Key
Definition
Result

Algebra II - Groups & Rings Summary

Part 1 - Groups

Chapter 1 - Groups

① **Def (Group):** Group $(G,*)$ is a set together w/ a binary operation $*: G\times G \longrightarrow G$ such that
① $g,h \in G \Rightarrow g*h \in G$ [closure]
② $(g*h)*k = g*(h*k) \ \forall g,h,k \in G$ [associativity]
③ $\exists e \in G$ s.t. $g*e = e*g = g \ \forall g \in G$ [identity]
④ $\forall g \in G \ \exists g^{-1}$ s.t. $g*g^{-1} = g^{-1}*g = e$ [inverse]
If G is abelian, then we also require
⑤ $g*h = h*g \ \forall g,h \in G$ [commutivity]

② **Elementary properties of a group G:**
- cancellation law Pf: $gh = gk = \cdots = h = k$
- unique identity & inverse Pf: similar
- $(gh)^{-1} = h^{-1}g^{-1}$ Proof: just consider $(h^{-1}g^{-1})(gh)$ & associativity

③ **Def (the order of a Group):** $|G|$ is # elements in G.

④ **Def (order of an element):** $g \in G$. $|g|$ is the least integer $n>0$ s.t. $g^n = 1$.
If n doesn't exist, $|g| = \infty$.

⑤ **Def (Cyclic Group):** G cyclic if $\exists g \in G$ s.t. $\forall h \in G \ \exists k \in \mathbb{Z}$ s.t. $g^k = h$.
g is a generator of G.

⑥ **Def (Isomorphism):** $\phi: G \longrightarrow H$ is a bijection from group G to H such that $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \ \forall g_1, g_2 \in G$. $G \cong H$ if a ϕ exists.
Note: $\phi(1_G) = 1_H$ and $\phi(g^{-1}) = \phi(g)^{-1} \ \forall g \in G$

useful to show two groups not isomorphic

⑦ **Prop (order preserved under isomorphism):** $\phi: G \longrightarrow H$ isomorphism, then $|g| = |\phi(g)| \ \forall g \in G$ (H has 4 elements order 2, then so should G)
finite: Proof: If $|g| = n$ (finite), $\phi(g)^n = \phi(g^n) = \phi(1_G) = 1_H \Rightarrow |\phi(g)| \leq n$ could be multiple
Let $m = |\phi(g)|$, then $\phi(g^m) = \phi(g)^m = 1_H = \phi(1_G) \Rightarrow g^m = 1_G \Rightarrow |g| \leq m$
Hence $|\phi(g)| \leq |g| \leq |\phi(g)| \Rightarrow |\phi(g)| = |g|$
infinite: If $|g| = \infty$, g^k distinct for $k \in \mathbb{Z}$, ϕ bijection so $\phi(g^k) = \phi(g)^k$ distinct $\forall k \in \mathbb{Z}$ so $|h| = \infty$

⑧ **Def (Symmetric Group):** X a set, $Sym(X) = \{$permutations on $X\} = \{$bijections $X \longrightarrow X\}$
a cycle $(a_1, \ldots, a_r)$ is a permutation $\phi \in Sym(X)$ s.t. $\phi(a_i) = a_{i+1}$, $\phi(a_r) = a_1$, $\phi(b) = b$ if $b \in X \setminus \{a_1, \ldots, a_r\}$.
Note: If $|X| = |Y|$, then $Sym(X) \cong Sym(Y)$

⑨ **Def (Dihedral Group):** $D_n = \{$isometries of an n-sided polygon in the plane$\}$
let a be a rotation by $\frac{2\pi}{n}$, b a reflection, then we see that
$G = \{a^k \mid 0 \leq k < n\} \cup \{a^k b \mid 0 \leq k < n\}$
Note: $ba = a^{n-1}b = a^{-1}b$, $ba^k = a^{-k}b$, $a^n = 1$, $b^2 = 1$

Chapter 2 - Subgroups

⑩ **Def (Subgroup):** $H \subset G$ is a subgroup if it forms a group under the same operation as G. Write $H \leq G$. Note: $1_H = 1_G$

⑪ **Lemma (subgroup criterion):** $H \leq G$ iff
(i) $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$ [closure]
(ii) $h \in H \Longrightarrow h^{-1} \in H$ [inverse]
Note: $\{1\}$ is the trivial subgroup, G is also a subgroup.
Proper subgroup - excludes G, non-trivial subgroup - excludes $\{1\}$

⑫ **Def (transpositions):** If $G = \mathrm{Sym}(X)$, then every permutation σ can be written as a product of disjoint cycles. A transposition is a cycle of length 2. So any permutation can be written as a product of transpositions. A permutation is even & odd if product of even or odd # of transpositions. [can't be both even & odd]
$\Rightarrow A_n = \{\sigma \in \mathrm{Sym}(n) : \sigma \text{ even}\}$

⑬ **Lemma (intersection of subgroups):** G group. If $H \leq G$, $K \leq G \Rightarrow H \cap K \leq G$
Let $H \leq G$ assumed here... [H subgroup of G]

⑭ **Def (cosets):** Let $g \in G$, left coset $gH = \{gh : h \in H\}$, same for right coset.

⑮ **Prop (technical coset criterion):** Following equivalent for $g, k \in G$
(i) $k \in gH$ (ii) $gH = kH$ (iii) $g^{-1}k \in G$ → so cosets partition G up

⑯ **Prop (cosets equal or disjoint):** Two left cosets $g_1 H$, $g_2 H$ equal or disjoint.
Pf: If $g_1 H \cap g_2 H \neq \emptyset \Rightarrow \exists k$ s.t. $k \in g_1 H \cap g_2 H \Rightarrow g_1 H = kH = g_2 H$

⑰ **Prop (cosets have same size):** If H finite, then all left cosets have size $|H|$.
Pf: As $gh_1 = gh_2 \Rightarrow h_1 = h_2$, then $\phi : H \longrightarrow gH$ w/ $\phi(h) = gh$ is a bijection so result.

⑱ **Def (Index of H in G):** # distinct left cosets of H in G is $[G:H]$.

⑲ **Thm (Lagrange's thm):** G a finite group, H a subgroup. Then $|H| \mid |G|$ or equivalently, $|G| = |H| \cdot [G:H]$
"order of G divides order of subgroup"

⑳ **Prop (order of element divides order of group):** G finite, then $\forall g \in G$ $|g|$ divides $|G|$.
Pf: Let $|g| = n$, $\{g^k \mid k \in \mathbb{Z}\}$ is a subgroup of H. g^k all distinct so $|H| = n$, hence $|G| = n \cdot [G:H]$ so $n \mid |G|$ by Lagrange.

㉑ **Def (normal subgroup):** We say $H \lhd G$ or $H \trianglelefteq G$ if left & right cosets are equal $\forall g \in G$, $gH = Hg$ $\forall g \in G$.

