MATH3030 Tutorials with answer

Contents

MATH3030 Tutorial 1

J. SHEN

14 September, 2022

1 Review of S_n

1.1 Definition

Recall that, given an integer $n \geq 2$, the n-th symmetric group S_n is the set of bijective maps from the set $I_n = \{1, ..., n\}$ onto itself equipped with the composition of maps.

1.2 Cycle Decomposition, Product of Transpositions

Theorem 1.1. *Each permutation can be written as a product of disjoint cycles.*

We will assume this theorem, and work the following example to devise our algorithm. To prove the theorem, you then only need to make this algorithm precise and formal and check its validity.

(HW1 Optional part Q2): Express the permutation of $\{1, 2, 3, 4, 5, 6, 7, 8\}$ as a product of disjoint cycles, then as a product of transpositions:

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 \end{pmatrix}$=(18)(364)(57)=(18)(36)(64)(57).

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 \end{pmatrix}$=(134)(26)(587)=(13)(34)(26)(58)(87).

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 7 & 2 & 5 & 8 & 6 \end{pmatrix}$=(13478652)=(13)(34)(47)(78)(86)(65)(52).

1.3 A map from S_n to $\mathrm{GL}_n(\mathbb{R})$

We define here a matrix $R_g \in M_n(\mathbb{R})$ for any $g \in S_n$.

Let $n \in \mathbb{Z}_{>0}$. Let $\{e_1, e_2, ..., e_n\}$ be the standard basis of $\mathbb{R}^n$. We may consider g as permuting the indices of this basis, that is, we let $g.e_i = e_{g(i)}$. Note that **this extends to a linear transformation** $\rho_g : \mathbb{R}^n \to \mathbb{R}^n$. We let R_g be the $n \times n$ real matrix that is associated to ρ_g.

For example, let $g = (1, 2, 3), h = (1, 2)$, then $g \circ h = (1, 3)$ and $h \circ g = (2, 3)$.

$$R_g = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, R_h = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

$$R_{g\circ h} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, R_{h\circ g} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

$$R_g R_h = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, R_h R_g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Theorem 1.2. *In general, $\rho_{g\circ h} = \rho_g \circ \rho_h$, and so $R_{g\circ h} = R_g R_h$. Therefore, we have a group homomorphism $\rho : S_n \to \mathrm{Aut}(\mathbb{R}_n)$, or a group homomorphism $R : S_n \to \mathrm{GL}_n(\mathbb{R})$. These are called the regular representation of S_n.*

Proof.

For each $i = 1, 2, ..., n$, $\rho_{g\circ h}(e_i) = e_{g\circ h(i)} = \rho_g(\rho_h(e_i))$. Since $\rho_{g\circ h}$ and $\rho_g \circ \rho_h$ are linear operators from $\mathbb{R}^n$ to $\mathbb{R}^n$, and they agree on a basis, they must be equal: $\rho_{g\circ h} = \rho_g \circ \rho_h$.

Taking their corresponding matrices, we get $R_{g\circ h} = R_g R_h$.

1.4 Sign of a permutation

Recall that the determinant function $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is a group homomorphism. We may now compose this with R and get a group homomorphism $\det \circ R : S_n \to \mathbb{R}^\times$.

Note that the image of $\det \circ R$ is $\{\pm 1\}$. We define $\mathrm{sgn} = \det \circ R$. Then $\mathrm{sgn}(gh) = \mathrm{sgn}(g) \circ \mathrm{sgn}(h)$ for any $g, h \in S_n$. Note that a transposition has sign -1. Therefore, if g is a product of an odd number of transpositions, $\mathrm{sgn}(g) = -1$, and we call g an **odd permutation**. On the other hand, if g is a product of an even number of transpositions, $\mathrm{sgn}(g) = 1$, and we call g an **even permutation**.

We have also shown that the product of an odd number of transpositions is never equal to the product of an even number of transpositions.

Decide the sign/parity of each of the permutations in 1.2.

Answer:

The permutation in (a) is even. The permutations in (b) and (c) are odd.

1.5 Conjugate Formula

Computation:

$(1,2,3)(1,2,3,4)(1,2,3)^{-1}$=(2,3,1,4).

$g(1,2,3,4)g^{-1}$=$(g(1), g(2), g(3), g(4))$.

$g(1,2,4)(3,5)g^{-1}$=$(g(1), g(2), g(4))(g(3), g(5))$.

Question: Are elements of the same cycle structure conjugate to each other? (For example: find $g \in S_7$ such that $g(2,3,5,7)(1,6)g^{-1} = (1,4,7,3)(2,5)$.)

Answer:

Yes. One may write out all the implicit 1-cycles, and match them. In this example, $g(2,3,5,7)(1,6)g^{-1} = g(2,3,5,7)(1,6)(4)g^{-1} = (g(2), g(3), g(5), g(7))(g(1), g(6))$ $(g(4)) = (1,4,7,3)(2,5)(6)$. We may make g map 2,3,5,7,1,6,4 to 1,4,7,3,2,5,6 respectively. Both are lists of elements in $\{1,2,3,4,5,6,7\}$, and thus $g \in S_7$.

1.6 Some sets of generators of S_n

Try to think of several sets of generators of S_n.

Answer: $I_1 =$ All transpostions in S_n.

$I_2 = \{(1,2),(2,3),...,(n-1,n)\}$.

$I_3 = \{(1,2),(1,3),...,(1,n)\}$

$I_4 = \{(1,2,...,n)(1,2)\}$

......

MATH3030 Tutorial 2

J. SHEN

21 September, 2022

2 Normal subgroups

2.1 Conjugate elements

The concept of conjugation is very important in algebra. We say that $g, h \in G$ are **conjugate** in G if $h = xgx^{-1}$ for some $x \in G$. This is an equivalence relation. The **conjugacy class** $[g]$ of g is the set of elements in G that are conjugate to g.

Note that two matrices $A, B \in \mathrm{GL}_n(F)$ are conjugate exactly when they are similar, and that two permutations g, h are conjugate exactly when they have the same cycle decomposition type (1.5). We used similar matrices to compute matrix powers.

Conjugate elements have a lot in common: Conjugate elements have the same order. Conjugate matrices have the same determinant, and conjugate cycles have the same parity and so on. The basic reason is that **conjugation by x defines an automorphism** $c_x : G \to G$, and conjugate elements are related by this automorphism.

2.2 Normal subgroups

Note that $\mathrm{SL}_n(F) < \mathrm{GL}_n(F)$ is the subgroup of elements of determinant 1, and $A_n < S_n$ is the subgroup of even permutations. These subgroups are unions of conjugate classes and are normal subgroups:

Definition 2.1. A subgroup N of G is said to be a **normal group** if for any $g \in G$, $a \in N$, the conjugate $gag^{-1} \in N$. We write $N \lhd G$.

The kernel of a group homomorphism $\phi : G \to H$ is a normal subgroup of G. This generalizes two examples above: $\mathrm{SL}_n(F) = \ker(\det)$, and $A_n = \ker(\mathrm{sgn})$.

Normal subgroups are analogues of ideals in ring theory. The natural multiplication law $aH.bH = (ab)H$ on G/H is well-defined exactly when $H \lhd G$. In this case, this law gives a group structure on G/H.

2.3 Equivalent definitions

Theorem 2.1. *Let H be a subgroup of G. The following are equivalent:*

1. *For any $g \in G$, $gHg^{-1} \subseteq H$.*
2. *For any $g \in G$, $gHg^{-1} = H$.*
3. *For any $g \in G$, $gH \subseteq Hg$.*
4. *For any $g \in G$, $gH = Hg$.*
5. *Every left coset of H in G is also a right coset in G.*

Proof. ($1 \iff 3$): Suppose $gHg^{-1} \subseteq H$. Then $gH = gHg^{-1}g \subseteq Hg$. Suppose $gH \subseteq Hg$, then $gHg^{-1} \subseteq Hgg^{-1} = H$. We can show $2 \iff 4$ in the same manner.

($3 \iff 4$) That $4 \implies 3$ is obvious. On the other hand, suppose we have $g'H \subseteq Hg'$ for any $g' \in G$. Fix a $g \in G$, then $gH \subseteq Hg$ and $g^{-1}H \subseteq Hg^{-1}$ as $g, g^{-1} \in G$. Thus, we have $Hg = gg^{-1}Hg \subseteq gHg^{-1}g = gH$. Therefore, $gH = Hg$.

($4 \iff 5$) Assuming 4, then every left coset gH of H in G is also equal to a right coset Hg in G.

Conversely, assuming 5, then for any $g \in G$, gH is a right coset in G. But $g \in gH$, so gH must be the right coset Hg.

2.4 Normal subgroups of S_3, S_4

List all nontrivial proper subgroups of S_3 on the table in the studying guide. Which of them is normal?

Answer. All the nontrivial subgroups of S_3 are $\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle, \langle(123)\rangle$. Since a normal subgroup must contain whole conjugate classes, $A_3 = \langle(123)\rangle$ is the only normal subgroup among them.

Write down the conjugate classes of elements in S_4. Normal subgroups must contain whole conjugate classes. Hence, list all nontrivial proper normal subgroups of S_4.

Answer. There are 5 conjugate classes: $[1], [(12)], [(123)], [(1234)], [(12)(34)]$, of sizes 1, 6, 8, 6, 3 respectively. If $N \lhd S_4$ is a nontrivial and proper normal subgroup of S_4, then $|N| \mid 24$, and $|N|$ is a sum of the numbers appearing above. Thus $|N| = 1 + 3$ or $1 + 3 + 8$ by enumeration. These correspond to the two cases $N = K = \{1, (12)(34), (13)(24), (14)(23)\}$ and $N = A_4$ respectively. The group K is the standard realization of the Klein 4 group.

2.5 Normal subgroups of S_n, A_n

Having figured out all the normal subgroups of S_3 and S_4, we mention that for $n \geq 5$, there is only one proper nontrivial normal subgroup of S_n, that is, A_n. On the other hand, A_n is simple (contain no proper nontrivial normal subgroup) for $n \geq 5$. For example, you may refer to the former tutorial notes with link on blackboard.

MATH3030 Tutorial 3

J. SHEN

28 September, 2022

3 Symmetries of solids

We now study several symmetries arising in geometry. We will in particular calculate the group of isometries of a regular tetrahedron (正四面体), a regular cube (正方体) or a regular octahedron (正八面体) and a regular dodecahedron (正十二面体) or a regular icosahedron (正二十面体).

