ABSTRACT ALGEBRA

Author
Persy

Contents

1 Groups

2 Section 13,14,15

Def 2.1. A subgroup N of G is called a normal subgroup, if a left coset of N is the same as the corresponding right coset of N.
i.e. gN = Ng for all g $\in G$
We write $N \triangleleft G$.

Theorem 2.2. For any group homomorphism $\phi : G \to G'$: $\ker\phi \triangleleft G$

Proof 2.3. 1. $\ker\phi <$ G.
2. To show that it is a normal, we show show $g(ker\phi) = (ker\phi)g$
And we do it by $\subseteq$ and $\supset$ and we take any$k \in ker\phi$.
$\subseteq: gk = (gkg^{-1})g$ Then to show $\phi(gkg^{-1}) = e$. The other side is similar.

Theorem 2.4. Assume $H < G$ The following statements are equivalent:

1. $H \triangleleft G$
2. $g^{-1}Hg = H$ for all $g \in G$
3. $g^{-1}Hg \subseteq H$ for all $g \in G$

Def 2.5. $H \triangleleft G$. S $= \{gH \mid g \in H\}$ Define a binary operation on S s.t. $(g_1H) * (g_2H) = (g_1g_2)H$

Note. Need to check it is well defined, that is to show take different representative of g1 and g2 we get the same result, which is to consider $g_1H = g'_1H$, $g_2H = g'_2H$

Theorem 2.6. The map: $\pi : G \to S = \{gH \mid g \in G\}$, S is the quotient group that has H as the identity, is a group homomorphism where $H \triangleleft G$.
The kernel: $\ker\pi = H$

Theorem 2.7. Fundamental theorem of group homomorphism.
Let $\phi : G \to G'$be a group homomorphism. Then:

1. $\phi(G) < G'$
2. ker$\phi \lhd G$
3. The quotient group $G/ker\phi$is isomorphic to $\phi(G)$ via the map:
   $\bar{\phi} : G/ker\phi \to \phi(G)$
   $gker\phi \mapsto \phi(g)$

Def 2.8. Automoprhism and adj.

Def 2.9. A group is called simple if it has no proper nontrivial normal subgroup.

Theorem 2.10. An, when $n \geq 5$ is simple.

Def 2.11. A maximal normal subgroup of a group G is a normal subgroup M not equal to G s.t. that there is no proper normal subgroup N of G properly contains M.

Theorem 2.12. M is a maximal normal subgroup of G $\Leftrightarrow$ G/M is simple

3 Ring

3.1 Section 18: Ring Fields

Def 3.1. A ring $(R, +, \cdot)$ is a set R with two bineary operations, addition and multiplication such that the following requirements hold:

1. $(R, +)$ is an abelian group.
2. $(R, \cdot)$ is associative.
3. $+ and \cdot$ satisfy left and right distributive law:
   for any $a, b, c \in \mathbb{R}$:
   $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
   $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Example 3.2. $(0, +,)$ 0 is a trivial ring

Example 3.3. $(\mathbb{Z}/\mathbb{Q}/\mathbb{R}, /\mathbb{C}, +, \cdot)$ are standard ring structures.

Example 3.4. $(nZ, +, \cdot)$ is a ring and a subring of $\mathbb{Z}$

Example 3.5. $(\mathbb{Z}_n, +, \cdot)$ is a ring.

Def 3.6. A map $\phi : R \to R'$ for rings R and R' is called a ring homomorphism if
1) $\phi(a + b) = \phi(a) + \phi(b)$
2) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ for all $a, b \in R$
(1) is equivalent to $\phi : (R, +) \to (R', +')$ is a group homomorphism. $\ker\phi$ is the kernel for such group homomorphism.

Example 3.7. Modulo map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ is a ring homomorphism.

Proof 3.8. ϕ is a group homomorphism.
$\phi(ab)? = \phi(a) \cdot \phi(b)$
we can denot $a = ln + \phi(a)$, $b = mn + \phi(b)$ as elements in $\mathbb{Z}_n$
$a \cdot b = (ln + \phi(a)) \cdot mn + \phi(b) = ln(mn + \phi(b) + \phi(a)mn + \phi(a) \cdot \phi(b)) = \phi(a) \cdot \phi(b)$

Def 3.9. A bijective ring homomorphism is called a ring isomorphism.

Example 3.10. $(\mathbb{Z}, +) \cong (3\mathbb{Z}, +)$ is a group isomorphism but not a ring somorphism.

Def 3.11. A ring $(R, +, \cdot)$ is called commutative if $(R, \cdot)$ is commutative. Unital or a ring with unity of $(R, \cdot)$ has the identity for $(R, \cdot)$
Rmk: Communtativity and unital property are preserced under ring isomorphism.

Theorem 3.12. Denote by 1 the unity of the unital ring R.
Then R is trivial iff 1= 0

Example 3.13.

- $\mathbb{Z}_n$ is commutative.
- $\mathbb{C}, \mathbb{R}, \mathbb{Q}.\mathbb{Z}$are unital.
- $\mathbb{Z}_n$ is unital.
- $n\mathbb{Z}$ is not unital when $n \geq 2$

Example 3.14. Show that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ as rings when m and n are coprime.

Proof 3.15. The group isomorphisms can be shown by mapping generator to generator. $\phi : 1 \mapsto (1, 1)$ And we show such it is a ring homomorphism too.

Def 3.16. Let R be a unital ring with $1 \neq 0$:
A multiplicative inverse of $a \in R$ is an element $b \in R$ so that $a \cdot b = 1 = b \cdot a$

Def 3.17. Let R be a untial ring with $1 \neq 0$.

- An element $u \in R$ is called a unit, if it has a multiplicative inverse.
  Denot by $R^{\times} = \{u \in R \mid \text{u is a unit}\}$
- If $R^{\times} = R^{*}$ then R is a divison ring.
- If R is commutative, it is called a field.

Example 3.18. $\mathbb{Z}_n$ is commutative unital ring. $\mathbb{Z}_n^{\times}$ =$\{m \in \mathbb{Z}_n \mid gcd(m, n) = 1\}$

3.2 Section 19: Integral Domains

Def 3.19. In a ring R, if $a, b \in R^*$ satisfy $a \cdot b = 0$ then a, b are called divisors of zero.

Theorem 3.20. $\mathbb{Z}_n = \{0, 1, \cdots n-1\}, m \in \mathbb{Z}_n$ is a divisor of zero iff $m \neq 0$ and gcd(m,n)$\neq 1$

Proof 3.21. Denote by d= gcd(m,n).
$\Rightarrow$ If m is a divisor of zero, there must be a $k \neq 0$ in $\mathbb{Z}_n$ that $mk = ln$.
If $gcd(m, n) = 1$, $n \mid k$, then $k = 0$ in $\mathbb{Z}_n$. Contradiction. Thus $gcd(m, n) \neq 1$
$\Leftarrow$ Note that $\frac{mn}{d} = \frac{m}{d} \cdot n$ in $\mathbb{Z}$
there is $[m][\frac{n}{d}] = [\frac{m}{d}n] = [0]$ in $\mathbb{Z}_n$.
If $d \neq 1$, $\frac{n}{d} \neq 0$ in $\mathbb{Z}_n$. We conclude must have $m = 0$

Def 3.22. An integral domain is a commutative unital ring with $1 \neq 0$ and containing no divisor of zero.
Cor: For any prime number p, $\mathbb{Z}_p$ is an integral domain.

Example 3.23. Show$\mathbb{Z}_p$ is a field when p is a prime number.