㉒ **Prop (index 2 ⇒ H normal):** $H \leq G$ with $[G:H] = 2 \Rightarrow H$ normal. $H \trianglelefteq G$.
Pf: If $[G:H] = 2$, only two distinct cosets. So as cosets partition G, they are H and $G \setminus H$. Same for right cosets so for $g \in G$, if $g \in H \Rightarrow gH = Hg = H$ and if $g \notin H \Rightarrow gH = Hg = G \setminus H$. Either way $Hg = gH \Rightarrow H$ normal subgroup.

(23) **Prop (test for $H \leq G$ normal):** H normal in $G \iff ghg^{-1} \in H \;\; \forall g \in G, h \in H$. ← idea is commutativity

Chapter 3 – Classification of Groups

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

(*)

$\boxed{\text{Do proofs here} \because \text{not results based!}}$

(24) **Def (Direct Product):** $G \times H = \{(g,h) : g \in G, h \in H\}$ w/ $(g_1,h_1)(g_2,h_2) = \dots$

(25) **Prop (Group of order 4 classification):** $G \cong C_4$ or $G \cong C_2 \times C_2$ ← Klein 4 group

Pf: let $G = \{1, a, b, c\}$. By Lagrange, $|g| = \{2, 4\}$ [can't be 1 as that element is unique]. If $|a| = 4$, then $G = \{1, a, a^2, a^3\}$ so cyclic. Otherwise $|a| = |b| = |c| = 2$. Consider ab. Cases:
- $ab = 1 \Rightarrow b = a^{-1} = a$, but $|a| = 2$ $\times$.
- $ab = b \Rightarrow a = 1$ $\times$.
- $ab = a \Rightarrow b = 1$ $\times$.

] so $ab = c$. Similarly $ba = c \Rightarrow a = bc$ & write multiplication table (*)

Hence classification.

(26) **Prop (Group has prime order then cyclic):** $|G| = p$ prime. Then $G \cong C_p$.

Pf: let $g \neq 1 \in G$, $|g| \mid p \Rightarrow |g| = p \Rightarrow 1, g, g^2, \dots, g^{p-1}$ distinct so cyclic.

(27) **Lemma (all of order two then abelian):** G group s.t. $g^2 = 1 \; \forall g \in G \Rightarrow G$ abelian.

Pf: $g^2 = 1$ $h^2 = 1$ $gh \in G \Rightarrow (gh)^2 = 1 \Rightarrow ghgh = gghh \Rightarrow hg = hg$.

(28) **Lemma (all order two forms subgroup):** G group s.t. $g^2 = 1 \; \forall g \in G$, then a, b distinct non identity, then $\{1, a, b, ab\}$ subgroup of G of order 4.

Pf: $ab \neq b$, $ab \neq a$, $ab \neq (1 = a^2) \Rightarrow a = b$ $\times$ $\Rightarrow |\{1, a, b, ab\}| = 4$

Show subgroup: (i) closure: know $1 = a^2 = b^2$, $ab = 1$ so e.g. $b(ab) = bab = b$

(ii) inverse: $g^2 = 1 \Rightarrow g = g^{-1} \; \forall g \in G$ so closed.

(29) **Prop (Order 6 classification):** If $|G| = 6$, then $G \cong C_6$ or $G \cong D_3$ $(\cong S_3)$

Pf: By Lagrange, $|g| = \{1, 2, 3, 6\}$. If $|g| = 6 \Rightarrow G \cong C_6$ so assume no $|g| = 6$.

① If all elements order 1 or 2, then G has order 4 subgroup, contradicting Lagrange. $\Rightarrow$ there must be an order 3 element.

prop (23) partition in two.

② If $|a| = 3$, then $N = \{1, a, a^2\}$ has index 2 in $G \Rightarrow$ normal subgroup.

Pick $b \in G \setminus N$, then $G = \{1, a, a^2, b, ab, a^2b\}$

③ What can b^2 be?
- $b^2 = b \Rightarrow b = 1$ $\times$.
- $b^2 = ab \Rightarrow b = a$ $\times$.
- $b^2 = a^2 b \Rightarrow b = a^2 \in N$ $\times$.
- $b^2 = a \Rightarrow b^3 = ab$, $b^4 = a\overset{a}{\overline{b^2}} = a^2$, $b^5 = a^2 b$ all not $1 \Rightarrow |b| = 6$ $\times$.
- $b^2 = a^2 \Rightarrow \dots \Rightarrow |b| = 6$ $\times$.

$\Longrightarrow b^2 = 1$ [only choice to avoid contradiction]

④ What can bab^{-1} be? [N is normal so $bab^{-1} \in N$]
- $bab^{-1} = 1 \Rightarrow a = 1$ $\times$.
- $bab^{-1} = a \Rightarrow ba = ab \Rightarrow (ab)^2 = a^2b^2 = a^2$, $(ab)^3 = b$, $(ab)^4 = a$, $(ab)^5 = a^2 b$, $(ab)^6 = 1$ $\times$

$\Rightarrow bab^{-1} = a^2 \Rightarrow ba = a^2 b \Rightarrow$ complete multiplication table & $G \cong D_3$

(30) **Def (generators / words):** $\{g_1, \dots, g_r\} \subset G$ generate G if every element in G can be obtained by repeated multiplication by g_i and inverses. [expression is a word in the generators & their inverses.

If you write down enough relations between words can classify groups upto isomorphism.

(31) Prop (Generators for D_n): $|G| = 2n$, generated by a, b satisfying $a^n = 1$, $b^2 = 1$, $ba = a^{-1}b$, then $G \cong D_n$

Pf: mess around w/ relations.

(32) Prop (Generators for $C_n \times C_m$): $|G| = mn$ generated by a, b satisfying $a^m = 1$, $b^n = 1$, $ab = ba$. Then $G \cong C_n \times C_m$

quaternion group

(33) Prop (Generators for Q_8): let G be $|G| = 8$, generated by a, b satisfying $a^4 = 1$, $b^2 = a^2$, $ba = a^{-1}b$. Then $G \cong Q_8$

way more complicated than abelian group case where nice thm for it

(34) Prop (classifying order 8): $|G| = 8$, then G isomorphic to one of C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_4, Q_8

Pf: Similar to order 6 case but 5 isomorphism classes, not two.

Chapter 4 - Homomorphisms & Quotient Groups

n	Groups of order n
1	$\{0\}$
2	C_2
3	C_3
4	C_4, $C_2 \times C_2$
5	C_5
6	C_6, $D_3 \cong S_3$
7	C_7
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_4, Q_8

(35) Lemma (coset element multiplication): Let $N \trianglelefteq G$, $g, h \in G$, Then if $p \in gN$, $q \in hN$, then $pq \in ghN$

Pf: $gn_1 \in gN$, $hn_2 \in hN$. Know $gN = Ng$ so $n_1 h = hn_3$ for $n_3 \in N$, so $(gn_1)(hn_2) = g(n_1 h)n_2 = g(hn_3)n_2 \in ghN$

(36) Lemma (normal coset multiplication): $N \trianglelefteq G$, gN, hN cosets, then $(gN)(hN) = (gh)N$.