3.1 Isometries

Let $X \subset \mathbb{R}^n$ be a bounded geometric shape. We consider the set of isometries of $\mathbb{R}^n$ that preserves X. That is, let $G = \{\phi : |\phi(x) - \phi(y)| = |x - y| \text{ for any } x, y \in \mathbb{R}^n, \phi(X) = X\}$. An **isometry** of $\mathbb{R}^n$ is a distance preserving map f from $\mathbb{R}^n$ to itself.

We know that [Artin, 6.2] any isometry ϕ is a rotation or reflection followed by a translation, that is, $\phi = t_v \circ r$, where $r \in \mathrm{O}_n(\mathbb{R})$, and $t_v(x) = x + v$ is translation by $v \in \mathbb{R}^n$. When $\det(r) = 1$, r is orientation-preserving, while if $\det(r) = -1$, r is orientation-reversing.

We will be mostly interested in the case where $G = \mathrm{Aut}(X)$ is finite. In this scenario, any $g \in G$ always fixes the center of mass x of X. Then G has a fixed point, which we may take as the origin. Then any $g \in G$ is an isometry that fixes the origin, then $|gx| = |x|$, $|gy| = |y|$, $|gx - gy| = |x - y|$ for any $x, y \in \mathbb{R}^n$. Note that $\langle x, y\rangle = ((|x|^2 + |y|^2) - |x - y|^2)/2$, we see that $\langle gx, gy\rangle = \langle x, y\rangle$. One may further show that g is linear [Artin theorem 6.2.3, (b) $\implies$ (c)]. Therefore, $g \in \mathrm{O}_n(\mathbb{R})$.

Conclusion: Any finite group of the symmetry of a geometric shape is a subgroup of $\mathrm{O}_n(\mathbb{R})$. Therefore, we may start by understanding $\mathrm{O}_2(\mathbb{R})$ and $\mathrm{O}_3(\mathbb{R})$.

3.2 $\mathrm{SO}_2(\mathbb{R})$ and $\mathrm{O}_2(\mathbb{R})$

Recall that $\mathrm{O}_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) : A^T A = I_2\} = \{T : \mathbb{R}^2 \to \mathbb{R}^2 \text{ linear} \mid \langle Tv, Tw\rangle = \langle v, w\rangle \text{ for any } v, w \in \mathbb{R}^2\}$ and $\mathrm{SO}_2(\mathbb{R}) = \{A \in \mathrm{O}_2(\mathbb{R}) : \det(A) = 1\}$.

Exercise 1. Show that $\mathrm{SO}_2(\mathbb{R}) = \{\begin{pmatrix} \cos(x) & -\sin(x) \\ \sin(x) & \cos(x) \end{pmatrix} : x \in \mathbb{R}\}$. Hence show that $\mathrm{SO}_2(\mathbb{R}) \simeq \mathbb{R}/\mathbb{Z}$.

Proof. Note that $A \in \mathrm{SO}_2(\mathbb{R}) \iff A^{-1} = A^T$ and $\det(A) = 1$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Since $A^{-1} = A^T$, we have $a = d, b = -c$. Since $\det(A) = 1$, we have $1 = ad - bc = a^2 + c^2$. Then $a = \cos(x), c = \sin(x)$ for some $x \in \mathbb{R}$. Thus $A = \begin{pmatrix} \cos(x) & -\sin(x) \\ \sin(x) & \cos(x) \end{pmatrix}$. Denote this matrix A as $A(x)$.

Define $\phi : \mathbb{R} \to \mathrm{SO}_2(\mathbb{R})$ by $\phi(x) = A(2\pi x)$. One can verify that $\phi(x + y) = \phi(x)\phi(y)$, and ϕ is surjective, with kernel $\mathbb{Z}$. Then by the first isomorphism theorem of groups, $\mathbb{R}/\mathbb{Z} \simeq \mathrm{SO}_2(\mathbb{R})$.

Exercise 2. Note that by Exercise 1, any element in $\mathrm{SO}_2(\mathbb{R})$ is a rotation. Show that any element in $\mathrm{O}_2(\mathbb{R}) - \mathrm{SO}_2(\mathbb{R})$ is a reflection (Hint: It suffices to show that ± 1 are eigenvalues of A).

Proof. Let $A \in O_2(\mathbb{R}) - \mathrm{SO}_2(\mathbb{R})$. Then $\det(A) = -1$. $\det(A+I) = \det(A+A^T A) = \det(A)\det(I + A^T) = -\det(I + A)$. Therefore, $\det(A + I) = 0$, and -1 is an eigenvalue of A. Similarly, or using the product of all eigenvalues is $\det(A) = -1$, we see that 1 is the other eigenvalue of A.

Thus A fixes a nonzero vector v, an sends another nonzero vector w to $-w$. It is easy to see that $\langle v, w\rangle = 0$, as $\langle v, -w\rangle = \langle Av, Aw\rangle = \langle v, w\rangle$. The two vectors v, w form an orthogonal basis of $\mathbb{R}^2$, and we see that A is the reflection along the line $\{kv : k \in \mathbb{R}\}$.

Exercise 3. Show that every finite subgroup of $\mathrm{SO}_2(\mathbb{R})$ is isomorphic to C_n for some n, and every finite subgroup of $\mathrm{O}_2(\mathbb{R})$ is isomorphic to C_n or D_n for some n.

Proof. A finite subgroup of $\mathrm{SO}_2(\mathbb{R})$ corresponds to that of $\mathbb{R}/\mathbb{Z}$, by Exercise 1. Let $G < \mathbb{R}/\mathbb{Z}$ be finite. For each $g \in G$, we take $\overline{g}$ be the unique element in $(g+\mathbb{Z}) \cap [0, 1)$.

We may assume $|G| > 1$. Then there is a unique element g in G with smallest postive $\overline{g}$. Then one can show that $G = \langle g \rangle$. Thus G is cyclic, and thus isomorphic to C_n.

Let $H < \mathrm{O}_2(\mathbb{R})$. Let $H' = H \cap \mathrm{SO}_2(\mathbb{R})$. Then $H' < \mathrm{SO}_2(\mathbb{R})$, hence is isomorphic to some C_n.

Case 1: $H' = H$. Then $H \simeq C_n$.

Case 2: $H' \subsetneq H$. Take any $s \in H - H'$. We claim that $H = H' \sqcup H's$. For any $h \in H - H'$, $hs \in H$, and $\det(hs) = -1 \times -1 = 1$. Thus $hs \in H' = H \cap \mathrm{O}_2(\mathbb{R})$. By Exercise 2, $s^2 = 1$, thus $h = hss \in H's$. Therefore, $H = H' \sqcup H's$.

It remains to note that $srs = r^{-1}$ for any rotation $r \in \mathrm{SO}_2(\mathbb{R})$. To see this, choose orthonormal basis e_1, e_2 such that $s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. If r is the matrix $A(x)$ as defined in Exercise 1, then $sA(x)s = A(-x) = r^{-1}$ by direct computation.

To conclude, we have shown $H' \simeq C_n = \langle r | r^n = 1 \rangle$, and $H = H' \sqcup H's$, with $s^2 = srsr = 1$. Then $H = \langle r, s | r^n = s^2 = rsrs = 1 \rangle = D_n$. (More details on this: Because H is generated by r, s and $r^n = s^2 = rsrs = 1$, we have a surjective map $\phi : D_n \to H$. Because $|D_n| = |H| = 2n$, ϕ is bijective, and thus $D_n \simeq H$.)

3.3 $\mathrm{SO}_3(\mathbb{R})$

We will focus on orientation-preserving isometries in 3D, which are achievable in our 3D space. Thus, we consider $\mathrm{SO}_3(\mathbb{R}) = \{A \in M_3(\mathbb{R}) : A^T A = I_3, \det(A) = 1\}$.

Exercise 4. Let $A \in \mathrm{SO}_3(\mathbb{R})$. Show that there exists a $v \in \mathbb{R}^3 - \{0\}$ such that $Av = v$.

Proof. We want to show that 1 is an eigenvalue of A. It suffices to show that $\det(A - I) = 0$.

Since $A \in \mathrm{SO}_3(\mathbb{R})$, $\det(A - I) = \det(A - A^T A) = \det(A)\det(I - A^T) = 1 \times \det(I - A) = \det(-I)\det(A - I) = (-1)^3 \det(A - I)$. Thus $\det(A - I) = 0$.

Note that then A fixes the plane V orthogonal to v, and A restricts to an element of $\mathrm{SO}(V)$. Therefore, A is a rotation along the $v-$axis. Because $\mathrm{SO}_3(\mathbb{R})$ is a group, it follows that a composition of two rotations in $\mathbb{R}^3$ is again a rotation. Think about how nontrivial it is in geometry.

3.4 The isometry of regular solids

We now calculate the groups of orientation-preserving isometries of regular solids. Let T be a regular tetrahedron, C be a regular cube, O be a regular octahedron, D be a regular dodecahedron, and I be a regular icosahedron, all centered at the origin.

Exercise 5. For X being each of the above shapes, Calculate $|\operatorname{Aut}(X)|$. Here, we only consider orientation-preserving isometries in $\mathbb{R}^3$, i.e. we consider $\operatorname{Aut}(X) < \mathrm{SO}_3(\mathbb{R})$. (Hint: How many ways can you fit a cube of side length 2 in $[-1,1]^3$.)

Answer. There are 12 ways to fit a regular tetrahedron in a given model. Each of the 4 faces can placed at the bottom, and each of the remaining 3 faces can be placed in front of you. Therefore, $|\operatorname{Aut}(T)| = 12$. Similarly, $|\operatorname{Aut}(C)| = 6 * 4 = 24$, and $|\operatorname{Aut}(D)| = 12 * 5 = 60$.

Exercise 6. What is the group $\operatorname{Aut}(T)$? (*What is $\operatorname{Aut}(C)$?)

Answer. By numbering the 4 vertices of a tetrahedron as $1, 2, 3, 4$, we see that each element $g \in \operatorname{Aut}(T)$ permutes the 4 vertices. Also, each g is decided by where the 4 vertices goes. Thus, we get an inclusion $\operatorname{Aut}(T) \hookrightarrow S_4$. Since $|\operatorname{Aut}(T)| = 12$ has index 2 in S_4, it must be a normal subgroup in S_4, which is A_4 by our discussion in Section 2.4. We can see that the 8 elements in the conjugate class $[(123)]$ corresponds to the 8 rotations along each of the 4 vertices, and the 3 elements in the conjugate class $[(12)(34)]$ corresponds to the 3 reflections along the 3 pairs of opposite edges.

What is $\operatorname{Aut}(C)$?