Proof 3.24. We only need to show that every nonzero element in $\mathbb{Z}_p$ is a unit.
Take $a \in \mathbb{Z}_p . a \neq 0$
Consider the map $\phi_a : \mathbb{Z}_p \to \mathbb{Z}_p$
$x \mapsto ax$ in $\mathbb{Z}_p$
We claim that ϕ_a is a bijection:

- ϕ_a is injective: $\phi_a(x) = \phi_a(y)$
  Then ax = ay $\Rightarrow a(x - y) = 0$
  Since $\mathbb{Z}_p$ is an integral domain and has no divisor of 0, then $a \neq 0$
  Thus $x = y$
- ϕ_a is a surjective map since $\mathbb{Z}_p$ order is finite and injectivity implis surjectivity.
  Then it is a bijective map.

Hence there is some $x \in \mathbb{Z}_p$ that $\phi_a(x) = 1$ which is $ax = 1$ and shows that a is a unit.

Theorem 3.25. Every finite integral domain is a field.

Example 3.26. $\mathbb{Z}$ is an example of integral domain, but not a field. Note it has infinite order.

Theorem 3.27. Every field is an integral domain.

Proof 3.28. That is to show for $a, b \in F, ab = 0$ either $a = 0$ or $b = 0$
If $a \neq 0$ then a is a unit, thus $a \cdot a' = 1 = a' \cdot a$.
Then $a'(ab) = a'0 = 0 = 1(b) = b$

Def 3.29. Let R be a ring. Define the charateristic of R as:
char(R) = min $\{n \in \mathbb{Z}^+ \mid n \cdot a = 0 \text{ for all } a \in R\}$
Define char(R) = 0 when such set is empty.

Example 3.30. char($\mathbb{Z}_n$) = n, char($\mathbb{Z}$) = 0

Theorem 3.31. For a unital ring R,
char(R) = min $\{n \in \mathbb{Z}^+ \mid n \cdot 1 = 0 \text{ for 1 is unity} \in R\}$

Proof 3.32. Easy to check if $\{n \in \mathbb{Z}^+ \mid n \cdot 1 = 0\} = \varnothing$ Then $\{n \in \mathbb{Z}^+ \mid n \cdot a = 0\} = \varnothing$ the char(R) does not exists = 0.
Other wise: denote $m = min\{n \in \mathbb{Z}^+ \mid n \cdot 1 = 0\}$ Want to show that $ma = 0$ for all $a \in R$.
Since ma = $a + a + ...a$(for m times) = $a * 1 + a * 1 + ...a * 1$(for m times)
=$a(1 + 1...1) = a(m \cdot 1) = a \cdot 0 = 0$

Note. Direct product of two integral domain is not an integral domain.

3.3 Section 20: Fermat's Euler's theorems

Theorem 3.33. Little Theorem of Fermat
Let $a \in \mathbb{Z}$ p is a prime number. $p \nmid a$. Then $a^{p-1} \equiv 1$ mod p
Cor: $a^p \equiv$ a mod p

Example 3.34. what is 8^{97} in $\mathbb{Z}_{13}$ (order12 Field)?
So $[8]^{12} = [1]$
$97 \div 12 = 8$ R 1
$8^{97} = 8^{12*8+1} = ([8]^{12})^8 \cdot [8] = [1]^8 \cdot [8]$

Using Cor: $8^{97} = 8^{13*7+12} = ([8]^{13})^7 \cdot ([8]^{12}) = [8]^7 \cdot [8]^{12} = [8]^7 \cdot [1]$
$[8] \equiv [-5]$ mod 3
Thus:
$[-5]^7 = [-5] \cdot [-5]^6 = [-5] \cdot ([-5]^2)^3 = [-5] \cdot ([25] \equiv [-1])^3$
$= [-5][-1] = 5$ mod 13

Example 3.35. show that $15 \mid (n^{33} - n)$ for all $a \in \mathbb{Z}$
Proof: 15 is not prime.
But $15 = 3 \cdot 5$
So it is enough to show that $3 \mid (n^{33} - n)$ and $5 \mid (n^{33} - n)$
We discuss by cases.

- If $\mathbf{3} \nmid n$ Then $n^{33} = (n^{\mathbf{2}})^{16} \cdot n = 1 \cdot n$ mod 3 (in Z3)

  Thus $3 \mid (n^{33} - n = 0$ in $\mathbb{Z}_3)$
- If $3 \mid n$ Then $3 \mid n \cdot (n^{32} - 1)$

  Thus $3 \mid (n^{33} - n)$

Similarly we show $5 \mid (n^{33} - n)$

- If $\mathbf{5} \nmid n$ Then $n^{33} = (n^{\mathbf{4}})^8 \cdot n = 1 \cdot n$ mod 5 (in Z5)

  Thus $5 \mid (n^{33} - n = 0$ in $\mathbb{Z}_5)$
- If $5 \mid n$ Then $5 \mid n \cdot (n^{32} - 1)$

  Thus $5 \mid (n^{33} - n)$

Note. $p1 < p2 < \cdots < pk$
let m $= c(p1-1)(p2-1)\cdots(pk-1)+1$ where c is some constant.
$\Rightarrow p1p2\cdots pk \mid n^m - n$

Def 3.36. Euler's generalization:
$\mathbb{Z}_n^\times$ = m $\in \mathbb{Z}_n$ | m is a unit
$= m \in \mathbb{Z}_n \mid gcd(m,n) = 1$

Proof 3.37. $gcd(m,n) = 1 \Leftrightarrow$ m is not a divisor of zero (*)
$\Rightarrow$ Assume we know gcd(m, n) = 1 and to show m is a unit.
Thus for such m, construct $\phi_m : \mathbb{Z}_n \to \mathbb{Z}_n$

$$a \mapsto ma$$

By previous proof, we know that such map is bijection for $\mathbb{Z}_p$ And bascially we generalize it to take everything that is coprime with n. So we know that m must be a unit.
$\Leftarrow$ Assume we know it is a unit to show gcd(m,n) = 1
Conversely, m is a unit imlies m is not a zero divisor, thus gcd(m,n) = 1

Def 3.38. Euler Phi-Function: $\varphi(n) = \#\{m \in \mathbb{Z}^+ \mid m \leq n$ gcd(m,n) = 1$\}$

Theorem 3.39. Any unital ring R, $R^\times = \{\ a \in R \mid$ a is a unit $\}$ is a group under multiplication.
Cor: $\mathbb{Z}_n^\times$ is a group of order $\varphi(n)$

Proof 3.40. closed: For $a_1, a_2 \in R^\times$ and each have inverse a_1^{-1} and a_2^{-1}. Thus we know that $a_1 a_2 a_2^{-1} a_1^{-1} = 1$ Thus for $a_1 a_2$ we have the inverse $(a_1 a_2)^{-1} = a_2^{-1} a_1^{-1}$ thus it is closed
Associative follows by multiplication. Identity is unity 1. Inverse follows immediate by definition of unit.

Example 3.41. $\varphi(12) = 4$. Which are the units of $\mathbb{Z}_{12}^\times$ that are 1, 5, 7, 11.

Theorem 3.42. Euler's theorem: For any $a \in \mathbb{Z}, n \in \mathbb{Z}^+$ with gcd(a,n) = 1.
There is $a^{\varphi(n)} \equiv 1$ mod n

Proof 3.43. gcd(a,n) = 1 implies $[a] \in Z_n^\times$ which then $|Z_n^\times| = \varphi(n)$
Then $a^{\varphi(n)} = 1$ in $\mathbb{Z}_n$ that is $a^{\varphi(n)} \equiv 1$ mod n

Example 3.44. Any $n \in \mathbb{Z}$ with gcd (n) then $n^4 \equiv 1$ mod 12
take n = 5, $5^4 = 625 = 52 * 12 + 1$

Note. Application to congruence equations
Solve $ax \equiv$ b mod n

Theorem 3.45. If gcd (a,n) = 1, then the equation has and only has one solution.

