

MA249
Algebra II
Groups and Rings

Ian Rogers
Based on the lecture notes¹ of Dr Dmitriy Rumynin

June 17, 2007

Contents

1	Basics	2
1.1	Groups and subgroups	2
1.2	Symmetric groups, rings, subrings	3
1.3	Isomorphisms and direct products	4
1.4	Cyclic groups, fields, units	5
1.5	Cosets, Lagrange's theorem	7
1.6	Applications of Lagrange and dihedral groups	8
1.7	Generators and relations	8
2	Homomorphisms	9
2.1	Homomorphisms, images, kernels	9
2.2	Normal subgroups	10
2.3	Ideals	11
2.4	Quotients and homomorphisms	13
2.5	More isomorphism theorems	14
3	Group action on sets	16
3.1	Actions, orbits, stabilisers	16
3.2	Fixed points and quotients	17
3.3	Conjugacy classes	19
3.4	Conjugacy classes in alternating groups	20
4	Factorisation	21
4.1	Divisibility	21
4.2	UFDs	23
4.3	Primes in $F[x], \mathbb{Z}[i]$	24
4.4	Gaussian primes	25
4.5	Fractions	26
4.6	Gauss' lemma	27
4.7	Polynomial factorisation	28
4.8	Polynomial quotients	29
4.9	Application to linear maps	30
4.10	Cyclic vector spaces	30

¹Available to download from <http://www.maths.warwick.ac.uk/~rumynin/alg2.html>

1 Basics

1.1 Groups and subgroups

Definition 1. *Group* is set G and binary operation $\circ: G \times G \rightarrow G$ s.t.

1. (*Closure*) $\forall g, h \in G \quad g \circ h \in G$
2. (*Associativity*) $\forall g, h, k \in G \quad (g \circ h) \circ k = g \circ (h \circ k)$
3. $\exists e \in G$ s.t.

1. (*Identity*) $e \circ g = g \quad \forall g \in G$
2. (*Inverse*) $\forall g \in G \exists h \in G$ s.t. $g \circ h = e$.

Definition 2. *Order* of G , $|G|$ = number of elements in G .

Definition 3. Group G called *abelian* if

4. (*Commutativity*) $\forall g, h \in G \quad g \circ h = h \circ g$.

Definition 4. $H \subseteq G$ called *subgroup* of G if it forms a group under same operation as that of G .

Lemma 1.1.1. *If $H \leq G$ then $1_H = 1_G$.*

Proof. Consider element $h \in H$. Then $h \in G$, so in G $hh^{-1} = 1_G$, and in H $hh^{-1} = 1_H$. Hence $1_G = 1_H$. \square

Proposition 1.1.2 (Two-step test). $\emptyset \neq H \subseteq G$. H subgroup iff

1. $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$
2. $h \in H \Rightarrow h^{-1} \in H$.

Proof. If H subgp then 1., 2. follow from closure and inverses axioms. If 1., 2. hold, then associativity is inherited from G , and if $h, h^{-1} \in H$ by 2., then $hh^{-1} = 1 \in H$ by 1. \square

Proposition 1.1.3 (One-step test). $\emptyset \neq H \subseteq G$. H subgp iff

$$h, g \in H \Rightarrow hg^{-1} \in H$$

Proof. (\Rightarrow) By two-step test (1.1.2) $g^{-1} \in H$ so $hg^{-1} \in H$.

(\Leftarrow) $h \in H$ so $hh^{-1} \in H$. Then $h^{-1} = (hh^{-1})h^{-1} \in H$.

Therefore if $h_1, h_2 \in H$, $h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H$. \square

Lemma 1.1.4. *Intersection of any set of subgroups of G is a subgroup of G .*

Proof. Let $H_j : j \in J$ be subgps of G . Then $1_G \in H_j \quad \forall j$ so $\bigcap_{j \in J} H_j \supset \{1_G\}$ non-empty.

Suppose $h_1, h_2 \in \bigcap_{j \in J} H_j$. All H_j are subgroups so by two-step test (1.1.2) $h_1 h_2 \in H_j$, $h_1^{-1} \in H_j \quad \forall j$ so $h_1 h_2, h_1^{-1} \in \bigcap_{j \in J} H_j$. Therefore $\bigcap_{j \in J} H_j$ is subgroup by 1.1.2. \square

1.2 Symmetric groups, rings, subrings

Definition 5 (Symmetric group). Let X be any set,

$$\text{Sym}(X) = \{\phi: X \rightarrow X \mid \phi \text{ bijection}\}$$

Proposition 1.2.1. $\text{Sym}(X)$ is group under composition.

Proof. Composition of two bijections is bijection, composition is associative. Identity is $\iota: X \rightarrow X$, inverse element is inverse map. \square

Lemma 1.2.2. Any permutation on X can be written as product of transpositions.

Definition 6. A permutation is:

- *even* if product of even number of transpositions,
- *odd* if product of odd number of transpositions.

Proposition 1.2.3. No permutation is both even and odd.

Definition 7 (Alternating group).

$$\text{Alt}(X) = \{\phi: X \rightarrow X \mid \phi \text{ bijection, } \phi \text{ even}\}$$

$$\text{Alt}(X) \leq \text{Sym}(X).$$

Definition 8. A *ring* is a set with two binary operations $+, \cdot: R \times R \rightarrow R$ s.t.

1. (Group under $+$) $(R, +)$ abelian group
2. (Associativity) $\forall a, b, c \in R, (ab)c = a(bc)$
3. (Distributivity) $\forall a, b, c \in R, (a + b)c = ac + bc, a(b + c) = ab + ac$
4. (Identity) $\exists 1 \in R$ s.t. $\forall a \in R, a1 = 1a = a$.

Lemma 1.2.4. R a ring. Then R has unique identity element.

Proof. Let $1, 1'$ be identity elements. Then $1 = 11' = 1'$. \square

Lemma 1.2.5. Let R be a ring s.t. $0 = 1$. Then $R = \{0\}$.

Proof. $\forall x, x = x1 = x0 = 0$. \square

Definition 9. Ring R is *commutative* if

5. (Commutativity) $\forall a, b \in R, ab = ba$.

Definition 10. $S \subseteq R$ is *subring* of R if it forms a ring under same operation with same identity element.

Proposition 1.2.6. S abelian subgroup of ring R . Then S subring iff

1. $a_1, a_2 \in S \Rightarrow a_1 a_2 \in S$
2. $1_R \in S$.

Lemma 1.2.7. Intersection of any set of subrings of R is itself a subring.

1.3 Isomorphisms and direct products

Definition 11. *Isomorphism*

- $\phi: G \rightarrow H$ is bijection s.t. $\phi(g_1g_2) = \phi(g_1)\phi(g_2) \forall g_1, g_2 \in G$.
- $\phi: R \rightarrow S$ is bijection s.t. $\phi(r_1r_2) = \phi(r_1)\phi(r_2), \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) \forall r_1, r_2 \in R$.

Proposition 1.3.1. *Let X, Y be two sets s.t. $|X| = |Y|$. Then*

$$\text{Sym}(X) \cong \text{Sym}(Y)$$

Proof. Let $\psi: X \rightarrow Y$ be bijection. Then $f \mapsto \psi f \psi^{-1}$ isomorphism. \square

Corollary 1.3.2. *X, Y finite sets with $|X| = |Y|$. Then*

$$\text{Alt}(X) \cong \text{Alt}(Y)$$

Example 1. $\mathbb{R}, \mathbb{R}_{>0}$ are isomorphic ($\phi(x) = e^x$) but the two sets are not equal.

Definition 12. Let $g \in G$. The *order* of g , $|g|$ is least $n > 0$ s.t. $g^n = 1$ if such n exists. If no such n then $|g| = \infty$.

Lemma 1.3.3. $|g| = 1 \iff g = 1_G$.

Lemma 1.3.4. $|g| = n \implies \forall x \in \mathbb{Z}, g^x = 1 \implies n|x$.

Lemma 1.3.5. *If $\phi: G \rightarrow H$ is isomorphism then $\phi(1_G) = 1_H$.*

Proof. Let $\phi(1_G) = h \in H$. Then ϕ surjective so $\exists g \in G$ s.t. $\phi(g) = h^{-1}$. Then

$$1_H = hh^{-1} = \phi(1_G)\phi(g) = \phi(1_Gg) = \phi(g)$$

so $\phi(g) = 1_H$. \square

Lemma 1.3.6. *If $\phi: G \rightarrow H$ is isomorphism then $|g| = |\phi(g)| \forall g \in G$.*

Proof. Let $|g| = m$. Then $\phi(g)^m = \phi(g^m) = \phi(1_G) = 1_H$ by 1.3.5, so $|\phi(g)| \mid m$. Suppose $\exists n < m$ s.t. $\phi(g)^n = 1_H$. Then $\phi(g^n) = 1_H \implies g^n = 1_G$ as ϕ injective. Contradiction as $n < |g|$. Hence $|g| = |\phi(g)|$. \square

Definition 13. *Direct product*

- $G \times H = \{(g, h) : g \in G, h \in H\}$, s.t. $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$.
- $R \times S = \{(r, s) : r \in R, s \in S\}$, s.t. $(r_1, s_1)(r_2, s_2) = (r_1r_2, s_1s_2)$,
 $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$.

Proposition 1.3.7. $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ iff m, n coprime.

Proof. (\implies) If m, n not coprime let $l = \text{lcm}(m, n) < mn$. The rings as additive groups are not isomorphic since $|1| = mn$ in $(\mathbb{Z}_{mn}, +)$ but $\forall (a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, $l(a, b) = 0$ so no element of $\mathbb{Z}_m \times \mathbb{Z}_n$ has order mn . Hence not isomorphic by lemma 1.3.6.

(\Leftarrow) m, n coprime $\implies \exists a, b$ s.t. $am + bn = 1$. Let $(x)_n$ be residue of x mod n .
Want to show that $\phi(x) = ((x)_m, (x)_n)$ is isomorphism.

Is clearly homomorphism so RTP bijection.

$$\begin{aligned}\phi(\phi^{-1}(y, z)) &= \phi((amz + bny)_{mn}) \\ &= (((amz + bny)_{mn})_m, ((amz + bny)_{mn})_n) \\ &= ((amz + bny)_m, (amz + bny)_n) \\ &= ((bny)_m, (amz)_n) \\ &= (y, z)\end{aligned}$$

since $am + bn = 1 \implies (bn)_m = (am)_n = 1$. □

Corollary 1.3.8. If $n = p_1^{a_1} \dots p_k^{a_k}$ then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \times \dots \times \mathbb{Z}_{p_k^{a_k}}$

1.4 Cyclic groups, fields, units

Definition 14. G cyclic if $\exists g \in G$ s.t. $\forall h \in G, h = g^x$ some $x \in \mathbb{Z}$. g is called generator of G .