The automorphism of a cube is S_4. Label the 4 pairs of opposite vertices as 1,2,3,4. Then $\operatorname{Aut}(C)$ permutes the 4 pairs, and each $g \in \operatorname{Aut}(C)$ affords a permutation $\phi_g \in S_4$. This way, we get a map $\phi : \operatorname{Aut}(C) \to S_4$, and it is a group homomorphism. For example, if g moves pair i to where pair j originally lies, and h moves pair j to where pair k originally lies, then $\phi_g(i) = j, \phi_h(j) = k$, and $h \circ g$ moves pair i to where pair k originally lies. Then $\phi_{h\circ g}(i) = k = \phi_h \circ \phi_g(i)$. Therefore, $\phi_{h\circ g} = \phi_h \circ \phi_g$. This shows that ϕ is a group homomorphism.

One may then proceed to show that ϕ is injective or to show that ϕ surjective, then conclude that ϕ is isomorphism by comparing the sizes of domain and codomain. For example, we show that ϕ is injective:

Suppose $\phi(g) = \text{id}$. Suppose $C = [-1,1]^3$, then $\phi(g)$ preserves each of the four lines $(\pm 1, \pm 1, 1)\mathbb{R}$. Moreover, let $v_1 = (1,1,1), v_2 = (-1,1,1), v_3 = (-1,-1,1), v_4 = (1,-1,1)$. Then each of v_1, v_2, v_3, v_4 is an eigenvector of A with eigenvalue 1 or -1. Any three of the 4 vectors are linearly independent. Let E_λ be the eigenspace of A with eigenvalue λ. Then $e_1, ..., e_4 \in E_1 \cup E_{-1}$. If two of them lies in E_1, and two of them lies in E_{-1}, then $\dim E_1 \geq 2, \dim E_{-1} \geq 2$. But $E_1 \cap E_{-1} = 0$. Contradiction arises. Therefore, at least three of the 4 vectors lies in E_1 or at least three of the 4 vectors lies in E_{-1}. Any 3 of the 4 vectors generate the whole $\mathbb{R}^3$. Therefore, $g = \pm I_3$. Since we require $\det(g) = 1$, $g = I_3 = \text{id}$.

Therefore, $\phi : \text{Aut}(C) \to S_4$ is injective. Then ϕ is an isomorphism because $|\text{Aut}(C)| = |S_4| = 24$.

The automorphism group $\text{Aut}(O) \simeq \text{Aut}(C)$, and $\text{Aut}(D) \sim \text{Aut}(I) \simeq A_5$. The last fact can be found at Artin Algebra section 7.4.

MATH3030 Tutorial 4

J. SHEN

5 October, 2022

4 More on symmetry

4.1 Isometries explained

Let ϕ be an isometry on $\mathbb{R}^n$, i.e, $|\phi(x) - \phi(y)| = |x - y|$ for any $x, y \in \mathbb{R}^n$. We will show that it is an orthogonal linear operator followed by a translation(平移):

Exercise 1. Assume that ϕ is an isometry on $\mathbb{R}^n$ fixing the origin. Show that $\langle \phi(v), \phi(w) \rangle = \langle v, w \rangle$ for all $v, w \in \mathbb{R}^n$, where $\langle -, - \rangle$ is the standard inner product in $\mathbb{R}^n$.

Proof. Let $\phi : \mathbb{R}^n \to \mathbb{R}^n$ be an isometry with $\phi(0) = 0$. Then $|\phi(x)| = |x|$ for any $x \in \mathbb{R}^n$. Note that $\langle \phi(v), \phi(w) \rangle = (|\phi(v)|^2 + |\phi(w)|^2 - |\phi(v) - \phi(w)|^2)/2 = (|v|^2 + |w|^2 - |v - w|^2)/2 = \langle v, w \rangle$.

Exercise 2. Let $v, w \in \mathbb{R}^n$. Suppose $\langle v, v \rangle = \langle v, w \rangle = \langle w, w \rangle$. Show that $v = w$.

Proof. $\langle v - w, v - w \rangle = \langle v, v \rangle + \langle v, w \rangle - 2\langle v, w \rangle = 0$. Therefore, $v - w = 0$.

Exercise 3. Assume that ϕ is an isometry on $\mathbb{R}^n$ fixing the origin. Let $v, w \in \mathbb{R}^n$, show that $\phi(v + w) = \phi(v) + \phi(w)$. Then show that $\phi(\lambda v) = \lambda \phi(v)$ for any $\lambda \in \mathbb{R}$. The conclusion of Exercises 1,3 is that such ϕ lies in $\mathrm{O}_n(\mathbb{R})$.

Proof. By Exercise 1, ϕ preserves inner product. Then

$\langle \phi(v + w), \phi(v + w) \rangle = \langle v + w, v + w \rangle$.

$\langle \phi(v + w), \phi(v) + \phi(w) \rangle = \langle \phi(v + w), \phi(v) \rangle + \langle \phi(v + w), \phi(w) \rangle = \langle v + w, v \rangle + \langle v + w, w \rangle = \langle v + w, v + w \rangle$.

$\langle \phi(v) + \phi(w), \phi(v) + \phi(w) \rangle = \langle \phi(v), \phi(v) \rangle + 2\langle \phi(v), \phi(w) \rangle + \langle \phi(w), \phi(w) \rangle = \langle v, v \rangle + 2\langle v, w \rangle + \langle w, w \rangle = \langle v + w, v + w \rangle$.

By Exercise 2, we conclude that $\phi(v + w) = \phi(v) + \phi(w)$.

We have two approaches for the last part:

A. Imitating this proof, we conclude that $\phi(\lambda v) = \lambda \phi(v)$.

B. By additivity, $\phi : (\mathbb{R}^n, +) \to (\mathbb{R}^n, +)$ is a group homomorphism. Thus $\phi(nv) = n\phi(v)$ for $n \in \mathbb{Z}$. Thus $\phi(v/n) = \phi(v)/n$ for any $n \in \mathbb{Z}_{>0}$. Thus $\phi(rv) = r\phi(v)$ for $r \in \mathbb{Q}$. Using continuity of ϕ to extend to $r \in \mathbb{R}$. (Isometries are continuous by checking the definition.)

Remark. By Exercise 3, ϕ is linear, and by Exercise 1, ϕ preserves the standard inner product $\langle v, w\rangle = v^T w$. If $\phi(v) = Av$, then Exercise 1 implies that $v^T A^T A w = v^T w$ for any $v, w \in \mathbb{R}^n$. Plug in $v = e_i, w = e_j$ for each $1 \leq i, j \leq n$, one sees that $A^T A = I$. Thus we see that $A \in \mathrm{O}_n(\mathbb{R})$ and $\phi \in \mathrm{O}_n(\mathbb{R})$.

Exercise 4. Let ϕ be an isometry on $\mathbb{R}^n$. Show that $\phi = t_v \circ \rho$ for some translation t_v by vector $v \in \mathbb{R}^n$, and some $\rho \in \mathrm{O}_n(\mathbb{R})$.

Proof. The translation $t_v : \mathbb{R}^n \to \mathbb{R}^n$ is defined by $t_v(x) = x + v$ for any $x \in \mathbb{R}^n$. It is clearly an isometry.

Let $v = \phi(0)$. Then $t_{-v} \circ \phi$ is an isometry mapping 0 to 0. Thus $t_v \circ \phi \in \mathrm{O}_n(\mathbb{R})$. Let $\rho = t_{-v} \circ \phi$. Then $\phi = t_v \circ \rho$.

4.2 Symmetry of higher dimensional objects

The higher dimensional analogues of tetrahedrons are regular simplices. For example, note that the convex hull of $\{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)\} \subseteq \mathbb{R}^4$ is a regular tetrahedron. Let $\{e_1, e_2, ..., e_{n+1}\}$ be the standard basis of $\mathbb{R}^{n+1}$. Then the convex hull of $e_1, ..., e_{n+1}$ will be a regular n-simplex. Its full automorphism group is S_{n+1}, and its orientation preserving automorphism group is A_{n+1}.

The higher dimensional analogues of cubes are n-cubes. An n-cube can be realized as $[-1, 1]^n$. Its full automorphism group is $\{\pm 1\}^n \rtimes S_n$. Its orientation preserving automorphism group is its even part.

MATH3030 Tutorial 5

J. SHEN

12 October, 2022

5 Linear Groups

Our next source of examples come from subgroups and quotients of linear groups.

5.1 Some common linear groups

Let k be a field.

$\mathrm{GL}_n(k) := \{A \in M_n(k) \mid \det(A) \neq 0\}$ is called the general linear group.

$\mathrm{SL}_n(k) := \{A \in M_n(k) \mid \det(A) = 1\}$ is called the special linear group.

$\mathrm{O}_n(k) := \{A \in M_n(k) \mid A^T A = AA^T = I_n\}$ is called the orthogonal group.

$\mathrm{T}_n(k) := \{A \in \mathrm{GL}_n(k) \mid a_{ij} = 0 \text{ for any } i > j\}$ is the group of invertible upper-triangular matrices. (This is often also referred to as B, a Borel subgroup of $\mathrm{GL}_n(k)$.)

$\mathrm{U}_n(k) := \{A \in \mathrm{T}_n(k) \mid a_{ii} = 1 \text{ for any } i\}$ is the group of unipotent upper-triangular matrices. (Unipotent means having 1 as the sole eigenvalue. This notation may collide with that of unitary groups, so we will call the latter $U(n, \mathbb{C})$ when necessary.)

$\mathrm{D}_n(k) := \{\mathrm{diag}(a_1, ..., a_n) \mid a_1, ..., a_n \in k^\times\}$ is the group of invertible diagonal matrices. (This is often also referred to as T, to indicate that it is a torus, i.e., isomorphic to $(k^\times)^n$. Unfortunately this collides with our $\mathrm{T}_n(k)$ above. We will stick to our notation.)

$\mathrm{PGL}_n(k) := \mathrm{GL}_n(k)/k^\times$, where $a \in k^\times$ is identified with the scalar matrix $aI_n = \mathrm{diag}(a, a, ..., a)$.

5.2 Properties of $\mathrm{GL}_n(k)$

Exercise 1. Suppose $|k| = q < \infty$. What is the order of $|\mathrm{GL}_n(k)|$?

Answer. For $A \in M_n(k)$, write $A = (A_1|A_2|...|A_n)$, where A_i is the i-th column of A. Then $A \in \mathrm{GL}_n(k) \iff A_1, ..., A_n$ are linearly independent. A_1 can be chosen arbitrarily from $k^n - \{0\}$, which has cardinality $q^n - 1$. After selecting $A_1, ..., A_i$, A_{i+1} should lie in $k^n - \langle A_1, ..., A_i \rangle$, which has cardinality $q^n - q^i$. Multiply these numbers up, we get $|\operatorname{GL}_n(k)| = (q^n - 1)(q^n - q)...(q^n - q^{n-1}) = \prod_{i=0}^{n-1}(q^n - q^i)$.