Proof 3.46. To show we have such a solution: since gcd (a,n) = 1, we know that $a \in \mathbb{Z}_n^{\times}$ which a is a unit.
Then we can find an inverse of a and then our $x \equiv ba^{-1}$ mod n.
To show such solution is unique, assume now we have $x_1, x_2 \equiv ba^{-1}$ mod n.
Thus $ax_1 = ax2$.
If a is not a divisor of zero, then what we state is true that $x_1 = x_2$.
a indeed is not a divisor of zero in $\mathbb{Z}_n$, since gcd(a,n) = 1

Example 3.47. Solve $3x \equiv 5$ mod 10.
gcd(3,10) = 1.
We first find our 3 inverse in 10, which $3^{-1} = 7$. Thus $x = 5 * 7 = 35 = 5$ mod 10
$x = 10n + 5$ for $n \in \mathbb{Z}$

Theorem 3.48. If gcd(a,n) = d, then the euqation has solution iff $d \mid b$. And then there are d solutions in $\mathbb{Z}_n$

Proof 3.49.
1) Show we have solution iff $d \mid b$.
$\Leftarrow$ Consider $[\frac{a}{d}][x] = [\frac{b}{d}]$ in $Z_{\frac{n}{d}}$
$gcd(\frac{a}{d}, \frac{a}{d}) = 1$
By previous thm:
we show there is a unique solution $[x_0]$ s.t. $\frac{a}{d}[x_0] - \frac{b}{d} = \frac{n}{d} \cdot l$ for $l \in \mathbb{Z}$ And multiply both sides by d we get $ax_0 - b = nl$

$\Rightarrow$ If $[a][x] = [b]$ in $\mathbb{Z}_n$ has a solution, then $ax - b = 0$ in $\mathbb{Z}_n$.
Then $ax - b = nl$ for $l \in \mathbb{Z}$. Divide both side by d, we get $\frac{a}{d} - \frac{b}{d} = l$
Since our l is an integer, we must conclude that $\frac{b}{d}$ is an integer.

2) Assume $d \mid b$ we want to show there are d solutions.
If $[x_0]$ is a solution, then for any solution $[x], [a][x_0] = [a][x]$ in $\mathbb{Z}_n$
and so $[\frac{a}{d}][x_0] = [\frac{a}{d}][x]$ in $\mathbb{Z}_{\frac{n}{d}}$
This implies $[x] = [x_0]$ in $\mathbb{Z}_{\frac{n}{d}}$ which we then can write
$x = x_0 + \frac{n}{d} \cdot l$ for $l \in \mathbb{Z}$
Thus $[x]$ can take on : $[x_0]$, $[x_0 + 2 \cdot \frac{n}{d}] \cdots$ $[x_0 + (d-1) \cdot \frac{n}{d}]$

Example 3.50. Solve $15x \equiv 27 \bmod 18$

gcd (15,18) $= 3 \mid 27$. Thus there are 3 solutions in $\mathbb{Z}_{18}$

Solve $5x \equiv 9$ in $\mathbb{Z}_6$

$x = 9 * 5 = 45 = 3$ in $\mathbb{Z}_6$

In $Z_1 8$, $x = 3$ or $3 + 6 * 1 = 9$ or $3 + 6 * 2 = 15$

3.4 Section 21: The Field of Fractions of Integral Domain

> **Note.** Main Task: Any integral Domain D can be enlarged to a field F by including fractions of D. Just as the same ways as from $\mathbb{Z}$ to $\mathbb{Q}$.

Construction from a given Integral Domain D.

- Step1: Consider an equivalence relation on $D \times D^*$ denoted by S as (a,b) (c,d) iff ad = bc.

  Check this is an equivalence relation:

  1)Reflexive: (a,b) (b,c)

  2)Symmetric: (a,b) (c,d)$\Rightarrow$ (c,d) (a,b)

  3)Transitive: (a,b) (c,d), (c,d) (e,f)$\Rightarrow$(a,b) (e,f)

  Define F:= $D \times D^*/$ There is a natural inclusion map: $D \to F$ as $a \mapsto [(a,1)]$ which is equivalence class of (a,1).

- Step2: Define + and $\bullet$ on F and check they coincide with + and $\bullet$ on D.

  Define [(a,b)+ (c,d)] = [(ad+bc), (bd)]; [(a,b)][(c,d)] = [(ac,bd)] Check they are well defined: To show our operations are well-defined, we take different representatives in S and applying this operation, we can get the same result.

  WTS: Take $(a_1, b_1) \in [(a,b)], (c_1, d_1) \in [(c,d)]$

  We want to show $(a_1d_1 + b_1c_1, b_1d_1) \in [(ad + bc, bd)]$
  and $(a_1c_1, b_1d_1) \in [(ac, bd)]$

  This is true because (a_1, b_1) (a, b) and $a_1b = b_1a$ similarly for $c_1d = d_1c$
  Then times both side by b_1b and d_1d, we get $a_1bd_1d = b_1ad_1d$ and $c_1db_1b = d_1cb_1b$
  Add them together,$a_1bd_1d + c_1db_1b = b_1ad_1d + d_1cb_1b$
  by axioms of integral domain such as communtative and distributitive property, we get $(a_1d_1 + b_1c_1)bd = b_1d_1(ad + bc)$ Thus we show it is well-defined addition. We can show the same for multiplication.

  Lastly, restricued on D, they are the orginial addition and multiplication.
  by $a + b \mapsto [(a, 1)] + [(b, 1)]$ $a \cdot b \mapsto [(a, 1)] \cdot [(b, 1)]$

Step3: Check $(F, +, \dot{)}$ is a field.

By check $(F, +, \dot{)}$ is a ring and it is commutative, unital and every nonzero element has multiplicative inverse. [(1,1)] as the unit.

Theorem 3.51. Let D be an integral domain. Then Frac(D) is the smallest field that contains D.
i.e. Every field L that contains D should have a subfield F that F is ring isomorphic to Frac(D).

Proof 3.52. Lets consider $D \subseteq L$ and L is a field. Take any $a, b \in D$ with $b \neq 0$, there must be $ab^{-1} \in L$.
We consider the map $\phi : Frac(D) \to L, [(a, b)] \mapsto ab^{-1}$ This map is well-defined: [(a,b)] = [(a', b')] $\Rightarrow ab^{-1} = a'b'^{-1}$ and is an injective ring homomorphism(Frac(D) with L).
This F:= ϕ Frac(D) is a subfield of L and contains D. It is isomorphism with Frac(D).

Example 3.53. D = $\{m + ni \mid m, n \in \mathbb{Z}\}$ Gaussian integers. $D \in \mathbb{C}$. Frac(D) = $\{m + ni \mid m, n \in \mathbb{Q}\}$ that is also a field contains i.
take $\frac{m+ni}{p+qi} = \frac{mp+nq+(np-mq)i}{p^2+q^2}$

3.5 Section 22: Rings of Polynomials

Def 3.54. Let R be a ring (coefficient ring):

R[x] = $\{\ a_0 + a_1x + a_2x^2 + ... + a_nx^n | a_0, a_1, ..a_n \in \mathbb{R}\}$

Naturally$R \to R[x]$ is injective that $a \mapsto a \in R[x]$

Note. $R[x]$ has a natural + and ·induced from (R, +, ·)

f(x) = $\sum_{k=0}^{n} a_k x^k$

g(x) = $\sum_{l=0}^{m} b_l x^l$

f(x) + g(x) = $\sum_{k=0}^{max\{n,m\}} (a_k + b_k)x^k$

f(x) · g(x) = $\sum_{k=0}^{m+n} (\sum_{i=0}^{k} a_i b_{k-i})x^k$

Theorem 3.55. R[x] is a ring when R is a ring.