Lemma 1.4.1. Let $G = \langle g \rangle$. If $|G| = \infty$ then $|g| = \infty$. If $|G| = n$ then $|g| = n$.

Proposition 1.4.2. • Any two infinite cyclic groups are isomorphic.

- Any two cyclic groups of order n are isomorphic.

Proof. • $G = \{g^x : x \in \mathbb{Z}\}, H = \{h^x : x \in \mathbb{Z}\}$. $\phi: G \rightarrow H, \phi(g^x) = h^x$ isomorphism.

- $G = \{g^x : x \in \mathbb{Z}_n\}, H = \{h^x : x \in \mathbb{Z}_n\}$. $\phi: G \rightarrow H, \phi(g^x) = h^x$ isomorphism. □

Remark 1. Denote cyclic group of order m C_m .

Definition 15. $x \in R$ a unit if $\exists x' \in R$ s.t. $xx' = x'x = 1_R$.

Lemma 1.4.3. Units in R (R^*) form group under multiplication.

Proof. Product on R^* associative since is in R . Identity of R^* is 1_R , inverse of x is x' . □

Definition 16. A field is commutative ring K s.t. $K^* = K \setminus \{0\}$.

Lemma 1.4.4. $x \in \mathbb{Z}_n^*$ iff x, n coprime.

Proof. (\Rightarrow) x, n not coprime then $d = \gcd(x, n) > 1$. d divides $xy \forall y \in \mathbb{Z}_n$ so $xy \neq 1$ and x not unit.

(\Leftarrow) x, n coprime then $\exists a, b \in \mathbb{Z}$ s.t. $ax + bn = 1$ in \mathbb{Z} . Therefore x is unit with $x^{-1} = (a)_n$. □

Corollary 1.4.5. \mathbb{Z}_p is field iff p is prime.

Definition 17 (Euler phi-function). $\varphi: \mathbb{N} \rightarrow \mathbb{N}$, $\varphi(m) = |\mathbb{Z}_m^*|$ (number of integers between 1 and $m - 1$ coprime with n).

Lemma 1.4.6. R, S rings. Then $(R \times S)^* \cong R^* \times S^*$ as groups.

Proof. Both are subsets of $R \times S$.

$$\begin{aligned} (r, s) \in (R \times S)^* &\iff \exists (a, b) \in (R \times S) \text{ s.t. } (a, b)(r, s) = (1_R, 1_S) \\ &\iff \exists a \in R, b \in S \text{ s.t. } ar = 1_R, bs = 1_S \\ &\iff r \in R^*, s \in S^* \\ &\iff (r, s) \in (R^* \times S^*) \end{aligned} \quad \square$$

Corollary 1.4.7. If m, n coprime then $\varphi(mn) = \varphi(m)\varphi(n)$.

Corollary 1.4.8. If $m = p_1^{a_1} \dots p_k^{a_k}$ p_i s distinct primes then

$$\varphi(m) = \prod_{i=1}^k (p_i^{a_i} - p_i^{a_i-1})$$

Proof. $\varphi(m) = \prod_{i=1}^k \varphi(p_i^{a_i})$ by 1.4.7. $m \in \mathbb{Z}_{p_i^{a_i}} \iff m, p_i^{a_i}$ coprime $\iff p_i \nmid m$. Residues divisible by p_i of form xp_i so are $p_i^{a_i-1}$ of them. \square

Definition 18. Units in $M_n(R)$ called *general linear group* $\text{GL}_n(R)$.

Lemma 1.4.9. Let R be commutative ring, $A \in M_n(R)$. Then $A \in \text{GL}_n(R)$ iff $\det(A) \in R^*$.

Definition 19. For commutative ring R , *special linear group*

$$\text{SL}_n(R) = \{A \in M_n(R) : \det(A) = 1_R\}$$

Lemma 1.4.10. Let R be commutative ring. Then $\text{SL}_n(R) \leq \text{GL}_n(R)$.

Proof. Clearly $\text{SL}_n(R) \subseteq \text{GL}_n(R)$ since $1_R \in R^*$, $\text{SL}_n(R)$ non-empty as

$$\begin{pmatrix} 1_R & & 0 \\ & \ddots & \\ 0 & & 1_R \end{pmatrix} \in \text{SL}_n(R).$$

Suppose $A, B \in \text{SL}_n(R)$. Then $\det(AB) = \det(A)\det(B) = 1_R$ so $AB \in \text{SL}_n(R)$. A^{-1} exists since $\det(A) \neq 0$ and

$$1_R = \det(AA^{-1}) = \det(A)\det(A^{-1}) \implies \det(A^{-1}) = 1_R$$

Hence $\text{SL}_n(R) \leq \text{GL}_n(R)$ by two-step test (1.1.2). \square

1.5 Cosets, Lagrange's theorem

Throughout this section H subgroup of G .

Definition 20. $g \in G, H \leq G$. Right coset $Hg = \{hg : h \in H\} \subseteq G$.

Proposition 1.5.1. $\forall g, k \in G$ TFAE:

1. $k \in Hg$
2. $Hg = Hk$
3. $kg^{-1} \in H$

Proof. (1. \Rightarrow 2.) $k \in Hg \Rightarrow k = hg$ some $h \in H \Rightarrow g = h^{-1}k$. Let $f \in Hg$. Then for some $h_1 \in H$, $f = h_1g = h_1h^{-1}k \in Hk$ so $Hg \subseteq Hk$. Similarly opposite inclusion.

(2. \Rightarrow 1.) $k \in Hk = Hg$ so $k \in Hg$.

(1. \Rightarrow 3.) $k \in Hg \Rightarrow k = hg$ some $h \in H \Rightarrow kg^{-1} = h \in H$.

(3. \Rightarrow 1.) $kg^{-1} = h \in H$ then $k = hg \in Hg$. □

Corollary 1.5.2. Two right cosets Hg_1, Hg_2 are either equal or disjoint.

Proof. If not disjoint then $\exists k \in Hg_1 \cap Hg_2$. But then by 1.5.1 $Hg_1 = Hk = Hg_2$. □

Corollary 1.5.3. The right cosets of H partition G .

Proposition 1.5.4. H finite $\Rightarrow |Hg| = |H| \forall g \in G$.

Proof. $h_1g = h_2g \Rightarrow h_1 = h_2$ so $\phi: H \rightarrow Hg$, $\phi(h) = hg$ bijection. □

Theorem 1.5.5 (Lagrange). Let $|G| < \infty$, $H \leq G$. Then $|H| \mid |G|$.

Definition 21. Number of distinct right cosets of H in G called *index* of H in G , $|G : H|$.

Remark 2. If $|G| < \infty$ then $|G : H| = \frac{|G|}{|H|}$.

Proposition 1.5.6. $|G| < \infty$. Then $\forall g \in G \quad |g| \mid |G|$.

Proof. Let $|g| = n$. Let $H = \langle g \rangle \leq G$. $|H| = n$, result by Lagrange (1.5.5). □

1.6 Applications of Lagrange and dihedral groups

Theorem 1.6.1 (Euler). *Let $a, n \in \mathbb{Z}$ coprime. Then $n \mid (a^{\varphi(n)} - 1)$.*

Proof. Let $b = (a)_n$. $b \in \mathbb{Z}_n^*$. $b \mid \varphi(n)$ by 1.5.6, so $b^{\varphi(n)} = 1$ in \mathbb{Z}_n^* . Then $a^{\varphi(n)} - 1 = (a^{\varphi(n)} - b^{\varphi(n)}) + (b^{\varphi(n)} - 1)$ divisible by n in \mathbb{Z} . \square

Corollary 1.6.2 (Fermat's little thm). *p prime, $a \in \mathbb{Z}$. Then $p \mid (a^p - a)$.*

Proof.

$$a^p - a = \underbrace{a(a^{p-1} - 1)}_A = \underbrace{a(a^{\varphi(p)} - 1)}_B$$

If $p \mid a$ then result from expression A , if not then result by Euler (1.6.1) from expression B . \square

Definition 22. *Dihedral group D_{2n} group of isometries of regular n sided polygon P .*

Let the n rotations be denoted a^k ($0 \leq k < n$) and the reflection in the bisector of P that passes through vertex 1 be denoted b . Then

$$D_{2n} = \{a^k : 0 \leq k < n\} \cup \{a^k b : 0 \leq k < n\}$$

1.7 Generators and relations

Definition 23. $\{g_1, g_2, \dots, g_r\} \subset G$ generate G if every element of G can be obtained by repeated multiplication of g_i and their inverses.

(Equivalently if every $g \in G$ can be written as a word in the g_i s.)

Example 2. • a, b generate D_{2n} .

- Set of all transpositions generate $\text{Sym}(X)$.
- Elementary matrices over K generate $\text{GL}_n(K)$.

Proposition 1.7.1. *Let $|G| = 2n$ generated by a, b s.t. $a^n = 1 = b^2$, $ba = a^{-1}b$. Then $G \cong D_{2n}$.*

Proof. Any element g of G can be written as product of a, b, a^{-1}, b^{-1} . $a^n = 1 = b^2$ so can replace a^{-1} by a^{n-1} , b^{-1} by b so only a, b appear in this product. Using $ba = a^{-1}b = a^{n-1}b$ to move a^s to left of expression, get $g = a^k b^l$ some $0 \leq k < n$, $0 \leq l < 2$ so have $2n$ different $a^k b^l$. $|G| = 2n$ so all represent distinct elements of G . Hence

$$G = \{a^k : 0 \leq k < n\} \cup \{a^k b : 0 \leq k < n\}$$

Can deduce the same multiplication table as for D_{2n} . \square

Proposition 1.7.2. *Suppose $|G| = mn$ generated by a, b s.t. $a^m = b^n = 1$, $ba = ab$. Then $G \cong C_m \times C_n$.*

Proof. Any element g of G can be written $a^k b^l$ with $0 \leq k < m, 0 \leq l < n$ so

$$G = \{a^k b^l : 0 \leq k < m, 0 \leq l < n\}$$

Defining relations enable deduction of multiplication table. □

Proposition 1.7.3. $|G| = 8$, generated by a, b s.t. $a^4 = 1, b^2 = a^2, ba = a^{-1}b$. Then $G \cong Q_8$.