Quotient Group / Factor Group of G by N.

(37) Thm (G/N forms a group): Let N be a normal subgroup of G. Then G/N (set of left cosets of N) forms a group under multiplication of sets.

Pf: ① Saw that $(gN)(hN) = ghN$ so have closure.

② associativity follows from associativity of G.

③ $(1N)(gN) = 1gN = gN = (gN)(1N)$ $\forall g \in G$ so $1N$ is identity.

④ $(g^{-1}N)(gN) = (gg^{-1})N = 1N$, $g^{-1}N$ is the inverse to gN for each coset ∎

left cosets = size of quotient group

Note: G finite $\Rightarrow$ $|G/N| = [G:N] = |G|/|N|$. so if N exists can split up G → G/N, → N

(38) Def (Homomorphisms): Let G, H be groups. A homomorphism ϕ from G to H is a map $\phi: G \to H$ s.t. $\phi(gh) = \phi(g)\phi(h)$ $\forall g, h \in G$

- injective homomorphism (monomorphism) has $\phi(g) = \phi(h) \Rightarrow g = h$
- surjective " (epimorphism) has $Im(\phi) = H$
- Isomorphism is a bijective homomorphism.

Note: $\phi(1_G) = 1_H$ & $\phi(g^{-1}) = \phi(g)^{-1}$ $\forall g \in G$.

(39) Def (kernel of a homomorphism): $\ker(\phi) = \{ g \in G : \phi(g) = 1_H \}$

(40) Prop (ϕ injective iff $\ker(\phi) = \{1_G\}$): $\phi: G \to H$ a homomorphism.

Pf: '$\Rightarrow$' $1_G \in \ker(\phi)$. As ϕ injective $\Rightarrow$ $\ker(\phi) = \{1_G\}$.

'$\Leftarrow$' Suppose $\ker(\phi) = \{1_G\}$. Pick $g_1, g_2 \in G$ w/ $\phi(g_1) = \phi(g_2)$ Then $1_H = \phi(g_1)^{-1}\phi(g_2) = \phi(g_1^{-1}g_2)$ $\Rightarrow$ $g_1^{-1}g_2 = 1_G$ $\Rightarrow$ $g_1 = g_2$ ∎

(41) Thm ($\ker(\phi)$ is normal & natural/canonical homomorphism def):

(i) Let $\phi: G \to H$ be a homomorphism. Then $\ker(\phi)$ is normal in G.

(ii) Let $N \trianglelefteq G$, then $\pi: G \to G/N$ defined by $\pi(g) = gN$ is a homomorphism with kernel N.

Pf: (i) $1_G \in \ker(\phi)$ so non-empty. Pick $g_1, g_2 \in \ker(\phi)$. Note that
$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = 1_H 1_H = 1_H \Rightarrow g_1 g_2 \in \ker(\phi)$ [closure]
$\phi(g_1^{-1}) = \phi(g_1)^{-1} = 1_H^{-1} = 1_H \Rightarrow g_1^{-1} \in \ker(\phi)$ [inverse]
If $g \in G$, $k \in \ker(\phi)$, then $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = 1_H$
so $gkg^{-1} \in \ker(\phi)$ so $\ker(\phi)$ normal.

(ii) For $a, b \in G$, $\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b)$ so $\pi: G \to G/N$ is a homomorphism. Take $xN \in G/N$, then $xN = \pi(x)$ so π surjective
$\pi(g) = 1_{G/N} \iff gN = 1_G N \iff g \in N$ so $\ker(\pi) = N$

(42) Prop (image of a homomorphism is a subgroup): $\phi: G \to H$ homomorphism, then $\mathrm{im}(\phi)$ is a subgroup.

(43) Thm (First Isomorphism Theorem): Let $\phi: G \longrightarrow H$ be a homomorphism, then $G/\ker(\phi) \cong \mathrm{im}(\phi)$. Precisely, $\exists$ isomorphism $\bar{\phi}: G/\ker(\phi) \longrightarrow \mathrm{im}(\phi)$ defined by $\bar{\phi}(gK) = \phi(g)$ $\forall g \in G$ [$K = \ker(\phi)$]

Pf: Hard part is checking the map is well defined. Do we really have a map from $\bar{\phi}: G/K \longrightarrow \mathrm{im}(\phi)$. We can have $gK = hK$ for $g \neq h$ and need $\phi(g) = \phi(h)$

(44) Thm (Second Isomorphism Theorem): G group, H a subgroup, K normal subgp then
(i) $HK = KH$ is a subgroup of G [$AB = \{ab \mid a \in A, b \in B\}$]
(ii) $H \cap K$ is a normal subgroup of H
(iii) $H/(H \cap K) \cong HK/K$

(45) Thm (Third Isomorphism Theorem): Let $K \subseteq H \subseteq G$ where K, H normal subgroups of G:
(i) K is a normal subgroup of H
(ii) H/K is a normal subgroup of G/K
(iii) $(G/K)/(H/K) \cong G/H$

Chapter 5 - Group Actions

$GL(n, \mathbb{R})$ 'acts' on $\mathbb{R}^n$ by $g \cdot x = gx$ (multiply matrix by a vector)

(46) Def (The action of a group on a set): Let G be a group, X a set. An action of G on X is a map $\cdot: G \times X \longrightarrow X$ such that
- A1: $1_G \cdot x = x$ $\forall x \in X$
- A2: $(gh)\cdot x = g\cdot(h \cdot x)$ $\forall g, h \in G$, $x \in X$

useful to set up a homomorphism to use in 1st iso thm

(47) Prop (if G acts on X, there's a homomorphism between G and $\mathrm{Sym}(X)$): Let $\cdot$ be an action of the group G on the set X. For $g \in G$, define $\phi(g): X \longrightarrow X$ by $\phi(g)(x) = g \cdot x$. Then $\phi(g) \in \mathrm{Sym}(X)$ and $\phi: G \longrightarrow \mathrm{Sym}(X)$ is a homomorphism.

