21-237 Notes

Justin Sun

Last Updated: December 17, 2022

Recitation reference material for 21-237 Math Studies Algebra under Professor Cummings.

Contents

1 Week 1

1.1 Definitions

Definition 1.1 (Group)**.** $(G, \times)$ is a group with underlying set G and binary operation $\times$ if it satisfies the following 4 properties.

1. Associativity: $\forall a, b, c \in G$ we have $a \times (b \times c) = (a \times b) \times c$
2. Identity: $\exists e \in G$ s.t. $\forall g \in G$ we have $e \times g = g \times e = g$. Such an element is provably unique (exercise).
3. Inverses: $\forall g \in G$, $\exists g^{-1} \in G$ s.t. $gg^{-1} = g^{-1}g = e$. This is also provably unique (exercise).
4. Closure: $\forall a, b \in G$ we have $a \times b \in G$.

$H \subseteq G$ is said to be a subgroup of G if it is also a group with the same binary operation. In this case we write $H \leq G$. Some common examples of groups are the following (see if you can find which pairs of groups are sub/supergroups of each other):

1. $(\mathbb{Z}, +)$, the additive group of integers.
2. $(\mathbb{R} \setminus \{0\}, \times)$, the multiplicative group of reals.
3. $\mathrm{GL}_n(\mathbb{R}) = \{n \times n$ invertible real matrices$\}$.
4. $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) : \det(A) = 1\}$.
5. $(\mathbb{Z}/p\mathbb{Z}, +)$, where addition is modulo p.
6. $((\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}, \times)$ or $(\mathbb{Z}/p\mathbb{Z})^\times$, where multiplication is modulo p (Exercise: What happens if p is not prime?).
7. S_n, the group of permutations on $\{1, 2, \ldots, n\}$.

Definition 1.2 (Homomorphism, Isomorphism, Automorphism)**.** If G, H are groups, then $\phi : G \to H$ is a homomorphism if

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

ϕ is called an isomorphism if ϕ is also a bijection, and ϕ is called an automorphism if it is an isomorphism and $H = G$.

Definition 1.3 (Generator)**.** If $g \in G$ where G is some group, then

$$\langle g \rangle = \bigcap_{H \leq G : g \in H} H$$

is called the subgroup of G generated by g. In this case, it happens to be the cyclic group that is just the power of g. We can extend this notion naturally to multiple elements

$$\langle g_1, \ldots, g_n \rangle = \bigcap_{H \leq G : g_i \in H \ \forall i \in [n]} H.$$

g is said to generate G if $G = \langle g \rangle$.

1.2 Problems

The following is a useful result.

Problem 1. Show that if $*$ is an associative operation, then any valid parenthetization of $g_1 * \ldots * g_n$ is equivalent to $g_1 * (g_2 * \ldots (g_{n-1} * g_n))$

Proof. We proceed by induction on n. The base case $n = 2$ is clear. Now fix $n \geq 3$ and assume that the statement holds for all integers $< n$. Consider an arbitrary parenthesization of $g_1 * \ldots * g_n$ as above, and decompose it as

$$e_1 * e_2 := (g_1 * \ldots * g_k) * (g_{k+1} * \ldots * g_n)$$

where $k < n$, and the left and right expressions are parenthesized in some arbitrary fashion. Then by inductive hypothesis, we have

$$e_1 = g_1 * (g_2 * \ldots * (g_{k-1} * g_k))$$

and so

$$e_1 * e_2 = (g_1 * (g_2 * \ldots * (g_{k-1} * g_k))) * e_2$$

by associatvity. Applying the hypothesis again yields the desired conclusion. □

Problem 2. Classify subgroups of $(\mathbb{Z}, +)$.

Proof. I claim they are $d\mathbb{Z}$ for $d \in Z_{\geq 0}$. Clearly $\{0\}$ is a subgroup. If $H \leq (\mathbb{Z}, +)$ is a subgroup s.t. $H \neq (\mathbb{Z}, +)$, then we can let $d = \min_{h \in H, h \neq 0} |h|$, which exists by well-ordering. It is easy to show by induction that $d\mathbb{Z} \leq H$ now.

Now suppose that $\exists h \in H$ s.t. $h \notin d\mathbb{Z}$. Then it must be by the division algorithm that

$$h = dq + r, 0 < r < d, q \in \mathbb{Z}.$$

But then since $d, -d \in H$, it must be that $h - dq = r \in H$, and we have contradicted the minimality of d. □

1.3 Dihedral Groups

We define the symmetry group of the square $ABCD$ as all relabellings of vertices s.t. the distance between pairwise vertices is preserved. In general, D_n is defined as the symmetry group of an n sided polygon.

Problem 3. What is $|D_4|$?

Proof. $|D_4| = 8$. There are 4 places to send A to, and once that has been decided, we can either go clockwise or counterclockwise in labelling BCD in that order. □

Definition 1.4 (Abelian)**.** G is said to be abelian if all of its elements commute, i.e. $gh = hg \; \forall g, h \in G$.

Problem 4. Is D_3 abelian? What about D_4, D_n?

Proof. Exercise! □

2 Week 2

2.1 Lagrange's Theorem

Definition 2.1 (Coset)**.** Given $H \leq G$ and $a \in G$, define the left coset

$$aH = \{ah : h \in H\}$$

and the right coset

$$Ha = \{ha : h \in H\}.$$

We use this to prove the following:

Theorem 2.1 (Lagrange's Theorem)**.** If $H \leq G$ then $|H| \mid |G|$.

Proof. It is easy to verify that the relation $a \sim b \iff aH = bH$ is an equivalence relation. Moreover, if $a \sim b$, then $ah_1 = bh_2$ for some $h_1, h_2 \in H$, and therefore $b = ah_1h_2^{-1} \implies b \in aH$. Also if $b \in aH$, it is clear that $bH = aHH = aH$ so that $[a]_\sim$ is just aH.

Since equivalence classes partition the group G and each equivalence class has $|aH| = |H|$ many elements, it follows that $|H| \mid |G|$. □

We generally write G/H to denote the set of equivalence classes under this equivalence relation. We also write $[G : H] = |G/H|$ as the index of H in G so that $|H| \, [G : H] = |G|$.

An important thing to note is that in general we cannot impose a group structure on G/H for $H \leq G$. This can only be done in the case $N \trianglelefteq G$, in which case we have $(aN)(bN) = a(bNb^{-1})bN = abNN = abN$. Lagrange's theorem also implies some useful corollaries.

Corollary 2.1. If $\phi : G \to H$ is some homomorphism from G, then we must have that $|G| = |\ker \phi| \, |\mathrm{Im}\, \phi|$.

Proof. First Isomorphism Theorem. □

Corollary 2.2. If $g \in G$, then $|g| \mid |G|$.

Proof. Consider the subgroup $\langle g \rangle$. □

2.2 Applications of Lagrange

Problem 5. Say G is a group with $|G| = p^n$ for some prime p and some $n \in \mathbb{N}$. Show that there exists an element of order p.

Proof. There must exist some element $g \in G$ with $|g| = p^k > 1$. If $k = 1$ then we are done. Otherwise we can consider $g^{p^{k-1}}$ which has order p. □

Problem 6. Let $|G| = 25$. Show there exists a subgroup of order 5, and if there is only 1 such subgroup, then G is cyclic.

Proof. The first part follows from the previous part. Now suppose that G is not cyclic, and suppose FTSOC there exists only 1 such subgroup. Since groups of prime order are cyclic, we can say $\langle g \rangle \leq G$ is the only subgroup of order 5, where $|g| = 5$.

But then if we take $h \notin \langle g \rangle$, we have $|h| \neq 25$ or else G would be cyclic, and $|h| \neq 1$ since h cannot be the identity. But then by Lagrange the only possibility is $|h| = 5$, and we have another subgroup of order 5, $\langle h \rangle$. □

Problem 7. Say $|G| = 35$. Show there exists an element of order 5 and 7.

Proof. Suppose not. First G cannot be cyclic since if $|g| = 35$ then g^5, g^7 have orders $7, 5$ respectively. Then every element in G has order $1, 5, 7$. If there are no elements of order 5, then we can write

$$G = \bigcup_{g \in G, g \neq e} \langle g \rangle$$

where every $\langle g \rangle$ is a cyclic group of order 7. Suppose we have some g, h s.t. $h \notin \langle g \rangle$. Then notably $h^a \notin \langle g \rangle$ for any $a \in (\mathbb{Z}/7\mathbb{Z})^\times$ since otherwise we would have

$$h^a = g^b \implies h^{aa^{-1}} = g^{ba^{-1}} \implies h = g^{ba^{-1}} \implies h \in \langle g \rangle$$

where a^{-1} is the modular inverse of a modulo 7. What this shows is that either $\langle h \rangle \cap \langle g \rangle$ is either $\langle g \rangle$ or the trivial intersection $\{e\}$. It follows then that since G is the union of these cyclic subgroups, the size of G can be expressed as $6k + 1$ for some $k \in \mathbb{N}$, where k is the number of pairwise cyclic subgroups that have trivial intersection. However this is impossible since $35 \not\equiv 1 \pmod 6$.

Analogous reasoning holds to show that there exists an element of order 5, just note that $35 \not\equiv 1 \pmod 4$. □

2.3 Miscellaneous Problems

Problem 8. If $H \leq G$ and $[G : H] = 2$ then $H \triangleleft G$.

Proof. Recall that from the coset decomposition of G, we can rewrite $G = H \sqcup gH$ for any $g \in G \setminus H$. Now consider the right coset decomposition of G, $G = H \sqcap Hg'$ for some $g' \in G \setminus H$. Since $g \notin H$, it follows that

$$Hg \neq H \implies Hg = Hg'$$

since there are only 2 equivalence classes of right cosets. As such, it follows that $G = H \sqcup gH = H \sqcup Hg \implies gH = Hg$. If we instead had $g \in H$, then clearly $gH = H = Hg$, so $\forall g \in G$ we have $gH = Hg \implies H \triangleleft G$. □

Problem 9. Classify the automorphism groups of C_4 and C_5. Generalize to C_n.

Proof. We show that the answer is in general $(\mathbb{Z}/n\mathbb{Z})^\times$. Suppose $C_n = \{1, g, g^2, \ldots, g^{n-1}\}$ and note that if $\phi : C_n \to C_n$ is an automorphism, then $|g| = |\phi(g)|$ (exercise). Moreover, all automorphisms are strictly determined by where g is sent, since we can then repeatedly multiply to get the behavior of ϕ on the entirety of g.

As such, the automorphisms of C_n can be restricted to $\phi_k : C_n \to C_n$ where $\phi_k(g) = g^k$. In order for $\left|g^k\right| = n$, it must be that $(g^k)^m = 1 \iff km \equiv 0 \pmod n \implies m \equiv 0 \pmod n \implies k \in (\mathbb{Z}/n\mathbb{Z})^\times$.

If $k \in (\mathbb{Z}/nZ)^\times$, then $\phi_k \in \mathrm{Aut}(C_n)$ since it is clearly a HM, and if $\phi_k(g^a) = \phi_k(g^b)$ for $a \neq b$, then it must be that $\phi_k(g^{a-b}) = 1 \implies k(a - b) \equiv 0 \pmod n \implies a \equiv b \pmod n$. Moreover, composition of automorphisms clearly corresponds to multiplication in $(\mathbb{Z}/n\mathbb{Z})^\times$, since we have that

$$(\phi_{k_1} \circ \phi_{k_2})(g) = g^{k_1 k_2}$$

so the structure of $\mathrm{Aut}(C_n)$ is the same as that of $(\mathbb{Z}/n\mathbb{Z})^\times$. It follows that $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Note that since the latter group is the *multiplicative* group of units in $\mathbb{Z}/n\mathbb{Z}$, it is not necessarily cyclic. In fact, it happens to be that it is cyclic iff $n = 2, 4, p^k, 2p^k$ for some prime p. We will potentially touch on this in a later recitation. □

3 Week 3

3.1 Conjugacy Classes and the Class Equation

Recall that conjugacy forms an equivalence relation that partitions an arbitrary group G into conjugacy classes. We write

$$C_g = \{g' \in G : g' = hgh^{-1}\}$$

to denote the conjugacy class of $g \in G$. Because of this, we can write

$$|G| = \sum_{\text{conjugacy classes } C} |C| .$$

which is frequently referred to as the *class equation* of a finite group G. One notable result is the following:

Theorem 3.1 (Normal Groups as unions of conjugacy classes)**.** If $N \trianglelefteq G$ is a normal subgroup of G, then it must be that $N = \cup_{g \in N} C_g$. In other words, N must be the union of conjugacy classes.

Proof. It is clear that $N \subseteq \cup_{g \in N} C_g$. Now suppose that $g \in N$, so that by definition of normal subgroups, we must have that $\forall h \in G$, $hgh^{-1} \in N \implies C_g \subseteq N$. As such, we clearly have $\cup_{g \in N} C_g \subseteq N$ so that $\cup_{g \in N} C_g = N$. □

One useful application of this result is being able to easily identify and construct normal subgroups. As an example, we will see this in action on permutation groups.

3.2 Permutation Groups

Recall that if we have some permutation $\sigma \in S_n$, we can decompose σ into cycles. Instead of writing out something like:

x	0	1	2	3	4	5	6	7	8	9
$\sigma(x)$	0	2	9	5	4	7	6	3	8	1

we can instead just write $\sigma = (129)(357)$ (note that we read from left to right inside the cycles, but applying them from right to left with this notation). We first show the following useful fact:

Problem 10. Show that disjoint cycles commute.