Moreover, if R is unital, then R[x] is unital. share unity 1.

If R is commutative, then R[x] is communtative.

Proof 3.56. on $(R[x], +, \cdot)$

- $(R[x], +, \cdot)$ is an belian group with 0 as identity. - $(\sum a_k x^k) = sum(-a_k)x^k$
- $(R[x], +, \cdot)$ is associative.

  - unfinished????
- $(+, \dot{)}$ has distribution law.

  When R is commutative, R[x] is also commutative.

  When R is unital, 1 is the unity of R[x].

Example 3.57. Consider the polynomial ring $\mathbb{Z}_2[x]$

$x + 1 \in \mathbb{Z}_2[x]$

1. $x^2 + 1$cannot be factorized into polynomials with lower degrees in R[x] but can be factorized in $\mathbb{Z}_2[x]$
2. $(x + 1) + (x + 1) = 0 * x + 0 = 0$ Thus char($\mathbb{Z}_2[x]$) = 2 =char($\mathbb{Z}_2$)

Theorem 3.58. Let R be a ring. Then char(R[x]) = char (R). R is a subring of R[x].

Proof 3.59. If char(R) = n > 0, then for any $\sum aix^i \in R[x]$ n($\sum aix^i$) = $\sum (nai)x^i \in R[x] = 0$ So char(R[x])$\leq n$

Because R is a subring of R[x], so char(R[x])$\geq n$ Then we show char(R[x]) = char(R).

Theorem 3.60. Let $\phi : R \to R'$ be a ring homomorphism.

Show that $\hat{\phi} : R[x] \to R'[x]$

$\hat{\phi} : (\sum a_i x^i) \to (\sum \phi(a_i) x^i)$ is a ring homomorphism.

Moreoever, when ϕ is injective, $\hat{\phi}$ is also injective, same as surjective.

Proof 3.61.

- Check $\hat{\phi}(f(x) + g(x)) = \hat{\phi}(f(x)) + \hat{\phi}(g(x))$
- Check $\hat{\phi}(f(x)g(x)) = \hat{\phi}(f(x))\hat{\phi}(g(x))$

Theorem 3.62. Let R be a ring, then the ring(R[x])[y] is isomorphic to the ring(R[y])[x].The isomorphism class is denoted by R[x,y].

Def 3.63. The evalutaion homomorphism:

E is a ring then Map(E,E) (map from E to E) is a ring.

Take $\alpha \in E, e\hat{v}_a : Map(E, E) \to E$ is a ring homomorphism.

Let F be a subring of E.

Construct $\phi : F[x] \to Map(E, E)$

f(x) = $\sum a_i x^i$ is mapped to $F : E \to E \equiv b \mapsto \sum a_i b^i$

Note. Important things to notice: Evaluation map is a ring homomorphism.

$\phi : F[x] \to F$ as $\phi(p(x)) = p(a)$

Detailed proof below. but here is another proof that after group homomorphism we only need to check it is multiplicative on monomials:

monomials *original proof*

Proof 3.64. Lemma:

ϕ is a ring homomorphism if E is commutative.

Proof:

1) Group Homomoprhism: Take $\phi(f(x) + g(x))(\beta)$ and WTS it equals $\phi(f(x)) + \phi(g(x))(\beta)$.

f(x) = $\sum aix^i$ g(x) =$\sum bjx^j$

$\phi(f(x) + g(x))(\beta) = \phi(\sum(ai + bi)x^i)$ if we assume i = max(i,j).

$\phi(\sum(ai + bi)x^i) = \sum(ai + bi)\beta^i = \sum ai\beta^i + \sum bi\beta^i = \phi(f(x)) + \phi(g(x))(\beta)$.

2) Ring Homomorphism: By similar argument, $f(x)g(x) = \sum_k(\sum_{i+k=k} aibj)x^k$

Evaluate x at β to get ϕ.

$\phi(f(x)(\beta) = \sum ai\beta^i$, $\phi(g(x)(\beta) = \sum bj\beta^j$. Equals when it is commutative.

Theorem 3.65. Let E be a field and let F be a subfield of it.

For any $a \in E$ the map $ev_\alpha = e\hat{v}_a \circ \phi$

$e\hat{v}_a : F[x] \to E, \sum aix^i \mapsto \sum ai\alpha^i$ is a ring homomorphism.

Note. Let F be a field. In general, the map $\phi : F[x] \to Map(F, F)$ is not injective, when $char(F) \neq 0$.

Consider $char(F) = p \Leftrightarrow \mathbb{Z}_p$: Consider $f(x) = x - x^p \in F_p[x]$

By FLT: $f(a) = a - a^p = 0 \in F_p = Z_p$ Then the kernel is not trivial, thus not injective.

Example 3.66. About field construction Consider $\mathbb{Q} \subseteq \mathbb{R}$, $\pi \in \mathbb{R}\backslash\mathbb{Q}$

$ev_\pi : \mathbb{Q}[x] \to \mathbb{R}$ is an injective homomorphism. i.e. π is a transendental number s.t. $f(\pi) = 0$ iff all coefficients are zero, $\ker(ev_\pi) = \emptyset$

$ev_\pi(\mathbb{Q}[x]) = \{\sum_{i=0}^n ai\pi^i \mid ai \in \mathbb{Q}, n \in \mathbb{Z}^+\}$ is a subring (subdomain) of $\mathbb{R}$ which is isomorphic to $\mathbb{Q}[x]$

Note. $\mathbb{Q} \subseteq \mathbb{Q}[x] \subseteq Frac(\mathbb{Q}[x]) \subseteq \mathbb{R}$

In general, Consider $\alpha \in E\backslash F$ which $\alpha \notin F$.

For any evaluation map: $ev_\alpha : F[x] \to E$, $F[x] \cong ev_\alpha(F(x)) \subseteq E$.

The transedental extentions being isomorphic to F[x] as follows: *proof on bijection, also going to do later*

Then $F \subseteq F[x] \subseteq Frac(ev_\alpha F(x)) \subseteq E$.

Example 3.67. Consider $\mathbb{R} \subseteq \mathbb{C}$. $i \in \mathbb{C} \backslash \mathbb{R}$. $ev_i : \mathbb{R}[x] \to \mathbb{C}$ is not injective. (Because 1) we know that the evaluation map is homomorphism 2) the kernel is not empty) $ev_i(x^2 + 1) = 0$ then i is an algebraic number over $\mathbb{R}$.

But ev_i is surjective since any $a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$

$a+bi = ev_i(a+bx)$ by Fundamental theorem of ring homomorphism: $\mathbb{R}[x]/ker(ev_i) \cong \mathbb{C}$ (which is the image of ev_i, and is $\mathbb{Z} \times \mathbb{Z}_i$)

$ker(ev_i) := \{f(x) \in \mathbb{R}[x] \mid f(i) = 0\} = (x^2 + 1)$ the ideal generated by $x^2 + 1$. Such $\mathbb{R}[x]/(x^2 + 1)$ is the algebraic construction of the complex field.

Theorem 3.68. If D is an integral domain, then $D[x]$ is also an integral domain. For this case, $deg(f * g) = deg(f) + deg(g)$, $f, g \neq 0, \in D[x]$

Proof 3.69.