(48) Def (kernel of an action): The kernel of an action $\cdot$ of G on X is the $K = \ker(\phi)$ where $\phi: G \longrightarrow \mathrm{Sym}(X)$ from (47)

$$K = \{g \in G \mid g \cdot x = x \quad \forall x \in X\}$$

$\cdot: G \times X \longrightarrow X$

An action is faithful if $K = \{1\}$

(49) Thm (Every group is isomorphic to a permutation group): $G \cong H \subset Sym(X)$

Pf: For a faithful action, $\phi: G \longrightarrow Sym(X)$ is a homomorphism and $K = \{1\}$, so by 1st isomorphism thm, $G \cong G/K \cong im(\phi) \leq Sym(X)$

Because $\phi: G \longrightarrow Sym(X)$ so $im(\phi) \leq Sym(X)$ and $K = 1$ so $G \cong G/K$

"fix x & cycle through G"

(50) Def (Orbit of G on X): let $\cdot$ be an action of G group on X set. Then

$$G \cdot x = Orb_G(x) = \{ y \in X : \exists g \in G \text{ s.t. } g \cdot x = y \} = \{ g \cdot x : g \in G \} \subset X$$

Note: Define relation $x \sim y \iff \exists g \in G$ s.t. $g \cdot x = y$, then the equivalence classes of $\sim$ are the orbits of G on X

An action is transitive if it has only a single orbit.

(51) Def (Stabiliser of x in G): Let G act on X, $x \in X$, then the stabiliser of x in G is

$$G_x = Stab_G(x) = \{ g \in G : g \cdot x = x \} \subset G$$

subset of G that leaves x fixed.

(52) Prop (Stabiliser is a subgroup): Let G act on X, $x \in X$, then

(i) $Stab_G(x)$ subgroup of G

(ii) $\bigcap_{x \in X} Stab_G(x)$ is the kernel of action G on X.

Pf: ez

(53) Thm (Orbit Stabiliser Theorem): Let G be a finite group acting on X. Let $x \in X$. Then $|G| = |Orb_G(x)| \times |Stab_G(x)|$

Proof: let $y \in Orb_G(x)$, then $\exists g \in G$ s.t. $g \cdot x = y$. Set $H = Stab_G(x)$

For $g' \in G$

$$g' \cdot x = y \iff g' \cdot x = g \cdot x \iff g^{-1} g' \cdot x = x \iff g^{-1} g' \in H \iff g' \in gH$$

Then $g' \in G$ s.t. $g' \cdot x = y$ are elements in the coset of H, but we know $|H| = |gH|$ so $\forall y \in Orb_G(x)$, there are $|H|$ elements $g' \in G$ with $g' \cdot x = y$ so total # $y \in Orb_G(x)$ is $|G|/|H|$, hence result.

(54) Def (Conjugation / Centraliser): Action of G on $X = G$, $\overbrace{g \cdot x = gxg^{-1}}^{\text{conjugation}}$, $x, g \in G$

Ⓐ orbits (Conjugacy classes of G). Ⓑ Stabiliser for conjugation ? Centraliser

orbit of $g \in G$

$$Cl_G(g) = \{ xgx^{-1} \mid x \in G \}$$

Elements of same conjugacy class are 'conjugate'. $g, h \in G$ conjugate iff $\exists x \in G$ s.t. $h = xgx^{-1}$

[conjugate elements have same order]

centraliser of g in G

$$C_G(g) = \{ x \in G \mid xg = gx \}$$

The $x \in G$ s.t. $x \cdot g = g \iff xgx^{-1} = g$

[the x that commute with g]

Ⓒ kernel is the center of G, $Z(G) = \{ x \in G : xg = gx \ \forall g \in G \}$

the x that commute w/ all G

Note: orbit-stabiliser thm gives $|Cl(g)| = |G| / |C_G(g)|$

(55) Conjugacy classes in Symmetric Groups

- Given g permutation in cyclic notation, conjugate fgf^{-1} of g is $X \ni x \mapsto f(x)$
- cycle type $2^{r_2} 3^{r_3} \ldots$ for a permutation if it has r_i cycles of length i for $i \geq 2$.
- Two permutations are conjugate iff they have the same cycle type.

E.g. S_3 has 3 cycle types $[1, 2^1, 3^1]$, S^4 has 5 $[1, 2^1, 2^2, 3^1, 4^1]$

(56) Conjugacy classes in Alternating Groups: let $G = S_n$, $H = A_n$. Then we have

$Cl_H(h) = Cl_G(h)$ or $|Cl_H(h)| = \frac{1}{2} |Cl_G(h)|$

Pf: orbit stab: $|Cl_G(h)| \cdot |C_G(h)| = |S_n| = 2|A_n| = 2|Cl_H(h)| \cdot |C_H(h)|$ & lagrange.

Example: calculate conjugacy classes in A_5...

obviously left & right cosets equal here... ???

S7 Results relating to simple groups:

- G is simple if its only normal subgroups are G and $\{1\}$.
  e.g. cyclic groups of prime order are simple. [subgroups are only order 1 or p]
- A simple abelian group is cyclic of prime order.
  Pf: guess g to generate w/ different cases.
- $H \leq G$ normal in $G \iff H$ is a union of conjugacy classes of G
  Pf: $H \trianglelefteq G \iff ghg^{-1} \in H \quad \forall g \in G, h \in H$. But this is exactly
  $H \trianglelefteq G \iff h \in H \Rightarrow Cl_G(h) \in H$ so result.
- Group A_5 is simple
  Pf: use above & info about conjugacy classes.
- (Converse to lagrange) $|H| \mid |G|$ but does G have subgroups of all orders that $\div |G|$?
  No: A_4 has no subgroup of order 6. $|A_4| = \frac{4!}{2} = 12$
  Pf: Order 6 subgroup has index 2 so normal $\Rightarrow$ union of conjugacy classes.
  cyclic or dihedral so has an order 2 element. List & they form an order 4 subgroup contradicting lagrange.

S8 Sylow's Theorem

n is largest power of prime p that divides $|G|$ so m is not divisible by p.

- Let G be finite grp $|G| = p^n \cdot m$. A subgroup of G of order p^n is a sylow p-subgroup.
- (Thm) Let G be a finite group, p prime, $|G| = p^n m$, $p \nmid m$. Then
  (a) G has a sylow p-subgroup. Any subgroup of G of order p^a, $1 \leq a \leq n$ is contained in a sylow p-subgroup.
  (b) Any two Sylow p-subgroups are conjugate in G.
  (c) The number r of sylow p-subgroups of G satisfies $r \equiv 1 \pmod p$ & $r \mid m$.

