. Therefore, $b \in< a >$ for all $b \in I$ and $I =< a > \implies D$ is a principal ideal domain. $\square$

Definition 0.92. Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$.

1. b is said to be a **divisor** of a in R, written $b \mid a$ if $\exists\ x \in R$ such that $ax = b$
2. $c \in R$ is a **common divisor** of a and b if $c \mid a$ and $c \mid b$.

Definition 0.93. Let R be a commutative ring and let $a, b \in R$. A **greatest common divisor** of a and b is a nonzero element $d \in R$ such that

1. d is a common divisor of a and b
2. If c is a common divisor of a and b, then $c \mid d$.

Theorem 0.94. *Let D be a Euclidean domain and $a, b \in D$ two nonzero elements of D. Then $\exists\ d \in D$ such that*

1. *d is a greatest common divisor of a and b*
2. *$\exists\ u, v \in D$ such that $d = ua + vb$.*

Proof. Let $I = \{xa + yb \mid x, y \in D\}$. I is an ideal of D (specifically the ideal generated by a and b). Because every Euclidean domain is a principal ideal domain, $I =< d >$ for some $d \in D$. Since $d \in I$ $\implies d = ua + vb$ for some $u, v \in D$. Since $I =< d >$, every element in I is of the form xd for $x \in D$. Since $a \in I$ by construction $\implies d \mid a$ (and the same thing for $b \implies d \mid b$). If $c \mid a$ and $c \mid b$ such that $a = xc$ and $b = yc \implies d = uxc + vyc = (ux + vy)c$ such that $c \mid d$ (and this concludes the proof!). $\square$

Proposition 0.95. *Let D be an integral domain and let $a, b \in D$. Then if d and d' are greatest common divisors of $a, b \in D$, then $d = ud'$ for some unit $u \in D$.*

Proof. Since both d and d' are greatest common divisors of a and b, $d \mid d'$ and $d' \mid d$. Therefore, $d = ud'$ and $d' = vd$ for some $u, v \in D$. This implies that $d = u(vd) = (uv)d \implies (1 - uv)d = 0$ and $d \neq 0$ $\implies uv = 1 \implies u$ is a unit with its inverse v in D. $\square$

Theorem 0.96. *Let D be a Euclidean domain. Then,*

1. *$\Upsilon(1) \leq \Upsilon(a)\ \forall\ 0 \neq a \in D$*
2. *$\Upsilon(1) = \Upsilon(a)$ if and only if a is a unit in D*

Proof.

1. $\Upsilon(1) \leq \Upsilon(1 * a) = \Upsilon(a)\ \forall\ 0 \neq a \in D$
2. If a is a unit in D, then $\Upsilon(a) \leq \Upsilon(a * a^{-1}) = \Upsilon(1) \leq \Upsilon(a)$. hence, $\Upsilon(1) = \Upsilon(a)$. Conversely, if $\Upsilon(1) = \Upsilon(a)$, by the division algorithm $\exists\ q, r \in D$ such that $1 = qa + r$ with $r = 0$ or $\Upsilon(r) < \Upsilon(a)$. But since $\Upsilon(a) = \Upsilon(1)$ and by (1), $\Upsilon(1) \leq \Upsilon(r)$, we cannot have $\Upsilon(r) < \Upsilon(a)$ and must have $r = 0$. Therefore, $1 = qa$ and a is a unit.

$\square$