Exercise 2. Suppose $|k| = q < \infty$. What are the orders of $|\operatorname{SL}_n(k)|$ and $|\operatorname{PGL}_n(k)|$?

Answer. We have two short exact sequences:

$$\begin{tikzcd} 1 \arrow[r] & \operatorname{SL}_n(k) \arrow[r] & \operatorname{GL}_n(k) \arrow[r, "\det"] & k^\times \arrow[r] & 1 \end{tikzcd}$$

$$\begin{tikzcd} 1 \arrow[r] & k^\times \arrow[r] & \operatorname{GL}_n(k) \arrow[r] & \operatorname{PGL}_n(k) \arrow[r] & 1. \end{tikzcd}$$

Therefore, $|\operatorname{SL}_n(k)| = |\operatorname{PGL}_n(k)| = |\operatorname{GL}_n(k)|/|k^\times| = \frac{1}{q-1}\prod_{i=0}^{n-1}(q^n - q^i)$.

Remark. In general, $\operatorname{SL}_n(k)$ may not be isomorphic to $\operatorname{PGL}_n(k)$. The natural map $\operatorname{SL}_n(k) \to \operatorname{PGL}_n(k)$ has the same kernel and cokernel as the map $k^\times \to k^\times$ by $a \mapsto a^n$.

Exercise 3. Show that $Z(\operatorname{GL}_n(k)) = k^\times$. (More precisely, $Z(\operatorname{GL}_n(k)) = k^\times I_n$.)

Proof. We may assume that $n \geq 2$. Suppose $A \in Z(\operatorname{GL}_n(k))$. Let e_{ij} be the matrix with ij-entry 1, and other entries 0. Then for $i \neq j$, $I_n + e_{ij} \in \operatorname{GL}_n(k)$. Then $A(I_n + e_{ij}) = (I_n + e_{ij})A$. Therefore, $Ae_{ij} = e_{ij}A$.

Note that $Ae_{ij} = a_{1i}e_{1j} + ...a_{ni}e_{nj}$, and $e_{ij}A = a_{j1}e_{i1} + ... + a_{jn}e_{in}$. Therefore, both sides only have e_{ij} term, and $a_{i'i} = 0$ if $i' \neq i$, $a_{j'j} = 0$ if $j' \neq j$, and $a_{ii} = a_{jj}$. As (i, j) runs through unequal pairs of $\{1, ..., n\}$, we see that $a_{ij} = 0$ for any $i \neq j$, and $a_{ii} = a_{jj}$ for any i, j. Thus $A = \operatorname{diag}(a, a, ..., a)$ for $a = A_{11} \in k^\times - \{0\}$.

Clearly, scalar matrices commutes with any other matrix. Thus, $Z(\operatorname{GL}_n(k)) = k^\times I_n$.

Remark. Note that the proof above applies also to $\operatorname{SL}_n(k)$, and will show that $Z(\operatorname{SL}_n(k)) = \mu_n(k)I_n = \{\operatorname{diag}(a, a, ..., a) \mid a \in k^\times, a^n = 1\}$.

Fact. For $n \geq 3$ or when $|k| \geq 3$, $[\operatorname{GL}_n(k), \operatorname{GL}_n(k)] = \operatorname{SL}_n(k)$. For $n \geq 3$ or when $|k| \geq 4$, $[\operatorname{SL}_n(k), \operatorname{SL}_n(k)] = \operatorname{SL}_n(k)$.

MATH3030 Tutorial 6

J. SHEN

19 October, 2022

6 Generators and Relations

We study the concepts of generators and relations in detail and solve some questions in previous homework sets. We refer to Artin §7.9-7.10.

6.1 Free groups

Let A be a set. The free group $\mathscr{F}(A)$ on A consists of all finite length reduced words with letters in $\{a : a \in A\} \cup \{a^{-1} : a^{-1} \in A\}$, where empty word ( ) is allowed, and multiplication is given by juxtaposition and reduction.

Let $W(A)$ be the set of all words with letters in $\{a : a \in A\} \cup \{a^{-1} : a^{-1} \in A\}$. Reduction R means cancelling out consecutive terms aa^{-1} or $a^{-1}a$ in a word $w \in W(A)$ as far as possible. Two words $w, w' \in W(A)$ are equivalent if and only if they have the same reduced form: $w \sim w' \iff R(w) = R(w')$. Then $F(A)$ may also be defined as $W(A)/\sim$.

The most important property for free groups is the mapping property:

Proposition 6.1. *Let F be the free group on a set $A = \{a, b, ...\}$, and let G be a group. Any map of sets $f : A \to G$ extends in a unique way to a group homomorphism $\phi : F \to G$, such that $\phi(a) = f(a)$ for any $a \in A$.*

6.2 Generators

Let G be a group, and let $S = \{x_1, ..., x_n\}$ be a subgroup of G. Recall that the **subgroup of G generated by S** is the intersection of all subgroups of G that contains H. It also has the description $\{g_1...g_l : \text{each } g_i \in S \cup S^{-1}\}$. That is,

$$\langle S\rangle = \bigcap_{S\subseteq H\leq G} H = \{g_1...g_l : \text{each } g_i \in S \cup S^{-1}\}.$$

The inclusion $S \hookrightarrow G$ induces a group homomorphism $\phi : F(S) \to G$ via proposition 6.1. The image of ϕ is exactly $\langle S \rangle$. Therefore, G is generated by S if and only if ϕ is surjective.

6.3 Relations

Let R be a subset of a group G. The intersection N of all normal subgroups of G contains R is again a normal subgroup of G, and is called the normal subgroup generated by R. That is,

$$N = \bigcap_{R \subseteq H \lhd G} H.$$

Elements of N may be described as follows (Artin Lemma 7.10.3):

(a) An element of G is in N if it can be obtained from the elements of R using a finite sequence of the operations of multiplication, inversion, and conjugation.

(b) Let R' be the set consisting of elements r and r^{-1} with r in R. An element of G is in N if it can be written as a product $y_1 ... y_r$ of some arbitrary length, where each y_ν is a conjugate of an element of R'.

Let $F(S)$ be the free group on a set $S = \{x_1, ..., x_n\}$, and let $R = \{r_1, ..., r_k\} \subseteq F(S)$. The group **generated by S with relations** $r_1 = ... = r_k = 1$ is the quotient group $G = F(S)/N(R)$, where $N(R)$ is the normal subgroup of $F(S)$ generated by R. This group is often denoted by $\langle x_1, ..., x_n | r_1, ..., r_k \rangle$ or $\langle x_1, ..., x_n | r_1 = ... = r_k = 1 \rangle$.

Proposition 6.2. *Let $S = \{x_1, ..., x_n\}$ be a subset of a group G, and let $R = \{r_1, ..., r_n\}$ be a set of relations of G among the elements of S. Let $F(S)$ be the free group on S, and $N(R)$ the normal subgroup of $F(S)$ generated by R. Then there is a canonical homomorphism $\psi : F(S)/N(R) \to G$ that sends x_i to x_i. Moreover, ψ is surjective if and only if S generates G.*

Exercise 1. When $|A| > 1$, show that the free group $F(A)$ is nonabelian.

Proof. There exists a group G that is nonabelian (e.g. S_3). Then there exists $g, h \in G$ such that $gh \neq hg$. Let x, y be two distinct elements in A. Define a function $f : A \to G$ by $f(x) = g, f(y) = h$, and $f(z) = e_G$ for any $z \neq x, y$. Let $\phi : F(A) \to G$ be the group homomorphism corresponding to f. Then $\phi(x) = a, \phi(y) = b$. If $xy = yx$, then $ab = \phi(xy) = \phi(yx) = ba$. Contradiction arises. Then $xy \neq yx$, so $F(A)$ cannot be abelian.

Exercise 2. Show that $\langle x, y | x^n = y^2 = xyxy = 1\rangle$ has at most $2n$ elements, and thus show that it is isomorphic to D_n.

Proof. Any element g in $G = \langle x, y | x^n = y^2 = xyxy = 1\rangle$ has the form $x^{i_1}y^{j_1}...x^{i_r}y^{j_r}$ for some $r \geq 0$, $i_1, ..., i_r, j_1, ..., j_r \in \mathbb{Z}$. Using $x^n = y^2 = 1$, one can assume each $i_1, ..., i_r \in \{0, 1, ..., n-1\}$, and each $j_1, ..., j_r \in \{0, 1\}$. Since $xyxy = 1$, $yx = x^{-1}y$. Then one can move y's to the end of the expression. Then $g = x^i y^j$ for some $i \in \mathbb{Z}, j \in \mathbb{Z}$. Use $x^n = y^2 = 1$ again to reduce i to $\{0, 1, ..., n-1\}$ and j to $\{0, 1\}$. Then $|G| \leq 2n$.

There exists elements r, s in D_n such that $r^n = s^2 = rsrs = 1$, which generate D_n. Define the map $\phi : \langle x, y\rangle \to D$ such that $\phi(x) = r, \phi(y) = s$. Then ϕ is surjective, and factors through the group G. Then we get a map $\psi : G \to D_n$, which is surjective. But $|G| \leq 2n, |D_n| \geq 2n$. Then ψ is bijective, so $G \simeq D_n$.

Exercise 3. Let a, b be distinct elements of order 2 in a group G. Suppose that ab has finite order $n \geq 3$. Prove that the subgroup $\langle a, b\rangle$ generated by a and b is isomorphic to the dihedral group D_n (which has $2n$ elements).

Proof. The subgroup $\langle a, b\rangle = \langle a, ab\rangle$ satisifies the relation: $a^2 = e, (ab)^n = e, b^2 = (a^{-1}ab)^2 = e$. Hence we have a surjective group homomorphism $\phi : D_n = \langle r, s \mid r^n = s^2 = rsrs = 1\rangle \to \langle a, b\rangle$ with $\phi(s) = a, \phi(r) = ab$.

Note that $\langle ab\rangle < \langle a, ab\rangle$. Because $\text{ord}(ab) \geq 3$, $ab \neq (ab)^{-1}$. Then $ab \neq ba$, so $\langle a, b\rangle$ is not abelian. Therefore, $[\langle a, b\rangle : \langle ab\rangle] \geq 2$. Then $|\langle a, b\rangle| \geq 2n$. Since $\phi : D_n \to \langle a, ab\rangle$ is surjective, it must be that $|\langle a, b\rangle| = 2n$, and that ϕ is bijective. Therefore, $\langle a, b\rangle \simeq D_n$.