Note: Let $Syl_p(G) = \{H \leq G \mid |H| = p^n\}$ is the set of sylow p-subgroups of G.
can show ① If $P \in Syl_p(G)$ & $g \in G$, then $gPg^{-1} \in Syl_p(G)$ [conjugation]
② $|Syl_p(G)|$ divides $m = |G|/|P|$

- If there's only one sylow p-subgroup, then it's a normal subgroup of G
  Pf: Sppse $|Syl_p(G)| = 1$ and P is the unique p-subgroup. Then $\forall g \in G$
  $gPg^{-1} \in Syl_p(G) \Rightarrow gPg^{-1} = P \Rightarrow P \trianglelefteq G$.
- Example: There's no simple groups of order 24.
  Pf: Assume contrary, let G be a simple group of order $2^3 \cdot 3$
  ① Take $p = 2$, then G has sylow 2-subgroups. $r_2 = |Syl_2(G)|$
  Then $r_2 \equiv 1 \pmod 2$, r_2 divides $\frac{24}{8} = 3 \Rightarrow r_2 = \{1, 3\}$
  Ⓐ If $r_2 = 1$, then unique subgroup so normal, contradiction to G simple.
  Ⓑ If $r_2 = 3$, G acts on $X = Syl_2(G)$ by conjugation. so $\exists$ non-trivial homomorphism $\phi: G \longrightarrow Sym(X)$. $|X| = 3$ so $Sym(X) \cong S_3$ so
  $\phi: G \longrightarrow S_3$. $\{1\} \neq im(\phi) \leq S_3$ so $1 < im(\phi) \leq 6$.
  First isomorphism thm: $im(\phi) \cong G/ker(\phi) \Rightarrow |ker(\phi)| = \frac{24}{6} = 4$
  so $4 \leq ker(\phi) < 24$ so $ker(\phi)$ proper non-trivial normal subgroup of G contradicting G simple.

Part 2 - Rings

Chapter 6 - Rings & subrings

(59) **Def (Ring):** A **ring** is a set R together w/ two binary operations $+, \cdot : R \times R \to R$ satisfying

note! No multiplicative inverse...

- R1 - $(R,+)$ is an abelian group (additive group)
- R2 - $(ab)c = a(bc)$ $\forall a,b,c \in R$ (associative multiplication)
- R3 - $(a+b)c = ac+bc$, $a(b+c) = ab+ac$ $\forall a,b,c \in R$ (distributivity)
- R4 - $\exists 1 = 1_R \in R$ s.t. $1a = a1 = a$ $\forall a \in R$ (multiplicative identity)
- [R5 - $ab = ba$ $\forall a,b \in R$] (commutativity)

for a commutative ring

(60) **Def (Subring):** $S \subset R$ is a **subring** if it forms a ring under same operations as R w/ same identity element.

- S is a subring of R iff
  - (a) S a subgroup of $(R,+)$ [addition subgroup]
  - (b) $a_1, a_2 \in S \Rightarrow a_1 a_2 \in S$ [multiplicative closure]
  - (c) $1_R \in S$ [multiplicative identity]

Best way to prove something is a ring is to show it is a subring of a known ring...

Note: intersections of subrings are subrings.

(61) **Def (Ring isomorphism):** $\phi : R \longrightarrow S$ between two rings R & S is an **isomorphism** if
- (i) ϕ bijection
- (ii) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ $\forall r_1, r_2 \in R$
- (iii) $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$ $\forall r_1, r_2 \in R$

Here R and S are **isomorphic**. write $R \cong S$.

Note: $\phi(0_R) = 0_S$, $\phi(1_R) = 1_S$.

note: $a \cdot 0 = 0 \cdot a = 0$
$(-1) \cdot a = a \cdot (-1) = -a$
multiplicative identity unique
If $1 = 0 \Rightarrow R = \{0\}$

(62) **Def (Direct product):** If R & S, two rings, then $R \times S = \{(r,s) : r \in R, s \in S\}$

ordered pair w/ obvious pairwise $+$ & $\cdot$

(63) **Thm (Sun Tzu / Chinese Remainder):** Rings $\mathbb{Z}_m \times \mathbb{Z}_n$ and $\mathbb{Z}_{nm}$ are isomorphic iff n & m coprime. ($\gcd(n,m) = 1$).

Pf: '$\Leftarrow$' Let $(x)_m$ be residue of x mod m. Set $\phi : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ by $\phi(x) = ((x)_m, (x)_n)$ & show isomorphism.

$\Rightarrow$ If $n = p_1^{a_1} \cdots p_k^{a_k}$ is a decomp of n into distinct primes, then
$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$$

(64) **Def (Integral domains / Fields):**
- **zero divisors:** $a \in R \setminus \{0\}$ is a zero divisor if $\exists b \in R \setminus \{0\}$ s.t. $ab = 0$ or $ba = 0$.
- **units:** $a \in R \setminus \{0\}$ is a unit if $\exists b \in R \setminus \{0\}$ s.t. $ab = ba = 1$

  two-sided inverse
- A ring R is an **integral domain / domain** if
  - (a) R is commutative
  - (b) R non-zero
  - (c) R has no zero divisors. [If $ab = 0 \Rightarrow a = 0$ or $b = 0$]

  {have cancelation law here: $ab = ac \Rightarrow a(b-c) = 0 \Rightarrow b = c$, $a \neq 0$}
- Units of R form a group R^* under multiplication.
- A **division ring** is a ring R s.t. $R \setminus \{0\}$ forms a group w/ multiplication
- A **field** is a commutative division ring.

Note: every field is an integral domain. [no non-zero divisors]
Suppose we have a non-zero divisor. Then $ab = 0$ with $a, b \neq 0$
But field so have a^{-1} & b^{-1}. Then $b = 0$ $\times$.

- R a ring, the **characteristic** is smallest $n \in \mathbb{N}$ s.t. $nx = 0$ $\forall x \in R$. If no n, char $= 0$

(65) **Polynomials** $3x_1^3x_2 - \frac{2}{3}x_1x_2^2 \in \mathbb{Q}[x_1, x_2]$

- R integral domain $\Rightarrow R[x]$ is
- R integral domain $\Rightarrow$ units of R & $R[x]$ match.
- Polynomial division w/ remainder: $f = qg + r$ w/ $\deg(r) < \deg(g)$ or $r = 0$
- Remainder Thm: $f = f(x) \in F[x]$, $a \in F$, $f(a) = 0 \iff (x-a) \mid f(x)$
- Polynomial of degree d has at most d roots.
- F a field, then any finite subgroup of F^* [multiplicative] is cyclic.

v useful to prove divisibility $\Downarrow$ get $\times$: $f(r) \neq 0$

Pf: contradiction, assume G finite subgp of F^* not cyclic. By abelian gp classification $G \cong C_{n_1} \times \dots \times C_{n_m}$ w/ $n_1 \mid n_2 \mid \dots \mid n_m$ $N = |G| = n_1 n_2 \dots n_m$. $m > 1$ as G not cyclic.
let $n = n_m$, then pick $(x_1, \dots, x_m) \in C_1 \times \dots \times C_{n_m}$. Then

$$(x_1, \dots, x_m)^n = (x_1^n, \dots, x_m^n) = (1, \dots, 1) \Rightarrow g^n = 1 \quad \forall g \in G$$

Pick $f(x) = x^n - 1 \in F[x]$. Then $N > n$ elements $a \in F$ s.t. $f(a) = 0$ so more roots than degree $\times$.

- p prime, then $\mathbb{Z}_p \setminus \{0\}$ is cyclic of order $p-1$ [multiplicative gp]

Chapter 7 – Ideals & Quotient Rings [v similar to groups!]