Example 3.70. Let D be an integral domain. What is $(D[x])^\times$ i.e. units of D[x]? Answer: $(D[x])^\times = D^\times$. f(x) * g(x) = 1 $\Rightarrow$ deg(f) + deg(g) = 0 $\Rightarrow$ deg(f) = 0 = deg(g) only constant terms.

e.g. $(\mathbb{Z}[x])^\times = \{\pm 1\}$

Note. In general, for $f, g \in \mathbb{R}[x], f \neq 0, g \neq 0$: $deg(fg) \leq deg(f) + deg(g)$

i.e. $\mathbb{Z}_6$ $deg(3x(2x + 1)) = 1 < deg(3x) + deg(2x + 1)$ But when $\mathbb{Z}_p$ it is an integral domain $deg(f * g) = deg(f) + deg(g)$.

3.6 Section 23: Factorization of Polynomials over a Field

Let F be a field. Then F[x] is an integral domain.

Theorem 3.71. Division Algorithm for F[x]: F[x] statisfies division algorithm: Given any $f(x) = a_0 + a_1x + ... + a_nx^m$, $g(x) = a_0 + a_1x + ... + a_nx^n$ there exist unique q(x), r(x) $\in F[x]$ s.t. f(x) = q(x)g(x) + r(x) with r(x) = 0 or $deg(r(x)) < deg(g(x)) = n$

Proof 3.72. We first show the existence:
If $degf < degg$, we write $f(x) = g(x) * 0 + f(x)$ with q(x) = 0, f(x) = r(x) Then we discuss the cases:
$degf < degg$ then we are done by taking $q(x) = 0, r(x) = f(x)$
Otherwise, we show by induction. Then show the uniquess: Prove by contradiction:
Assume $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$
Then $r_1(x) - r_2(x) = (q_2(x) - q_1(x))g(x)$.
If $q_2(x) - q_1(x) \neq 0$, deg(RHS) = deg($q_2(x) - q_1(x)$) + deg(g(x))$\geq$ deg(g(x)) =n deg(LHS)$< n$. Contradiction.

Example 3.73. $f(x) = x^4 - 3x^3 + 2x^3 + 4x - 1$, $g(x) = x^2 - 2x + 3$ in F5[x]. we can use long division to get $q(x) = x^2 - x - 3$, $r(x) = x + 3$.

Theorem 3.74. cor1: For any $f(x) \in F(x)$ where F is a field, an element $a \in F$ is a zero of f(x) i.e. f(a) = 0 iff $f(x) = (x - a)g(x)$ for some $g(x) \in F[x]$
cor2: Assume $f(x) \in F[x]$, $f(x) \neq 0$ and $deg(f) = n$. Then f has at most n zeros in F.

Proof 3.75.

1. Cor1:

   $\Leftarrow$ obvious.

   $\Rightarrow$ To show that if a is a zero of $f(x)$ then we have $f(x) = (x-a)g(x)$, we notice that by division algorithm, our $f(x) = q(x)g(x) + r(x)$ thus WTS $r(x) = 0$. Here, our $g(x) = (x - a)$, then we conclude that $degr < 1, degr = 0$. Thus $r(x)$ is a constant polynomial, denoted by r.
   When a is a zero of $f(x)$, $f(a) = (a - a)q(a) + r$ thus $r = 0$

2. Cor2: Using induction.

Example 3.76. Use the above cor2: we can show that any finite subgroup of $(F*, \cdot)$ is cyclic where F is a field. In particular, for any finite field, $(F*, \cdot)$ is cyclic.

Def 3.77. A non-constant polynomial $f(x) \in F[x]$ is called irreducible over F if f(x) can NOT be written as $g(x)h(x)$ with $g, h \in F[x]$, $deg(g) < deg(f)$, $deg(h) < deg(f)$ otherwise f is called reducible over F.

Example 3.78. $x^2 + 1$ is irreducible over R, but reducible over C.

Example 3.79. $x^2 - 2$ is irreducible over Q, but reducible over R.

Note. $f(x) \in F[x]$ and non-constant, f is irreducible over F $\Leftrightarrow$ When f(x) = g(x)h(x) for $g, h \in F[x]$ then must be g or h is a unit (a constant). **(A unit in F[x] is nonzero constant polynomial in F[x], which are units in F)**

Theorem 3.80. For any $f(x) \in F[x]$ with deg(f) = 2 or 3, f is irreducible over F iff f has no zero in F.

Note. For degree 2 or 3:If f(x)has a root in F, it can be factored into linear factors (degree 1), proving it's reducible. If f(x) has no root in F, it can't be factored into lower degree polynomials, so it's irreducible.
For higher degrees (4 or more):The absence of a root in F doesn't guarantee irreducibility. A polynomial of degree 4 or higher might not have roots in F but could still be factored into irreducible polynomials of lower degree (greater than 1), making it reducible.

Proof 3.81. We show that "f is reducible over F iff f has zero in F." basically expand the above idea.

Theorem 3.82. Check whether it is irreducible over$\mathbb{Q}$ is the same as check whether it is irreducible over $\mathbb{Z}$

Theorem 3.83. Eisenstein Criterion:
Let $p \in \mathbb{Z}$ that is a prime number. $f(x) = a_n x^n + ... + a_1 x + a_0$ which $a_n \neq 0$ mod p, $a \equiv 0$ mod p for $i < n$, and $a_0 \neq 0$ mod p^2. Then f(x) is irreducible over $\mathbb{Q}$

Proof 3.84. Basic Idea: We WTS that it is irreducible over $\mathbb{Z}$. And we write $f(x) = (b_r x^r + ... + b_0)(c_s x^s + ... + c_0)$ Then we want to follow the criterion in the theorem and try to figure out a contradiction.

Note. Cor: For any prime number p:
$1 + x + x^2 + ... + x^{p-1} =: \Phi_p(x)$ is irreducible over $\mathbb{Q}$.

Theorem 3.85. F[x] is UFD = Unique factorization Domain.
Any non-constant $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials. The way is unique except for order and for unit factors in F.

3.7 Section 26: Fundamental theorem of ring homomorphism

Def 3.86. A map: $\phi R \to R'$ for rings R, R' is a ring homomorphism, if:
$\phi(a+b) = \phi(a) + \phi(b)$
$\phi(ab) = \phi(a)\phi(b)$

Theorem 3.87. For a ring homomoprhism: $\phi : R \to R'$

1. For any subring S of R, $\phi(s)$ is a subring of R'.
2. For any subring S' of R', $\phi(s')$ is a subring of R.
3. $\phi(1)$ is the unity of $\phi(R)$ if 1 is the unity of R.

Note. It is possible that $\phi : R \to R'$ is ring homomorphism, R is unital but R' is not.
e.g. R = $\mathbb{Z}$, R = $\mathbb{Z} \times 3\mathbb{Z}$.
$\phi : \mathbb{Z} \to \mathbb{Z} \times 3\mathbb{Z}$

Def 3.88. Let $\phi : R \to R'$ be a ring homomorphism. s.t. $\ker\phi = \phi^{-1}(0)$

Example 3.89. The modulo n map: $\phi : \mathbb{Z} \to \mathbb{Z}_n$ is a ring homomorphism with $\ker(\phi) = n\mathbb{Z}$

Def 3.90. Let R be a ring. An additive subgroup I of R is called an ideal of R if:
$aI \subseteq I$, $Ia \subseteq I$ for all $a \in R$

Note. (1) An ideal is a subring of R since for any $a, b \in I$: $ab \in aI \subseteq I$
(2) 0 is always an ideal called trivial ideal of R.

Theorem 3.91. Let $\phi : R \to R'$ be a ring homomorphism. Then the kernel is an ideal of R.