2 Homomorphisms

2.1 Homomorphisms, images, kernels

Definition 24. • *Group homomorphism* $\phi: G \rightarrow H$ is function s.t.

$$\phi(g_1 g_2) = \phi(g_1) \phi(g_2) \quad \forall g_1, g_2 \in G$$

• *Ring homomorphism* $\phi: R \rightarrow S$ is function s.t.

$$\phi(r_1 r_2) = \phi(r_1) \phi(r_2), \quad \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) \quad \forall r_1, r_2 \in R$$

Lemma 2.1.1. $\phi: G \rightarrow H$ hom. Then $f(1_G) = 1_H$ and $f(g^{-1}) = f(g)^{-1} \quad \forall g \in G$.

Proof. Let $f(1_G) = h \in H$. Then

$$1_H h = h = f(1_G) = f(1_G 1_G) = f(1_G) f(1_G) = hh$$

so $h = 1_H$.

Similarly if $f(g) = h$ then

$$f(g^{-1}) f(g) = f(g^{-1} g) = f(1_G) = 1_H = h^{-1} h = f(g)^{-1} f(g). \quad \square$$

Proposition 2.1.2. If $g, k \in G$ then $|g| = |kgk^{-1}|$.

Proof. Follows from 1.3.6. □

Proposition 2.1.3. $\phi: G \rightarrow H$ group homomorphism. Then $\text{im}(\phi) \leq H$.

Proposition 2.1.4. $\phi: R \rightarrow S$ ring homomorphism. Then $\text{im}(\phi)$ subring of S .

Definition 25 (Kernels). $\phi: G \rightarrow H$

$$\ker(\phi) = \{g \in G : \phi(g) = 1_H\}$$

or in the case of additive groups or rings

$$\ker(\phi) = \{g \in G : \phi(g) = 0_H\}$$

Remark 3. $1_G \in \ker(\phi) \quad \forall \phi$ by lemma 2.1.1.

Definition 26. $H \leq G$ called *normal* in G if $gH = Hg \quad \forall g \in G$. Write $H \trianglelefteq G$.

Proposition 2.1.5. $\phi: G \rightarrow H$ group homomorphism. Then $\ker(\phi) \trianglelefteq G$.

Proof. $K = \ker(\phi)$ subgroup using one-step test (1.1.3). Pick $a, b \in K$. Then $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = 1 \cdot 1^{-1} = 1 \cdot 1 = 1$ so $ab^{-1} \in K$.

Show K normal. Let $g \in G, k \in K$. $\phi(k) = 1_H$ so

$$\phi(g^{-1}kg) = \phi(g^{-1})1_H\phi(g) = \phi(g)^{-1}\phi(g) = 1_H$$

so $g^{-1}kg \in K$. Hence $gK = Kg \quad \forall g \in G$. □

Definition 27. Additive subgroup of ring R called *ideal* in R if $xI \subseteq I \supseteq Ix \quad \forall x \in R$. Write $I \trianglelefteq R$.

Proposition 2.1.6. $\phi: R \rightarrow S$ ring hom. Then $\ker(\phi) \trianglelefteq R$.

Proof. $K = \ker(\phi)$ additive subgroup of R by 2.1.5. If $p \in K, x \in R$ then

$$\phi(xp) = \phi(x)\phi(p) = \phi(x)0_S = 0_S$$

so $xp \in K$. Similarly $px \in K$. □

Proposition 2.1.7. $\phi: G \rightarrow H$ homomorphism. ϕ injective iff $\ker(\phi) = \{1_G\}$ (or $\{0_G\}$).

Proof. (\Rightarrow) $1_G \in \ker(\phi)$ so if ϕ injective then $\ker(\phi) = \{1_G\}$.

(\Leftarrow) Let $g_1, g_2 \in G$ with $\phi(g_1) = \phi(g_2)$. Then

$$1_H = \phi(g_1)^{-1}\phi(g_2) = \phi(g_1^{-1}g_2)$$

so $g_1^{-1}g_2 \in \ker(\phi) = \{1_G\}$. $g_1^{-1}g_2 = 1_G \iff g_1 = g_2$ so ϕ injective. □

2.2 Normal subgroups

Example 3. $\bullet \{1\}, G \trianglelefteq G$

- $\bullet G$ abelian then all subgroups normal.

Proposition 2.2.1. $H \leq G$ with $|G : H| = 2$. Then $H \trianglelefteq G$.

Proof. $|G : H| = 2$ so there are two distinct right cosets of H , H and $G \setminus H$. Similarly for left cosets. Then for $g \in G$:

- \bullet if $g \in H$ then $gH = H = Hg$,
- \bullet if $g \notin H$ then $gH = G \setminus H = Hg$. □

Proposition 2.2.2. $H \leq G$. Then $H \trianglelefteq G$ iff $ghg^{-1} \in H \quad \forall g \in G, h \in H$.

Proof. (\Rightarrow) $gh \in Hg \Rightarrow \exists h' \in H$ with $gh = h'g$. Then $ghg^{-1} = h' \in H$.

(\Leftarrow) For $gh \in gH$, $ghg^{-1} \in H$ so $gh = h'g$ some $h' \in H$. Therefore $gH \subseteq Hg$.
Similarly $gH \supseteq Hg$. \square

Definition 28. If $A, B \subseteq G$ define *product* $AB = \{ab : a \in A, b \in B\}$.

Lemma 2.2.3. $N \trianglelefteq G$ then $(Ng)(Nh) = (Ngh)$.

Proof. Let $n_1g \in Ng$, $n_2h \in Nh$. $gN = Ng$ so $\exists n_3 \in N$ s.t. $gn_2 = n_3g \in Ng$.
Then

$$(n_1g)(n_2h) = n_1(gn_2)h = n_1(n_3g)h = (n_1n_3)(gh) \in Ngh$$

so $(Ng)(Nh) \subseteq Ngh$. $ngh = (ng)(1h) \in (Ng)(Nh)$ so $Ngh \subseteq (Ng)(Nh)$. \square

Proposition 2.2.4. $N \trianglelefteq G$. Then $\frac{G}{N}$ set of right cosets Ng of N in G form group under multiplication of sets.

Proof. $(Ng)(Nh) = Ngh$ by 2.2.3, so have closure. Associativity follows from G . $(N1)(Ng) = N1g = Ng \quad \forall g \in G$ so $N1$ identity and Ng^{-1} inverse to Ng . \square

Definition 29. Group $\frac{G}{N}$ called *quotient group* of G by N .

Remark 4. If G finite, $|\frac{G}{N}| = |G : N| = \frac{|G|}{|N|}$.

Proposition 2.2.5. $N \trianglelefteq G$. $\phi: G \rightarrow \frac{G}{N}$, $\phi(g) = Ng$ surjective gp hom with kernel N .

Proof. Clearly surjective gp hom.

$$\phi(g) = 1_H \iff Ng = N1_G \iff g \in N \iff \ker(\phi) = N \quad \square$$

2.3 Ideals

Proposition 2.3.1. R a ring, $x \in R$. Then

$$(x) = \left\{ \sum_{k=1}^n r_k x s_k : r_k, s_k \in R \right\}$$

is an ideal in R .

Proof. (x) clearly non-empty.

Difference of two sums $\sum_{k=1}^n r_k x s_k$ also such a sum.

$$a \left(\sum_{k=1}^n r_k x s_k \right) = \sum_{k=1}^n (ar_k) x s_k \in (x) \text{ and } \left(\sum_{k=1}^n r_k x s_k \right) a = \sum_{k=1}^n r_k x (s_k a) \in (x). \quad \square$$

Remark 5. If R commutative $(x) = \{xr : r \in R\}$.

Lemma 2.3.2. Let R be commutative ring, $x \in R$. Then $x \in R^*$ iff $(x) = R$.

Proof.

$$\begin{aligned} x \in R^* &\iff \exists y \text{ s.t. } xy = 1_R \\ &\iff 1_R \in (x) \\ &\iff (x) = R \end{aligned}$$

(as $1_R \in I \Rightarrow a = a1_R \in I \forall a \in R$.) □

Definition 30. Non-zero $a, b \in R$ s.t. $ab = 0_R$ called *zero-divisors*.

Definition 31. A *domain* is a non-zero commutative ring without zero-divisors.

Proposition 2.3.3. • *A field is a domain.*

- *A subring of a domain is a domain.*
- *A polynomial ring over a domain is a domain.*

Proof. • R field $\Rightarrow R^* = R \setminus \{0_R\}$. Suppose \exists non-zero $a, b \in R$ s.t. $ab = 0_R$. Then $a \in R^*$ so $\exists a^{-1}$. Hence

$$0_R = a^{-1}0_R = a^{-1}ab = b$$

This is a contradiction.

- Clear as share same zero element, same binary operations.
- Prove by induction on n , the number of variables.

Let $f(x_1)$ and $g(x_1)$ be two non-zero polynomials in $R[x_1]$ and let a_f, b_g be their leading coefficients respectively. Thus $a_f \neq 0_R, b_g \neq 0_R$ and because R has no zero divisors, $a_f b_g \neq 0$. But the product $a_f b_g$ is the leading coefficient of $f(x_1)g(x_1)$ so $f(x_1)g(x_1)$ cannot be the zero polynomial. Consequently, $R[x_1]$ has no-zero divisors.

Suppose $R[x_1, \dots, x_{n-1}]$ has no zero-divisors. Let $f(x_1, \dots, x_n), g(x_1, \dots, x_n)$ be non-zero polynomials in $R[x_1, \dots, x_n]$. Then as the polynomial ring is commutative can write

$$f(x_1, \dots, x_n) = \sum_{i=1}^{\infty} x_n^i f_i(x_1, \dots, x_{n-1})$$

where not all f_i are zero. Similarly for g . Then $fg \neq 0_{R[x_1, \dots, x_n]}$ since not all of the products $x_n^i f_i x_n^j g_j$ are zero. □

Definition 32. A domain R is *principal ideal domain* (PID) if any ideal of R is principal.

Definition 33. A *euclidean domain* (ED) is domain R that admits norm function $\nu: R \setminus \{0\} \rightarrow \mathbb{N}$ s.t.

1. $\nu(ab) \geq \nu(b) \forall a, b \in R$
2. $\nu(ab) = \nu(b) \iff a \in R^*$

3. $\forall a, b \exists q, r$ s.t. $a = qb + r$ and either $r = 0$ or $\nu(b) > \nu(r)$.

Example 4. • \mathbb{Z} are ED, $\nu(x) = |x|$. q, r from division with remainder.