(66) **Def (Ring Homomorphism):** R, S rings. $\phi: R \longrightarrow S$ is a ring homo if
(i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ $\forall r_1, r_2 \in R$
(ii) $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$ $\forall r_1, r_2 \in R$
(iii) $\phi(1_R) = 1_S$

isomorphism if also bijective

(67) **Def (kernel & image):**

define as kernel of additive groups

$\text{im}(\phi) = \{\phi(r) : r \in R\}$ $\ker(\phi) = \{r \in R : \phi(r) = 0_S\}$

$\text{im}(\phi)$ subring of S $\ker(\phi)$ is an ideal in R

why? $r \in k$, $x \in R$, $\phi(xr) = \phi(x)\underbrace{\phi(r)}_{0} = 0$ so $xr \in k$ $\Rightarrow k$ ideal.

(68) **Def (Ideal):** $I \subset R$ is an ideal if
(i) I subgp of $(R, +)$
(ii) $\forall x \in R$, $y \in I$, $xy \in I$, $yx \in I$ (closure)

$1_R \in I \iff I = R$
ideals $\neq$ subrings

note: $(a) = \{ra : r \in R\}$ is the principal ideal generated by a.

(69) **Prop (Quotient Rings):** The cosets of an ideal form a ring under addition in the quotient group. (ideals of rings are our new normal subgroups)
and multiplication $(I + a)(I + b) = I + ab$
E.g. quotient ring $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Isomorphism $\phi: \mathbb{Z}_n \longrightarrow \mathbb{Z}/(n)$ is $m \mapsto m + (n)$

(70) **Prop (Ring homomorphism):** The map $\pi: R \longrightarrow R/I$, $\pi(a) = a + I$ is a surjective ring homomorphism w/ kernel $\ker(\pi) = I$.

(71) **Thm (1st iso Thm for rings):** Let $\phi: R \longrightarrow S$ be a ring homomorphism w/ kernel I. Then $\text{im}(\phi) \cong R/I$

Chapter 8 – Domains

ring R is an integral domain so commutative here → no zero divisors.

Recall that the principal ideals are $(a) = aR$ for $a \in R$ fixed.

(72) **Def (Principal Ideal Domain):** Domain R is a PID if every ideal of R is principal.
PID = "every ideal is generated by a single element.

(23) Thm: For every field F, polynomial ring $F[x]$ is a PID. *generated by 1 element.*

Pf: Pick an ideal I in $F[x]$. If $I = \{0\} \Rightarrow I = (0)$ so principal.
So pick $g \in F[x]\setminus\{0\}$ (small as possible). WTS $I = (g)$ [the ideal is principal]
① $(g) \subseteq I$ by def. $(g) = \{fg \mid f \in F[x]\}$. I an ideal so $fg \in I \ \forall f \in F[x]$
② $I \subseteq (g)$. Why? Pick $f \in I$. so $f = gq + r$ [$r = 0$ or $\deg(r) < \deg(g)$]
If $r \neq 0 \Rightarrow r = f - gq \in I$. $\deg(r) < \deg(g)$ ✗ to g choice.
So $r = 0 \Rightarrow f = gq \in (g)$ so $I \subseteq (g) \Rightarrow I = (g)$ principal.

(24) Divisibility in integral domains: (Generalising divisibility in $\mathbb{Z}$)

- $x, y \in R$, $x \mid y$ if $y = rx$ for some $r \in R$.
- Following equivalent:
  - $x \mid y$
  - $y \in (x)$
  - $(x) \supseteq (y)$

  Think $3 \mid 6$ & $\overbrace{\{3,6,9,12,\dots\}}^{(3)} \supset \overbrace{\{6,12,18,\dots\}}^{(6)}$
- $x, y \in R$. x, y associate $(x \sim y)$ if $x \mid y$ & $y \mid x$.
- Following equivalent:
  - $x \sim y$
  - $(y) = (x)$
  - $\exists$ unit $q \in R$ s.t. $x = qy$
- $x, y \in R$, $\gcd(x,y) = d$ s.t.
  (i) $d \mid x$, $d \mid y$
  (ii) if $z \in R$ w/ $z \mid x, z \mid y \Rightarrow z \mid d$

  $x, y \in R$, $\operatorname{lcm}(x,y) = l$ s.t.
  (i) $x \mid l$, $y \mid l$
  (ii) if $z \in R$, $x \mid z, y \mid z \Rightarrow l \mid z$
- Prop (Generalised Bezout's lemma): R is a PID, then $\operatorname{lcm}(x,y)$, $\gcd(x,y)$ exist $\forall x, y \in R$ & $\exists r, s \in R$ s.t. $rx + sy = \gcd(x,y)$

(25) Prime & Irreducible elements: (Two different ways to define a prime)

irreducible
$r \in R\setminus\{0\}$ is irreducible if
(i) r is not a unit
(ii) if $r = ab$, $a, b \in R$
$\Downarrow$
either a or b is unit

$\overset{R=\text{domain}}{\Longleftarrow}$ $\quad$ $\overset{R=\text{PID}}{\Longrightarrow}$

Prime
$r \in R\setminus\{0\}$ is prime if
(i) r is not a unit
(ii) if $r \mid xy \Rightarrow r \mid x$ or $r \mid y$

If R is a domain, then every prime is irreducible

Pf: Let r be prime $\Rightarrow r$ not unit
Sppse $r = ab$, then $r \mid ab$
$\Rightarrow r \mid a$ or $r \mid b$. WLOG $r \mid a$
Then $a \mid r$ as $r = ab$
$\Rightarrow a \sim r$ so $r = aq$ w/ q unit.
$\Rightarrow ab = aq \Rightarrow b = q$
so b unit $\Rightarrow r$ irreducible

Prop: If R is a PID, then every irreducible is prime *Tricky...*

Pf: Let r be irreducible. Then r not unit. suppose $r \mid ab$ with $a, b \in R$.
$\boxed{\text{As } R \text{ is a PID, } \gcd(x,y) \text{ exists } \forall x,y \in R \text{ and } \exists r,s \in R \text{ s.t. } rx+sy=\gcd(x,y)}$
So $\exists c = \gcd(r,a) \Rightarrow r = ct$ for some $t \in R$
r irreducible $\Rightarrow$ either c or t is a unit.
case 1: If t unit, $r \sim c$, $c \mid a \Rightarrow r \mid a$ ✓
case 2: If c unit, then $(*) \Rightarrow c = xa + yr$ for $x, y \in R \Rightarrow cb = xab + yrb$.
know: ① $r \mid ab$ ② $r \mid yrb \Rightarrow r \mid cb$
Equivalently $ru = cb$ for $u \in R$. But c unit $\Rightarrow c^{-1}$ exists $\Rightarrow r \mid b$ ✓

Example: show $R = \mathbb{Z}[\sqrt{-5}]$ is not a PID
$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. (Claim 2 irreducible BUT not prime)

2 not prime:
$2x = 1 \pm \sqrt{-5}$
$\Rightarrow x \notin R$
so 2 doesn't divide $1 \pm \sqrt{-5}$

2 is irreducible:
Guess $2 = ab$ with $a, b \in \mathbb{Z}[\sqrt{-5}]$ and show a or b are units. $\to$ irreducible but not prime in PID ✗.
$\left.\begin{array}{l} a = x + y\sqrt{-5} \\ b = s + t\sqrt{-5} \end{array}\right\}$ $4 = |a|^2|b|^2 = (x^2+5y^2)(s^2+5t^2)$ & cases on $|a|, |b|$ that make $|a|^2$ or $|b|^2 = 1 \Rightarrow$ unit & no integer soln for $|a| = |b| = 2$.