Proof. Consider $\sigma = (a_1 a_2 \dots a_k), \tau = (b_1 b_2 \dots b_l)$ where all a_i, b_j are pairwise distinct. Routine computation yields that

$$(\sigma \circ \tau)(x) = (\tau \circ \sigma)(x) = \begin{cases} a_{i+1} \pmod{k} & x = a_i \\ b_{j+1} \pmod{l} & x = b_j \\ x & \text{otherwise} \end{cases} .$$

□

It is also useful to be able to do these computations by hand:

Problem 11. Compute $(129)(357)(132)(49)$ in S_9.

Proof. Since permutations are applied on the left (binary operation of S_n is function composition), we need to do computation from right to left. The easiest way to do this is to just compute the new cycle decomposition. In other words, if we let $\sigma = (129)(357)(132)(49)$ then we have that

$$\begin{aligned} \sigma(1) &= 5 \\ \sigma(5) &= 7 \\ \sigma(7) &= 3 \\ \sigma(3) &= 9 \\ \sigma(9) &= 4 \\ \sigma(4) &= 1 \end{aligned}$$

for the first cycle. For the next cycle, we start at the first element not currently included in our previous cycles, i.e. $\sigma(2) = 2$. For $\sigma(6), \sigma(8)$, we can notice since they never appear in any of the cycles σ is composed of, they are sent to the same place, it follows then that $\sigma = (157394)$. □

Problem 12. Show that if $\sigma, \tau \in S_n$ s.t. $\sigma = \pi\tau\pi^{-1}$ (i.e. σ, τ are conjugates), then σ, τ have the same cycle decomposition (same number of cycles, same size for each cycle).

Proof. Suppose that $\tau = (a_1a_2a_3 \dots a_k)(b_1b_2b_3 \dots b_l)\dots$. Then note that we can write

$$\pi\tau\pi^{-1} = \pi(a_1a_2a_3 \dots a_k)\pi^{-1}\pi(b_1b_2b_3 \dots b_l)\pi^{-1} \dots \pi(\dots)\pi^{-1}.$$

So since disjoint cycles commute, it suffices to show that $\pi(a_1a_2a_3 \dots a_k)\pi^{-1}$ is a cycle of size k, and that it is disjoint from all of the other cycles $\pi(b_1b_2b_3 \dots b_l)\pi^{-1}$ etc. Now note that if $x \in [n]$ then

$$(a_1a_2a_3 \dots a_k)\pi^{-1}(x) = \begin{cases} a_{i+1 \pmod k} & x = \pi(a_i) \\ \pi^{-1}(x) & x \neq \pi(a_i) \end{cases}$$

so that

$$\pi(a_1a_2a_3 \dots a_k)\pi^{-1}(x) = \begin{cases} \pi(a_{i+1 \pmod k}) & x = \pi(a_i) \\ x & x \neq \pi(a_i) \end{cases}$$

and it becomes clear that

$$\pi(a_1a_2a_3 \dots a_k)\pi^{-1} = (\pi(a_1)\pi(a_2)\pi(a_3) \dots \pi(a_k)).$$

This is clearly a cycle of size k, and since $(a_1a_2a_3 \dots a_k)$ was disjoint from the other cycles in τ, it follows that the cycles will still be disjoint upon conjugating by π. As such, it must be that conjugate elements in S_n have the same cycle decompositions. □

Problem 13. Show the converse of the previous statement, i.e. if σ, τ have the same cycle decomposition, then σ, τ must be conjugates.

Proof. Once again it suffices to show this in the case σ, τ are single cycles, say $(a_1a_2 \dots a_k)$ and $(b_1b_2 \dots b_k)$ respectively. Suppose that $c_1, c_2, \dots, c_{n-k}$ and $d_1, d_2, \dots, d_{n-k}$ are the elements disjoint from $a_1, a_2, \dots, a_k$ and $b_1, b_2, \dots, b_k$ respectively. Then if we just define $\pi(a_i) = b_i, \pi(c_i) = d_i$ otherwise, we have from the prior problem that

$$\pi(a_1a_2 \dots a_k)\pi^{-1} = (b_1b_2 \dots b_k)$$

as desired. □

3.3 $A_n \lhd S_n$

Definition 3.1. An inversion (i, j) of some permutation σ is an ordered pair s.t. $i < j$ and $\sigma(i) > \sigma(j)$.

Theorem 3.2. Every permutation $\sigma \in S_n$ can be expressed as the product of 2-cycles. In other words, 2-cycles generate S_n.

Proof. We can induct, starting with the identity permutation and swapping elements to their "correct" places in σ one-by-one. □

Recall from 21-242 now that we say a permutation $\sigma \in S_n$ is even if it has an even number of inversions, and odd otherwise. We now show a result that let's us give an equivalent definition:

Problem 14. Show that if $\sigma \in S_n$ even is written as the product of 2-cycles, then there is an even number of 2-cycles. Also, show that the product of an even number of 2-cycles is even.

Proof. It suffices to show that if π is an arbitrary two-cycle and τ is odd, then $\pi\tau$ is even. If τ is even, then $\pi\tau$ is odd. To do this, suppose $\pi = (ij)$ and $\tau(i) = x, \tau(j) = y$. If we write out where τ sends $[n]$, we see that

$$\tau \sim \dots x \dots y \dots \to \dots y \dots x \dots \sim \pi\tau.$$

There are $j - i - 1$ elements in between x, y in τ, let a be the number of them $< x$ and b be the number of them $< y$ respectively. Then we have that the change in the number of inversions is

$$\pm 1 - (a) + (j - i - 1 - a) + b - (j - i - 1 - b) = \pm 1 + 2a + 2b \equiv 1 \pmod 2$$

where ± 1 comes from whether $x < y$ or $y < x$. In any case, we see that multiplying by an inversion changes the number of inversions by $1 \pmod 2$. It follows that a product of an even number of 2-cycles must be even, and the product of an odd number of 2-cycles must be odd. Moreover if

$$\sigma = \prod_{i=1}^{m} (a_i b_i)$$

is the product of m 2-cycles, then if σ is even m is even and if σ is odd then m is odd. So while the decomposition of σ into 2-cycles is not unique, its parity is, and we have an equivalent definition of σ's parity as the parity of the number of 2-cycles in any of its 2-cycle decompositions. □

Recall now the matrix associated with σ, or

$$(A_\sigma)_{ij} = \begin{cases} 1 & \text{if } \sigma(i) = j \\ 0 & \text{otherwise} \end{cases}$$

so that

$$(0 \dots 1 \dots 0)(A_\sigma) = e_k(A_\sigma) = e_{\sigma(k)}$$

where e_k is the standard basis element with a 1 in its kth position only. Note that this let's us view $S_n \leq GL(\mathbb{R})_n$ as a subgroup of the group of invertible matrices, since it also the case that $A_\sigma A_\tau = A_{\sigma \circ \tau}$ (exercise). Moreover, since $\det : GL_n(\mathbb{R}) \to (\mathbb{R}^\times, \cdot)$ is a homomorphism, $\det$ restricted to S_n is as well.

This gives us another way to define $\operatorname{sgn} : S_n \to (\mathbb{R}^\times, \cdot)$ as

$$\operatorname{sgn}(\sigma) = \det(A_\sigma) = \pm 1$$

where $+1$ corresponds to σ being even and -1 corresponds to σ being odd. One way you can show this is noting that any 2-cycle corresponds to the elementary matrix operation of swapping two rows, which has determinant -1. Thus by decomposing σ as a product of 2-cycles and using that definition of permutation parity, we can easily get an equivalence with the determinant definition. From this, since the kernel of any homomorphism is a normal subgroup, we have that

$$\ker(\operatorname{sgn}) = A_n = \{\sigma \in S_n : \sigma \text{ even}\} \lhd S_n.$$

Another way to see this is to note that $[S_n : A_n] = 2$, and use the result from last week's recitation.

3.4 Normal Subgroups of S_n

Problem 15. Classify the normal subgroups of S_3, S_4, S_5.

Proof. Using the previous facts, we can easily classify the conjugacy classes of each of these subgroups. We start with S_3, noting that it's conjugacy classes are

Identity: e
2-cycles: $(12), (23), (13)$
3-cycles: $(123), (132)$.

Now we know that N has to be the union of some subset of these conjugacy classes (one of which must be the identity), and that it must still maintain a group structure. Clearly the trivial and entire group work, so the only ones to consider are the ones that contain only one of the 2-cycle or 3-cycle conjguacy class. But $\{e, (12), (23), (13)\}$ cannot be a group by Lagrange's theorem. On the other hand

$$(123)^2 = (132) \implies (123)(132) = (123)^3 = 1 = (132)(123)$$

so that $A_3 = \{e, (123), (132)\}$ is the only nontrivial normal subgroup.

We proceed similary for S_4, noting that its conjugacy classes are

Identity: e
2-cycles: $(12), (13), (14), (23), (24), (34)$
3-cycles: $(123), (132), (134), (143), (124), (142), (234), (243)$
4-cycles: $(1234), (1243), (1324), (1342), (1423), (1432)$
2 2-cycles: $(12)(34), (13)(24), (14)(23)$

with sizes $1, 6, 8, 6, 3$ respectively. The only ways to make nontrivial divisors of 24 with these numbers is

$$4 = 1 + 3, 12 = 1 + 3 + 8.$$

For the first, we verify if the group structure is valid by looking at

$$(12)(34) \circ (13)(24) = (23)(14)$$

and noting that the other cases are symmetric. This yields $\{e, (12)(34), (13)(24), (14)(23)\}$ as a normal subgroup. The other normal subgroup is just

$$A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (134), (143), (124), (142), (234), (243)\}.$$

We now consider S_5. Since 5 is big, we instead compute the number of elements in each conjugacy class

$$\begin{aligned}
&\text{Identity} : 1\\
&\text{2-cycles} : \binom{5}{2} = 10\\
&\text{3-cycles} : \binom{5}{3} \cdot 2 = 20\\
&\text{4-cycles} : \binom{5}{4} \cdot 6 = 30\\
&\text{5-cycles} : 4! = 24\\
&\text{2 2-cycles} : \binom{5}{4} \cdot 3 = 15\\
&\text{2-cycle and 3-cycle} : \binom{5}{3} \cdot 2 = 20.
\end{aligned}$$

Now note that the only ways to make nontrivial divisors of $|S_5| = 120$ are

$$60 = 1 + 20 + 24 + 15, 40 = 1 + 24 + 15.$$

If $N \lhd S_5$ with $|N| = 40$, then it must contain all 5-cycles and products of 2 2-cycles. But then $(12345)(12)(34) = (135) \in N$, which is absurd. It follows that $|N| = 60$, containing 5-cycles, products of 2 2-cycles, and one of 2/3-cycles or 3-cycles. If we choose to include odd cycles, we just have A_5, and if we choose 2-cycles and 3-cycles we get that

$$(12345)(12)(345) = (1354) \notin N$$

since we specified N cannot contain 4-cycles. It follows that the only normal subgroups of S_5 are $1, A_5, S_5$. □

It is important to note that if $H \lhd G$, then it is not necessarily the case that the conjugacy classes of H coincide with those of G. As an example, consider $C_3 \cong \{e, (123), (132)\} \lhd S_3$. $(123), (132)$ are conjugate in S_3 via the swap (23), but not in C_3 since it is a cyclic group (conjugacy classes are all singletons).

4 Week 4

4.1 A_n is simple for $n \geq 5$

Recall the alternating group $A_n \lhd S_n$. It was defined as the even permutations of S_n, and it was shown in last week's recitation that if $\sigma \in A_n$ is written as the product of 2-cycles, then it must be an even number of 2-cycles.

Some useful facts about A_n are that $[S_n : A_n] = 2$, which automatically implies that $A_n \lhd S_n$. Another way to view A_n, S_n was in terms of permutation matrices - A_n is just the kernel of S_n w.r.t. the determinant.

Definition 4.1. A group G is simple if the only $N \trianglelefteq G$ are $N = 1, G$.

The main goal of this week's recitation is to show that A_n is simple for $n \geq 5$. To do this, we will need some auxilary results.

Theorem 4.1. *A_n is generated by 3-cycles for $n \geq 5$.*

Proof. Recall that every element in A_n can be written as the product of an even number of 2-cycles. It then suffices to show that every product of 2 2-cycles can be generated by 3-cycles.

There are 2 classes of products of 2-cycles, ones that change 3 elements of $[n]$, and ones that change 4 elements of $[n]$. As an example, consider $(12)(13)$ and $(12)(34)$ respectively. However, we can write these two permutations as the product of 3-cycles as follows:

$$(12)(13) = (123), (12)(34) = (324)(132).$$

This computation easily generalizes to any four numbers in $[n]$, so since every element in A_n is the product of an even number of 2-cycles, it follows that A_n is generated by 3-cycles as well. □

We now show that 3-cycles are conjugate to each other in A_n. This shows that if $N \lhd A_n$ and N contains a 3-cycle, then it contains all 3-cycles and subsequently $N = A_n$.

Problem 16. Show that 3-cycles are conjguate to each other in A_n. Equivalently, show that any $(abc) \in A_n$ is conjugate to (123).

Proof. We know from last week's theorem that elements in S_n with the same cycle decomposition are conjugate, so $\exists \pi \in S_n$ s.t. $\pi(abc)\pi^{-1} = (123)$. The issue is that we don't know if $\pi \in A_n$. If $\pi \in A_n$, then we're done, but otherwise if π is odd we can consider $(45)\pi$ (which is even) so that

$$(45)\pi(abc)\pi^{-1}(45)^{-1} = (45)(123)(45)^{-1} = (123).$$

It follows that all 3-cycles are conjugate to (123) in A_n for $n \geq 5$ and subsequently each other as well. □

Note the importance of $n \geq 5$ in this proof. As an example of this failing otherwise, note that $(132), (123)$ are not conjugate to each other in A_4 and A_3.