- $K[x]$ (K a field) is ED. $\nu(P) = \deg P$. q, r from polynomial division with remainder.
- Gaussian integers $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$ are subring of \mathbb{C} so a domain. Is ED with $\nu(x) = |x|^2$:
 1. Clear.
 2. $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$ since $q^{-1} = \frac{\bar{q}}{|q|^2}$.
 3. Pick $q \in \mathbb{Z}[i]$ closest to $\frac{a}{b}$. Then $|q - \frac{a}{b}| \leq \frac{1}{\sqrt{2}}$. Let $r = a - qb$. If $r \neq 0$, $\nu(r) = |a - qb|^2 = |q - \frac{a}{b}|^2 |b|^2 \leq \frac{\nu(b)}{2}$.

Theorem 2.3.4. $ED \implies PID$.

Proof. Let R be ED, $I \trianglelefteq R$. Choose $b \in I \setminus \{0\}$ with smallest possible norm. Clearly $(b) \subseteq I$. For $a \in I$ write $a = bq + r$ with either $r = 0$ or $\nu(b) > \nu(r)$. If $r \neq 0$ then $r = a - bq \in I$ smaller norm than b . Contradiction, so $a = bq \in (b)$. \square

2.3.1 Applications

Minimal polynomial of matrix

$A \in M_n(K)$ defines ring hom $f_A: K[x] \rightarrow M_n(K)$, $f_A(F(x)) = F(A)$ evaluation hom.

f_A linear map from infinite dim vector space to finite dimensional one, so has non-zero kernel. $K[x]$ is PID so $\ker(f_A) = (m_A)$ some $m_A \in K[x]$. This is minimal polynomial of A .

Characteristic of a ring

$f_R: \mathbb{Z} \rightarrow R$, $f_R(n) = n1_R$. Kernel of this hom is (m) some $m \geq 0$. This m is characteristic of R .

2.4 Quotients and homomorphisms

Proposition 2.4.1. *Cosets of ideal I form ring under addition in quotient group and the multiplication $(I + a)(I + b) = I + ab$.*

Proof. Let $I + a = I + x$, $I + b = I + y$. Then

$$ab = ab - ay + ay - xy + xy = a(b - y) + (a - x)y + xy.$$

Hence $ab - xy \in I$ and $I + ab = I + xy$. \square

Example 5. $\frac{\mathbb{Z}}{(n)} \cong \mathbb{Z}_n$. $\phi: \mathbb{Z}_n \rightarrow \frac{\mathbb{Z}}{(n)}$, $\phi(m) = m + (n)$.

Proposition 2.4.2. $I \trianglelefteq R$. $\phi: R \rightarrow \frac{R}{I}$, $\phi(g) = I + g$ is surjective ring hom with kernel I .

Proof. Is clearly surjective ring hom. $\phi(x) = 0 \iff I + x = I \iff x \in I$ so $\ker(\phi) = I$. \square

Theorem 2.4.3 (First isomorphism theorem (groups)). $\phi: G \rightarrow H$ gp hom with kernel K . Then

$$\boxed{\frac{G}{K} \cong \text{im}(\phi)}$$

There is isomorphism $\varphi: \frac{G}{K} \rightarrow \text{im}(\phi)$ defined by $\varphi(Kg) = \phi(g) \quad \forall g \in G$.

Proof. IDEA: PROVE THAT φ IS AN ISOMORPHISM.

Check φ well defined: $Kg = Kh \Rightarrow g = kh$ some $k \in K$. Then

$$\phi(g) = \phi(k)\phi(h) = \phi(h).$$

$\text{im}(\varphi) = \text{im}(\phi)$, φ clearly hom.

$$\varphi(Kg) = 1_H \iff \phi(g) = 1_H \iff g \in K \iff Kg = K1_G = 1_{G/K}$$

hence φ is injective by 2.1.7. Therefore φ isom. \square

Theorem 2.4.4 (First isomorphism theorem (rings)). Let $\phi: R \rightarrow S$ be ring hom with kernel I . Then

$$\boxed{\frac{R}{I} \cong \text{im}(\phi)}$$

More precisely \exists isomorphism $\varphi: \frac{R}{I} \rightarrow \text{im}(\phi)$, $\varphi(I + x) = \phi(x) \quad \forall x \in R$.

Theorem 2.4.5 (Cayley). Every group G is isomorphic to a permutation group. If G finite the set X can be chosen finite.

Proof. Let $X = G$. Homomorphism $\phi(x)(y) = xy$. By 1st isom thm (2.4.3) $\frac{G}{\ker(\phi)} \cong A \leq \text{Sym}(X)$. $x \in \ker(\phi) \Rightarrow x = x1 = \phi(x)(1) = 1$. \square

2.5 More isomorphism theorems

Lemma 2.5.1. If $H \leq G$, $K \trianglelefteq G$ then $HK = KH$ subgp of G .

Proof. Let $hk \in HK$. K normal so $hk \in hK = Kh \subset KH$, so $HK \subseteq KH$, opposite similar.

Product of two elements of HK lies in $HKHK = HHKK = HK$, inverse $k^{-1}h^{-1}$ of element $hk \in HK$ lies in $KH = HK$, so $HK \leq G$ by 1.1.2. \square

Theorem 2.5.2 (Second isomorphism theorem (groups)). $H \leq G$, $K \trianglelefteq G$. Then $H \cap K \trianglelefteq G$ and

$$\boxed{\frac{H}{H \cap K} \cong \frac{HK}{K}}$$

Proof. By 2.2.2 $H \cap K \trianglelefteq K$.

$\phi: G \rightarrow \frac{G}{K}$, $\phi(g) = Kg$ surjective group hom, kernel K by 2.2.5.

Then $\phi(H) = \{Kh : h \in H\} = \frac{KH}{K} \stackrel{2.5.1}{=} \frac{HK}{K} \leq \frac{G}{K}$. I.e. $\text{im}(\phi_H) = \frac{HK}{K}$.
 $\ker(\phi_H) = H \cap \ker(\phi) = H \cap K$. By 2.4.3 applied to ϕ_H , $\frac{H}{H \cap K} \cong \frac{HK}{K}$. \square

Theorem 2.5.3 (Second isomorphism theorem (rings)). S subring, I ideal of R . $S \cap I$ ideal in S and

$$\boxed{\frac{S}{S \cap I} \cong \frac{S+I}{I}}$$

Proof. By 2.5.2 for additive groups, $\frac{S}{S \cap I} \cong \frac{S+I}{I}$ of groups under addition, homomorphism $\eta: S \rightarrow \frac{S+I}{I}$, $\eta(s) = s + I$.

Observe $S+I$ subring, I ideal in it. η ring hom as is restriction of quotient hom $R \rightarrow \frac{R}{I}$ to S . \square

Theorem 2.5.4 (Third isomorphism theorem (groups)). $K \subseteq H \subseteq G$, $K, H \trianglelefteq G$. Then

$$\boxed{\frac{(G/K)}{(H/K)} \cong \frac{G}{H}}$$

Proof. Define $\phi: \frac{G}{K} \rightarrow \frac{G}{H}$ by $\phi(Kg) = Hg \quad \forall g \in G$. Well defined as $K \subseteq H$ so $Kg_1 = Kg_2 \Rightarrow Hg_1 = Hg_2$. $\text{im}(\phi) = \frac{G}{H}$, $\ker(\phi) = \frac{H}{K}$, result by 2.4.3. \square

Theorem 2.5.5 (Third isomorphism theorem (rings)). $I \subseteq J \subseteq R$, $I, J \trianglelefteq R$. Then $\frac{J}{I}$ ideal in $\frac{R}{I}$ and

$$\boxed{\frac{(R/I)}{(J/I)} \cong \frac{R}{J}}$$

Proof. $\phi: \frac{R}{I} \rightarrow \frac{R}{J}$, $\phi(I+r) = J+r$ well defined ring hom. $\text{im}(\phi) = \frac{R}{J}$, $\ker(\phi) = \frac{J}{I}$, result by 2.4.4. \square

Theorem 2.5.6 (Chinese remainder). $n_i \in \mathbb{N} \quad i = 1, \dots, t$ s.t. $\gcd(n_i, n_j) = 1 \quad i \neq j$. System of comparisons $x + (n_i) = k_i + (n_i)$ admits solution in \mathbb{Z} . Any two solutions differ by multiple of $N = n_1 n_2 \dots n_t$.

Proof. Consider ring hom $\psi: \mathbb{Z} \rightarrow \prod_i \frac{\mathbb{Z}}{(n_i)}$, $\psi(x) = (x + (n_1), \dots, x + (n_t))$. $\ker(\psi)$ is all x divisible by all n_i , so divisible by N since n_i coprime. Hence $\ker(\psi) = (N)$. By first isomorphism (2.4.4) $Z_N \cong$ subring of $\prod_i \frac{\mathbb{Z}}{(n_i)}$. Both rings have same number of elements so isomorphism. Hence ψ surjective. Surjectivity ensures exists solution since can write system $\psi(x) = (k_1, \dots, k_t)$. If x, x' two solutions, $x - x' \in \ker(\psi) = (N)$. \square

3 Group action on sets

3.1 Actions, orbits, stabilisers

Definition 34. G gp, X set. An *action* of G on X is a map $\cdot : G \times X \rightarrow X$ s.t.

1. $(gh) \cdot x = g \cdot (h \cdot x) \forall g, h \in G, x \in X$.
2. $1_G \cdot x = x \forall x \in X$.

Proposition 3.1.1. Let \cdot be action of G on set X . For $g \in G$ define $\phi(g) : X \rightarrow X$ by $\phi(g)(x) = g \cdot x$. Then $\phi(g) \in \text{Sym}(X)$, $\phi : G \rightarrow \text{Sym}(X)$ hom.

Proof. $\phi(1_G)$ is identity $I_X : X \rightarrow X$ by 2., so by 1. $\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = I_X$ and $\phi(g^{-1})\phi(g) = I_X$ so $\phi(g), \phi(g^{-1})$ inverse maps; so $\phi(g) : X \rightarrow X$ bijection. Hence $\phi(g) \in \text{Sym}(X)$. ϕ hom by property 1. \square

Definition 35. Kernel K of action \cdot of G on X is

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

Definition 36. Action is *faithful* if $K = \{1\}$.

Proposition 3.1.2. If \cdot is faithful action of G on X then $G \cong$ subgroup of $\text{Sym}(X)$.