Proof 3.92. Kernel is a subgroup shown before. Now we check for any $r \in R$, we take $k \in ker(\phi)$. WTS $rk \in ker(\phi)$. $\phi(rk) = \phi(r)\phi(k) = 0$ Thus $rk \in ker(\phi)$.

Note. Group $\leftrightarrow$ Ring, Normal subgroup $\leftrightarrow$ ideal, Quotient Group $\leftrightarrow$ Quotient Ring.

Theorem 3.93. Let R be a ring and I be an ideal of it. Then the quotient group R/I of $(R, +)$ has a natural ring structure induced from the ring R.

The quotient map $\phi : R \to R/I$ is a surjective ring homomorphism with $\ker(\phi) =$ I.

Proof 3.94.

Notice binary operations on R/I: $(a+I)(b+I) = ab+I$ and $(a+I)+(b+I) = (a+b)+I$

1. We check if multiplication is well defined on R/I. Just as the construction in quotient groups, we define:
   $(a+I)(b+I) = ab+I$ we check by different representation of a and b, which $a+I = a'+I$, $b+I = b'+I$ ....details unfinished for next week Then we checked it is a ring.

2. Then we check the quotient map $\phi : R \to R'$ is a ring homomorphism. We know it is a group homomorphism and surjective by construction, then we know that: By our construction: $\phi(ab) = ab + I = (a + I)(b + I) = \phi(a)\phi(b)$ with kernel = I.

Theorem 3.95. Fundamental theorem of ring homomorphism:

Let $\phi : R \to R'$ be a ring homomorphism with kernel k.

Then (1) $\phi(k)$ is a subring of R'

(2) K is an ideal of R.

(3) The quotient ring R/k is ring isomorphic to $\phi[R]$ via the map:

$\bar{\phi} : R/k \to \phi(R)$

$\bar{\phi} : a + I \mapsto \phi(a)$

Proof 3.96. We did that $\phi(R)$ is a subring of R' and the quotient map$\pi : R \to R/I$ is a surjective ring homomorphism with kernel = I.

Now we want to show that $\hat{\phi} : R/K \to \phi(R)$ which is $a + I \mapsto \phi(a)$ is a ring isomorphism.

We check that $\hat{\phi}$ is well defined: Idea: Consider different representative $a' + k = a + k$ but $\hat{\phi}(a' + K) = \hat{\phi}(a + K)$

Then we already know that $\hat{\phi}$ is a group isomorphism. Only need to check it is a ring homomorphism.

Example 3.97. Definition for nilradical:

N:= $\{a \in R \mid a^n = 0$ for some $n \in \mathbb{Z}^+\}$ is an ideal of R.

Example 3.98. Definition for radical:

$\sqrt{N} := \{a \in R \mid a^n = N$ for some $n \in \mathbb{Z}^+\}$ is an ideal of R.

Example 3.99. What is the nilradical of R/N for an ideal N in a commutative ring R?

Consider $(a + N)^n = a^n + N = 0 + N$

Thus $a^n \in N, a \in \sqrt{(}N)$ that $a + N$ is in the nilradical of R/N.

3.8 Section 27:Prime and Maximal ideals

Note. Some difference between Normal subgroup and Ideal:

Ideal has the property that $Ia \subseteq I$ while normal subrgoup only is that $gh = hg$

If we are considering $\mathbb{Z}$, we get normal subgroup by addition, but get ideal by considering closure under multiplication with ring elements.

Ideal is ring. closed under addition, and closed under multiplication with Ring Elements.

Although **the quotient ring is a ring.**

Def 3.100. A **maximal ideal** of a ring R is an ideal M different from R such that there is no proper ideal N of R properly containing M.

Def 3.101. An ideal$N \neq R$ in a commutative ring R **is a prime ideal** if $ab \in N$ implies that either $a \in N$ or $b \in N$ for $a, b \in R$.

Note that $\{0\}$ is a prime ideal in $\mathbb{Z}$, and indeed, in any integral domain.

Note. All nontrivial ring has 2 ideals: itself and $\{0\}$.

Also, for a unital ring, if an ideal I contains a unit, then I = R.

We can show that by proof: $a \in R$ write $a = u(u^{-1}a) \in I(u^{-1}a) \subseteq R$

Example 3.102. When n is prime, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ is a field.

When n is not prime, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ is not an integral domain.

(n) is maximal ideal and prime ideal when n is prime.

Theorem 3.103. A field contains no proper nontrivial ideals.

Proof 3.104. Any improper nontrivial ideal in a field must contain unit element, and then is the field itself.

Theorem 3.105. If I, J are two ideals of ring R, then $I \cap J$ and $I + J = \{a + b \mid a \in I, b \in J\}$ are ideals of R.

Theorem 3.106. Let R be a commutative untial ring, and I is an ideal of R.

- I is a prime ideal $\Leftrightarrow$ R/I is an integral domain.
- I is a maximal ideal $\Leftrightarrow$ R/I is a field.

Cor: A maximal ideal in a commutative unital ring must be a prime ideal since a field must be an integral domain.

Proof 3.107. 1) "$\Rightarrow$"I is a prime ideal: we want to show that R/I is an integral domain. Only need to show that R/I has no divisor of zero. Consider element in R/I which $(a+I)(b+I) = 0+I \Rightarrow (ab)+I$ By how we take coset: $ab \in I$. Since I is a prime ideal, thus either $a \in I$ or $b \in I \Rightarrow a+I \in I$ or $b+I \in I$. Thus it is an integral domain.
1) "$\Leftarrow$" If R/I is an integral domain, then $(a+I)(b+I) = 0+I \Rightarrow$ either $a+I = I \Rightarrow a \in I$ or $b+I = I \Rightarrow b \in I$. Consider $ab \in I$ thus we either have $a \in I$ or $b \in I$.
2) "$\rightarrow$" I is a maximal ideal, to show that R/I is a field, we show any $a+I$ is a unit. Consider element $a \notin I$, and the any $(a) := ax|x \in R$ is an ideal. By previous theorem, $I+(a)$ is an ideal in R. We know that $I \subset I+(a)$ but I is the maximal ideal, thus $I+(a) = R$. Thus $I+(a)$ contains unity 1. Then we consider $(a+I)(x+I) = ax+I = I+(a)$ which contains 1. So there exists $x \in R$ s.t. $(a+I)(x+I) = 1$ and $a+I$ is a unit.
2) "$\leftarrow$" If R/I is a field, we want to show that I is the maximal ideal. $a+I \in R/I$ is a unit, thus $(a+I)(x+I) = 1 = ax+I$ for some $x \in R$. We claim that $(a) = ax$ is the smallest ideal we can get, thus anything strictly bigger than I must contain unity, and thus $= R$. Then we show that I is the maximal ideal.

Note. If I1 is an ideal of A, I2 is an ideal of B, then $I1 \times I2$is an ideal of $A \times B$

Theorem 3.108. If R is a ring with unity and N is an ideal of R containing a unit, then N = R.

Proof 3.109. If $1 \in I$ then I = R since $r1 = r$ for all $r \in R$. If N contains a unit element, then $r * u \in I$ that u is the unit element in ideal. If we take $r = u^{-1}$, then $1 \in I$, then N = R.

Ideal Structure of F[x]:

Def 3.110. If R is a commutative ring with unity and $a \in R$, the ideal $\{ra \mid r \in R\}$ of all multiples of a is the **principal ideal generated by a** and denoted by $< a >$. An ideal N of R is **a principal ideal** if $N =< a >$ for some $a \in R$.

Def 3.111. An integral domain D is called a principal ideal domain (PID) if every ideal of D is a principal ideal.

Theorem 3.112. F[x] with F is a field is a PID.
? In fact, any integral domain with division algorithm is a PID.
$\mathbb{Z}$ is a PID.