Exercise 4. Prove that every finite group is finitely presented.

Proof. Let $X = \{g_1, ..., g_n\}$ be the set of all elements of G, then we can define the surjective homomorphism $\phi : F(X) \to G$ which maps all words to the corresponding words in G. Therefore, G is finitely generated. The relations of G are finitely generated. It suffices to use all the $g_i g_j g_{\phi(i,j)}^{-1} = e$ kind of relation, where $\phi(i, j)$ is such that $g_i g_j = g_{\phi(i,j)}$. The number of generating relations used is n^2.

MATH3030 Tutorial 7

J. SHEN

9 November, 2022

7 Semidirect Product

7.1 Definition

Let G, H be two groups, and let $\theta : H \to \operatorname{Aut}(G)$ be a group homomorphism. Denote $\theta_h = \theta(h) \in \operatorname{Aut}(G)$. We could define the semidirect product of G and H by θ as:

$$G \rtimes_\theta H := (G \times H, \cdot_\theta),$$

where $(g_1, h_1) \cdot_\theta (g_2, h_2) = (g_1\theta_{h_1}(g_2), h_1h_2)$.

Remark. When θ is trivial, this reduces to the usual direct product.

Exercise 1. Check that $G \rtimes H = (G \times H, \cdot_\theta)$ is a group.

Proof. We write $\cdot$ for $\cdot_\theta$ in the following. We will frequently use $\theta_{hh'} = \theta_h\theta_{h'}$ and $\theta_h^{-1} = \theta_{h^{-1}}$. To see this, recall that θ is a homomorphism from H to $\operatorname{Aut}(G)$ and that $\theta_h := \theta(h)$

(Identity) Let $g \in G, h \in H$. Then $(g, h) \cdot (e_G, e_H) = (g\theta_h(e_G), he_H) = (g, h)$, and $(e_G, e_H) \cdot (g, h) = (e_G\theta_{e_H}(g), e_Hh) = (g, h)$. Therefore, (e_G, e_H) is an identity in $G \rtimes H$.

(Inverse) First, $(g, h)\cdot(\theta_{h^{-1}}(g^{-1}), h^{-1}) = (g\theta_h(\theta_{h^{-1}}(g^{-1})), hh^{-1}) = (g\theta_h\theta_{h^{-1}}(g^{-1}), e) = (g\theta_e(g^{-1}), e) = (e, e)$. Second, $(\theta_{h^{-1}}(g^{-1}), h^{-1}) \cdot (g, h) = \theta_{h^{-1}}(g)\theta_{h^{-1}}(g^{-1}), h^{-1}h) = (\theta_{h^{-1}}(g^{-1}g), e)$. Then $(\theta_{h^{-1}}(g^{-1}), h^{-1})$ is the inverse to (g, h).

(Associativity) Take any $g, g', g'' \in G, h, h', h'' \in H$. Then $((g, h) \cdot (g', h')) \cdot (g'', h'') = (g\theta_h(g'), hh') \cdot (g'', h'') = (g\theta_h(g')\theta_{hh'}(g''), hh'h'')$, and $(g, h) \cdot ((g', h') \cdot (g'', h'')) = (g, h) \cdot (g'\theta_{h'}(g''), h'h'') = (g\theta_h(g'\theta_{h'}(g'')), hh'h'') = (g\theta_h(g')\theta_{hh'}(g''), hh'h'')$. The two expressions agree. Thus the associativity holds.

7.2 Internal semidirect product

Note that $G \rtimes H$ contains a copy of G: $G' := \{(g,e) : g \in G\} \simeq G$, and a copy of H: $H' := \{(e,h) : h \in H\} \simeq H$. Note that G', H' satisfies $G'H' = G \rtimes H, G' \cap H' = \{e\}$, and $G' \lhd G \rtimes H$. This is much comparable to the case of direct product. We say that G is an (internal) semidirect product of two normal subgroups N and H if $NH = G$, $N \cap H = \{e\}$, and $N \lhd G$. This is justified by the following:

Proposition 7.1. *Let G be a group. Let $N \lhd G, H < G$ be such that $NH = G$ and $N \cap H = \{e\}$. Let $\theta : H \to \mathrm{Aut}(N)$ be the group homomorphism that that $\theta_h(n) = hnh^{-1}$. Then $N \rtimes_\theta H \simeq G$.*

Proof. Note that $\theta_h = i_h|_N$, the conjugation by h restricted to N. For $h, h' \in H$, $i_h|_N \circ i_{h'}|_N = (i_h \circ i_{h'})|_N = i_{hh'}|_N$. Then $\theta_{hh'} = \theta_h \circ \theta_{h'}$. Hence, $\theta : H \to \mathrm{Aut}(N)$ is a group homomorphism.

Define $\phi : N \rtimes_\theta H \to G$ by $\phi(n,h) = nh$. Then $NH = G$ implies that ϕ is surjective. For $n, n' \in N$, $h, h' \in H$, $(n,h) \cdot_\theta (n',h') = (n\theta_h(n'), hh') = (nhn'h^{-1}, hh')$. Then $\phi((n,h) \cdot_\theta (n',h')) = \phi(nhn'h^{-1}, hh') = nhn'h^{-1}hh' = nhn'h' = \phi(n,h)\phi(n',h')$. Then ϕ is a group homomorphism. The condition $N \cap H = \{e\}$ implies that $\ker(\phi) = \{e\}$. Then ϕ is injective.

It follows that $\phi : N \rtimes_\theta H \to G$ is an isomorphism.

Remark. If further $H \lhd G$, then $N \times H \simeq G$. That is, G is an internal direct product of N and H.

7.3 Example: Groups of order pq

Let p, q be primes, with $p < q$. Let G be a group of order pq. Then there exists a subgroup $P < G$ of order p, and a unique subgroup $Q < G$ of order q (e.g. use Sylow III). Therefore, $Q \lhd G$. Then $G \simeq Q \rtimes_\theta P$, for some $\theta : P \to \mathrm{Aut}(Q)$.

Since $P \simeq \mathbb{Z}_p, Q \simeq \mathbb{Z}_q$, and $\mathrm{Aut}(Q) \simeq \mathbb{Z}_{q-1}$, the number of group homomorphism from P to $\mathrm{Aut}(Q)$ is 1 if $p \nmid q$, and is p if $p \mid q$. Then the only group of order pq is $Q \times P \simeq \mathbb{Z}_{pq}$ if $p \nmid q - 1$. When $p \mid q - 1$, we illustrate the situation by taking $p = 3$, $q = 7$:

Take $P = \langle h | h^3 = 1\rangle$, $Q = \langle g | g^7 = 1\rangle$. Then $\mathrm{Aut}(Q) \simeq \mathbb{Z}_7^\times \simeq \mathbb{Z}_6$: Elements of $\mathrm{End}(Q)$ are $\alpha_i : g^k \mapsto g^{ik}$ for each k. Then $i \in \mathbb{Z}_7$, and $\alpha_i \in \mathrm{Aut}(Q)$ exactly when $i \in \mathbb{Z}_7^\times$. The map $i \mapsto \alpha_i$ gives the isomorphism $\mathbb{Z}_7 \simeq \mathrm{Aut}(Q)$. We know from number theory or from this course (using FTFGAG) that $\mathbb{Z}_7^\times$ is cyclic.

One generator of the cyclic group $\mathbb{Z}_7^\times$ is 3, and the corresponding generator of $\mathrm{Aut}(Q)$ is $\alpha_3 : g^k \mapsto g^{3k}$. A homomorphism $\theta : P \to \mathrm{Aut}(Q)$ shall map x to an order 1 or 3 element in $\mathrm{Aut}(Q)$, and they are α_1, α_2 and α_4. Denote by θ_i the homomorphism with $\theta_i(h) = \alpha_i$, where $i = 1, 2, 4$.

In $G = Q \rtimes_{\theta_i} P$, we write g for (g, e), and h for (e, h) as usual. Then $hg = \theta_h(g)h = g^i h$. The group G satisfies $g^7 = h^3 = 1$, and $hg = g^i h$. Let $G' = \langle g, h | g^7 = h^3 = g^i h g^{-1} h^{-1} = 1\rangle$. Then there is a surjection $G' \twoheadrightarrow G$. But $|G'| \leq 21$, and $|G| = 21$, therefore, that surjection must be a bijection. That is, G has the presentation $\langle g, h | g^7 = h^3 = g^i h g^{-1} h^{-1} = 1\rangle$.

When $i = 1$, we get the usual cyclic group $\mathbb{Z}_7 \times \mathbb{Z}_3 \simeq \mathbb{Z}_{21}$.

The other two groups $Q \rtimes_{\theta_2} P$ and $Q \rtimes_{\theta_4} P$ are in fact isomorphic. Note that $(\theta_2)_h(g) = g^2$, and $(\theta_4)_h(g) = g^4$. Then $(\theta_2)_{h^2}(g) = g^4$. Then the h^2 in $Q \rtimes_{\theta_2} P$ corresponds to the h in $Q \rtimes_{\theta_4} P$. One may verify that $\langle g, h | g^7 = h^3 = g^2 h g^{-1} h^{-1} = 1\rangle \to \langle g, h | g^7 = h^3 = g^2 h g^{-1} h^{-1} = 1\rangle$ by $g \mapsto g, h \mapsto h^{-1}$ extends to a group isomorphism.

Therefore, there are two isomorphism class of groups of order 21. This holds in general for any p, q with $p | q - 1$. When $p = 2$, and q is an odd prime, the two isomorphism classes are C_{2p} and D_p.

MATH3030 Tutorial 8

J. SHEN

16 November, 2022

8 Basic theorems of ring theory

8.1 Properties of ring homomorphisms

Proposition 8.1 (Fraleigh 8th ed. thm 30.11)**.** *Let R be a ring (with 1, not assuming commutativity). Let $\phi : R \to R'$ be a ring homomorphism. Then*

1. $\phi(0) = 0$
2. *For any $a \in R$, $\phi(-a) = -\phi(a)$.*
3. *If S is a subring of R, then $\phi(S)$ is a subring of R'*
4. *If S' is a subring of R', then $\phi^{-1}(S')$ is a subring of R.*
5. *If N is an ideal of R, then $\phi(N)$ is an ideal of $\phi(R)$.*
6. *If N' is an ideal of either R' or $\phi(R)$, then $\phi^{-1}(N')$ is an ideal of R. (Ideals mean two-sided ideals.)*

Proof. Property 1 and 2 follows from $\phi : (R, +) \to (R', +')$ being a group homomorphism.