Theorem 4.2. *A_n is simple for $n \geq 5$.*

Proof. Let $N \lhd A_n$ be nontrivial, and let $e \neq \alpha \in N$ be the permutation which has the most fixed points, or permutes the least number of elements. Clearly α permutes at least 2 elements - otherwise it would be an odd 2-cycle. Our goal is to show that α permutes 3 elements so that it is a 3-cycle.

We first assume that α is the product of disjoint 2-cycles. Then it must be the product of ≥ 2 disjoint 2-cycles since α is even, so we may rewrite

$$\alpha = (ab)(cd)\beta$$

where β is also the product of disjoint (possibly 0) 2-cycles, and β does not permute any of a, b, c, d. Now consider $k \neq a, b, c, d$ and let $\tau = (cdk)$. Then consider $\tau\alpha\tau^{-1} \in N$ and $\alpha^{-1} \in N$ s.t. $[\tau, \alpha] = \tau\alpha\tau^{-1}\alpha^{-1} \in N$. But note that $[\tau, \alpha](a) = a, [\tau, \alpha](b) = b$, fixing two more elements from the original α. Moreover, if $t \neq a, b, c, d, k$ was originally fixed by α, then we still have $[\tau, \alpha](t) = t$.

So $[\tau, \alpha]$ now fixes a, b at the tradeoff of potentially no longer fixing k. But this means $[\tau, \alpha]$ has more fixed points than α, and we have contradicted our original assumption. It follows then that α cannot be the product of disjoint 2-cycles, and that it must contain a cycle of length > 2.

In the case that α must have a cycle of longer than 2, suppose that

$$\alpha(a) = b, \alpha(b) = c, \alpha(c) = \dots$$

for $a, b, c \in [n]$ distinct. Now we consider two cases:

1. $\alpha(c) = a$. In this case, if a, b, c are the only permuted points of α, then we are done since we have a 3-cycle. Otherwise, there must be some other points α moves, say $\alpha(i) = j$ for $i, j \neq a, b, c$. Then if we let $\tau = (cij)$ then

$$[\tau, \alpha](a) = (\tau\alpha\tau^{-1}\alpha^{-1})(b) = b,$$

where moreover $[\tau, \alpha] = (\tau\alpha\tau^{-1})\alpha^{-1} \in N$. Here fixed points of α stay fixed points of $[\tau, \alpha]$, but also b becomes a fixed point, contradicting the assumption that α had the most fixed points.

2. $\alpha(c) \neq a$ (cycle containing a has length > 3). In this case, suppose $\alpha(c) = d$ distinct from the numbers already chosen, and let $\tau = (cba)$. Then we have that

$$[\tau, \alpha] = (\tau\alpha\tau^{-1}\alpha^{-1})(b) = b$$

where once again $[\tau, \alpha] = (\tau\alpha\tau^{-1})\alpha^{-1} \in N$. As in the previous case, fixed points of α stay fixed in $[\tau, \alpha]$, and b also becomes a fixed point, contradicing the original assumption about α.

In any case, we've shown that if α permutes $m > 3$ elements, then there is always a way to construct another element in N s.t. it permutes $< m$ elements. It follows then that there must exists $\alpha \in N$ that permutes exactly 3 elements, which can only be a 3-cycle. By the two previous exercises, N contains all 3-cycles and therefore contains A_n as well, so A_n must be simple. □

4.2 Dihedral Groups

Recall in the first week we touched on dihedral groups D_n, which were loosely defined as the symmetries of n-gons. Another way to think about D_n is as a relabelling of the vertices of the n-gon s.t. the main structure is still preserved (distance between pairwise points). In this manner, we can think of D_n as

$$D_n \cong \langle (1, 2, \dots, n), (2, n)(3, n-1) \dots (\dots) \rangle = \langle r, s \rangle \leq S_n$$

where $r = (1, 2, \dots, n)$ corresponds to rotating the n-gon, and $s = (2, n)(2, n-3) \dots (\dots)$ corresponds to reflecting it. Formally, D_n can be expressed using the group presentation

$$\langle r, s : r^n = s^2 = e, rs = sr^{-1} \rangle.$$

Problem 17. Verify that $rs = sr^{-1}$ via viewing D_n as a subset of the permutation group.

Proof. If $i \in [n]$, then rotating and reflecting i sends it to $(i+1) \to n + 2 - (i+1) \equiv 1 - i \pmod{n}$. Similarly, reflecting and rotating backwards sends i to $n + 2 - i \to -1 + (n + 2 - i) \equiv 1 - i \pmod{n}$. □

4.3 Problems

Problem 18. Compute the centers and Sylow subgroups of D_4, A_4, S_4.

Proof. (a) For $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$, one can easily verify by hand that $Z(D_4) = \{e, r^2\}$.

For the Sylow subgroups, note that $|D_4| = 2^3$ so that the only sylow subgroup of D_4 is just itself.

(b) For the center of A_4, note that $(234) = (321)((12)(34))$ and $(314) = ((12)(34))(321)$ so that $(12)(34)$ and (321) don't commute. By symmetry, it follows that no 3-cycle can be in $Z(A_4)$ and no product of 2 2-cycles can be in $Z(A_4)$ so that $Z(A_4)$ is trivial.

For the Sylow subgroups, note that $|A_4| = 2^2 * 3$ so that $n_2|3$ and $n_2 \equiv 1 \pmod 2$. Moreover, $n_3|4, n_3 \equiv 1 \pmod 3$. It is easy to see the Sylow 3-groups are just the cyclic subgroups

$$H_1 = \langle(123)\rangle, H_2 = \langle(124)\rangle, H_3 = \langle(134)\rangle, H_4 = \langle(234)\rangle.$$

For the 2-groups, they cannot contain any 3-cycles by Lagrange's Theorem, but there are 8 3-cycles as seen above. As such, there can only be one 2-group

$$V = \{e, (12)(34), (13)(24), (14)(23)\}.$$

(c) $Z(S_4) = \{e\}$ since if $x \in Z(G)$ is nontrivial, it's conjugacy class must be just itself. However by the classification of conjugacy classes of S_n done last week, this is absurd.

For the Sylow subgroups, note $|S_4| = 2^3 * 3$. Then $n_3|8$ and $n_3 \equiv 1 \pmod 3$ by the Sylow theorems, so that there are 1 or 4 sylow subgroups. But since the Sylow 3-groups have order 3, they are cyclic, and it's easy to see they are just the groups generated by 3 cycles, i.e.

$$H_1 = \langle(123)\rangle, H_2 = \langle(124)\rangle, H_3 = \langle(134)\rangle, H_4 = \langle(234)\rangle.$$

Then $n_2|3$ and $n_2 \equiv 1 \pmod 2$ by the Sylow theorems. We know one of the Sylow subgroups is just D_4, or

$$D_4 \cong \{e, (1234), (13)(24), (1432), (24), (14)(23), (13), (12)(34)\}.$$

The second Sylow theorem tells us that conjugates of D_4 are also Sylow subgroups. Noticing that D_4 contains only 2 of the 6 2-cycles, we can conjugate to get the two other groups that have the rest of the 2-cycles.

$$\{e, (1324), (12)(34), (1423), (34), (14)(23), (12), (13)(24)\}, \text{ conjugation via } \pi = (23)$$
$$\{e, (1243), (14)(23), (1342), (23), (13)(24), (14), (12)(34)\}, \text{ conjugation via } \pi = (34)$$

as desired.

□

5 Week 5

We begin by building off of a previous result.

Problem 19. Let G be a finite group, and $H \leq G$ s.t. $[G : H]$, where p is the smallest prime dividing $|G|$. Then $H \triangleleft G$.

Proof. Let $S = \{gH : g \in G\}$ be the left cosets of H in G. Then we can define the group action $\alpha : G \times S \to S$ as

$$\alpha(x, gH) = x \cdot (gH) = (xg)H.$$

This α induces a homomorphism $\phi_\alpha : G \to S_p$ depending on how x permutes S, the left cosets of H in G. Our goal is to show $H = \ker \phi_\alpha$, then it will follow that $H \triangleleft G$ since kernels are normal subgroups.

First, $\ker \phi_\alpha \subseteq H$ since $x \in \ker \phi_\alpha \implies xH = H \implies x \in H$. Now we look at $G/\ker \phi_\alpha$. Clearly we need $|G/\ker \phi_\alpha| \mid |G|$, and since p is the smallest prime dividing G, any prime dividing $|G/\ker \phi_\alpha|$ is $\geq p$. But also we can view $G/\ker \phi_\alpha \leq S_p$, the latter of which has order $p!$.

As such, we either have $|G/\ker \phi_\alpha| = 1$ or p. It can't be 1 since then $G = \ker \phi_\alpha \subseteq H$ which is absurd, so $[G : \ker \phi_\alpha] = p = [G : H]$. But then since $\ker \phi_\alpha \subseteq H$, it must be that $H = \ker \phi_\alpha$ so that $H \triangleleft G$, as desired. □

5.1 Sylow's Theorems

Problem 20. Show that a group of order pq, where p, q are distinct primes, is not simple.

Proof. The core idea of this proof is that the second Sylow Theorem tells us maximal p-groups are all conjugate to each other. As such, if we show that n_p or $n_q = 1$, we will be done. In this case, we know from the third Sylow Theorem that

$$\begin{aligned} n_p &\equiv 1 \pmod p, n_p | q \\ n_q &\equiv 1 \pmod q, n_q | p. \end{aligned}$$

If we assume WLOG that $q > p$, then $n_q | p \implies n_q \leq p < q$, so $n_q \equiv 1 \pmod q$ and $n_q < q \implies n_q = 1$. As such, there is only 1 q-group, and its orbit under conjugation is just itself by the second Sylow Theorem, so it must be normal. □

Problem 21. Show that a group of order $p^2 q$, where p, q are distinct primes, is not simple.

Proof. The key idea for this proof is the same as above. In the case that $p > q$, and from the third Sylow Theorem we have that

$$\begin{aligned} n_p &\equiv 1 \pmod p, n_p | q \\ n_q &\equiv 1 \pmod q, n_q | p^2. \end{aligned}$$

So that $n_p = 1$, and the p-group is a normal subgroup, as desired.

In the case that $q > p$, we still have

$$\begin{aligned} n_p &\equiv 1 \pmod p, n_p | q \\ n_q &\equiv 1 \pmod q, n_q | p^2. \end{aligned}$$

but it is much less clear how to show $n_p = 1$. Suppose that $n_p \neq 1 \implies n_p = q$, and then consider $n_q | p^2$. If $n_q = 1$ then there is a normal q-group, but if not then either $n_q = p$ or $n_q = p^2$. In each case

$$n_q = p, n_q \equiv 1 \pmod q \implies p = 1$$

as $p < q$, but this is absurd since we know p is prime. Otherwise,

$$n_q = p^2, n_q \equiv 1 \pmod q \implies p^2 \equiv 1 \pmod q \implies p \equiv \pm 1 \pmod q.$$

We've already ruled out the $1 \pmod q$ case, so it must be that $p \equiv -1 \pmod q \implies p = q - 1$ as $p < q$. So $p = 2, q = 3$, and if we assume our group is simple, we must have $n_2 = 3, n_3 = 4$. But the Sylow 3-groups here are cyclic, so if there are 4 distinct ones, they must have trivial intersections. As such, we can decompose our group as

1. The identity.
2. $4(3 - 1) = 8$ elements of order 3.
3. Remaining elements.

So there are 4 elements of our group G that do not have order 3. Since since elements of order 3 cannot be contained in the Sylow 2-groups, and the Sylow 2-groups have order 4, all three remaining elements and the identity must be in any Sylow 2-group. But then we can only make one such 2-group, so $n_2 = 1$ and we have a contradiction.

In any case, we've shown that one of $n_p, n_q = 1$, so by the second Sylow theorem, any group of order p^2q contains a nontrivial normal subgroup. □

5.2 Solvability and Nilpotence

Recall the following definitions:

Definition 5.1. Given a group G, the commutator $[g, h]$ of two elements $g, h \in G$ is defined via

$$[g, h] = ghg^{-1}h^{-1}$$

and can be extended to sets via

$$[A, B] = \langle [a, b] : a \in A, b \in B \rangle.$$

Note that an easy result is $gh = hg \iff [g, h] = e$. In class, we showed that if $N \triangleleft G$ with G/N abelian, then $[G, G] \leq N$. In other words, $[G, G]$ is the least normal subgroup $N \triangleleft G$ s.t. G/N is abelian.

Definition 5.2. If G is a group, a series in G is a finite sequence of subgroups $\langle G_i : i \in [n] \rangle$ s.t. $G_1 = \{e\}$, $G_n = G$, and $G_{i-1} \leq G_i$. Such a series is

1. Subnormal if $G_{i-1} \triangleleft G_i$.
2. Normal if $G_i \triangleleft G$.
3. Characteristic if G_i char G.

Definition 5.3. G is solvable if there is some subnormal series $\langle G_i : i \in [n] \rangle$ s.t. G_{i+1}/G_i is abelian $\forall i$.

Definition 5.4. The derived series of a group G is the sequence of subgroups $\langle G^{(i)} \rangle$ where $G^{(i)} = [G^{(i+1)}, G^{(i+1)}]$. The lower central series of a group G is the sequence of subgroups $\langle G^i \rangle$ where $G_i = [G, G_{i+1}]$.

It was shown in class that G is solvable iff its derived series terminates, or $G^{(i)} = \{e\}$ for some $i \in \mathbb{N}$.

Definition 5.5. A group G is nilpotent if its lower central series terminates, i.e. $G^i = \{e\}$ for some $i \in \mathbb{N}$.

The following result is not particularly interesting right now, but will be next semester. It has a close relationship to the fact that there is not a closed form radical solution to polynomials of degree $n \geq 5$ (i.e. no quintic formula). It is also why we use the term "solvable" when describing these groups.