Proof 3.113. To show that $F[x]$ is a PID, we show all ideals are principal.
Take $I \in F[x]$ that is the ideal.
We want to show that all $f(x) \in I$ is generated by some polynomial $p(x)$.
Thus we take $p(x)$ to be the polynomial with min degree.
If $I = 0$, then I $= < 0 >$. We consider when $p(x)$ has degree 0, then $p(x)$ is a unit, and by previous theorem, if our ideal contains unit, then $I = F[x]$, it is true that all $f(x) \in I$.
Now, take $p(x)$ to be the polynomial that at least have a degree 1. Because our $F[x]$ has division algorithm, we can show that $f(x) = q(x)p(x) + r(x)$ which $r(x)$ has degress < 1 or $r(x) = 0$. Thus our job is to show that $r(x) = 0$ then we are done. Notice that $f(x), p(x) \in I$, thus $q(x)g(x) \in I$, $f(x) - q(x)g(x) = r(x) \in I$. We define $p(x)$ to have the minimum degree and $p(x) >= 1$ so $r(x)$ can only be 0.

Example 3.114. Consider the ideal $I = (x) + (3) := x, 3, x + 3, 2x + 3, ...$
I is a principle ideal in $Q[x]$, which $Q[x]$ is PID, but not a principle ideal in $Z[x]$. Consider $(2x + 3)/(x + 3) \notin Z[x]$ but $\in Q[x]$ which the latter has division algorithm.

Theorem 3.115. In a PID, any nontrivial prime ideal is a maximal ideal.

Proof 3.116. Consider $P = (p) \in D$ that D is a PID, and P is a prime ideal. WTS P is a maximal ideal.

Take ideal $I = (q)$ that $P \subset I \subseteq D$ We want to show that I = D.

Consider that take $p \in P$, $p \subset I = (q)$ thus $p \in (q)$. we can write $p = a \cdot q$ for some $a \in D$. Then notice that P is a prime ideal. Thus if $p = aq \in P$, either have $a \in P$ or $q \in P$. If $q \in P$, then I is not strictly larger than P, contradict our assumption, thus $a \in P = (p)$. We can write $a = bp | b \in D$.

Then: $p = a \cdot q = bp \cdot q \Rightarrow 1 = bq$. Thus we can show that $q \in (q) = I$ is a unit, thus I = D.

Example 3.117. Consider $F[x]$ which F is a field, then $F[x]$ has divison algorithm $\Rightarrow F[x]$ is PID. $\Rightarrow$ In $F[x]$ non prime ideal is maximal ideal.

When $f(x) \neq 0, (f(x))$ is maximal $\Leftrightarrow f(x)$ is irreducible.

Proof 3.118. When $f(x) \neq 0$: 1) WTS that when $(f(x))$ is maximal $\Rightarrow f(x)$ is irreducible.

Assume by contradiction, we can factorize $f(x) = p(x)q(x)$

s.t.deg $p(x)$ and deg $q(x) <$ deg $f(x)$.

Thus since all maximal ideals are prime ideal, $p(x) \in (f(x))$ or $q(x) \in (f(x))$. Then we either $p(x)$ or $q(x)$ will have $f(x)$ as a factor, that then has degree >= degree of $f(x)$.

Thus, it is not possible to have $f(x) = p(x)q(x)$ s.t.deg $p(x)$ and deg $q(x) <$ deg $f(x)$.

2) WTS that when $f(x)$ is irreducible $\Rightarrow (f(x))$ is maximal ideal. We want to show that assume we have ideal N that $(f(x)) \subset N \subset F[x]$. Then by that $F[x]$ is PID, we know N can be written as $N = (g(x))$. Since $(f(x)) \subset N = (g(x)) \Rightarrow$, for $f(x) \in (f(x))$, $f(x) \in (g(x)) \Rightarrow$, $f(x) = q(x)g(x)$, but since we know that $f(x)$ is irreducible, either $q(x)$ or $g(x)$ has degree 0, we know that $g(x)$ has a degree $0 \Rightarrow g(x)$ is a unit. Thus $(g(x)) = N = F[x]$.

Otherwise, $q(x)$ has degree 0 and a unit. $(f(x)) = F[x]$. Still contradiction. Thus $(f(x))$ is maximal if it is irredcible.

Theorem 3.119. A PID is a UFD.

Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x)s(x)$ for$r(x), s(x) \in F[x]$, then either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$.

Proof 3.120. Suppose $p(x)$ divides $r(x)s(x)$, Then $r(x)s(x) \in < p(x) >$, which is maximal. Then $< p(x) >$ is prime ideal. Hence $r(x)s(x) \in < p(x) > \Rightarrow$ implies $r(x) \in < p(x) >$ or $s(x) \in < p(x) >$ giving $p(x)$ divides $r(x)$ and also $s(x)$.

3.9 Section 29: Extension Fields

Note. Consider to find the zero of $f(x) = x^2 + 1 \in \mathbb{R}[x]$ then we extend to complex field.

Def 3.121. A field extension if a pair of fields $F \subseteq E$ so that the operations of F are the restriction of the operations of E, i.e. F is a subfield of E. E is called an extension of F.

Theorem 3.122. Kronecker's theorem: Let F be a field. $f(x) \in F[x]$, $f(x)$ is not constant polynomial. Then there must be an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.

Proof 3.123. We can explicitly construct such an extension E as follows:
$f(x) = p_1(x)p_2(x)p_3(x)...p_n(x)$ each p_i is irreducible, as $f(x) \in F[x]$. $(p_1(x))$is the maximal ideal $\Rightarrow F[x]/(p_1(x)) =:$ E is a field.
(1) E is an extension field of F: construct $\phi : F \to E$, $a \mapsto a + (p_1(x))$ We want to show such map is an injective map, thus it make sense to have $F \subseteq E$. To show such map is injective, we can either directly show $\phi(a) = \phi(b) \Rightarrow a = b$ or show that it is a homomorphism then kernel is empty.
We can directly show that $\phi(a) = \phi(b) \Rightarrow a = b$ by considering
$\phi(a) = a + (p_i(x)) = b + (p_i(x)) = \phi(b) \Rightarrow a - b \in (p_i(x))$
Thus we know that $a - b$ is a multiple of $(p_i(x))$, but the latter has a degree ≥ 1 by construction. $a - b \in F$ either $a - b$ is a constant polynomial of degree 0, or is the zero polynomial. But if it has degree 0, it will contradict the fact that $(p_i(x))$ at least has degree 1 and it can only be the zero polynomial. Thus a = b.
IF we want do the other way: we know that is it a homomophism considering
$Map : F \to F[x] \to F[x]/(p_i(x))$. It is the composition of two homomorphisms, the first is homomorphism by the evaluation map is injective homomorphism, the second is true by the quotient map is a surjective homomorhism. Then now we consider the kernel of such map: $ker(\phi) = \{a \in F \mid a + (p_1(x)) = 0 + (p_1(x))\}$ Following the previous argument, $a \in (p_1(x)$ thus $a = 0$ Thus ϕ is injective.

Proof 3.124. Continue.

(2) $f(x) \in F[x] \subseteq E[x] = F[x]/(f(x))$ **has zero for f(x) in E.** Consider any f(x) = p(x) in the following arguments: Let us set $\alpha = x + (p(x))$ is a solution as well as an element in the quotient field.

Thus consider the evaluation homomorphism $\phi_a : F[x] \to E$. If $p(x) = a_0 + a_1 x + ... + a_n x^n$ where $a_i \in F$ then we have:

$\phi_a(p(x)) = p(\alpha) = a_0 + a_1(x + (p(x))) + ... + a_n(x + (p(x)))^n$ in $E = F[x]/(p(x))$.