Proof.

$$G \underset{\text{faithful}}{\cong} \frac{G}{K} \underset{2.4.3}{\cong} \text{im}(\phi) \quad \square$$

Definition 37. Let \cdot be action of G on X . Relation \sim on X defined by:

$$x \sim y \iff \exists g \in G \text{ s.t. } y = g \cdot x$$

Lemma 3.1.3. The relation \sim is an equivalence relation.

Proof. • $\boxed{x \sim x} : x = 1_G \cdot x$.

$$\bullet \boxed{x \sim y \iff y \sim x} : y = g \cdot x \iff g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = 1_G \cdot x = x.$$

$$\bullet \boxed{x \sim y, y \sim z \Rightarrow x \sim z} : y = g \cdot x, z = h \cdot y \Rightarrow z = h \cdot (g \cdot x) = \underbrace{(hg)}_{\in G} \cdot x. \quad \square$$

Definition 38. The *orbits* of G on X are the equivalence classes of \sim .

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

Definition 39. G acts on X , $x \in X$. *Stabiliser* of $x \in X$,

$$\text{Stab}_G(x) = \{g \in G : g \cdot x = x\}$$

Proposition 3.1.4. Let G act on X , $x \in X$. Then

1. $\text{Stab}_G(x) \leq G$
2. $\bigcap_{x \in X} \text{Stab}_G(x)$ is kernel of the action of G on X .

Proof. 1. Let $g_1, g_2 \in \text{Stab}_G(x)$. Then $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot x = x$ so $g_1 g_2 \in \text{Stab}_G(x)$.

Consider $g_1^{-1} \cdot x$. $x = g_1 \cdot x$ so

$$\begin{aligned} g_1^{-1} \cdot x &= g_1^{-1} \cdot (g_1 \cdot x) \\ &= (g_1^{-1} g_1) \cdot x \\ &= x \end{aligned}$$

so $g_1^{-1} \in \text{Stab}_G(x)$. Hence $\text{Stab}_G(x) \leq G$ by 2-step test (1.1.2).

2.

$$\begin{aligned} g \in \bigcap_{x \in X} \text{Stab}_G(x) &\Rightarrow \forall x \in X, g \cdot x = x \\ &\Rightarrow g \in \{\tilde{g} \in G : \tilde{g} \cdot x = x \quad \forall x \in X\} = K \\ &\Rightarrow \bigcap_{x \in X} \text{Stab}_G(x) \subseteq K \end{aligned}$$

$g \in K \Rightarrow g \cdot x = x \quad \forall x \Rightarrow g \in \text{Stab}_G(x) \quad \forall x$ so have equality. \square

Theorem 3.1.5 (Orbit-Stabiliser). *Let G be group acting on X , $x \in X$. Then \exists bijection between elements of $\text{Orb}_G(x)$ and left cosets of $\text{Stab}_G(x)$. In particular*

$$|\text{Orb}_G(x)| = |G : \text{Stab}_G(x)|$$

Proof. $\psi: G \rightarrow X$, $\psi(g) = g \cdot x$. Let $y \in \text{Orb}_G(x)$. Then $\exists g \in G$ s.t. $g \cdot x = y$. Let $H = \text{Stab}_G(x)$. For $g' \in G$,

$$\begin{aligned} g' \cdot x = y &\iff g' \cdot x = g \cdot x \\ &\iff (g^{-1} g') \cdot x = x \\ &\iff g^{-1} g' \in H \\ &\iff g' \in gH. \end{aligned} \quad \square$$

3.2 Fixed points and quotients

Definition 40. G acts on X . Quotient set $\frac{X}{G}$ is set of orbits.

Definition 41 (Fixed points). $T \subseteq G$.

$$X^T = \{x \in X : \forall g \in T, g \cdot x = x\}$$

In particular we are interested in $X^g := X^{\{g\}}$ and X^G .

Proposition 3.2.1 (Orbit-Stabiliser formula). *G finite group acting on finite set X . Then $\forall x \in X$*

$$|G| = |\text{Orb}_G(x)| |\text{Stab}_G(x)|$$

Proposition 3.2.2 (Counting formula). *Let G finite gp acting on finite set X . Then*

$$|X| = |X^G| + \sum_x \frac{|G|}{|\text{Stab}_G(x)|}$$

where sum is taken over representatives of all orbits containing > 1 element.

Proof. X disjoint union of orbits. One element orbits form X^G . Number of elements in larger orbits is

$$\sum_x |\text{Orb}_G(x)| \stackrel{3.2.1}{=} \sum_x \frac{|G|}{|\text{Stab}_G(x)|} \quad \square$$

Theorem 3.2.3 (Burnside formula). *G finite group acting on finite set X . Then*

$$\left| \frac{X}{G} \right| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Proof. Let $A = \{(g, x) \in G \times X : g \cdot x = x\}$.

$$|A| = \sum_{g \in G} |X^g|$$

and also

$$\begin{aligned} |A| &= \sum_{x \in X} |\text{Stab}_G(x)| \\ &= \sum_{x \in X} \frac{|G|}{|\text{Orb}_G(x)|} \\ &= |G| \sum_{\text{orbits}} \sum_{\substack{x \in \\ \text{orbit}}} \frac{1}{|\text{Orb}_G(x)|} \\ &= |G| \sum_{\text{orbits}} 1 \\ &= |G| \left| \frac{X}{G} \right| \quad \square \end{aligned}$$

3.2.1 Colouring regular n -gons

Count number of geometrically distinct colourings of regular n -gon using m colours. Let S be set of all sides. Colouring is function $f: \mathbb{Z}_m$, set of all colourings C has $|C| = m^n$.

What are geometrically the same colourings?

Example 6 (Pentagon). D_{10} acts on S , action on C given by $g \cdot c(s) = c(g^{-1} \cdot s)$ where $g \in D_{10}, s \in S, c \in C$.

Two colourings same if in same D_{10} orbit (or C_5 if only interested in comparison on rotational symmetries).

C_5 case

Want to count number of C_5 -orbits. 1 fixes all colourings but any non-trivial rotation only fixes colourings that use the same colour for all sides. Then by Burnside:

$$\left| \frac{C}{C_5} \right| = \frac{m^5 + m + m + m + m}{5} = \frac{m^5 + 4m}{5}$$

D_{10} case

If we also allow reflective symmetry have to count the number of D_{10} orbits. Each of the five reflections fixes colouring using 3 colours. Then by Burnside:

$$\left| \frac{C}{D_{10}} \right| = \frac{m^5 + 4m + 5n^3}{10}$$

3.3 Conjugacy classes

Definition 42 (Conjugation). • The action of G on itself, $g \cdot x = gxg^{-1}$ for $g, x \in G$ called *conjugation*.

- The orbits of this action called *conjugacy classes*; conjugacy class containing g denoted $\text{Cl}_G(g)$
- Elements in same conjugacy class called *conjugate*.

Definition 43. *Centraliser* of g in G is $\text{Stab}_G(g)$ for action of conjugation. Write

$$\text{C}_G(g) = \{f \in G : fg = gf\}$$

Definition 44. *Centre* of group G is kernel of this action:

$$\text{Z}(G) = \{f \in G : fg = gf \forall g \in G\}$$

Remark 6. $g \in \text{Z}(G) \iff \text{Cl}_G(g) = \{g\}$

Proposition 3.3.1. G finite group, $g \in G$. Then

1. $|\text{Cl}_G(g)| = \frac{|G|}{|\text{C}_G(g)|}$
2. $|G| = |\text{Z}(G)| + \sum_x \frac{|G|}{|\text{C}_G(x)|}$ where summation taken over representatives of all conjugacy classes.
3. $\left| \frac{G}{G} \right| = \frac{1}{|G|} \sum_{g \in G} |\text{C}_G(g)|$

Proposition 3.3.2. *A group of order p^n , p prime has non-trivial centre.*

Proof. By 3.3.1 1. sizes of conjugacy classes are powers of p . By 3.3.1 2. $p \mid |Z(G)|$ so centre non-trivial. \square

3.4 Conjugacy classes in alternating groups

Proposition 3.4.1. *Given permutation g in cyclic notation, conjugate fgf^{-1} of g obtained by replacing each element $x \in X$ in cycles of g by $f(x)$.*

Example 7. $X = \{1, 2, 3, 4, 5, 6, 7\}$, $g = (1, 5)(2, 4, 7, 6)$, $f = (1, 3, 5, 7, 2, 4, 6)$ then $fgf^{-1} = (3, 7)(4, 6, 2, 1)$.

Definition 45. Permutation has *cycle-type* $2^{r_2}3^{r_3} \dots$ if has r_i cycles length i , $i \geq 2$.

Proposition 3.4.2. *Two permutations of $\text{Sym}(X)$ conjugate in $\text{Sym}(X)$ iff have same cycle-type.*

Proof. (\Rightarrow) Conjugate permutations have same cycle type by 3.4.1.

(\Leftarrow) If g, h have same cycle type $\exists f \in \text{Sym}(X)$ with $fgf^{-1} = h$ (Choose f to map each element in turn). \square

Proposition 3.4.3. *Let $|G| < \infty$, $H \leq G$ of index 2, $x \in H$. Exactly one of the following holds:*

1. $\exists g \in G \setminus H$ s.t. $gx = xg$. Then $\text{Cl}_H(x) = \text{Cl}_G(x)$.
2. $\forall g \in G \setminus H$ $gx \neq xg$. Then $\text{Cl}_G(x) = \text{Cl}_H(x) \cup \text{Cl}_H(y)$ for any $y \in \text{Cl}_G(x) \setminus \text{Cl}_H(x)$.
Moreover $\frac{|\text{Cl}_G(x)|}{2} = |\text{Cl}_H(x)| = |\text{Cl}_H(y)|$.

Proof. $H \trianglelefteq G$ by 2.2.1. Hence $\text{Cl}_G(x) \subseteq H$.

1. $C_H(x)$ proper subgroup of $C_G(x)$. Hence by Lagrange (1.5.5) $|C_G(x)| \geq 2|C_H(x)|$.
By 3.3.1

$$\begin{aligned} |\text{Cl}_G(x)| &= \frac{|G|}{|C_G(x)|} \\ &\leq \frac{2|H|}{2|C_H(x)|} \\ &= |C_H(x)| \end{aligned}$$

so $\text{Cl}_G(x) = \text{Cl}_H(x)$.