$a \in R$ s.t. $\exists b \in R$ w/ $ab = 1$

(76) Unique Factorisation Domains:

- An integral domain is a **factorisation domain (FD)** if each non-unit $x \in R \setminus \{0\}$ admits a factorisation $x = r_1 r_2 \dots r_n$ [r_i irreducible elements]
- A FD R is a **UFD** if:
  - (i) R is a FD [factorisation unique upto reordering]
  - (ii) $\forall$ non units $x \in R \setminus \{0\}$, and any two factorisations $r_1 r_2 \dots r_n = s_1 s_2 \dots s_m$ where r_i, s_i irreducible, we have $m = n$ & $\exists \sigma \in S_n$ s.t. $r_i = s_{\sigma(i)}$ $\forall i$

If R is a UFD then every irreducible element is prime

Pf: Pick $x \in R$ irreducible so x not a unit.
WTS $x \mid ab \Rightarrow x \mid a$ or $x \mid b$
Factorise a, b to get $ab = r_1 \dots r_k \dots r_n$
Also $x \mid ab \Rightarrow ab = xy$ for $y \in R$
Factorise $y \Rightarrow ab = x s_1 \dots s_t$
As UFD $x \sim r_i$ for some i
factors match up
$i \le k \Rightarrow x \mid a$, $i > k$ $x \mid b$
so x prime!

A PID is a FD

Pf: use contradiction!
Let R be a PID, $x \in R \setminus \{0\}$ not unit. Assume x cannot be factorised into product of irreducibles.
$\Rightarrow x = yz$ where y, z not units.
⋮
nasty!

Every PID is a UFD

Pf: use induction on $n+m$
$x \in R \setminus \{0\}$ not unit.
$x = r_1 \dots r_n = s_1 \dots s_m$
If $x = s_1 = r_1$ true. Now $n > 1$
$r_n \mid x$, r_n irreducible $\Rightarrow r_n$ prime.
so $r_n \mid s_i$ for some i
$\Rightarrow r_n q = s_i$. s_i irreducible so q unit. Induct.

Any finite collection of elements in UFD has gcd, lcm

Chapter 9 - Fields

state that $(I,+) \le (R,+)$ $\forall x \in I$, $\forall r \in R$, $xr \in I$

(77) **Def (Maximal Ideals):** An ideal I of a ring R is maximal if $I \ne R$ but if J is any ideal s.t. $I \subseteq J \subseteq R \Rightarrow J = I$ or $J = R$

(78) **Prop (Ideals & Fields):** (An ideal I in commutative ring R maximal) $\Longleftrightarrow$ (R/I is a field)

quotient group

Proof: '$\Rightarrow$' suppose I is maximal. WTS $\forall x \in R \setminus I$ (not in), $x + I$ has multiplicative inverse in R/I
I maximal & $x \notin I \Rightarrow$ Ideal $I + (x) = R \Rightarrow 1 \in I + (x) \Rightarrow \exists y \in R$ s.t. $1 \in I + xy$
Then $I + 1 = I + xy = (I + x)(I + y)$
'$\Leftarrow$' J ideal s.t. $I \subseteq J \subseteq R$. $\Rightarrow \dots \Rightarrow J = R$ so maximal ideal.

(79) **Prop (maximal vs irreducible):** ($a \ne 0$, any ideal (a) in PID R maximal) $\Longleftrightarrow$ (a is irreducible)

Proof: '$\Rightarrow$' If (a) maximal, then $(a) \ne R$ so a not a unit. If $a = bc$
$\Rightarrow (a) \subseteq (b) \subseteq R$ so cases
① $(a) = (b) \Rightarrow c$ unit
② $(b) = R \Rightarrow b$ unit
$\underbrace{\hphantom{xxxxxxxxxxxx}}_{a \text{ irreducible}}$

Ideal is addition so if $(a) = R$ $\Rightarrow a$ is unit

'$\Leftarrow$' If a irreducible, then a not unit. So $(a) \ne R$. If $(a) \subseteq (b) \subseteq R$
$\Rightarrow b \mid a \Rightarrow a = bc$ for some $c \in R$
① c unit $\Rightarrow (a) = (b)$
② b unit $\Rightarrow (b) = R$
$\underbrace{\hphantom{xxxxxxxxxxxx}}_{(a) \text{ is maximal ideal.}}$

(78) Number Fields

(multiplication mod f)
- F field, $f \in F[x]$, $\deg(f) > 0 \Rightarrow F[x]/(f)$ = polynomials in f of degree less than f
- f irreducible $\Rightarrow F[x]/(f)$ is a field.
- Def: $\alpha \in \mathbb{C}$ **algebraic** (over $\mathbb{Q}$) if $f(\alpha) = 0$ for some $f \in \mathbb{Q}[x]$, $\deg(f) > 0$. Otherwise, α is **transcendental**.
- (Minimal polynomial): $\forall \alpha \in \mathbb{C}$, $f(x) \longmapsto f(\alpha)$ is a ring homomorphism $\phi_\alpha : \mathbb{Q}[x] \longrightarrow \mathbb{C}$. Consider cases on α

① α transcendental

② α algebraic

$\Rightarrow$ no $f \in \mathbb{Q}[x]$ s.t. $f(\alpha)=0$

$\Rightarrow \ker(\phi_\alpha) = \{0\}$

$\Rightarrow \underbrace{\mathrm{im}(\phi_\alpha) \cong \mathbb{Q}[x]}_{\text{1st iso Thm for rings}}$

$\exists f(x) \in \mathbb{Q}[x]$ non-zero s.t. $f(\alpha)=0 \Rightarrow f \in \ker(\phi_\alpha)$

$\ker(\phi_\alpha)$ is an ideal of of PID $\mathbb{Q}[x]$

$\Rightarrow \ker(\phi_\alpha) = (m)$ for $m \in \mathbb{Q}[x]$

make m monic & this is the minimal polynomial of α (over $\mathbb{Q}$)

The minimal polynomial

Prop: If $\alpha \in \mathbb{C}$ algebraic, then $\exists$ unique non-zero polynomial $m \in \mathbb{Q}[x]$ monic s.t. $m(\alpha)=0$ & m irreducible

① First iso Thm for rings:

$\mathrm{im}(\phi_\alpha) \cong \mathbb{Q}[x]/(f)$

f irreducible $\Rightarrow$ (f) maximal ideal $\Downarrow$ $\mathbb{Q}[x]/(f)$ is a field $\Rightarrow$ $\mathrm{im}(\phi_\alpha)$ is a subfield of $\mathbb{C}$ denote $\mathbb{Q}[\alpha]$ or $\mathbb{Q}(\alpha)$ ← number field

② Let f be monic irreducible $f \in \mathbb{Q}[x]$.