3. Since S is a subring of R, it is closed under $-, \times$, and $1_R \in S$. Then for $x, y \in \phi(S)$, there exist $a, b \in S$ such that $\phi(a) = x, \phi(b) = y$. Then $a-b, ab \in S$, and so $x - y = \phi(a - b) \in \phi(S)$, and $xy = \phi(ab) \in \phi(S)$. Moreover, $1_{R'} = \phi(1_R) \in \phi(S)$. It follows that $\phi(S)$ is a subring of R'.

4. Let S' be a subring of R'. Then it is closed under $-, \times$, and $1_{R'} \in S'$. For $a, b \in \phi^{-1}(S')$, $\phi(a), \phi(b) \in S'$. Then $\phi(a - b) = \phi(a) - \phi(b) \in S'$ and $\phi(ab) = \phi(a)\phi(b) \in S'$. Since $\phi(1_R) = 1_{R'} \in S'$, $1_R \in \phi^{-1}(S')$. Therefore, $\phi^{-1}(S')$ is a subring of R.

5. Since N is an ideal of R, it is an additive subgroup of R, and for $r \in R$, $n \in N$, $rn, nr \in N$. Then $\phi(N)$ is an additive subgroup of $\phi(R)$ and for $x \in \phi(R)$, $y \in \phi(N)$, there exists $r \in R, n \in N$ such that $\phi(r) = x, \phi(n) = y$. Then $xy =$

$\phi(r)\phi(n) = \phi(rn) \in \phi(N)$, and $yx = \phi(n)\phi(r) = \phi(nr) \in \phi(N)$. Then, $\phi(N)$ is an ideal of $\phi(R)$.

6. If N' is an ideal of R', then it is also an ideal of $\phi(R)$. So we suppose N' is an ideal of $\phi(R)$. Then $\phi^{-1}(N')$ is an additive subgroup of R. Let $r \in R, n \in \phi^{-1}(N')$, $\phi(r) \in \phi(R)$ and $\phi(n) \in N'$. Then $\phi(rn) = \phi(r)\phi(n) \in N'$, $\phi(nr) = \phi(n)\phi(r) \in N'$. Then $rn, nr \in \phi^{-1}(N')$. It follows that $\phi^{-1}(N')$ is an ideal of R.

8.2 First isomorphism theorem

Proposition 8.2 (First isomorphism theorem, Artin 11.4.2, Fraleigh 7th 26.17, 8th 30.17)**.** *Let $\phi : R \to R'$ be a ring homomorphism. Then $\phi^{-1}(0) \subseteq R$ is an ideal. Moreover, ϕ induces $\overline{\phi} : R/\phi^{-1}(0) \to \phi(R)$, which is an isomorphism and which satisfies the following commutative diagram:*

More generally, given ideal $I \subseteq \phi^{-1}(0)$, there exists a unique $\overline{\phi} : R/I \to R'$ satisfying $\phi = \overline{\phi} \circ \pi$, where $\pi : R \to R/I$ is the natural surjection $r \mapsto r + I$.

Proof. Let $\phi : R \to R'$ be a ring homomorphism. That $\phi^{-1}(0) \subseteq R$ is an ideal follows from part 6 of the previous proposition. By the group version of the 1st isomorphism theorem, ϕ induces $\overline{\phi} : R/\phi^{-1}(0) \to \phi(R)$, which is an additive group isomorphism, such that $\overline{\phi}(\overline{r}) = \phi(r)$ for each $r \in R$. It remains to show that $\overline{\phi}$ is a ring homomorphism. Clearly, $\overline{\phi}(\overline{1_R}) = \phi(1_R) = 1_{R'}$. For $r, r' \in R$, $\overline{\phi}(\overline{r} \cdot \overline{r'}) = \overline{\phi}(\overline{rr'}) = \phi(rr') = \phi(r)\phi(r') = \overline{\phi}(\overline{r})\overline{\phi}(\overline{r'})$. Then ϕ is a ring isomorphism.

The second statement is proved by defining $\overline{\phi}(\overline{r}) = \phi(r)$ and verifying that $\overline{\phi}$ is well-defined and is a ring homomorphism satisfying $\phi = \overline{\phi} \circ \pi$.

8.3 Correspondence theorem

The following theorem is called the correspondence theorem, or the fourth isomorphism theorem, and is quite useful in identifying rings.

Proposition 8.3 (Artin 11.4.3)**.** *Let $\phi : R \to R'$ be a surjective homomorphism with kernel K. Then there is an order-preserving bijection between*

$\{$Ideals of R containing $K\} \longleftrightarrow \{$Ideals of $R'\}$, given by

$\alpha : I \mapsto \phi(I)$, and $\beta : \phi^{-1}(I') \mapsfrom I'$

Moreover, $R/I \simeq R'/I'$ if $I \leftrightarrow I'$.

Proof. Let $\phi : R \to R'$ be a surjective homomorphism with kernel K. Let $S =\{I$: I is an ideal of R containing $K\}$, and $S' =\{I'$: I' is an ideal of $R'\}$. For $I \in S$, $\phi(I)$ is an ideal of R' by property 5 in 8.1. Then $\alpha : I \mapsto \phi(I)$ defines a map from S to S'. For $I' \in S'$, $\phi^{-1}(I')$ is an ideal of R by property 6 in 8.1. Clearly $K \subseteq \phi^{-1}(I')$. Then β defines a map from S' to S. For $I_1 \subseteq I_2$, $I_1, I_2 \in S$, $\alpha(I_1) = \phi(I_1) \subseteq \phi(I_2) = \alpha(I_2)$. Therefore, α is order-preserving. Similarly, β is also order-preserving.

For $I \in S$, $\beta \circ \alpha(I) = \phi^{-1}(\phi(I)) \supseteq I$. For $a \in \phi^{-1}(\phi(I))$, $\phi(a) \in \phi(I)$. Then there exists some $b \in I$ such that $\phi(a) = \phi(b)$. Then $\phi(a-b) = 0$ and $a-b \in K \subseteq I$. Then $a = a-b+b \in I$. Therefore, $\beta\circ\alpha(I) = \phi^{-1}(\phi(I)) = I$. Since I was arbitrarily chosen, $\beta \circ \alpha = \mathrm{id}_S$.

For $I' \in S'$, $\alpha\circ\beta(I') = \phi(\phi^{-1}(I')) = I'\cap\phi(R) = I'\cap R' = I'$ since ϕ is surjective. Then $\alpha \circ \beta = \mathrm{id}_{S'}$.

Therefore, α and β defines a correspondence (i.e. bijection) between S and S'.

For $I \in S$, let $I' = \alpha(I)$. Then the natural projection $\pi : R' \to R'/I'$ is a surjective ring homomorphism. Since ϕ is also a surjective homomorphism, so is $\psi := \pi \circ \phi : R \to R'/I'$. Let $r \in R$. Then $r \in \ker(\psi) \iff \pi(\phi(r)) = 0 \iff \phi(r) \in I' \iff r \in \beta(I') = \beta\alpha(I) = I$. Then $\ker(\psi) = I$. Since ψ is a surjective ring homomorphism, ψ induces a ring isomorphism $\overline{\psi} : R/I \to R'/I'$ by $\overline{r} \mapsto \psi(r) = \pi \circ \phi(r) = \overline{\phi(r)}$.

Exercise 1. (Artin Q11.4.3) Identify the following rings: **(a)** $\mathbb{Z}[x]/(x^2-3, 2x+4)$, **(b)** $\mathbb{Z}[i]/(2+i)$, **(c)** $\mathbb{Z}[x]/(6, 2x-1)$, **(d)**$\mathbb{Z}[x]/(2x^2-4, 4x-5)$, **(e)** $\mathbb{Z}[x]/(x^2+3, 5)$.

Our strategy is to use the correspondence theorem, which states that if $\phi : R \to R'$ is surjective, and $I \supset \ker(\phi)$, then $R/I \simeq R'/\phi(I)$. We will often choose $\ker(\phi)$ to be $(x-r)$ or (m) for some $r, m \in \mathbb{Z}$.

There is a useful property of a surjective homomorphism ϕ: $\phi((x_1, x_2, ..., x_n)) = (\phi(x_1), \phi(x_2), ..., \phi(x_n))$. The proof is straightforward, and we will use this without further explanation.

Answer. (a) Let $R = \mathbb{Z}[x]$, $I = (x^2-3, 2x+4)$. Then $2x^2+4x \in I$, $4x+6 = 2x^2+4x-2(x^2-3) \in I$, and $2 = 2(2x+4)-(4x-6) \in I$. Let $R' = R/(2) = \mathbb{F}_2[x]$. Let $\phi : R \to R'$ be the natural projection. Then $\phi(I) = (\phi(x^2-3), \phi(2x+4)) = (x^2+1)$, and $I \supseteq \ker(\phi) = (2)$. Then I corresponds to $\phi(I)$ as in the correspondence theorem, so $R/I \simeq R'/\phi(I) = \mathbb{F}_2[x]/(x^2+1) = \mathbb{F}_2[x]/(x+1)^2$.

(b) Let $R = \mathbb{Z}[x]$. The evaluation homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}[i]$ with $\phi(x) = i$ is surjective with $\ker(\phi) = (x^2+1)$. Let $I = (x^2+1, 2+x)$, then $I \supseteq \ker(\phi)$ and $\phi(I) = (0, 2+i)$. Then by the correspondence theorem, $R/I \simeq \mathbb{Z}[i]/(2+i)$.

Let $\psi : R \to \mathbb{Z}$ be the evaluation map such that $\phi(x) = -2$. Then ψ is surjective, $\ker(\psi) = (x+2) \subseteq I$, and $\phi(I) = ((-2)^2+1, -2+2) = (5)$. By the correspondence theorem, $R/I \simeq \mathbb{Z}/(5) \simeq \mathbb{F}_5$.

(c) Let $R = \mathbb{Z}[x]$, and $I = (6, 2x-1)$. Then $3 = 6x - 3(2x-1) \in I$. Let $R' = \mathbb{F}_3[x]$ and $\phi : R \to R'$ be the natural projection. Then $\ker(\phi) = (3) \subseteq I$, and $\phi(I) = (0, -x-1) = (x+1)$. Then by the correspondence theorem, $R/I \simeq \mathbb{F}_3[x]/(x+1) \simeq \mathbb{F}_3$.