2. $C_H(x) = C_G(x)$ so by 3.3.1

$$\begin{aligned} |\text{Cl}_G(x)| &= \frac{|G|}{|C_G(x)|} \\ &= \frac{2|H|}{|C[H]x|} \\ &= 2|\text{Cl}_H(x)| \end{aligned}$$

Pick $g \in \text{Cl}_G(x) \setminus \text{Cl}_H(x)$. $\frac{|\text{Cl}_G(x)|}{2} = |\text{Cl}_H(g)|$ but $g = axa^{-1}$ some $a \in G$ so $C[H]g = aC_H(x)a^{-1}$ and $|\text{Cl}_G(x)| = 2|\text{Cl}_H(g)|$. \square

Lemma 3.4.4. $H \leq G$ is normal in G iff H consists of union of conjugacy classes of G .

Proof. By 2.2.2

$$H \trianglelefteq G \iff ghg^{-1} \in H \quad \forall g \in G, h \in H \iff (h \in H \Rightarrow \text{Cl}_G(h) \subset H) \quad \square$$

Definition 46. G is simple if $\{1\}$ and G only normal subgroups.

Lemma 3.4.5. A_5 has 5 conjugacy classes of sizes 1,15,20,12,12.

Theorem 3.4.6. A_5 is simple.

Proof. Normal subgroup N of A_5 would be union of its conjugacy classes by 3.4.4. No combination of 1, 15, 20, 12, 12 containing 1 adds up to a proper divisor of 60. Result by Lagrange (1.5.5). \square

4 Factorisation

4.1 Divisibility

Throughout R is domain.

Definition 47. R domain, $x, y \in R$. x divides y ($x|y$) if $y = xr$ some $r \in R$.

Lemma 4.1.1. $\forall x, y \in R$, TFAE:

1. $x|y$
2. $y \in (x)$
3. $(x) \supseteq (y)$.

Definition 48. R domain, $x, y \in R$. x and y associate ($x \sim y$) if $x|y$ and $y|x$.

Lemma 4.1.2. TFAE:

1. $x \sim y$
2. $(y) = (x)$
3. $\exists q \in R^*$ s.t. $x = qy$.

Proof. (1. \Rightarrow 3.) Clear if $x = 0$. W.l.o.g. assume $0 \neq x$, $0 \neq y$. Then $\exists r, t \in R$ s.t. $x = ry$, $y = tx$. Then $x = ry = r(tx)$ and $(1 - rt)x = 0$. R domain so $1 - rt = 0$ and $q = r \in R^*$.

Other implications obvious. \square

Definition 49. $x, y \in R$.

- *Greatest common divisor* $\gcd(x, y)$ is $d \in R$ s.t. $d|x, d|y$ and if $z|x, z|y$ then $z|d$.
- *Least common multiple* $\text{lcm}(x, y)$ is $l \in R$ s.t. $x|l, y|l$ and if $x|z, y|z$ then $l|z$.

Proposition 4.1.3. *If R is PID then $\text{lcm}(x, y), \gcd(x, y)$ exist $\forall x, y \in R$.*

Proof. Pick $d, l \in R$ s.t. $(d) = (x) + (y), (l) = (x) \cap (y)$.

$(x) \subseteq (d) \supseteq (y)$ and whenever $(x) \subseteq (z) \supseteq (y)$ follows that $(z) \supseteq (x) + (y) = (d)$.

Similarly $(x) \supseteq (l) \subseteq (y)$ and whenever $(x) \supseteq (z) \subseteq (y)$ it follows that $(z) \subseteq (x) \cap (y) = (l)$. \square

Definition 50. $r \in R \setminus (R^* \cup \{0\})$ is *irreducible* if $r = ab \Rightarrow a \in R^*$ or $b \in R^*$.

Definition 51. $p \in R$ is *prime* if $p \in R \setminus R^*$ and $p|xy \Rightarrow p|x$ or $p|y$.

Proposition 4.1.4. *A prime element p is irreducible.*

Proof. Let $p = ab$. Then $p|a$ or $p|b$. Suppose $p|a$. Then $p \sim a$ and $p = aq$ with $q \in R^*$ by 4.1.2. R domain so $q = b$. \square

Proposition 4.1.5. *If R is PID, irreducible r is prime.*

Proof. r irreducible, $r|ab$. By 4.1.3 $\exists \tilde{a} = \gcd(r, a)$. Then $r = \tilde{a}t$ some $t \in R$. r irreducible so \tilde{a} or ta a unit:

- t unit $\Rightarrow r \sim \tilde{a}, r|a$.
- \tilde{a} unit $\Rightarrow (\tilde{a}) = (1) = (a) + (r)$. Hence $1 = xa + yr$ some $x, y \in R$. $r|xab = (1 - yr)b = b - yrb$. Hence $b = (b - yrb) + ybr \in (r)$ so $r|b$ and r prime as either $r|a$ or $r|b$. \square

Example 8. Let $\mathbb{Z}[i\sqrt{5}]$. In R , 2 is irreducible but not prime.

Proof. $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. $2 \nmid 1 \pm i\sqrt{5}$ since $2x = 1 \pm i\sqrt{5} \Rightarrow x = \frac{1}{2} \pm i\frac{\sqrt{5}}{2} \notin R$. So 2 not prime.

If $2 = ab$ with $a = x + yi\sqrt{5}, b = s + ti\sqrt{5} \in R$ then $4 = |a|^2|b|^2 = (x^2 + 5y^2)(s^2 + 5t^2)$. $|a|^2, |b|^2 \in \mathbb{N}$.

- $|a|^2 = 1$ then $a^{-1} = \frac{\bar{a}}{|a|^2} = x - yi\sqrt{5} \in R$, and $a \in R^*$.
- $|a|^2 = 4$ then $b^2 = 1$ and $b \in R^*$.
- $|a|^2 = 2$ gives contradiction: $|a|^2 = x^2 + 5y^2 = 2 \Rightarrow (x + (5))^2 = 2 \in \mathbb{Z}_5$. Impossible.

This shows that 2 is irreducible in $\mathbb{Z}[i\sqrt{5}]$. \square

Hence $\mathbb{Z}[i\sqrt{5}]$ not PID so not Euclidean.

Proposition 4.1.6. *R domain. $0 \neq p \in R$ prime iff $\frac{R}{(p)}$ domain.*

Proof. (\Rightarrow) Suppose $(r_1 + (p))(r_2 + (p)) = (p)$ then $r_1 r_2 + (p) = (p)$ so $r_1 r_2 \in (p)$
 $\stackrel{4.1.1}{\iff} p|r_1 r_2 \Rightarrow p|r_1$ or $p|r_2$.

Therefore by 4.1.1 either $r_1 \in (p)$ or $r_2 \in (p)$. Hence $\frac{R}{(p)}$ has no zero divisors, so is domain (is clearly a ring).

(\Leftarrow) $\frac{R}{(p)}$ domain so has no zero divisors, so $p = r_1 r_2 \Rightarrow (r_1 + (p))(r_2 + (p)) = (p)$.
 Therefore either $r_1 \in (p)$ or $r_2 \in (p) \Rightarrow p|r_1$ or $p|r_2 \Rightarrow p$ prime. \square

4.2 UFDs

Definition 52. Domain R is *factorisation domain* (FD) if each $x \in R \setminus (R^* \cup \{0\})$ admits factorisation $x = r_1 r_2 \dots r_n$ where r_i irreducible.

Definition 53. FD R is *unique factorisation domain* (UFD) if for any two factorisations of $x \in R$, $x = r_1 r_2 \dots r_n = s_1 s_2 \dots s_m$ (r_i, s_j irreducible) then $m = n$ and $\exists \sigma \in S_n$ s.t. $r_i \sim s_{\sigma(i)} \forall i$.

Proposition 4.2.1. *Let R be FD. Then R is UFD iff every irreducible element is prime.*

Proof. (\Rightarrow) Let x be irreducible s.t. $x|ab$. Let $a = r_1 \dots r_k$, $b = r_{k+1} \dots r_n$ get factorisation $ab = r_1 \dots r_n$. Also $ab = xy$. Let $y = s_1 \dots s_t$, then get $ab = x s_1 \dots s_t$. R UFD so $x \sim r_i$ some i . If $i \leq k$ then $x|a$. If $i > k$ then $x|b$ so x prime.

(\Leftarrow) Let

$$x = r_1 \dots r_n = s_1 \dots s_m \quad (1)$$

Induction on n .

If $n = 1$ then $x = r_1$ irreducible, result follows.

If done for $n - 1$ then $r_n | s_1 \dots s_m$. r_n prime so divides some s_i . Hence $r_n = q s_i$ some $q \in R^*$. Then $q r_1 \dots r_{n-1} r_n = s_1 \dots s_{i-1} s_{i+1} \dots s_m s_i$ by (1). This gives $q r_1 \dots r_{n-1} = s_1 \dots s_{i-1} s_{i+1} \dots s_m$ and by induction assumption, $m - 1 = n - 1$, each $r_i \sim s_j$ some j . \square

Theorem 4.2.2. *A PID is a UFD.*

Proof. IDEA: SHOW R IS FD BY DEFINING ITERATIVE PROCESS AND PROVE IT MUST TERMINATE AT SOME STAGE.

In PIDs all irreducibles are prime by 4.1.5, and then if R is FD, by 4.2.1 R must be UFD. Have to factorise $x \in R \setminus (R^* \cup \{0\})$. If x irreducible we are done. If not we can write $x = x_{1,1} x_{1,2}$ where $x_{1,i}$ are not units.

Suppose after n steps we have $x = x_{n,1}x_{n,2} \dots x_{n,k}$ where none of the $x_{n,i}$ units. If $x_{n,i}$ irreducible $\forall i$ then we have factorisation of x and the process stops.

If not pick all $x_{n,i}$ not irreducible, write as $x_{n,i} = x_{n+1,i}x_{n+1,i+1}$ where $x_{n+1,j}$ not units and repeat the process.

Suppose the process does not terminate for some $x \in R$. We then get a set of decompositions $x = x_{n,1}x_{n,2} \dots x_{n,k_n}$ for each $n \in \mathbb{N}$. Think of the process of a binary tree branching out wherever $x_{i,j}$ not irreducible. Process non-terminating so have infinite path through this tree. Let $y_n = x_{n,i}$ be element of this path at level n . $y_0 = x$. Then

$$\dots y_{n+1} \mid y_n \mid \dots \mid y_1 \mid y_0$$

so we get the *proper inclusions*

$$\dots (y_{n+1}) \supset (y_n) \supset \dots \supset (y_1) \supset (y_0).$$

Their union, $I = \bigcup_{n=1}^{\infty} (y_n)$ is an ideal. R is PID so $I = (d)$ some $d \in R$.