Problem 22. Show that S_5 is not a solvable group.

Proof. We have that

$$1 \lhd A_5 \lhd S_5$$

is a subnormal series of S_5, but A_5 is not abelian. In fact, since we showed in previous weeks that the only normal subgroups of S_5 were $\{e\}, A_5, S_5$, and A_5 is simple, it follows that this is the only nontrivial subnormal series. In either case, since S_5, A_5 are not abelian, it cannot be that S_5 is solvable. □

Problem 23. Recall the dihedral group of the n-gon defined via $D_n = \langle r, s : r^n = s^2 = e, rs = sr^{-1}\rangle$. Show that D_n is solvable, and that it is nilpotent iff n is a power of 2.

Proof. For solvability, we want to find some subnormal series with abelian quotients. An easy normal subgroup of D_n is just $\langle r\rangle \cong C_n \lhd D_n$, the subgroup of rotations. It is normal because $[D_n : C_n] = 2$, and since $|D_n/C_n| = 2$, $D_n/C_n \cong C_2$ which is abelian.

Now C_n is cyclic, so it is abelian, and $1 \lhd C_n$ so that $1 \lhd C_n \lhd D_n$ is the desired subnormal series.

For nilpotency, we analyze $[G, G]$. In general, if $g_1 = r^{i_1}s^{j_1}$ and $g_2 = r^{i_2}s^{j_2}$ then

$$(g_1g_2)(g_1^{-1}g_2{-}1) = r^{i_1}s^{j_1}r^{i_2}s^{j_2}s^{j_1}r^{-i_1}s^{j_2}r^{-i_2}.$$

If where we use the fact that $s^{-1} = s$. We can then case on the values of j_1, j_2, and liberally use the fact that $r^is = sr^{-i}$ in general.

1. $j_1 = j_2 = 0$, then the expression simplifies to the identity.
2. $j_1 = 0, j_2 = 1$, then the expression becomes
$$r^{i_1+i_2}sr^{-i_1}sr^{-i_2} = r^{2i_1+i_2}r^{-i_2} = r^{2i_1}.$$
3. $j_1 = 1, j_2 = 0$, then the expression becomes
$$r^{i_1}sr^{i_2}sr^{-i_1-i_2} = r^{i_1-i_2}r^{-i_1-i_2} = r^{-2i_1}.$$
4. $j_1 = j_2 = 1$, then the expression becomes
$$r^{i_1}sr^{i_2}ssr^{-i_1}sr^{-i_2} = r^{i_1-i_2}r^{i_1-i_2} = r^{2(i_1-i_2)}.$$

It becomes clear from this that $D_n^1 = [D_n, D_n] = \langle r^2\rangle$. Furthermore, we have that

$$D_n^2 = [D_n, D_n^1] = \langle r^is^jr^{2k}s^jr^{-i}r^{-2k}\rangle.$$

In the case that $j = 0$ we have that everything cancels out, and when $j = 1$ we have that

$$r^isr^{2k}sr^{-i}r^{-2k} = r^ir^{-2k}r^{-i}r^{-2k} = r^{-4k}$$

so that $D_n^2 = [D_n, D_n^1] = \langle r^4\rangle$. By induction, it is clear that $D_n^m = \langle r^{2^m}\rangle$, so if we want $D_n^m = \langle r^{2^m}\rangle = \langle e\rangle$ at some point, it must be that $r^{2^m} = e \implies n|2^m$ is a power of 2, as desired. □

Problem 24. What if we consider $D_{\mathbb{N}}$? Here $D_{\mathbb{N}} = \langle r, s : |r| = \infty, s^2 = e, rs = sr^{-1}\rangle$. Another way to think of $D_{\mathbb{N}}$ is $D_{\mathbb{N}} \cong \langle \sigma, \tau\rangle \leq S_{\mathbb{Z}}$ where $\sigma(x) = x + 1$ and $\tau = -x$.

Proof. Solvability still holds, since $1 \lhd \mathbb{Z} \lhd D_{\mathbb{N}}$. For nilpotency, we can repeat the previous process and get that

$$D_{\mathbb{N}}^m = \langle r^{2^m}\rangle.$$

Since r has infinite order, it follows that we will never have $D_{\mathbb{N}}^m = \{e\}$ so that $D_{\mathbb{N}}$ is not nilpotent. However, it gets very "close" to nilpotency as $\cap_m D_{\mathbb{N}}^m = \{e\}$. □

6 Week 6

6.1 Conjugacy in A_n

A frequent error on the homework was citing the result that two permutations with the same cycle decomposition are conjugate to each other in A_n. As a counterexample:

Problem 25. Show that (123) and (132) are not conjugate in A_3.

Proof. It turns out that A_3 is abelian, so these can't be in the same conjugacy class since conjugacy classes are just singleton elements. □

We showed in a previous week (proving A_n simple for $n \geq 5$) that 3-cycles are conjugate to each other in A_n for $n \geq 5$. If you recall, the general idea was that we can show any 3-cycle is conjugate to (123), by first taking a witness $\pi \in S_n$ s.t. $\pi(abc)\pi^{-1} = (123)$, and if π was not even, we could just wack on a (45) term to get

$$((45)\pi)(abc)((45)\pi)^{-1} = (45)(123)(45)^{-1} = (123).$$

A big part of this proof was using the fact that with 3-cycles, we can wiggle in an inversion (45) that doesn't intersect with (123) and force our conjugating element to be even. In general, however, we will not be able to do this if the cycles we deal with are too large w.r.t. the A_n we are working in.

Problem 26. Show that there exist a pair of non-conjugate 5-cycles in A_5. Generalize this to non-conjugate n-cycles for A_n when n is odd. Is there a way to construct "bad examples" when n is even?

Proof. Suppose FTSOC that all 5-cycles were conjugate to each other in A_5. Then partitioning A_5 into orbits under the group action of conjugation, we have that

$$|\text{Orb}_{A_5}((12345))| = \frac{|A_5|}{|C_{A_5}((12345))|}$$

where $\text{Orb}_{A_5}((12345))$ is the conjugacy class of 5-cycles, and $C_{A_5}((12345))$ is the centralizer of (12345), or the stabilizer of (12345) under the group action of conjugation. If we assume that the 5-cycles are all in the same conjugacy class, then $|\text{Orb}_{A_5}((12345))| = 4!$, so we can rewrite the prior expression as

$$24 = \frac{60}{|C_{A_5}((12345))|}$$

but then we have a contradiction since $24 \not| 60$. In general, for n odd, we cannot have all n-cycles in the same conjgacy class. If we could, then applying orbit-stabilizer in the manner above, we would have

$$(n-1)! = \frac{\frac{n!}{2}}{|C_{A_n}((12\ldots n))|} \implies |C_{A_n}((12\ldots n))| = \frac{n}{2} \notin \mathbb{Z}.$$

This method also generalizes to even n, though this time we can't use n-cycles and the previous idea because $\frac{n}{2} \in \mathbb{Z}$. We still want "big" cycles that will break things, so we look at $(n-1)$-cycles instead, supposing FTSOC that they are all in the same conjugacy class. To count the number of $(n-1)$-cycles, there are n ways to pick the fixed point, and after that there are $(n-2)!$ ways to orient the remaining $(n-1)$ elements. As such we have that

$$\begin{aligned}
|\text{Orb}_{A_n}((1,2,\ldots,n-1))| &= \frac{|A_n|}{|C_{A_n}((1,2,\ldots,n-1))|} \\
\implies n(n-2)! &= \frac{\frac{n!}{2}}{|C_{A_n}((1,2,\ldots,n-1))|} \\
\implies |C_{A_n}((1,2,\ldots,n-1))| &= \frac{n-1}{2}.
\end{aligned}$$

But since n is even, $\frac{n-1}{2} \notin \mathbb{Z}$, and we have a contradiction. □

6.2 Polynomial Review

Recall the vector space of polynomials with real coefficients,

$$\mathbb{R}[x] = \{a_n x^n + \ldots + \ldots a_0 : a_i \in R, n \in \mathbb{Z}_{\geq 0}\}.$$

In the coming weeks, we will transition from group theory to ring theory, and a ring that comes up often is polynomial rings. For $\mathbb{R}[x]$ specifically, there are a few interesting results and definitions that we should recall.

Definition 6.1. (Degree) Given some polynomial $p(x) \in \mathbb{R}[x]$ s.t. $p(x) = a_n x^n + \ldots + a_0$ with $a_n \neq 0$, we say $\deg(p) = n$. If $p(x) = 0$, then $\deg(p)$ is not defined.

Problem 27. Given $p(x), q(x) \in \mathbb{R}[x]$ nonzero, we have that $\deg(p) + \deg(q) = \deg(pq)$.

Proof. Just take the product of leading coefficients and note that it is nonzero. □

Problem 28. (Division Algorithm) Suppose we have $a(x), b(x) \in \mathbb{R}[x]$ with $b \neq 0$. Then there exist polynomials $r(x), q(x) \in \mathbb{R}[x]$ s.t.

$$a(x) = b(x)q(x) + r(x)$$

where $\deg(r) < \deg(b)$. Moreover, this representation is unique.

Proof. Fixing $b(x)$, we can induct on the degree of $a(x)$. Our base case is when $\deg(a) < \deg(b)$. In this case, we can just let $a(x) = r(x)$ and $q(x) = 0$, so we're done. For our inductive step, suppose

$$a(x) = a_n x^n + \ldots + a_0$$
$$b(x) = b_m x^m + \ldots + b_0$$

where $\deg(a) = n \geq m = \deg(b)$. Then since $b_m \neq 0$, we can consider

$$a(x) - \frac{a_n}{b_m} x^{n-m} b(x) = \left(a_{n-1} - \frac{a_n b_{m-1}}{b_m}\right) x^{n-1} + \ldots + \left(a_0 - \frac{a_n b_0}{b_m}\right)$$

which is a polynomial of degree $< n$. As such, we can invoke the inductive hypothesis and rewrite this as

$$a(x) - \frac{a_n}{b_m} x^{n-m} b(x) = q'(x)b(x) + r'(x) \implies a(x) = \left(\frac{a_n}{b_m} x^{n-m} + q'(x)\right) b(x) + r'(x)$$

where $\deg(r') < \deg(b)$. But then letting $r = r'$ and $q = \frac{a_n}{b_m} x^{n-m} + q'(x)$ we're done. For uniqueness, suppose that

$$a(x) = b(x)q_1(x) + r_1(x) = b(x)q_2(x) + r_2(x) \implies (r_1 - r_2)(x) = b(x)(q_1 - q_2)(x).$$

If $r_1 \neq r_2$, then $r_1 - r_2$ is a polynomial of degree $< \deg(b)$, but this is impossible since the degree of the RHS is $\geq \deg(b)$. □

Note that a major part of this proof relies on the fact that inverses of nonzero elements exist in $\mathbb{R}$. Specifically, we can repeatedly use the leading term of $b(x)$ to cancel out whatever the leading term is in $a(x)$, and then continue to reduce its degree until it is sufficiently small. Notably, this proof generalizes to polynomials in $\mathbb{C}[x]$, but doesn't generalize to other polynomial rings like $\mathbb{Z}[x]$. As an example consider

$$a(x) = x^2 + 1, b(x) = 2x.$$

We want to find $q(x) \in \mathbb{Z}[x]$ that minimizes the degree of $a(x) - b(x)q(x)$, but this is impossible since the coefficient of x^2 in $a(x)$ is $\equiv 1 \pmod 2$, but all coefficients of $b(x)q(x)$ must be even. As such, the x^2 term will always remain and there will be no way to get a remainder $r(x)$ with degree < 1.

Here are some other useful results.

Theorem 6.1. (Fundamental Theorem of Algebra) Any $p(x) \in \mathbb{C}[x]$ has a root $r \in \mathbb{C}$. Consequently, we can write $p(x) = (x - r_1) \dots (x - r_n)$ as the product of linear terms.

Proof. Math Studies Analysis. □

Theorem 6.2. (Conjugate Root Theorem) If $p(x) \in \mathbb{R}[x]$ and $r = a + bi \in \mathbb{C}$ is a root of $p(x)$, then $\overline{r} = a - bi$ is also a root of $p(x)$.

Proof. We have that

$$\begin{aligned} p(r) &= \sum_{i=0}^{n} a_i r^i = 0 \\ \implies p(\overline{r}) &= \sum_{i=0}^{n} a_i \overline{r}^i = \overline{\sum_{i=0}^{n} a_i r^i} = 0 \end{aligned}$$

as conjugacy distributes across sums and products. □

Notably, we can show the following:

Problem 29. Any polynomial $p(x) \in \mathbb{R}[x]$ splits into linear and quadratic factors (in $\mathbb{R}[x]$).

Proof. First we can pull out all real roots of p, writing $p(x) = (x - r_1) \dots (x - r_k)q(x)$ s.t. $q(x)$ only has complex roots. At this point, if $r = a + bi$ is a complex root of $q(x)$ (so that $b \neq 0$), we have that $\overline{r}$ is as well, and so

$$q(x) = (x - r)(x - \overline{r})s(x) = (x^2 - 2ax + (a^2 + b^2))s(x)$$

for some polynomial $s(x) \in \mathbb{R}[x]$ that only has complex roots. Now inductively we can factor $s(x)$ into the product of quadratic factors in $\mathbb{R}[x]$, so we're done. Note this implies that if $p(x) \in \mathbb{R}[x]$ has only complex roots, it must have even degree. □

In future weeks we will transition from group theory to ring theory, and one subject of particular interest is polynomial rings. Here we have classified how polynomials factorize into "irreducibles" in the rings $\mathbb{R}[x]$ and $\mathbb{C}[x]$, but rings like $\mathbb{Z}[x]$ are not as obvious.