(d) Let $R = \mathbb{Z}[x]$, and $I = (2x^2-4, 4x-5)$. Then $5x - 8 = 2(2x^2-4) - x(4x-5) \in I$. Then $x - 3 = 5x - 8 - (4x-5) \in I$. Let $\phi : R \to \mathbb{Z}$ be the evaluation map with $\phi(x) = 3$. Then $\ker(\phi) = (x-3) \subseteq I$, ϕ is surjective, and $\phi(I) = (2 \cdot 3^2 - 4, 4 \cdot 3 - 5) = (14, 7) = (7)$. By the correspondence theorem, $R/I \simeq \mathbb{Z}/(7) \simeq \mathbb{F}_7$.

(e) Let $R = \mathbb{Z}[x]$, $I = (x^2+3, 5)$, and let $\phi : R \to \mathbb{F}_5[x]$ be the natural projection. Then $\ker(\phi) = (5) \subseteq I$, and $\phi(I) = (x^2+3, 0)$. By the correspondence theorem, $\mathbb{Z}[x]/I \simeq \mathbb{F}_5[x]/(x^2+3)$.

Note that x^2+3 is irreducible, $\mathbb{F}_5[x]/(x^2+3)$ is a field of 25 elements, that is $\mathbb{Z}[x]/I \simeq \mathbb{F}_{25}$.

Exercise 2. (Artin Q11.4.4) Are the rings $\mathbb{Z}[x]/(x^2+7)$ and $\mathbb{Z}[x]/(2x^2+7)$ isomorphic?

Proof. No. The two rings are not isomorphic. We give a proof.

Suppose there is a ring isomorphism $\phi : \mathbb{Z}[x]/(2x^2+7) \to \mathbb{Z}[x]/(x^2+7)$. Then $\phi(1) = 1$, and $\phi(x) = ax + b$ for some $a, b \in \mathbb{Z}$. Then $0 = \phi(2x^2+7) = 2(ax+b)^2 + 7 = 2a^2x^2 + 4abx + 2b^2 + 7 = 4abx + 2b^2 + 7 - 14a^2$ in $\mathbb{Z}[x]/(x^2+7)$. Then $4ab = 2b^2 + 7 - 14a^2 = 0$. Since $a, b \in \mathbb{Z}$, $14a^2 = 2b^2 + 7 > 0$. Then $a \neq 0$. Then $b = 0$ by $4ab = 0$, and so $7 = 14a^2$. There is no solution where $a \in \mathbb{Z}$. Contradiction arises. Therefore, the two rings are not isomorphic.

9 Factorization in $\mathbb{Z}[i]$

9.1 Factorization, PID and UFD

We record here some relations among prime elements, irreducible element, prime ideals, and maximal ideals.

Proposition 9.1. *Let R be an integral domain. Let $r \in R$,*

$$\begin{tikzcd}
\textit{1. } r \textit{ is irreducible.} & \textit{2. } r \textit{ is a prime element.} \arrow[l, Rightarrow] \arrow[d, Leftrightarrow] \\
\textit{4. } (r) \textit{ is a maximal ideal.} \arrow[r, Rightarrow] & \textit{3. } (r) \textit{ is a prime ideal.}
\end{tikzcd}$$

When R is a PID, $1 \Longrightarrow 4$, and so the four statements 1-4 are all equivalent.

An integral domain R is called a unique factorization domain (UFD) if
(U1) Any element in $R - (R^\times \cup \{0\})$ is a product of irreducible elements.
(U2) The factorization is unique up to associates and reordering.

Proposition 9.2. (a) *Condition (U1) is equivalent to ACCPI: If $(a_1) \subseteq (a_2) \subseteq ... \subseteq (a_n) \subseteq ...$, then there exists some n such that $(a_n) = (a_{n+1}) = ...$*

(b) *Under (U1), (U2) is equivalent to $1 \implies 2$ in proposition 9.2, that is, any irreducible element is a prime.*

(c) *Any PID is a UFD.*

9.2 Euclidean domains, Gaussian integers

An integral domain R is called an Euclidean domain (ED) if there is a size function $\sigma : R - \{0\} \to \mathbb{Z}_{\geq 0}$ on R such that the division with remainder is possible in the following sense:
(ED1) Let $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\sigma(r) < \sigma(b)$.
(ED2) When $a \neq 0$, $\sigma(ab) \geq \sigma(b)$.

Artin's definition does not require (ED2), which is included for discussion of units.

Proposition 9.3. *Any ED is a PID.*

Proof. Let R be an ED, with size function σ. Let I be an ideal in R. If $I = 0$, then I is generated by 0. If $I \neq 0$, $\sigma(I - \{0\})$ is a nonempty subset of $\mathbb{Z}_{\geq 0}$, hence contains a minimal element $\sigma(b)$, where $b \in I$. Then $(b) \subseteq I$. Conversely, let $a \in I$, then $a = bq + r$ for some $q, r \in R$ with $r = 0$ or $\sigma(r) < \sigma(b)$. But note that $r = a - bq \in I$, so $\sigma(r) < \sigma(b)$ cannot happen when $r \neq 0$. Therefore $r = 0$, so $a = bq \in (b)$. Therefore, $I = (b)$. It follows that R is a PID.

Examples. $\mathbb{Z}$ is an ED with $\sigma(n) = |n|$.
$\mathbb{F}[x]$ is an ED with $\sigma(f) = \deg(f)$.
Recall the definition the ring of Gaussian integers $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$.

Proposition 9.4. *$\mathbb{Z}[i]$ is an ED with $\sigma(a) = |a|^2$ for any $a \in \mathbb{Z}[i]$.*

Proof. Define $\sigma(a) = |a|^2$ for any $a \in \mathbb{Z}[i]$. Then $\sigma(ab) = \sigma(a)\sigma(b)$, and $\sigma(a) \geq 1$ for $a \neq 0$. Then, ED2 is clear.

Let $a, b \in \mathbb{Z}[i]$ with $b \neq 0$. Then $\frac{a}{b} \in \mathbb{C}$. There exists some $m, n \in \mathbb{Z}$ such that $\mathrm{Re}(\frac{a}{b}) \in [m - \frac{1}{2}, m + \frac{1}{2}]$ and $\mathrm{Im}(\frac{a}{b}) \in [n - \frac{1}{2}, n + \frac{1}{2}]$. Then $|\frac{a}{b} - (m + ni)| \leq |\frac{1}{2} + \frac{i}{2}| = \frac{\sqrt{2}}{2} < 1$. Let $q = m + ni$, and $r = a - bq$. Then $|\frac{a}{b} - q| < 1$, so $|r| < |b|$. Then $\sigma(r) < \sigma(b)$. We have proved ED1.

Therefore, $\mathbb{Z}[i]$ is an ED.

Remark. We often write $N(z) = \sigma(z) = |z|^2$, and say that N is a norm function, because N is multiplicative, and agrees with the norm function in field theory.

9.3 Factorization in $\mathbb{Z}[i]$

We characterize units and prime (irreducible) elements in $\mathbb{Z}[i]$.

Proposition 9.5. (*a*) *Units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.*

(*b*) *If $a \in \mathbb{Z}[i]$ is a prime element, then either a is associate to an integer prime, or $a\overline{a}$ is an integer prime.*

(*c*) *Let p be an integer prime, then either p remains a prime in $\mathbb{Z}[i]$, or p factors into $\pi\overline{\pi}$ for some prime $\pi \in \mathbb{Z}[i]$.*

(*d*) *An integer prime p remains a prime in $\mathbb{Z}[i]$ exactly when $p \equiv 3 \pmod 4$, and p factors in $\mathbb{Z}[i]$ exactly when $p = 2$ or $p \equiv 1 \pmod 4$.*

Therefore, up to associates, we can list all primes in $\mathbb{Z}[i]$ as $\{3, 7, 11, 19, ...\} \cup \{1 + i, 2 + i, 2 - i, 3 + 2i, 3 - 2i, ...\}$.

Proof.

(a) Let u be a unit in $\mathbb{Z}[i]$, then $uv = 1$ for some $v \in \mathbb{Z}[i]$. Then $1 = N(uv) = N(u)N(v)$. Since $N(u), N(v) \in \mathbb{Z}_{\geq 0}$, we have $N(u) = 1$. Conversely, if $u \in \mathbb{Z}[i]$ satisfies $N(u) = 1$, then $u\overline{u} = 1$, and $\overline{u} \in \mathbb{Z}[i]$. Then u is a unit in $\mathbb{Z}[i]$.

It follows that $u = a + bi \in \mathbb{Z}[i]$ is a unit if and only if $N(u) = a^2 + b^2 = 1$, and this holds exactly when $(a, b) = (1, 0), (-1, 0), (0, 1), (0, -1)$, that is $u = \pm 1$ of $\pm i$.

(b) Let a be a prime in $\mathbb{Z}[i]$. Then so is $\overline{a}$. Factorize $a\overline{a}$ in $\mathbb{Z}$ as $a\overline{a} = p_1 ... p_r$. Then $a \mid p_1 ... p_r$ in $\mathbb{Z}[i]$, and since a is a prime in $\mathbb{Z}[i]$, $a \mid p_j$ for some j, say, $a \mid p_1$. Then $a\overline{a} \mid p_1^2$. Since a is not a unit, $a\overline{a} > 1$. Then $a\overline{a} = p_1$ or p_1^2. If $a\overline{a} = p_1^2$, then p_1 must be a prime associate to a, in view of the unique factorization of $\mathbb{Z}[i]$. Therefore, either a is associate to an integer prime, or $a\overline{a}$ is an integer prime.

(c) Factorize p into irreducible elements in $\mathbb{Z}[i]$: $p = \pi_1 ... \pi_r$. Then $p^2 = N(p) = N(\pi_1) ... N(\pi_r)$. In view of unique factorization in $\mathbb{Z}$, $r \leq 2$. When $r = 1$, p remains a prime in $\mathbb{Z}[i]$. When $r = 2$, $p^2 = N(\pi_1)N(\pi_2)$, so $p = N(\pi_1) = N(\pi_2)$. Then $p = \pi\overline{\pi}$.