Then $d \in (y_n)$ some n , so $I = (d) \subseteq (y_n)$. Hence

$$I = (d) = (y_n) = (y_{n+1}) = \dots$$

contradicting the fact that all the inclusions of ideals were proper. Therefore the process must terminate and R is FD. \square

4.3 Primes in $F[x], \mathbb{Z}[i]$

Proposition 4.3.1 (Remainder theorem). *Let $f = f(x) \in F[x]$. If $f(a) = 0$ some $a \in F$ then $x - a$ divides f .*

Proof. $f(x) = g(x)(x - a) + r$, $\deg r < 1$ so $r \in F$. Substitute $x = a$ to get $0 = f(a) = r$. \square

Definition 54. Field F is *algebraically closed* if $\forall f(x) \in F[x]$ of degree at least 1 $\exists a \in F$ s.t. $f(a) = 0$.

Proposition 4.3.2. *If F algebraically closed then primes in $F[x]$ are $x - a$ as a runs over F .*

Proof. $x - a$ irreducible since any divisors must have degree 0 or 1. If a divisor has degree:

- 0 then it is a unit.
- 1 then it is associate to $x - a$.

$F[x]^* = F^*$, so $x - a$ associate only to $bx - ab \forall b \in F^*$. Hence $(x - a_1 \sim x - a_2$ if $a_1 \neq a_2$). If $f \in F[x]$ prime, $\deg(f) \leq 1$. F algebraically closed so $\exists a \in F$ s.t. $f(a) = 0$. By 4.3.1, $x - a \mid f$ so $f \sim x - a$. \square

Theorem 4.3.3. *F a field. Then any finite subgroup of F^* is cyclic group.*

Proof. G finite abelian group, so by **Algebra I**, $G \cong C_{n_1} \times \cdots \times C_{n_m}$ where $n_1 \mid n_2 \mid \cdots \mid n_m$ orders of C_{n_1}, \dots, C_{n_m} , and $|G| = N = n_1 n_2 \dots n_m$.

Suppose G not cyclic. Then $n_m < N$ (i.e. there are at least two elements in the above decomposition). Then $\forall g \in G, g^{n_m} = 1$. Therefore the polynomial $f(x) = x^{n_m} - 1 \in F[x]$ has each of the N elements of G as a root.

4.3.1 $\Rightarrow \forall a \in G, (x - a) \mid f(x)$. $x - a$ is prime and $F[x]$ is UFD, so

$$\prod_{a \in G} (x - a) \mid f(x).$$

This is a contradiction. A polynomial of degree N cannot divide a polynomial of degree $n_m < N$. \square

Corollary 4.3.4. \mathbb{Z}_p^* cyclic of order $p - 1$.

4.4 Gaussian primes

Definition 55. The primes in $\mathbb{Z}[i]$ as called *Gaussian primes*.

Recall that in $\mathbb{Z}[i]$ the norm $\nu(x) = |x|^2$. If $x \mid y$ in $\mathbb{Z}[i]$ then $\nu(x) \mid \nu(y)$ in \mathbb{Z} .

Proposition 4.4.1. *If for $x \in \mathbb{Z}[i]$, $\nu(x)$ is prime in \mathbb{Z} then x is Gaussian prime.*

Proof. By 4.2.1 and the fact that $\mathbb{Z}[i]$ is UFD it suffices to show that x is irreducible.

Suppose $y \mid x$. Then $\nu(y) \mid \nu(x) = p \in \mathbb{Z}$ so $\nu(y) = p$ or 1 . If $\nu(y) = p$ then $y \sim x$. If $\nu(y) = 1$ then y a unit. \square

Proposition 4.4.2. *Let $p \in \mathbb{Z}$ prime. Then either p is Gaussian prime or $p = x\bar{x}$ where x is Gaussian prime.*

Proof. If p not Gaussian prime then \exists Gaussian prime x s.t. $p = xy$ and neither x nor y a unit. Hence $\nu(x)\nu(y) = \nu(p) = p^2$. Then $\nu(x) = \nu(y) = p$ so x, y prime by 4.4.1.

$$\bar{x} = x^{-1}\nu(x) = \left(\frac{y}{p}\right)p = y. \quad \square$$

Proposition 4.4.3. *Let $q \in \mathbb{Z}[i]$ Gaussian prime. Then $\nu(q)$ is either prime or square of prime.*

Proof. Let $n = \nu(q) = q\bar{q}$. Take decomposition of n into primes in \mathbb{Z} , $n = p_1 \dots p_t$. Then $q \mid p_j$ in $\mathbb{Z}[i]$ some j . \square

Theorem 4.4.4. *Primes in $\mathbb{Z}[i]$ obtained from primes in \mathbb{Z} . $\forall p \in \mathbb{Z}, p \equiv 3 \pmod{4}$ Gaussian prime. $p = 2$ gives Gaussian prime q s.t. $2 \sim q^2$. Each $p \in \mathbb{Z}, p \equiv 1 \pmod{4}$ give two conjugate Gaussian primes q, \bar{q} s.t. $p = q\bar{q}$.*

Proof. By 4.4.3 have two cases. If q is Gaussian prime then either $\nu(q) = p$ or $\nu(q) = p^2$ some prime $p \in \mathbb{Z}$.

- Suppose q s.t. $p = \nu(q)$ prime. Then p gives two Gaussian primes, q, \bar{q} with $p = q\bar{q} = \nu(q)$.
- Suppose q s.t. $\nu(q) = p^2$ some prime p . Then $q \mid p$ in $\mathbb{Z}[i]$, pick s s.t. $p = qs$. Then $|s| = \frac{|p|}{|q|} = 1$, s a unit. Then $q \sim p$ \square

Corollary 4.4.5 (Fermat). *Every prime congruent 1 mod 4 sum of integer squares in unique way.*

Proof. Existence by 4.4.4. If $p = x^2 + y^2 = a^2 + b^2$ then $p = (x + iy)(x - iy) = (a + ib)(a - ib)$ both prime decompositions in $\mathbb{Z}[i]$. $\mathbb{Z}[i]$ UFD. \square

Corollary 4.4.6. *There are ∞ -many primes congruent 1 mod 4.*

Proof. Suppose only exist p_1, \dots, p_n prime in \mathbb{Z} . Let $p_0 = 2$, $q_0 = 1 + i$, $p_j = q_j\bar{q}_j$ prime decomposition of p_j . Consider prime decomposition of $x = 2p_1p_2 \dots p_n + i \in \mathbb{Z}[i]$. No prime $p \in \mathbb{Z}$ congruent 3 mod 4 divides x since $\frac{x}{p}$ has $\frac{1}{p}$ as coefficient of i , so not in $\mathbb{Z}[i]$. Hence one of Gaussian primes q_j divides x . Hence $p_j = \nu(q_j) \mid \nu(x) = 4p_1^2p_2^2 \dots p_n^2 + 1$. Contradiction. \square

4.5 Fractions

Definition 56. R domain, $W = R \times (R \setminus \{0\})$. Equivalence relation $(a, b) \sim (c, d)$ whenever $ad = bc$. Equivalence class of (a, b) called a *fraction* denoted $\frac{a}{b}$. Let $Q = Q(R)$ set of all equivalence classes on W .

Proposition 4.5.1. *If R domain then $Q(R)$ a field under the operations addition and multiplication (defined as for regular fractions). Also $\pi: R \rightarrow Q(R)$, $\pi(r) = \frac{r}{1}$ injective ring homomorphism.*

Proof. Need to show:

- operations well defined,
- satisfies field axioms,
- π injective hom.

Operations well defined:

Denominators non-zero as R domain. Given $\frac{a}{b} = \frac{x}{y}$, $\frac{c}{d} = \frac{u}{w}$. Then:

- $ay = bx, cw = du \implies acyw = bdxu \implies \frac{ac}{bd} = \frac{xu}{yw}$.
- $adyw - bdxw = dw(ay - bx) = 0$, $bdyu - bcyw = by(dw - cw) = 0 \implies adyw - bdxw = bdyu - bcyw \implies \frac{ad+bc}{bd} = \frac{xw+yu}{yw}$

Field axioms:

- $\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf+(bcf+bde)}{bdf} = \frac{a}{b} + \frac{cf+de}{df} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right).$
- $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{c}{d} + \frac{a}{b}.$
- $0 = \frac{0}{1}.$
- $-\left(\frac{a}{b}\right) = \frac{-a}{b}.$
- $\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right).$
- $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{c}{d} \cdot \frac{a}{b}.$
- $1 = \frac{1}{1}.$
- $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}, a = 0 \iff a \cdot 1 = b \cdot 0 \iff \frac{a}{b} = \frac{0}{1} = 0.$
- $\left(\frac{a}{b} + \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ad+bc}{bd} \cdot \frac{e}{f} = \frac{ade+bce}{bdf} = \frac{ade}{bdf} + \frac{bce}{bdf} = \frac{a}{b} \cdot \frac{e}{f} + \frac{c}{d} \cdot \frac{e}{f}.$

Ring homomorphism since $\pi(1_R) = \frac{1}{1} = 1_Q$. $\pi(xy) = \frac{xy}{q} = \frac{x}{1} + \frac{y}{1} = \pi(x)\pi(y)$.
 $\pi(x+y) = \frac{x+y}{1} = \frac{x}{1} + \frac{y}{1} = \pi(x) + \pi(y)$. $x \in \ker(\pi) \iff \frac{x}{1} = \frac{0}{1} \iff x \cdot 1 = 0 \cdot 1 \iff x = 0$. \square

Definition 57. $Q = Q(R)$ called *field of fractions* of domain R .

Example 9. $Q(\mathbb{Z}) = \mathbb{Q}$.

Proposition 4.5.2. *If R is ED then any element of $Q(R)$ can be represented as $r + \sum_j \frac{r_j}{p_j^{n_j}}$ where $r, r_j, p_j \in R$, $n_j \in \mathbb{N}$, p_j pairwise non-associate primes.*

4.6 Gauss' lemma

Definition 58. Polynomial $f(x)$ called

- *monic* if coefficient of highest degree term is 1.
- *primitive* if gcd of all coefficients of $f(x)$ is 1.