Some important questions to think about as the course transitions are when these irreducible factorizations exist, whether they are unique, and finally when they are, how granular can they get in terms of the degrees of their factors?

7 Week 7

7.1 Ring Theory

Definition 7.1. A *ring* $(R, +, \times)$ is a set R equipped with two binary operations $+, \times$ s.t. $(R, +)$ is an abelian group, and $\times$ is an associative operation (i.e. $a \times (b \times c) = (a \times b) \times c$). R must be closed under both of these operations, and moreover multiplication distributes w.r.t. addition, meaning that

$$a \times (b + c) = (a \times b) + (a \times c) \text{ and } (b + c) \times a = (b \times a) + (c \times a).$$

A ring is said to be commutative if $\times$ is a commutative operator. It is said to contain 1 or have an identity if $\exists 1 \in R$ s.t. $1 \times r = r \times 1 = r \; \forall r \in R$.

Rings are not necessarily commutative nor must they contain 1. Some examples of rings are as follows:

1. $(\mathbb{Z}, +, \times)$.
2. $(\mathbb{R}, +, \times)$.
3. $(2\mathbb{Z}, +, \times)$, a commutative ring without 1.
4. $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$ or $(\mathbb{R}^{2\times 2}, +, \times)$, a ring with 1 but noncommutative.
5. $((2\mathbb{Z})^{2\times 2}, +, \times)$, a noncommutative ring that has no 1.
6. $(\mathbb{Z}/p\mathbb{Z}, +, \times)$, integers modulo p for p prime.
7. $(\mathbb{Z}/m\mathbb{Z}, +, \times)$, integers modulo m for $m \in \mathbb{N}$ arbitrary.
8. $(R[x], +, \times)$, polynomials with coefficients in R.

Note that it is not necessarily the case that $rs = 0 \implies r = 0$ or $s = 0$ (Zero product property). As an example $2 \times 3 = 0$ in $\mathbb{Z}/6\mathbb{Z}$. You may also notice that some of these rings have multiplicative inverses for their nonzero elements, like $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{R}$. Rings that exhibit this property ($R \setminus \{0\}$ is an abelian group under multiplication) are called *fields*. If you recall last weeks discussion of division algorithms for polynomial rings, we essentially showed that $R[x]$ admits a nice division algorithmm when R is a field.

Problem 30. Show that $0 \times r = r \times 0 = 0$ for any $r \in R$.

Proof. We must have by distributivity that

$$r \times (0 + 0) = r \times 0 + r \times 0 \implies r \times 0 = r \times 0 + r \times 0 \implies 0 = r \times 0$$

as desired. □

Problem 31. Additive and multiplicative identities are unique. In other words, if $r + s = r \; \forall r \in R$, we must have that $s = 0$, and if $r \times s = r \; \forall r \in R$, then $s = 1$. Is it ever the case that $0 = 1$? In what rings does this occur?

Proof. Uniqueness of the additive identity follows since $(R, +)$ is a group and therefore has a unique identity element. For uniqueness of the multiplicative identity, note that we have

$$r \times s = r \implies 1 \times s = 1 \implies s = 1$$

by plugging in $r = 1$.

Suppose that $0 = 1$ so that $\forall r \in R$ we have

$$r \times 0 = r \times 1 \implies 0 = r.$$

As such, unless R is the "trivial" ring $R = \{0\}$, the additive and multiplicative identities do not coincide. □

Problem 32. Show that $-r = (-1) \times r = r \times (-1)$ and subsequently that $(-r) \times (-s) = r \times s$ for any $r, s \in R$.

Proof. For the first statement, we note that

$$r + (-r) = 0 \implies (r \times 1) + (-r) = 0 \implies (r \times (-1)) + (r \times 1) + (-r) = r \times (-1).$$

By distributivity on the LHS, we get that

$$r \times ((-1) + 1) + (-r) = r \times (-1) \implies r \times 0 + (-r) = r \times (-1) \implies -r = r \times (-1)$$

as desired. The proof for $(-1) \times r$ is analogous. Now for the last part of the problem, we note that

$$(-r) \times (-s) = ((-1) \times r) \times ((-1) \times s) = ((-1) \times (-1)) \times (r \times s)$$

using the previous parts so that it suffices to show $(-1) \times (-1) = 1$. To see this, note that

$$\begin{aligned} &0 = (1 + (-1)) \times (1 + (-1)) = (1 \times 1) + (1 \times (-1)) + ((-1) \times 1) + ((-1) \times (-1)) \\ \implies &0 = 1 + (-1) + (-1) + ((-1) \times (-1)) \\ \implies &1 = (-1) \times (-1). \end{aligned}$$

□

Definition 7.2. A *ring homomorphism* between two rings R, S is a mapping $\phi : R \to S$ s.t. $\phi(r+s) = \phi(r)+\phi(s)$ and $\phi(rs) = \phi(r)\phi(s)$ for $r, s \in R$. In the case that R, S contain 1, ϕ is said to be *unital* if $\phi(1_R) = 1_S$.

The following exercises construct some ring homomorphisms and show that they are well-defined.

Problem 33. Suppose R is a ring with 1. Show that there exists a unique unital ring HM $\phi : \mathbb{Z} \to R$.

Proof. We need $\phi(0) = 0_R$ and $\phi(1) = 1_R$, so a simple induction yields that

$$\phi(n) = \sum_{i=1}^{n} 1_R$$

where $\sum$ is defined for addition in R. For negative numbers, we also must have that

$$\phi(n + (-n)) = \phi(0) = 0_R \implies \phi(-n) = -\sum_{i=1}^{n} 1_R.$$

As such, if ϕ exists, then it must be defined as above. Verifying that this is a HM is left as an exercise. □

Problem 34. Show that $\phi : R \to R[x]$ via $\phi(r) = r$ is an injective ring homomorphism.

Proof. It is easy to verify that the properties of a ring HM hold. It is injective since $\phi(r) = 0 \implies \phi(r) = r = 0$. □

Problem 35. Let R, S be commutative rings with 1, $f : R \to S$ be a unital homomorphism, and $s \in S$. Show that there exists a unique ring HM $g : R[x] \to S$ that satisfies $g \circ \phi = f$ and $g(x) = s$, where ϕ is as defined in the previous problem.

Proof. Given $a_n x^n + \ldots + a_0 \in R[x]$, we need

$$\begin{aligned} g(a_n x^n + \ldots + a_0) &= g(a_n x^n) + \ldots + g(a_0) \\ &= f(a_n) g(x)^n + \ldots + f(a_0) g(1) \\ &= f(a_n) s^n + \ldots + f(a_0) \\ &= \sum_{i=0}^{n} f(a_i) s^i. \end{aligned}$$

As such, if g exists s.t. $g \circ \phi = f$ and $g(x) = s$, it must evaluate according to the rules above. To show that g is a HM, we note that if $\sum_{i=0}^n a_i x^i$ and $\sum_{j=0}^m b_j x^j \in R[x]$ then we have that

$$\begin{aligned} g\left(\sum_{i=0}^n a_i x^i\right) + g\left(\sum_{j=0}^m b_j x^j\right) &= \sum_{i=0}^n f(a_i)s^i + \sum_{j=0}^m f(b_j)s^j \\ &= \sum_{i=0}^{\max(n,m)} (f(a_i) + f(b_i))s^i \\ &= \sum_{i=0}^{\max(n,m)} f(a_i + b_i)s^i \\ &= g\left(\sum_{i=0}^{\max(n,m)} (a_i + b_i)x^i\right) \end{aligned}$$

as desired. For multiplication, we note that

$$\begin{aligned} g\left(\sum_{i=0}^n a_i x^i\right) \times g\left(\sum_{j=0}^m b_j x^j\right) &= \left(\sum_{i=0}^n f(a_i)\right) s^i \times \left(\sum_{j=0}^m f(b_j)s^j\right) \\ &= \sum_{i=0}^n f(a_i)s^i \left(\sum_{j=0}^m f(b_j)s^j\right) \\ &= \sum_{i=0}^n \sum_{j=0}^m f(a_i)f(b_j)s^{i+j} \\ &= \sum_{i=0}^n \sum_{j=0}^m f(a_i b_j)s^{i+j} \\ &= \sum_{k=0}^{m+n} \sum_{i=0}^k f(a_i b_{k-i})s^k \\ &= \sum_{k=0}^{m+n} f\left(\sum_{i=0}^k a_i b_{k-i}\right) s^k \\ &= g\left(\sum_{k=0}^{m+n} a_i b_{k-i} x^k\right) \\ &= g\left(\left(\sum_{i=0}^m a_i x^i\right) \times \left(\sum_{j=0}^n b_j x^j\right)\right). \end{aligned}$$

□

This essence of this construction is the universal property of polynomial rings. The following commutative diagram illustrates what's going on under the hood:

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\phi"] & S \\ R[x] \arrow[ur, "g"] & \end{tikzcd}.$$

One way to think about this is that any time we want to extend R to contain some $s \notin R$, we can first send $R \to R[x]$ and then send $x \to s$ for our desired s. The fact that this works for any $s \in S$ makes $R[x]$ a "universal" extension of R.

8 Week 8

8.1 Ideals

Definition 8.1. An *ideal* I of a ring R is a subset $I \subseteq R$ s.t. $I \leq R$ as an additive subgroup and $rI \subseteq I, Ir \subseteq I$ for any $r \in R$.

Sometimes in the case where R is not commutative, we differentiate between left ideals where it is only the case that $rI \subseteq I$ and right ideals, where it is only the case that $Ir \subseteq I$ for $r \in R$. For the purposes of this recitation we will assume our ideals are two-sided.

Problem 36. Show that if I, J are ideals of R, then $I \cap J$ is also an ideal.

Proof. Intersections of subgroups are still subgroups. Also, if $x \in I \cap J$, then

$$rx \in I, J \implies rx \in I \cap J \implies r(I \cap J) \subseteq I \cap J.$$

□

Note that the above proof also generalizes to arbitrary intersections.

Definition 8.2. For $A \subseteq R$, we can let (A) denote the ideal generated by A, i.e.

$$(A) = \bigcap_{A \subseteq I \subseteq R, I \text{ ideal}} I.$$

In the case where $A = \{a\}$ is a singleton element, we write $(A) = (a)$ and call (a) the *principal ideal* generated by a.

Problem 37. Classify the ideals of $\mathbb{Z}$.

Proof. Suppose that $I \subseteq \mathbb{Z}$ is an ideal. Let $n \in I$ be the least nonnegative element of I. Such an element exists since $\mathbb{Z}$ is well-ordered. We have two cases:

Case 1: $n = 0$.
In this case, $I = (0)$, since $\nexists m \in \mathbb{Z}$ s.t. $m > 0$ by assumption, and there cannot exist $m < 0$ s.t. $m \in \mathbb{Z}$ or else we would have $-m \in \mathbb{Z}$ and $-m > 0$. Therefore $I = (0)$.

Case 2: $n > 0$.
In this case $I = (n) = n\mathbb{Z}$. Clearly $(n) = n\mathbb{Z}$ since $n \in (n) \implies nm \in (n)$ for any $m \in \mathbb{Z}$, and it is easy to verify that $n\mathbb{Z}$ is an ideal. As such, we have that $(n) \subseteq I$. Suppose FTSOC that $\exists m \in I$ s.t. $n \not| m$. Then by division algorithm, we can rewrite

$$m = nq + r, 0 < r < n \implies r = m - nq \in I.$$

But this clearly violates the minimality of n, so we have a contradiction and $I = (n)$. □

We showed a pretty interesting result about $\mathbb{Z}$, specifically that all of its ideals are generated by single elements. This turns out to be a property that comes up with other rings, and we can introduce the following definition to generalize.

Definition 8.3. When R is an integral domain (commutative ring with no zero-divisors), R is called a *Principal Ideal Domain* or a PID if it is the case that all ideals I can be written as $I = (r)$ for some $r \in R$. In other words, every ideal is principal.

Problem 38. Show that $\mathbb{F}[x]$ is a PID for fields $\mathbb{F}$.

Proof. The idea is the same as for $\mathbb{Z}$, we just need to use the division algorithm. First take some ideal $I \subseteq \mathbb{F}[x]$ and assume that $I \neq (0)$. Then I contains elements with well-defined degrees, so pick any $p(x)$ s.t. $\deg(p)$ is minimal.

We show that $I = (p)$. Clearly $p(x)\mathbb{F}[x] = (p) \subseteq I$, so suppose FTSOC that $\exists a(x) \in I$ s.t. $a(x) \notin (p)$. Then by division algorithm,

$$a(x) = p(x)q(x) + r(x), 0 \leq \deg(r) < \deg(p) \implies r(x) = a(x) - p(x)q(x) \in I$$

but this clearly violates the minimality of $\deg(p)$ unless $r = 0$. Note in the case that $\deg(p) = 0$ and p is a constant, we have that $p \in \mathbb{F}$ so therefore $p\mathbb{F}[x] = \mathbb{F}[x]$, and we're done. □

Ideals can also give an interesting way of classifying fields. Last week we defined fields as commutative rings with 1 that had inverses for all nonzero elements (i.e. all nonzero elements are units). Alternatively, we have that

Problem 39. Suppose that R is an ID (integral domain) with 1. Show that R is a field iff its only ideals are $(0), R$.

Proof. Clearly if R is a field and $I \subseteq R$ is an ideal, then if $I \neq (0)$, $\exists r \in I$ s.t. $r \neq 0$. But then $1 = rr^{-1} \in I \implies I = (1) = R$.

If R is a ring with only the trivial ideals, then it must be that for any $r \neq 0$, we have $(r) = R$. But then $(r) = rR \implies \exists r^{-1}$ s.t. $rr^{-1} = r^{-1}r = 1$, and therefore all nonzero elements are units. □

Problem 40. Suppose R is a finite integral domain that contains 1. Show that R is actually a field.