We take our x as the representative of the coset $\alpha = x + (p(x))$.

For example $a_1(x + (p(x))) = a_1 x + (p(x))$ therefore:

$p(\alpha) = a_0 + a_1(x + (p(x))) + ... + a_n(x + (p(x)))^n = (a_0 + a_1 x + a_2 x^2 + ..a_n x^n) + (p(x))$ $= p(x) + (p(x)) = (p(x)) = 0$ in E $= F[x]/(p(x))$ Thus we can conclude that $p(\alpha) = 0$ and it is has zero in E.

Example 3.125. Take our $F = \mathbb{R}$. Let $f(x) = x^2 + 1$ which has no zero over $\mathbb{R}$ and is thus is irreducible over R, and $(f(x))$ is a maximal ideal in R.

WTS that if we take: $\mathbb{R}/(f(x))$, then this is a zero for $f(x)$ in quotient field that is:

$\alpha = x + (f(x)) = x + (x^2 + 1)$

Then consider the evalution of $f(x)$ in E at α, consider $I = x^2 + 1$:

$f(\alpha) = a^2 + 1 \in F \Rightarrow (x + I)^2 + 1) \in E$

$= (x + I)^2 + = 1 = (x^2 + I) + 1 = (x^2 + 1) + I = 0 + I$

Example 3.126. $F = \mathbb{Q}$, $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$

Then $E1 := \mathbb{Q}[x]/(x^2 - 2)$, $E2 := \mathbb{Q}[x]/(x^2 - 3)$

Def 3.127. Let $F \subseteq E$ be a field extension. An element $\alpha \in E$ is called algebraic over F, if there is some $f(x) \in F[x]$ s.t. $f(\alpha) = 0$. Otherwise, α is called transcendental over F.

Example 3.128. 1) $\mathbb{R} \subseteq \mathbb{C}$ i is algebraic over R.

2) $\mathbb{Q} \subseteq \mathbb{R}$ $\sqrt{3}$ is algebraic over $\mathbb{Q}$.

3) π, e are transecendental over $\mathbb{Q}$ but they are algebraic over $\mathbb{R}$ like $(x - \pi \in \mathbb{R}[x]$.

Theorem 3.129. Let $F \subseteq E$ be a field extension, $\alpha \in E$ is algebraic over F. Then $ker(eV_\alpha) = \{f(x) \in F[x] \mid eV_\alpha(f) = 0\}$ (Note that this counts for **ALL** $f(x)$ that take α as a zero) is a principal ideal of F[x], which is generated by some irreducible polynomial $p(x) \in F[x]$ with degree ≥ 1. This degree is independent of the choices of generators of $ker(eV_\alpha)$ and is defined as the degree of α over F, written as $deg(\alpha; F)$

Proof 3.130. There is a few things to note.

1) Consider the evaluation map: $eV_\alpha : F[x] \to E$ this is a ring homomorphism. And thus kernel is an ideal lives in $F[x]$. Since it is a PID, we know the kernal is a principle ideal.

2) It is generated by irreducible polynomial $p(x)$ with degree ≥ 1 because when we show all ideals are principle in proving it is PID, we take our $p(x)$ to be the ideal with min degree. And if $p(x)$ is reducible, then there exists other polynimal with degree less than deg $p(x)$. Here just consider $ker(eV_\alpha) = I$, and all polynomials $f(\alpha) = 0 \in I$, thus $f(x) = p(x)q(x) = (p(x))$ s.t. it is irreducible.

3) Degree is independent of the choice of generator because of the same reason, as it is the minimal degree.

4) An example of this would be consider $\alpha = \sqrt{1+\sqrt{3}}$ that is algebraic over $\mathbb{Q}$ with $f(x) = x^4 - 2x^3 - 2 \in \mathbb{Q}[x]$, $f(\alpha) = 0$ in E. And our polynomial has degree 4, so $p(x) = x^4 - 2x^3 - 2$ but there are other polynomials can be in $ker(eV_\alpha)$ such as $2(x^4 - 2x^3 - 2)$ or anything $(x^4 - 2x^3 - 2)$.

Example 3.131. Consider:
$(x^2 - 2) \in \mathbb{Q}[x]$ is irreducible. $(x^2 - 2) = ker(eV_{\sqrt{2})}$, deg$(\sqrt{2}, \mathbb{Q})$ =2. deg$(\sqrt{2}, \mathbb{R})$ =1

Let $F \subseteq E$ be a field extension. $\alpha \in E$:

Two cases:

(1) α is transecendental over F.

(1) α is algebraic over F.

Consider the ring homomoprhism: $eV_\alpha : F[x] \to E$.

Case (1) $\Leftrightarrow$ eV_α is injective. In this case, eV_α

Def 3.132. Ab extension field E of a field F is a simle extension of F if E = F(α) for some $\alpha \in E$.

Theorem 3.133. Let E be a simple extension F(α) if a field F, and let α be algebraic over F. Let the degree irr(α,F) be $n \geq 1$, then every element β of E = F(α) can be uniquely expressed in the form:
$\beta = b_0 + b_1\alpha + ... + b_{n-1}a^{n-1}$ where b_i are in F.

Proof 3.134. For the usual evaluation homomorphism ϕ_α, every element of $F(\alpha) = \phi_\alpha[F[x]]$ is of the form $\phi_\alpha(f(x)) = f(\alpha)$, a form polynomial in α with coefficients in F.
Let irr(α, F) = p(x) = $x^n + a_{n-1}x^{n-1} + ... + a_0$
Then $p(\alpha) = 0$, so
$\alpha^n = -a_{n-1}\alpha^{n-1} - ... - a_0$. This equation in $F(\alpha)$ can be used to express every monomial ^{m} for $m \geq n$ in terms of powers of α that are less than n. For example, $\alpha^{n+1} = \alpha\alpha^n = -a_{n-1}\alpha^n - a_{n-2}\alpha^{n-1} - ... - a_0\alpha = -a_{n-1}(-a_{n-1}\alpha^{n-1} - ... - a_0) - a_{n-2}\alpha^{n-1} - ... - a_0\alpha$
Unique Representation: Now, consider any element β in $F(\alpha)$. Since β is in $F(\alpha)$, it can be written as a polynomial in α with coefficients in F. Let's say

$$\beta = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_m\alpha^m.$$

If $m < n$, we are already in the desired form. However, if $m \geq n$, we use the relation

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_0$$

to express α^m (for $m \geq n$) in terms of powers of α that are less than n.
By repeatedly applying this process, any power of α greater than or equal to n is reduced to a linear combination of $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. Hence, every element β in $E = F(\alpha)$ can be uniquely expressed as

$$\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1},$$

where each b_i is in F.

Example 3.135. An example of this is consider $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible over $\mathbb{Z}_2$. By this theorem, we can say that $\mathbb{Z}_2(\alpha)$ has an elements $0 + 0\alpha$,$0 + 1\alpha$, $1 + 0\alpha$, $1 + 1\alpha$.

Also WTS the extension $\mathbb{R}[x]/ < x^2+1 >\simeq \mathbb{C}$ Consider $\mathbb{R}(\alpha) = \mathbb{R}[x]/ < x^2+1 >$ by this theorem, we can know that all elements in $\mathbb{R}(\alpha)$ are in the form of $a + b\alpha$. And $\alpha = x+ < x^2 + 1 >$ by construction, $\alpha^2 + 1 = 0$, we see that α plays the role of $i \in \mathbb{C}$ and that $(a + b\alpha) = (a + bi) \in \mathbb{C}$