Theorem 4.6.1. *Let R be UFD with field of fractions $Q = Q(R)$. If $f = gh \in R[x]$ some $g, h \in Q[x]$ then $\exists a, b \in Q$ s.t. $\tilde{g} = ag \in R[x]$, $\tilde{h} = bh \in R[x]$ and $f = \tilde{g}\tilde{h}$.*

Proof. Let a_1 be lcm of all denominators of coefficients of $g(x)$, a_2 gcd of all coefficients of $a_1g(x)$, $a = \frac{a_1}{a_2} \in Q(R)$. Define $\tilde{g} = ag \in R[x]$. Similarly $\tilde{h} = bh \in R[x]$. \tilde{g}, \tilde{h} primitive. Hence $f = \frac{u}{v}\tilde{g}\tilde{h}$ and $vf = u\tilde{g}\tilde{h}$ some $u, v \in R$. $\gcd(u, v) = 1$.

Suffices to prove $v \in R^*$. Suppose not. Then $\exists p \in R$ prime, $p \mid v$. Consider ring hom $\pi: R[x] \rightarrow \frac{R}{(p)}[x]$, $\pi(\sum_k a_k x^k) = \sum_k (a_k + (p))x^k$. $\pi(v) = 0$ so $\pi(v)\pi(f) = \pi(u)\pi(\tilde{g})\pi(\tilde{h})$. $\frac{R}{(p)}[x]$ domain so one of $\pi(u), \pi(\tilde{g}), \pi(\tilde{h}) = 0$ This is a contradiction:

- $\pi(u) \neq 0$ since $p \nmid u$ since $\gcd(u, v) = 1$.
- $\pi(\tilde{g}) \neq 0 \neq \pi(\tilde{h})$ since these polynomials are primitive. \square

Corollary 4.6.2. *If R is UFD then are two types of primes in $R[x]$: primes in R and primitive elements in $R[x]$ that are prime in $Q[x]$.*

Corollary 4.6.3. *R is UFD $\Rightarrow R[x]$ is UFD.*

Corollary 4.6.4. *F field then $F[x_1, \dots, x_n]$ is UFD.*

Proof. Induction on n . If $n = 1$ $F[x]$ is ED, so PID, so UFD. If true for $n - 1$ observe $F[x_1, \dots, x_n] \cong F[x_1, \dots, x_{n-1}][x_n]$ also UFD by 4.6.3. \square

Corollary 4.6.5. *$\mathbb{Z}[x_1, \dots, x_n]$ is UFD.*

Proof. Induction of n . If $n = 1$ $\mathbb{Z}[x]$ is UFD by 4.6.3 since \mathbb{Z} is ED so PID so UFD. Suppose true for $n - 1$ then $\mathbb{Z}[x_1, \dots, x_n] \cong \mathbb{Z}[x_1, \dots, x_{n-1}][x_n]$ also UFD by 4.6.3. \square

4.7 Polynomial factorisation

Proposition 4.7.1 (Eisenstein's Criterion). *Let R be UFD. $f(x) = \sum_{k=0}^n a_k x^k \in R[x]$. Assume \exists prime $p \in R$ s.t. $p \mid a_k \forall k < n$, $p \nmid a_n$, $p^2 \nmid a_0$. If $\gcd_k a_k = 1$ then $f(x)$ irreducible in $R[x]$.*

Proof. Factorisation with one polynomial of zero degree impossible as coefficients no common divisors. Suppose $f(x) = \sum_{k=0}^n a_k x^k = (\sum_{k=0}^m b_k x^k) (\sum_{k=0}^t c_k x^k)$ both of non-zero degree. Then $a_k = \sum_{r+s=k} b_r c_s \quad \forall k$.

$p \mid a_0 = b_0 c_0$ divides either b_0 or c_0 but not both as $p^2 \nmid a_0$. W.l.o.g. $p \mid b_0$, $p \nmid c_0$.

Induction: $p \mid b_j \quad \forall 0 \leq j \leq m < n$. Suppose done $\forall j < l$. Then

$$b_l c_0 = a_l - (b_{l-1} c_1 + b_{l-1} c_2 + \dots)$$

$p \mid$ each term in RHS so $p \mid b_l c_0$. $p \nmid c_0$ so $p \mid b_l$. Hence $p \mid a_n = b_m c_t$. Contradiction. Therefore f is irreducible in $R[x]$. \square

Example 10. p prime in $R \Rightarrow x^n + p$ prime in $R[x] \quad \forall n$.

Proof. $p \mid a_0$, $p \nmid a_n$, $p^2 \nmid a_0$. $\gcd(p, 1) = 1 \Rightarrow x^n + 1$ irreducible in $R[x] \Rightarrow x^n + 1$ prime as $R[x]$ is UFD. \square

Proposition 4.7.2. *Let R be PID. If $p \in R$ prime then $\frac{R}{(p)}$ field.*

Proof. $\frac{R}{(p)}$ domain by 4.1.6. Need inverse for non-zero $x + (p) \in \frac{R}{(p)}$. $x + (p) \neq 0$ so $p \nmid x$. p prime so $\gcd(x, p) = 1$. $(x) + (p) = (\gcd(x, p))$ so $\exists a, b \in R$ s.t. $1 = ax + bp$. Hence $(x + (p))^{-1} = a + (p) \in \frac{R}{(p)}$. \square

4.8 Polynomial quotients

Proposition 4.8.1. *F field, $f = f(x) \in F[x]$ irreducible. Field $\frac{F[x]}{(f)}$ contains root of $f(x)$.*

Proof. Root of $f(x)$ in $\frac{F[x]}{(f)}$ is $a = x + (f)$. If $f(x) = \sum_{k=0}^n a_k x^k$ then

$$f(a) = \sum_{k=0}^n a_k (x^k + (f)) = \sum_{k=0}^n a_k x^k + (f) = f + (f) = 0. \quad \square$$

Corollary 4.8.2. *For any field F , polynomial $f \in F[x] \exists$ field K s.t.*

1. $K \supset F$ as subring,
2. K finite dimensional vector space over F ,
3. $f(x)$ factorises into linear polynomials in $K[x]$.

Proof. Induction on $n = \deg(f)$. If $n = 1$ take $K = F$. Assume true for $n - 1$. Then \exists field $L \geq F$ s.t. L contains root α of f , L finite dimensional vector space over F by 4.8.1. Induction for $\frac{f(x)}{(x-\alpha)}$ and L , arrive at required K . $\dim_F(K) = \dim_F(L) \cdot \dim_L(K) < \infty$. \square

Corollary 4.8.3. *Any field F , matrix $A \in M_n(F) \exists$ field K s.t.*

1. $K \supset F$ as subring,
2. K finite dimensional vector space over F ,
3. A has eigenvector in K^n and JNF in $M_n(K)$.

Theorem 4.8.4 (Chinese remainder theorem for polynomials). *Let F field, $f \in F[x]$. If $f = q_1^{a_1} \dots q_n^{a_n}$ irreducible factorisation in $F[x]$ then*

$$\phi(h + (f)) = (h + (q_1^{a_1}), \dots, h + (q_n^{a_n}))$$

ring isomorphism between $\frac{F[x]}{(f)}$ and $\frac{F[x]}{(q_1^{a_1})} \times \dots \times \frac{F[x]}{(q_n^{a_n})}$.

Proof. Ring homomorphism $\phi: F[x] \rightarrow \prod_i \frac{F[x]}{(q_i^{a_i})}$, $\phi(h) = (h + (q_1^{a_1}), \dots, h + (q_n^{a_n}))$ has kernel those $h(x)$ divisible by all $q_i^{a_i}$, i.e. (f) . By first isomorphism (2.4.4) $\frac{F[x]}{(f)} \cong \text{im}(\psi)$.

ϕ, ψ linear maps of vector spaces over F and $\frac{F[x]}{(f)}$, $\frac{F[x]}{(q_1^{a_1})} \times \dots \times \frac{F[x]}{(q_n^{a_n})}$ same dimension: $\deg(f)$. \square

4.9 Application to linear maps

Definition 59 (Idempotents). F field, $f = q_1^{a_1} \dots q_n^{a_n} \in F[x]$ factorised into distinct irreducible elements in $F[x]$. Let 1_j be identity element of $\frac{F[x]}{(q_j^{a_j})}$. Then $e_j = (0, \dots, 0, 1, 0, \dots, 0) \in \frac{F[x]}{(f)}$ called *idempotents*.

Proposition 4.9.1. *Idempotents e_j satisfy*

1. $\sum_{j=1}^n e_j = 1$
2. $e_j \cdot e_j = e_j$
3. $e_i \cdot e_j = 0 \quad i \neq j$.

V vector space over F , $\dim n$. Pick $v \in V$, linear map

$$\pi_v: F[x] \rightarrow V, \quad \pi_v(h(x)) = (\pi(T))(v).$$

Proposition 4.9.2. $\ker(\pi_v)$ *non-zero ideal.*

Proof. π_v linear maps so kernel is vector subspace. $F[x]$ infinite dim, V finite dim, so non-zero kernel. RTP kernel ideal:

$$\begin{aligned} h \in \ker(\pi_v) &\implies \\ \pi_v(fh) &= f(T)(h(T)(v)) \\ &= f(T)(0) = 0 \implies fh \in \ker(\pi_v). \quad \square \end{aligned}$$

Definition 60. *Minimal polynomial of T at v $\mu_{v,T}$ s.t. $(\mu_{v,T}) = \ker(\pi_v)$.*

$\mu_{v,T} \mid \mu_T$.

Definition 61. *Characteristic polynomial of $T: V \rightarrow V$, $\chi_T(x) = \det(A - xI)$ where A matrix of T .*

Consider $R = \frac{F[x]}{(\chi_T)}$. $\forall r \in R$, $r(T): V \rightarrow V$ well defined. $\chi_T = q_1^{a_1} \dots q_m^{a_m}$ prime factorisation of χ_T in $F[x]$, e_j corresponding idempotents in R . Let

$$V_j = V(f_j) = \{v \in V : (q_j^{a_j}(T))(v) = 0\} = \{v \in V : \mu_{v,T} \mid q_j^{a_j}\} \leq V.$$

Definition 62. V_j as defined above *primary component* of V .

Proposition 4.9.3 (Primary decomposition). V_j *image of $e_j(T)$ and*

$$V = V_1 \oplus \dots \oplus V_m.$$

4.10 Cyclic vector spaces

Definition 63. (V, T) where V finite dimensional vector space over F , $T: V \rightarrow V$ linear called *cyclic vector space* if \exists polynomial $f(x) \in F[x]$ and linear bijection $\psi: \frac{F[x]}{(f)} \rightarrow V$ s.t.

$$\psi(hx + (f)) = T(\psi(h + (f))) \quad \forall h \in F[x].$$

Theorem 4.10.1. (V, T) *cyclic iff $\mu_T \sim \chi_T$.*