Proof. We need to show that all nonzero elements $r \in R$ are units. Since R is finite, we have that $R = \{0, r_1, r_2, \ldots, r_n\}$. Consider $rR = \{0, rr_1, \ldots, rr_n\}$, and note that for $i, j \in [n]$ we have

$$rr_i = rr_j \implies r(r_i - r_j) = 0 \implies r_i - r_j = 0 \implies r_i = r_j$$

as R is an integral domain. As such, the elements of rR are all distinct so that $|rR| = |R|$, and $rR \subseteq R \implies rR = R$. Since $0 \neq 1$, it must be that $\exists i \in [n]$ s.t. $rr_i = r_ir = 1$, and therefore r is a unit, as desired. □

8.2 Zorn's Lemma and More Ideals

Recall Zorn's lemma:

Theorem 8.1. (Zorn) Suppose we have a poset $\mathbb{P}$ s.t. every chain $\mathcal{C}$ in $\mathbb{P}$ has an upper bound in $\mathbb{P}$. Then $\mathbb{P}$ contains a maximal element.

Zorn's Lemma is often useful in studying maximal ideals, which are defined as

Definition 8.4. In a ring R, a proper ideal I (i.e. $I \neq R$) is called *maximal* if $I \subseteq J$ and J is an ideal $\implies J = R$.

Problem 41. Show that any ring with 1 contains a maximal ideal.

Proof. Consider the poset $\mathbb{P}$ of proper ideals ordered by maximality. To apply Zorn's lemma, we show that any chain $\mathcal{C}$ has an upper bound. To do this, fix some arbitrary chain $\mathcal{C}$ and take

$$J = \bigcup_{I \in \mathcal{C}} I$$

which we claim is a proper ideal. To see why it is an ideal, note that if $x, y \in J$, then $\exists I \in \mathcal{C}$ s.t. $x, y \in I$. As such, we have that

$$x, y \in J \implies x, y \in I \implies x + y \in I \implies x + y \in J$$

and so J is closed under addition. Moreover, if $x \in J$, then we have that $\forall r \in R$,

$$x \in J \implies \exists I \in \mathcal{C} \text{ s.t. } x \in I \implies rx \in I \implies rx \in J$$

so that J is an ideal. To see why J is proper, note that an ideal is proper $\iff$ it contains 1. As such, since $1 \notin I \; \forall I \in \mathbb{P}$, we have that $1 \notin \cup_{I \in \mathcal{C}} I = J$, and J must be a proper ideal containing all $I \in \mathcal{C}$. By Zorn's Lemma, $\mathbb{P}$ must have a maximal element. □

9 Week 9

9.1 Prime Ideals

Definition 9.1. $I \subset R$ is a *prime ideal* if $I \neq R$ and $ab \in I \implies a \in I$ or $b \in I$.

Problem 42. Suppose $I, J \subseteq R$ are ideals. Show that $I + J = \{i + j : i \in I, j \in J\}$ is an ideal and that it is the smallest ideal contianing I, J.

Proof. First if $K \supseteq I, J$ is an ideal, then it contains all $i \in I$ and $j \in J$, so by closure under addition it follows that $i + j \in K$, and therefore $I + J \subseteq K$. It suffices to show that $I + J$ is an ideal. Closure under addition is easy, since

$$i_1 + j_1, i_2 + j_2 \in I + J \implies (i_1 + i_2) + (j_1 + j_2) \in I + J$$

and if $r \in R$, then we have that

$$i + j \in I + J \implies ri + rj \in I + J \implies r(i + j) \in I + J.$$

So $I + J$ is the smallest ideal containing I, J. □

Problem 43. Show that if I is maximal in a commutative ring with 1, then it is also prime.

Proof. Suppose $ab \in I$ but neither $a \in I$ nor $b \in I$. We wish to contradict the maximality of I, so consider $I + (a)$, the smallest ideal containing both I and (a). By maximality, $I + (a) = R$, so we have that

$$\exists i \in I, r \in R \text{ s.t. } i + ra = 1 \implies ib + rab = b \implies b \in I$$

as $ib \in I$ and $ab \in I \implies rab \in I$. But then this contradicts our original assumption. □

Problem 44. Classify the prime ideals of $\mathbb{Z}$. Classify the maximal ideals of $\mathbb{Z}$.

Proof. Suppose that $(n) \subseteq \mathbb{Z}$ is prime. Then

$$n|ab \iff ab \in (n) \iff a \in (n) \text{ or } b \in (n) \iff n|a \text{ or } n|b.$$

This clearly works if n is prime, so if n is prime then (n) is a prime ideal. In the case that n is composite, it can be written as $a \cdot b = n$ for $1 < a, b < n$ (assume $n > 0$). But then clearly $a, b \notin (n)$ but $ab \in (n)$, so (n) cannot be prime. Note also that (0) is prime.

For maximal ideals, they must be prime. It is easy to verify that all of the previous ideals are maximal with the exception of (0). To see why this is true, note that when p is prime and we add some non-multiple of p to (p), we can use Bezout's lemma to generate 1 in the newly formed ideal. □

9.2 Products and Coproducts

Definition 9.2. Let $\mathcal{C}$ be a category with $X_1, X_2 \in \text{Obj}(\mathcal{C})$. The product $X_1 \times X_2$ is another object in $\mathcal{C}$ s.t. there exist morphisms $\pi_1 : X_1 \times X_2 \to X_1, \pi_2 : X_1 \times X_2 \to X_2$ satisfying the following universal property:

$$\forall Y \in \text{Obj}(\mathcal{C}), f_1 : Y \to X_1, f_2 : Y \to X_2, \exists! f : Y \to X_1 \times X_2 \text{ s.t. the following diagram commutes}$$

$$\begin{tikzcd}
 & Y \arrow[dl, "f_1"'] \arrow[d, dashed, "f"] \arrow[dr, "f_2"] & \\
X_1 & X_1 \times X_2 \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & X_2
\end{tikzcd}$$

Problem 45. Show that if the product $X_1 \times X_2$ exists, it is unqiue up to isomorphism.

Proof. Suppose that $X = X_1 \times X_2$ with projection morphisms π_1, π_2 and X' is another "product" with projection morphisms π_1', π_2'. By commutativity of the diagram with $Y = X'$, we have that $\exists! f : X' \to X$ s.t.

$$\pi_1' = \pi_1 f, \pi_2' = \pi_2 f$$

and moreover, swapping positions of X, X', we have that $\exists! f' : X \to X'$ s.t.

$$\pi_1 = \pi_1' f', \pi_2 = \pi_2' f' \implies \pi_1 = \pi_1 f f', \pi_2 = \pi_2 f f'.$$

It suffices to show that $ff' = \mathrm{id}_X$. But note that $\pi_1 = \pi_1 ff', \pi_2 = \pi_2 ff'$ means that ff' satisfies the universal property for $Y = X = X_1 \times X_2$ in the above commutative diagram. But clearly, id_X also satisfies the commutativity of the diagram, so by uniqueness of the $Y \to X$ morphism, we have $\mathrm{id}_X = ff'$ as desired. By symmetry, $f'f = \mathrm{id}_{X'}$, and so $X_1 \times X_2$ is unique up to isomorphism. $\square$

Now we look at what products are in some familiar categories.

Problem 46. Verify that the products in the category of sets is just the cartesian product, and verify that products in the category of groups are product groups.

Proof. We know from the previous problem that if the product exists, it is unique up to isomorphism, so we just need to verify the required properties. Suppose S_1, S_2 are sets, and let $S_1 \times S_2$ denote their cartesian product. Intuitively, we want the morphisms/functions $\pi_1 : S_1 \times S_2 \to S_1$ and $\pi_2 : S_1 \times S_2 \to S_2$ to satisfy

$$\pi_1(s_1, s_2) = s_1, \pi_2(s_1, s_2) = s_2.$$

We now verify that these morphisms make $S_1 \times S_2$ the product of sets S_1, S_2 in the category of sets. Suppose that T is a set with morphisms/functions $f_1 : Y \to X_1, f_2 : Y \to X_2$. In order for $f : T \to S_1 \times S_2$ to satisfy the universal property, we need

$$f_1(t) = \pi_1(f(t)), f_2(t) = \pi_2(f(t)) \ \forall t \in T \implies f(t) = (f_1(t), f_2(t)).$$

It is easy to verify that $f : T \to S_1 \times S_2$ is a valid function, and the above shows that it is uniquely defined, so $S_1 \times S_2$ must be the product in the category of sets.

We now do the same for groups. Let G_1, G_2 be groups, $G_1 \times G_2$ be the direct product, and $\pi_1 : G_1 \times G_2 \to G_1, \pi_2 : G_1 \times G_2 \to G_2$ be the obvious projection homomorphisms. Let H be a group with homomorphisms $f_1 : H \to G_1, f_2 : H \to G_2$. We need $f : H \to G_1 \times G_2$ s.t.

$$f_1(h) = \pi_1(f(h)), f_2(h) = \pi_2(f(h)) \ \forall h \in H \implies f(h) = (f_1(h), f_2(h)).$$

So if $f : H \to G_1 \times G_2$ exists, it is unique. We verify it is a homomorphism by noting that

$$f(h_1h_2) = (f_1(h_1h_2), f_2(h_1h_2)) = (f_1(h_1)f_1(h_2), f_2(h_1)f_2(h_2)) = (f_1(h_1), f_2(h_1))(f_1(h_2), f_2(h_2)) = f(h_1)f(h_2)$$

So the direct product $G_1 \times G_2$ is the product of G_1, G_2 in the category of groups. $\square$

Definition 9.3. Let $\mathcal{C}$ be a category with $X_1, X_2 \in \mathrm{Obj}(\mathcal{C})$. The coproduct $X_1 \sqcup X_2$ is another object in $\mathcal{C}$ s.t. there exist morphisms $i_1 : X_1 \to X_1 \sqcup X_2, i_2 : X_2 \to X_1 \sqcup X_2$ satisfying the following universal property:

$$\forall Y \in \mathrm{Obj}(\mathcal{C}), f_1 : X_1 \to Y, f_2 : X_2 \to Y, \exists! f : X_1 \sqcup X_2 \to Y \text{ s.t. the following diagram commutes}$$

$$\begin{tikzcd}
 & Y & \\
X_1 \arrow[ur, "f_1"] \arrow[r, "i_1"'] & X_1 \coprod X_2 \arrow[u, dashed, "f"] & X_2 \arrow[ul, "f_2"'] \arrow[l, "i_2"]
\end{tikzcd}$$

Problem 47. Prove that the coproduct is unique up to isomorphism.

Proof. Proceed in the same way as with products, letting $X = X_1 \sqcup X_2$ and X' be two non-isomorphic coproducts of the two categories with corresponding morphisms

$$i_1 : X_1 \to X, i_2 : X_2 \to X, i_1' : X_1 \to X', i_2' : X_2 \to X'.$$

Then we must have that letting $Y = X'$ in the above diagram, and $f_1 = i_1', f_2 = i_2'$, $\exists! f : X \to X'$ and $f' : X' \to X$ s.t.

$$i_1' = fi_1, i_1 = f'i_1', i_2' = fi_2, i_2 = f'i_2' \implies i_1 = f'fi_1, i_2 = f'fi_2.$$

But now note that setting $Y = X$ in the above commutative diagram so that $f_1 = i_1$ and $f_2 = i_2$, $f'f$ satisfies the commutativity of the diagram. But id_X also satisfies commutativity, so by uniqueness of the morphism, $f'f = \mathrm{id}_X$. By symmetry, $ff' = id_{X'}$, so X, X' are isomorphic, as desired. □

Problem 48. Classify coproducts in the category of sets.

Proof. Intuitively, if we have S_1, S_2, we just want their coproduct to be the union of the sets, then define f as f_1 or f_2 depending on which set the argument belongs to. This fails, however, when S_1, S_2 have a nontrivial intersection, so we fix this by defining the *disjoint union*

$$S_1 \sqcup S_2 = (\{1\} \times S_1) \cup (\{2\} \times S_2)$$

with

$$i_1(s) = (1, s), i_2(s) = (2, s)$$

and given $f_1 : S_1 \to T, f_2 : S_2 \to T$, letting

$$f(i, s) = f_i(s).$$

We now show that this construction is a valid coproduct. Given some set T and functions $f_1 : S_1 \to T, f_2 : S_2 \to T$, we must have that

$$f_1(s) = f(i_1(s)) = f(1, s), f_2(s) = f(i_2(s)) = f(2, s)$$

which is uniquely satisfied by our construction, so $S_1 \sqcup S_2$ is the coproduct. □

While in sets we can just take disjoint unions, the same does not necessarily hold for other algebraic structures like groups, as unions of groups are not necessarily groups. We start with a simpler example first:

Problem 49. Find the coproduct of two copies of $(\mathbb{Z}, +)$ in the category of groups.

Proof. For the purposes of this problem, we let the first copy of $(\mathbb{Z}, +) \cong \langle a \rangle$ and the second copy of $(\mathbb{Z}, +) \cong \langle b \rangle$ where $|a| = |b| = \infty$ so that we can distinguish the two groups. It's clear that if $\phi_1 : \langle a \rangle \to G$ and $\phi_2 : \langle b \rangle \to G$ are homomorphisms, then they are uniquely defined by where they send their generators a, b. Moreover, we want to be able to "embed" $\langle a \rangle$ and $\langle b \rangle$ into $\langle a \rangle \sqcup \langle b \rangle$ so that if $\phi : \langle a \rangle \sqcup \langle b \rangle \to G$, then

$$\phi_1(a) = \phi(i_1(a)), \phi_2(b) = \phi(i_2(b)).$$

However in this case with groups, it is not as clear how to deal with products of elements from the first and second group (i.e. where would we send ab or $abab$?) This motivates setting $\langle a \rangle \sqcup \langle b \rangle = Free(\{a, b\})$ with $i_1(a) = a$ and $i_2(b) = b$.