(d) p is not a prime in $\mathbb{Z}[i]$

$$\begin{aligned} &\iff \mathbb{Z}[i]/(p) \text{ is not an integral domain} \\ &\iff \mathbb{Z}[x]/(x^2+1,p) \text{ is not an integral domain} \\ &\iff \mathbb{F}_p[x]/(x^2+1) \text{ is not an integral domain} \\ &\iff x^2+1 \text{ is not irreducible (i.e. has a root) in } \mathbb{F}_p[x]. \\ &\iff p=2 \text{ or there is an element of order 4 in } \mathbb{F}_p[x]. \\ &\iff p=2 \text{ or } p \equiv 1 \pmod 4. \end{aligned}$$

Corollary. *An integer prime p can be written as a^2+b^2 for some $a,b \in \mathbb{Z}$ exactly when $p=2$ or $p \equiv 1 \pmod 4$.*

PROOF. Combine (c) and (d) of Prop 9.5. By (d), p is not irreducible in $\mathbb{Z}[i]$ exactly when $p=2$ or $p \equiv 1 \pmod 4$. By (c), p is irreducible if and only if $p = N(\pi) = a^2+b^2$ for some integers $a,b \in \mathbb{Z}$.

MATH3030 Tutorial 10

J. SHEN

30 November, 2022

10 Product rings and the Chinese Remainder theorem

10.1 Definition and characterization of product rings

10.1.1 Product rings

Let R, R' be rings. Then $R \times R' := \{(r, r') : r \in R, r' \in R'\}$ is a ring with component-wise addition and multiplication. The unity is $(1_R, 1_{R'})$.

We have two projections: $\pi_1 : R \times R' \to R$ by $\pi_1(r, r') = r$, and $\pi_2 : R \times R' \to R'$ by $\pi_2(r, r') = r'$. The two maps preserves identity, addition, and multiplication. The kernels are $0 \times R'$ and $R \times 0$ respectively.

In other word, we have two short exact sequences:

$$\begin{tikzcd} 0 \arrow[r] & 0 \times R' \arrow[r] & R \times R' \arrow[r, "\pi_1"] & R \arrow[r] & 0. \end{tikzcd}$$

$$\begin{tikzcd} 0 \arrow[r] & R \times 0 \arrow[r] & R \times R' \arrow[r, "\pi_2"] & R' \arrow[r] & 0. \end{tikzcd}$$

Note that $R \times 0$ is a ring with unity $e_1 = (1, 0)$, and it is isomorphic to R. But it is not a subring of $R \times R'$ because the unity of the two rings are not the same. Similar things hold for $0 \times R'$, which has unity $e_2 = (0, 1)$.

Note that $e_1^2 = e_1$. We say that an element with this property as e_1 is **idempotent**.

10.1.2 A characterization of product rings

In fact, in the commutative case, product rings are characterized by idempotent elements:

Proposition 10.1. *Let S be a commutative ring. Let $e \in S$ be an idempotent element, that is, $e^2 = e$.*

1. *The element $e' = 1 - e$ is also idempotent, and $ee' = e'e = 0$.*

2. *eS and $e'S$ are rings with identity elements e and e'. Moreover, $m_e : S \to eS$ and $m_{e'} : S \to e'S$ are ring homomorphisms, where $m_a(s) = as$ for $a, s \in S$.*

3. *$S \simeq eS \times e'S$.*

PROOF.

1. In the commutative ring R, since $e^2 = e$, $ee' = e'e = (1-e)e = e - e^2 = 0$ and $(e')^2 = e'(1-e) = e' - e'e = e'$.

2. Note that $m_e : S \to S$ is additive: $m_e(s + s') = e(s + s') = es + es' = m_e(s) + m_e(s')$ for any $s, s' \in S$, so its image eS is an additive subgroup of S. Let $es, es' \in eS$ with $s, s' \in S$. Then $eses' = e(ses') \in eS$. Therefore, eS is closed under multiplication. Moreover, for any $s \in S$, $e(es) = e^2 s = es$. Then e is an identity element in eS. It follows that eS is a ring with identity element e.

   Note that $m_e(1) = e$, and for any $s, s' \in S$, $m_e(s + s') = m_e(s) + m_e(s')$ and $m_e(s)m_e(s') = eses' = e^2 ss' = ess' = m_e(ss')$. Therefore, m_e is a ring homomorphism.

   The statements for e' are analogous.

3. Define $\phi : S \to eS \times e'S$ by $\phi(s) = (es, e's) = (m_e(s), m_{e'}(s))$. By 2, ϕ is a ring homomorphism. Let $s \in \ker(\phi)$, then $es = e's = 0$. Then $s = (e + e')s = 0$. Therefore ϕ is injective. Let $(a, b) \in eS \times e'S$. Write $(a, b) = (es_1, e's_2)$, where $s_1, s_2 \in S$. Then $\phi(a+b) = (ea+eb, e'a+e'b) = (ees_1+ee's_2, ee's_1+e'e's_2) = (es_1, e's_2) = (a, b)$. Therefore, ϕ is bijective. Thus, $\phi : S \simeq eS \times e'S$.

10.2 The Chinese remainder theorem

Theorem 10.2. *Let $I, J \subseteq R$ be ideals, such that $I + J = R$. Then*

1. *$I \cap J = IJ$.*

2. *$R/IJ \simeq R/I \times R/J$.*

PROOF.

1. Clearly, $IJ \subseteq I$ and $IJ \subseteq J$. Then $IJ \subseteq I \cap J$. Conversely, let $x \in I \cap J$. Since $I + J = R$, there exists some $a \in I$, $b \in J$ such that $a + b = 1$. Then $x = x(a + b) = xa + xb$. Now, $x \in J$ and $a \in I$ imply that $xa \in IJ$; $x \in I$ and $b \in J$ imply that $xb \in IJ$. Therefore, $x = xa + xb \in IJ$. It follows that $IJ = I \cap J$.

2. Define $\phi : R \to R/I \times R/J$ by $\phi(r) = (r + I, r + J)$. Then ϕ is a ring homomorphism. The kernel is $\ker(\phi) = I \cap J = IJ$.

   Let $a \in I, b \in J$ be such that $a+b = 1$. Then $\phi(a) = (a+I, a+J) = (0+I, a+b+J) = (0+I, 1+J)$, and $\phi(b) = (b+I, b+J) = (a+b+I, 0+J) = (1+I, 0+J)$. Then for any $u, v \in R$, $\phi(ub+va) = (u+I, v+J)$. Therefore, ϕ is surjective. By the first isomorphism theorem, ϕ induces an isomorphism $R/IJ \simeq R/I \times R/J$.

Example. 1. $\mathbb{Z}/(105) \simeq \mathbb{Z}/(3) \times \mathbb{Z}/(5) \times \mathbb{Z}/(7)$.
2. $\mathbb{Z}[i]/(5) \simeq \mathbb{F}_5[x]/(x^2 + 1) \simeq \mathbb{F}_5[x]/(x - 2) \times \mathbb{F}_5[x]/(x + 2) \simeq \mathbb{F}_5 \times \mathbb{F}_5$.
3. $\mathbb{Z}[i]/(13) \simeq \mathbb{F}_{13}[x]/(x^2 + 1) \simeq \mathbb{F}_{13}[x]/(x - 5) \times \mathbb{F}_{13}[x]/(x + 5) \simeq \mathbb{F}_{13} \times \mathbb{F}_{13}$.

10.3 Using Gauss's Lemma

Let R be a UFD. Let $F = \text{Frac}(R)$. Then $\{p : p \text{ is a prime in } R[x]\} = \{p : p \text{ is a prime in } R\} \bigcup \{f : f \text{ is irreducible in } F[x], \text{ and the content } c(f) = 1\}$.

Recall that in MATH2070, we have the following tools to decide whether a polynomial f is irreducible.

(a) When $f \in \mathbb{F}[x]$, if $\deg(f) = 2$ or 3, and if f has no root in $\mathbb{F}$, then f is irreducible in $\mathbb{F}[x]$.

(b) Reduce f mod p. If $\overline{f} \in \mathbb{F}_p[x]$ is irreducible, and $\deg(f) = \deg(\overline{f})$, then f is irreducible in $\mathbb{Z}[x]$.

(c) Eisenstein's criterion. Let $f = \sum_{i=0}^{n} a_i x^i$ be primitive. Let p be a prime. Suppose $p \mid a_0, a_1, ..., a_{n-1}$, $p \nmid a_n$, and $p^2 \nmid a_0$, then f is irreducible in $\mathbb{Z}[x]$.

Note that method (b) and (c) generalize: We can replace $\mathbb{Z}$ by any UFD R, and replace $p \in \mathbb{Z}$ by a prime $p \in R$.

Exercise. (a) Factorize $x^p + y^p$ in $\mathbb{C}[x, y]$.

(b) Show that $x^p + y^p + z^p$ is irreducible in $\mathbb{C}[x, y, z]$. (Hint: Eisenstein criterion)

(c) Show that $xy + zw$ is irreducible in $\mathbb{C}[x, y, z, w]$.

Answer. (a) $x^p + y^p = \prod_{i=0}^{p-1} (x - y\zeta_{2p}^{2i+1})$, where $\zeta_{2p} = e^{\frac{2\pi i}{2p}}$.

(b) Consider $g = x - y\zeta_{2p} \in \mathbb{C}[y][x]$. It is irreducible in $\mathbb{C}(y)[x]$ as its degree in x is 1. Since the leading coefficient of g is 1, g is primitive, thus it is a prime in $\mathbb{C}[y][x] = \mathbb{C}[x, y]$.

Consider $f = x^p + y^p + z^p \in \mathbb{C}[x, y][z]$, that is, as a polynomial in z. Then f is primitive, and $x - y\zeta_{2p}$ is a prime in $\mathbb{C}[x, y]$ that divides $x^p + y^p$, but $(x - y\zeta_{2p})^2 \nmid x^p + y^p$, and $(x - y\zeta_{2p}) \nmid 1$. By Eisenstein's criterion, f is irreducible in $\mathbb{C}[x, y][z] = \mathbb{C}[x, y, z]$

(c) Let $f = xy + zw$, and let $R = \mathbb{C}[y, z, w]$. Note that f is a polynomial of degree 1 in $\text{Frac}(R)[x]$. Then f is irreducible in $\text{Frac}(R)[x]$. It remains to show that f is primitive, that is, $\gcd(y, zw) = 1$ in R.

Since y is a prime in $\mathbb{C}[y]$, it is also a prime in R. If $\gcd(y, zw) \neq 1$, then $y \nmid 1$. Then $zw = gy$ for some $g \in \mathbb{C}[z, w, y] = \mathbb{C}[z, w][y]$. But $\deg_y(zw) = 0$, and $\deg_y(gy) \in \{\infty\} \cup \mathbb{Z}_{\geq 1}$. Then $zw \neq gy$, so $\gcd(y, zw) = 1$.

Now, f is primitive in $R[x]$, and f is irreducible in $\text{Frac}(R)[x]$, so f is irreducible in $R[x] = \mathbb{C}[xy, zw]$.