$\mathbb{C}$ closed algebraically $\Rightarrow$ f has a root $\alpha \in \mathbb{C}$

$\Rightarrow f \in \ker(\phi_\alpha)$.

Also, $\mathbb{Q}[x]$ is PID $\Rightarrow$ $\ker(\phi_\alpha)$ PID

f irreducible $\Rightarrow \ker(\phi_\alpha) = (f)$

$\Rightarrow$ f is minimal polynomial of α & $\mathbb{Q}[x]/(f) \cong \mathrm{im}(\phi_\alpha) = \mathbb{Q}[\alpha]$ ← subfield of $\mathbb{C}$.

Example $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, this has $f = x^2 - 2$ minimal polynomial for $\sqrt{2} \in \mathbb{C}$ chosen

// $\mathrm{im}(\phi_\alpha)$ where $\underbrace{\mathbb{Q}[x]/(x^2-2)}_{\text{field!!!}} \cong \mathbb{Q}[\sqrt{2}]$

$\phi_\alpha : f(x) \longmapsto f(\alpha)$

why field? $\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{\cdots}{c^2 - 2d^2}$ so closed!

STEPS:
① Pick some $\alpha \in \mathbb{C}$
② $\exists$ some $f \in \mathbb{Q}[x]$ monic & irreducible, $f(\alpha)=0$
③ $\mathbb{Q}[x]/(f) \cong \mathrm{im}(\phi_\alpha)$ is a field!

Chapter 10 – Polynomials

(79) **Def (Algebraically closed)**: A field F is algebraically closed if $\forall f \in F[x]$, $\deg(f) \geq 1$, $\exists \alpha \in F$ s.t. $f(\alpha)=0$ [e.g. $\mathbb{C}$, every polynomial has a root]

Note: The algebraic numbers $A \subseteq \mathbb{C}$ are the $\alpha \in \mathbb{C}$ s.t. $f(\alpha) = 0$ for some $f \in \mathbb{Q}[x]$ make a field?!?!

(80) **Prop (irreducibles in $F[x]$)**: If F algebraically closed field, then the irreducibles in $F[x]$ are the polynomials of degree 1. [each irreducible is an associate of $(x-a)$ for $a \in F$ unique.

Pf: See L.N.

(81) **Prop (primes in $\mathbb{R}[x]$)**: The monic primes in $\mathbb{R}[x]$ are $(x-a)$ & x^2+bx+c $\forall a, b, c \in \mathbb{R}$ s.t. $b^2 - 4c < 0$

Pf: v good exercise but non-examb...

$3 \mid 6x^3 + 12x + 9$ in $\mathbb{Z}[x]$

let R = UFD

(82) **Eisenstein's criterion**: Sufficient test for $\mathbb{Z}[x]$ polynomial irreducibility.

- an element $0 \neq f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ is primitive if $\gcd(a_0, \ldots, a_n) = 1$

Note: any $f \in R[x]$ can be written as $f = a f_0$ where $a \in R$, f_0 primitive.

- (EC). Let R = UFD, $f = a_0 + a_1 x + \cdots + a_n x^n$ primitive polynomial in $R[x]$. Suppose $\exists$ prime $p \in R$ s.t. $p \nmid a_n$, $p \mid a_i$ for $1 \leq i < n$. $p^2 \nmid a_0$ $\Rightarrow$ f irreducible in $R[x]$

Note: can swap: $\left(p \mid a_n,\ p \nmid a_i \text{ for } 1 \leq i < n \text{ and } p^2 \nmid a_0 \right) \Longleftrightarrow \left(p \nmid a_0,\ p \mid a_i \text{ for } 1 < i \leq n \text{ and } p^2 \nmid a_n \right)$

Pf: See notes...

(83) **Gauss' Lemma**: A primitive polynomial in $\mathbb{Z}[x]$ remains irreducible in $\mathbb{Q}[x]$.

List of Example Groups

① If k is any field, then $(k,+)$ group, $k^* = k \setminus \{0\}$ so $(k^*, \cdot)$ is a multiplicative group. $k = \mathbb{R}, \mathbb{C}, \mathbb{Q}$ etc...

② $C_n = \mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ w/ addition modulo n.

③ $U_n = \{a \in \mathbb{Z}_n : \gcd(a,n) = 1\}$

Pf: Need Bezout's lemma $\gcd(a,n) = 1 \iff \exists x, y \in \mathbb{Z}$ s.t. $ax + ny = 1$

④ $GL(n,k) = \{M \in k^{n \times n} : \det(M) \neq 0\}$, $SL(n,k) = \{M \in k^{n \times n} : \det(M) = 1\}$
$O(n,k) = \{M \in k^{n \times n} : M^T = M^{-1}\}$

⑤ If $g \in G$, then $\{g^k : k \in \mathbb{Z}\}$ is the cyclic subgroup generated by g.

⑥ Any subgroup of an abelian group is normal.

⑦ Quaternion Group Q_8

⑧ $H \trianglelefteq G$, then $\phi : H \longrightarrow G$ by $\phi(h) = h$ is homomorphism

⑨ $\phi : G \to G$ by $\phi(g) = kgk^{-1}$ is homomorphism

⑩ $\det(AB) = \det(A)\det(B) \Rightarrow \phi : GL(n,k) \longrightarrow k^*$ by $\phi(g) = \det(g)$ is a

⑪ $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ subring of $\mathbb{C}$ [Gaussian integers]

⑫ Ring homomorphisms:

- remainder mod n $\mathbb{Z} \longrightarrow \mathbb{Z}_n$
- $\phi(z) = \bar{z}$ complex conj
- $\phi_a : R[x] \longrightarrow S$ by $\phi_a(f) = f(a)$ [evaluation map]
- $\phi : R \longrightarrow S$ ring homomorphism.
  $\psi : R[x] \longrightarrow S[x]$ $\psi(a_n x^n + \dots + a_0) = \phi(a_n)x^n + \dots + \phi(a_0)$

Subring S	ideal I
• $(S,+) \leq (R,+)$ • $a_1, a_2 \in S \Rightarrow a_1 a_2 \in S$ • $1_R \in S$	• $(I,+) \leq (R,+)$ • $\forall x \in I, r \in R$ $rx \in I$