If $\langle a \rangle \sqcup \langle b \rangle = Free(\{a, b\})$, then we must have $\phi(a) = \phi_1(a)$ and $\phi(b) = \phi_1(b)$ by the logic above. Then by the universal property of free groups, $\exists! \phi : Free(\{a, b\}) \to G$ satisfying this property. It is easy to see this ϕ makes the diagram commute, so since it is unique we're done. □

In general, the coproduct of two groups can be classified via something called the *free product*, which generalizes what we've done above (the free product of two copies of $\mathbb{Z}$ is just the free group on two elements). s Free products are something that come up a lot in Algebraic Topology, and you'll dive into this more on the homework.

10 Week 10

10.1 Euclidean Domains

Definition 10.1. Let R be an integral domain. Then a *Euclidean function* $f : R \setminus \{0\} \to \mathbb{N}^{\geq 0}$ is a function f satisfying the division algorithm. That is, for any $a, b \in R$ with $b \neq 0$ then $\exists q, r \in R$ s.t.

$$a = bq + r \text{ and } r = 0 \text{ or } f(r) < f(b).$$

A *Euclidean domain* is an R that admits a Euclidean function. Note that the Euclidean function is not guaranteed to be unique, and it is only required that it be unique.

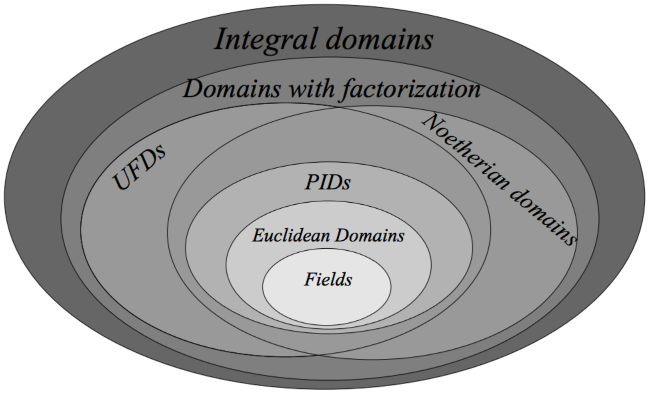
Problem 50. Show that Euclidean domains are PIDs.

Proof. Take some ideal $I \subseteq R$ s.t. $I \neq (0), R$. Let $0 \neq b \in I$ be chosen s.t. $f(b)$ is minimal. Then $\forall a \in I$, apply the division algorithm to get that

$$a = bq + r \implies a - bq = r \in I$$

as $a \in I, b \in I$. By the properties of a Euclidean domain, either $f(r) < f(b)$ or $r = 0$, but we can only have the latter or else our minimality assumption for b is violated. □

The following diagram gives a way of tying in all the different types of domains.



Examples of rings with those specific properties are as follows:

1. Field: $\mathbb{R}$.
2. Euclidean Domain: $\mathbb{Z}$ (not Field).
3. PID: $\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-19})\right]$ (not Euclidean, proof too complicated).
4. UFD and Noetherian: $\mathbb{Z}[x]$ (not PID).
5. Domain with Factorization: $Z[\sqrt{-5}]$ (not UFD, consider $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$).

10.2 Gaussian Integers

Definition 10.2. We define the ring of Gaussian integers as

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

where $i = \sqrt{-1}$.

Definition 10.3. We define the norm $N : \mathbb{Z}[i] \to \mathbb{Z}$ as the (multiplicative) group homomorphism

$$N(a + bi) = (a + bi)\overline{(a + bi)} = a^2 + b^2.$$

Problem 51. Verify that N is multiplicative.

Proof. Routine to verify that

$$\begin{aligned}N((a+bi)(c+di)) &= N((ac-bd)+(ad+bc)i)\\&=(ac-bd)^2+(ad+bc)^2\\&=a^2c^2+b^2d^2+a^2d^2+b^2c^2\\&=(a^2+b^2)(c^2+d^2)\\&=N(a+bi)N(c+di).\end{aligned}$$

□

Note that the previous proof works regardless of whether $a+bi, c+di \in \mathbb{Z}[i]$ or $\mathbb{C}$, so we can extend our definition of N to any complex number and it will still be multiplicative.

Problem 52. Use N to classify the units of $\mathbb{Z}[i]$.

Proof. Suppose that $\alpha \in \mathbb{Z}[i]$ is a unit so that $\exists \beta \in \mathbb{Z}[i]$ s.t. $\alpha\beta = 1$. Then $N(\alpha)N(\beta) = 1$. However, $N(\alpha), N(\beta)$ are nonnegative integers, and this can only occur when

$$N(\alpha) = N(\beta) = 1.$$

So if $\alpha = a+bi$ then $a^2+b^2 = 1 \implies \alpha = \pm 1$ or $\pm i$. □

Theorem 10.1. $\mathbb{Z}[i]$ is Euclidean.

Proof. We wish to show that $\mathbb{Z}[i]$ admits a division algorithm. Suppose $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$ s.t.

$$\frac{\alpha}{\beta} = a+bi \in \mathbb{Q}[i].$$

Let $a = a_0 + a_1, b = b_0 + b_1$, where $a_0, b_0 \in \mathbb{Z}$ are the closest integers to a, b respectively, and therefore $a_1, b_1 \in \left[-\frac{1}{2}, \frac{1}{2}\right]$. As such, we have that

$$\alpha = \beta(a_0+b_0i) + \beta(a_1+b_1i).$$

Let $q = a_0 + b_0 i \in \mathbb{Z}[i]$, and note that this implies

$$r = \beta(a_1+b_1i) = \alpha - \beta(a_0+b_0i) \in \mathbb{Z}[i].$$

But we also have that

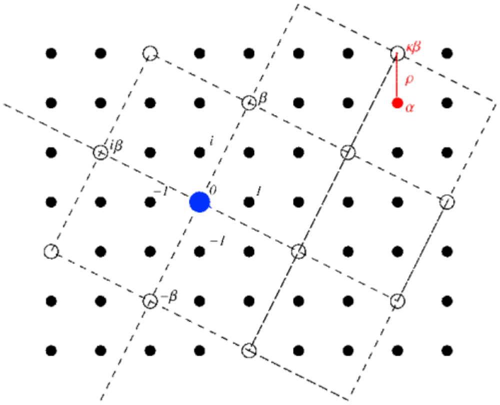
$$N(r) = N(\beta)N(a_1+b_1i) \leq \frac{2}{4}N(\beta) = \frac{1}{2}N(\beta)$$

where we have used the fact that N generalizes to any complex number as well. As such, for any $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, $\exists q, r \in \mathbb{Z}[i]$ s.t. $\alpha = \beta q + r$ and $N(r) \leq \frac{1}{2}N(\beta) < N(\beta)$, so $\mathbb{Z}[i]$ is Euclidean. □

Theorem 10.2. Geometrically classify the ideals of $\mathbb{Z}[i]$.

Proof. Since $\mathbb{Z}[i]$ is Euclidean, it is a PID and every ideal is of the form $(\beta) = \beta\mathbb{Z}[i]$ for some $\beta \in \mathbb{Z}[i]$. It turns out that this is just exactly the lattice generated by the two vectors $\beta, \beta i$ since you can then generate any $\beta(a + bi)$ for $a + bi \in \mathbb{Z}[i]$. □

It turns out that the above classification of ideals gives motivation for a geometric proof of the division algorithm in $\mathbb{Z}[i]$. Consider the following diagram:



For any $\alpha \in \mathbb{Z}[i]$, it is located in one of the boxes with four vertices that are all multiples of β in $\mathbb{Z}[i]$. To best approximate α as a multiple of β, we can just pick the closest vertex of the box and take the difference of those points as our remainder r.

In the worst case, α is equally spaced from all four vertices of the box, and in that case $N(r) = \left(\frac{1}{\sqrt{2}}\right)^2 N(\beta) < N(\beta)$, so the divison algorithm still works out.

Problem 53. Consider the ring $\mathbb{Z}/p\mathbb{Z}$ where p is prime. For which primes p is x^2+1 irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$? What is the structure of $(\mathbb{Z}/p\mathbb{Z})[x]/(x^2+1)$?

Proof. Suppose that $x^2 + 1$ reduces in $(\mathbb{Z}/p\mathbb{Z})$. Then since all nonzero scalars are units in $(\mathbb{Z}/p\mathbb{Z})$, it must be that

$$x^2 + 1 = (ax + b)(cx + d)$$

for nonzero $a, c \in \mathbb{Z}/p\mathbb{Z}$. But this implies that $x^2 + 1$ has roots $-ba^{-1}$ and $-dc^{-1}$, so it must be that -1 is a perfect square modulo p. It is well-known that this occurs iff $p \equiv 1 \pmod 4$, so $x^2 + 1$ is irreducible if $p \equiv 3 \pmod 4$.

When $p \equiv 1 \pmod 4$, it is not the case that $x^2 + 1$ is irreducible since if $a^2 \equiv -1 \pmod 4$ then we have that

$$(x - a)(x + a) = x^2 - ax + ax - a^2 = x^2 + 1.$$

Now we consider $(\mathbb{Z}/p\mathbb{Z})[x]/(x^2 + 1)$. Since $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$ is a field, we know via division algorithm that

$$\mathbb{F}[x]/(x^2 + 1) = (\mathbb{Z}/p\mathbb{Z})[x]/(x^2 + 1) = \{ax + b : a, b \in \mathbb{Z}/p\mathbb{Z}\}.$$

However, it turns out that the structure of the above ring is different based on whether $p \equiv 1, 3 \pmod 4$. First consider when $p \equiv 1 \pmod 4$ and $-1 \equiv i^2 \pmod 4$ where $i \in \mathbb{Z}/p\mathbb{Z}$. We have a ring with p^2 elements, but it turns out that it isn't even a domain, since

$$(x + i)(x - i) = x^2 + 1 = 0$$

as $i \in \mathbb{Z}/p\mathbb{Z} \implies x \pm i \in (Z/p\mathbb{Z})[x]$.

In the other case where $p \equiv 3 \pmod 4$, note that (x^2+1) is irreducible in $\mathbb{F}[x] = (\mathbb{Z}/p\mathbb{Z})[x]$, so since $\mathbb{F}[x]$ is a PID, it follows that (x^2+1) is a prime ideal. So $(\mathbb{Z}/p\mathbb{Z})[x]/(x^2+1)$ is an integral domain, but it is finite, so it is also a field. Note that here we've explictly constructed a field with p^2 elements.

The case where $p = 2$ is left as an exercise. □

11 Week 11

Shorter recitation this week because of Thanksgiving break.

11.1 $\mathbb{Z}[\sqrt{-5}]$

The classical example of a $\mathbb{Z}[\alpha]$ which isn't a UFD is $\mathbb{Z}[\sqrt{-5}]$. To see this, we first note that by defining the norm

$$N(a+b\sqrt{-5}) = a^2 + 5b^2$$

we get the same multiplicative properties as in $\mathbb{Z}[i]$, as in $N(\alpha\beta) = N(\alpha)N(\beta)$. In general, we also have the following result

Problem 54. $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is a unit $\iff$ $N(\alpha) \in \mathbb{Z}$ is a unit.

Proof. First if $N(\alpha) = N(a+b\sqrt{-5}) = \pm 1$, then $(a+b\sqrt{-5})(a-b\sqrt{-5}) = \pm 1$. In either case for the ±, we have found the multiplicative inverse of $a+b\sqrt{-5}$.

On the other hand, if $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is a unit with $\alpha\beta = 1$, then clearly $N(\alpha)N(\beta) = N(1) = 1$. Since $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$, this shows $N(\alpha)$ is a unit in $\mathbb{Z}[\sqrt{-5}]$. □

Now with this property, we can show that the following violates unique factorization in $\mathbb{Z}[\sqrt{-5}]$.

Problem 55. Show that $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ are distinct irreducible factorizations in $\mathbb{Z}[\sqrt{-5}]$.

Proof. We first need to show that $2, 3, 1 \pm \sqrt{-5}$ are irreducible. We know that $N(2) = 4$, so that if $2 = \alpha\beta$ where α, β are not units, then $4 = N(\alpha)N(\beta)$ where $N(\alpha), N(\beta)$ are not units. But since N for $\mathbb{Z}[\sqrt{-5}]$ only maps to nonnegative integers, we get that $N(\alpha) = N(\beta) = 2$. But this is absurd, as $a^2 + 5b^2 = 2$ has no integer solutions.

The same logic works for showing 3 is irreducible, and finally for $1 \pm \sqrt{-5}$, note that $N(1 \pm \sqrt{-5}) = 6$. As such, if $1 \pm \sqrt{-5} = \alpha\beta$, then $6 = N(\alpha)N(\beta)$, but the only way for this to work if α, β are not units is if one has norm 2, and the other norm 3. These clearly don't work, so all factors here are irreducible.

Finally we would have to verify that the irreducible elements in each of the factorizations are not associates of each other. This is obvious, however, as if 2 was associate to either $1 \pm \sqrt{-5}$, they would have the same norm, but they don't as $N(2) = 4$ and $N(1 \pm \sqrt{-5}) = 6$. □

Problem 56. Show that $\mathbb{Z}[\sqrt{-5}]$ is Noetherian.

Proof. First notice that $\mathbb{Z}[x]$ is Noetherian by Hilbert's Basis Theorem. Moreover, we can rewrite $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2+5)$ via the first isomorphism theorem. As such, since the quotient of a Noetherian ring is Noetherian, we're done. □

An example of a ring that is a UFD but not Noetherian is $\mathbb{F}[x_1, x_2, \ldots]$ for some field $\mathbb{F}$.

11.2 More $\mathbb{Z}[i]$

Another useful fact about the norm is that it let's us translate irreducibility features.

Problem 57. If $N(\alpha)$ is irreducible in $\mathbb{Z}$, then α is irreducible in $\mathbb{Z}[i]$.

Proof. Suppose $\alpha = \beta\gamma$. Then $N(\beta)N(\gamma) = N(\alpha) \implies$ one of β, γ is a unit. □

Problem 58. Which irreducibles in $\mathbb{Z}$ remain irreducible in $\mathbb{Z}[i]$?

Proof. We first note that for $p = 2$, we have $2 = (1+i)(1-i)$ so that 2 is not irreducible.

For $p \equiv 3 \pmod 4$, we have that if $\alpha\beta = p$, then

$$p^2 = N(p) = N(\alpha)N(\beta)$$

so that if $\alpha\beta$ is a nontrivial factorization, we must have $N(\alpha) = N(\beta) = p$. But note that $N(\alpha), N(\beta)$ are sums of squares, so modulo 4 they can only take on values $0, 1, 2$, as $0, 1$ are the only quadratic residues modulo 4. As such, we must have one of $N(\alpha), N(\beta) = 1$, and therefore p remains irreducible.

For $p \equiv 1 \pmod 4$, we utilize two facts, that -1 is a quadratic residue modulo p, and that if $\pi \in \mathbb{Z}[i]$ is irreducible, then $\pi | \alpha\beta \implies \pi|\alpha$ or $\pi|\beta$. Since -1 is a perfect square modulo p, we have that

$$\exists n \in \mathbb{Z}, n^2 \equiv 1 \pmod p \implies p | n^2 + 1 \implies p|(n+i)(n-i).$$

But then if $p \in \mathbb{Z}[i]$ remained irreducible, then we must have $p|n+i$ or $p|n-i$. This is impossible, however, as $\frac{n}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$, so we're done. □

Problem 59. Use the above to show Fermat's sum of two squares theorem. That is $p \equiv 1 \pmod 4 \implies p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Proof. Since p is not irreducible in $\mathbb{Z}[i]$, we can write $p = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$ not units. As such, $N(\alpha) = N(\beta) = p$. But if $\alpha = a + bi$, then this implies $a^2 + b^2 = N(\alpha) = p$, as desired. □

11.3 Finite Fields

Problem 60. Given an abelian group G with $|a| = m, |b| = n$ and $\gcd(m, n) = 1$, we have $|ab| = mn$.

Proof. Clearly $(ab)^{mn} = 1$. If $(ab)^k = 1$, then it must also be that

$$(ab)^k = 1 \implies (ab)^{km} = 1 \implies b^{km} = 1 \implies n|km \implies n|k$$

as $\gcd(n, m) = 1$. As such, $n|k$, and by analogous reasoning, $m|k$, so $mn|k$ and $|ab| = mn$. □

Theorem 11.1. (Wedderburn) Every finite field is commutative.

Proof. Beyond scope of recitation. □

Problem 61. The multiplicative group of units $\mathbb{F}^\times$ of a finite field $\mathbb{F}$ is cyclic.

Proof. Let $m = |\mathbb{F}^\times|$ so that $a^m = 1\ \forall a \in \mathbb{F}^\times$. Now fix $d|m$ and consider $x^d - 1, x^m - 1 \in \mathbb{F}[x]$. It is well known that $x^d - 1 | x^m - 1$, as

$$x^m - 1 = (x^d - 1)\left(\sum_{i=0}^{\frac{m}{d}-1} x^{id}\right).$$

$x^d - 1$ has $\leq d$ distinct roots, $\left(\sum_{i=0}^{\frac{m}{d}-1} x^{id}\right)$ has $\leq m - d$ distinct roots, and $x^m - 1$ has exactly m distinct roots. As such, it must be that $x^d - 1$ has exactly d distinct roots for $d|m$.

Now let $m = p_1^{e_1} \dots p_k^{e_k}$ be the canonical prime factorization of m. For any $i \in [k]$, $x^{p_i^{e_i}} - 1$ has exactly $p_i^{e_i}$ distinct roots, but $x^{p_i^{e_i - 1}} - 1$ has only $p_i^{e_i - 1}$ dinstinct roots. But if $a^{p_i^{e_i}} = 1$ and $a^{p_i^{e_i - 1}} \neq 1$, we must have $|a| = p_i^{e_i}$. As such, $\exists a_i \in \mathbb{F}^\times$ with $|a_i| = p_i^{e_i}$, and by problem 7, it follows that $|a_1 a_2 \dots a_k| = m$. □

12 Week 12

12.1 More Polynomials

We first start with an important result.

Problem 62. Show that if $\mathbb{F}$ is a field, then a degree n polynomial $p(x) \in \mathbb{F}[x]$ has at most n distinct roots in $\mathbb{F}$.

Proof. We can induct on the degree of n. The degree 0 case is obvious since $p(x) = k$ for some nonzero $k \in \mathbb{F}$, and this clearly has no roots.

In general, let $\deg(p) = n$ and suppose that $p(x)$ has some root $a_1 \in \mathbb{F}$ so that we can write

$$p(x) = (x - a_1)p_1(x)$$

where $\deg(p_1) = \deg(p) - 1$. By induction, $p_1(x)$ has $\leq \deg(p) - 1 = n - 1$ distinct roots, call them $a_2, \ldots, a_n$. As such, for $b \in \mathbb{F}$ with $b \neq a_i \; \forall i \in [n]$, we have that $p(b) = (b - a_1)p_1(b) \neq 0$ as $b - a_1, p_1(b) \neq 0$, and $\mathbb{F}$ is a field that satisfies the zero-product property. So p has $\leq n$ roots and our inductive step is complete. □

We now move on to study irreducibility in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

Theorem 12.1. (Eisenstein's Criterion) Suppose we have the polynomial $Q(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$. If there exists a prime p s.t.

1. $p | a_i$ for $0 \leq i < n$
2. $p \nmid a_n$
3. $p^2 \nmid a_0$

then Q is irreducible over $\mathbb{Z}$, and subsequently over $\mathbb{Q}$ as well.

Proof. The key idea for Eisenstein's criterion is noting that if $Q(x) = Q_1(x)Q_2(x)$ where $Q_1, Q_2 \in \mathbb{Z}[x]$, then we must also have $Q(x) \equiv Q_1(x)Q_2(x) \pmod p$ (i.e. the same equality holds in $(\mathbb{Z}/p\mathbb{Z})[x]$). Suppose FTSOC that Q is reducible in $\mathbb{Z}[x]$, and we have $Q(x) = Q_1(x)Q_2(x)$ with $\deg(Q_1), \deg(Q_2) > 0$. In this case, we have that

$$Q(x) \equiv a_n x^n \pmod p \implies Q_1(x)Q_2(x) = a_n x^n \text{ in } (\mathbb{Z}/p\mathbb{Z})[x].$$

The only way this can occur is if $Q_1(x) = k_1 x^a, Q_2(x) = k_2 x^b$ in $(\mathbb{Z}/p\mathbb{Z})[x]$, where $k_1 k_2 \equiv a_n \pmod p$ and $a, b > 0$. But then Q_1, Q_2 have constant term divisible by p in $\mathbb{Z}[x]$, so the constant term of $Q(x) = Q_1(x)Q_2(x)$ must be divisible by p^2, and we have a contradiction.

We've shown Q is irreducible in $\mathbb{Z}[x]$, but it is also irreducible in $\mathbb{Q}[x]$ via Gauss's Lemma. □

Problem 63. Show that the following polynomials are irreducible in $\mathbb{Q}[x]$ using Eisenstein's criterion.

1. $x^5 - 4x + 22$
2. $-7x^4 + 25x^2 - 15x + 10$
3. $x^4 + 4x + 1$

Proof. For the first two just use Eisenstein with $p = 2$ and $p = 5$ respectively. For the last one, we note that in general if $P(x) = Q_1(x)Q_2(x)$ is reducible, then we must also have that $P(ax + b) = Q_1(ax + b)Q_2(ax + b)$ is reducible. With this in mind, consider

$$Q(x) = P(x + 1) = (x + 1)^4 + 4(x + 1) + 1 = x^4 + 4x^3 + 6x^2 + 8x + 6$$

which we know is irreducible by Eisenstein with $p = 2$. As such, if P were reducible, then $P(x + 1)$ would also be reducible, but since it isn't, P must be irreducible. □

We can also use these reults to study the irreducibility of Cyclotomic polynomials. Note that in general, for $n \in \mathbb{N}$ we can factor

$$x^n - 1 = (x-1)(x^{n-1} + \ldots + 1)$$

and when p is prime, we define $\Phi_p(x) = \frac{x^p - 1}{x-1} = (x^{p-1} + \ldots + 1)$ as the p-th cyclotomic polynomial. In $\mathbb{C}$, it's easy to see that Φ_p splits into $p-1$ distinct roots since

$$x^p - 1 = \prod_{k=0}^{p-1}(x - e^{\frac{2\pi k i}{p}}) \implies \Phi_p(x) = \prod_{k=1}^{p-1}(x - e^{\frac{2\pi k i}{p}}).$$

However, this is a factorization in $\mathbb{C}[x]$, and we're instead interested in how $\Phi_p(x)$ behaves in $\mathbb{Q}[x]$.

Problem 64. Show that $x^{p-1} + \ldots + 1$ is irreducible over $\mathbb{Z}[x]$.

Proof. Unforunately a naive Eisenstein argument doesn't work here, but we can instead look at this polynomial applied to linear transforms of x. Consider

$$\begin{aligned}(x+1)^{p-1} + \ldots + 1 &= \sum_{i=0}^{p-1}\sum_{j=0}^{i}\binom{i}{j}x^j \\ &= \sum_{j=0}^{p-1}\sum_{i=j}^{p-1}\binom{i}{j}x^j \\ &= \sum_{j=0}^{p-1}\binom{p}{j+1}x^j\end{aligned}$$

where the last step follows by the Hockey-Stick identity. We have that $p \nmid \binom{p}{p-1+1} = 1$, and for $0 \leq j < p-1 \implies 1 \leq j+1 < p$ clearly $p | \binom{p}{j+1}$ since there is never a p term in the denominator. Finally at $j = 0$ we have that the coefficient is $\binom{p}{1} = p$, which p^2 does not divide. As such, by Eisenstein the transformed polynomial is irreducible, and the original $x^{p-1} + \ldots + 1$ is as well. □

12.2 Finite Fields

We've shown that there exists a field of order p, p^2 via $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}[i]/(p)$ respectively ($p \equiv 3 \pmod 4$ for the second one). In general, we'd also like to make stronger statements about the sizes of finite fields, such as finding their factorizations.

Problem 65. Show that if p, q are distinct primes and $\mathbb{F}$ is a finite field, then $p, q | \, |\mathbb{F}|$ is impossible. In other words, $|\mathbb{F}| = p^n$ for some integer prime p for any finite field $\mathbb{F}$.

Proof. Consider $(\mathbb{F}, +)$ as an additive abelian group and let $p = |1|$ be the additive order of 1. First note that p is prime, since if $p = mn$ with $m, n > 1$, then we have that

$$0 = \sum_{i=1}^{p} 1 = \left(\sum_{j=1}^{m} 1\right)\left(\sum_{k=1}^{n} 1\right)$$

with $\sum_{j=1}^{m} 1, \sum_{k=1}^{n} 1 \neq 0$ as $m, n < p$. So p must be prime or else $\mathbb{F}$ violates the zero-product property of fields. Now suppose that $q | \, |\mathbb{F}|$ for some $q \neq p$ also prime. Then by Cauchy, $\exists a \in \mathbb{F}$ with additive order q so that

$$0 = \sum_{i=1}^{q} a = a\left(\sum_{i=1}^{q} 1\right).$$

But $a \neq 0$ since $|a| = q > 1$ and $\sum_{i=1}^{q} 1 \neq 0$ since $p \nmid q$, and we have another violation of zero-product property. It follows then that p is the only prime that can divide $|\mathbb{F}|$, so $|\mathbb{F}| = p^n$ for some prime p. □

In general, we can construct fields of order p^n by considering $(\mathbb{Z}/p\mathbb{Z})[x]$ and modding out by a degree n irreducible. As an example, $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2 + x + 1)$ is a field of order 4. A natural follow-up question is then whether there always exists a field of order p^n for any prime p and $n \in \mathbb{N}$, and subsequently whether there always exists an irreducible polynomial of degree n in $(\mathbb{Z}/p\mathbb{Z})[x]$.

13 Week 13

13.1 Problem 6

Hint for problem 6 on homework 10 since it is pretty hard.

Problem 66 (Problem 6)**.** Show that $\mathbb{Z}^{\mathbb{N}}$ is not a free $\mathbb{Z}$-module, or that it does not admit a basis.

The following lemma will be useful for this problem.

Lemma 13.1. Let M be a free $\mathbb{Z}$-module. Then if $v \in M$ with $v \neq 0$, then there are only finitely many $n \in \mathbb{N}$ s.t. $v = nw$ has a valid solution for $w \in M$.

Proof. Let M have the basis $B = \{b_s : s \in S\}$ where S is some indexing set. Then we can write

$$v = \sum_{i=1}^{k} x_i b_{s_i}, 0 \neq x_i \in \mathbb{Z}$$

as $v \neq 0$ and M has a basis. Suppose that $v = nw$ and let $y_i \in \mathbb{Z}$ denote the coefficient of w in the basis representation of w. Matching basis representations, it follows that we must have $ny_i = x_i \implies n | x_i$ $\forall i \in [k]$. But the $x_i \neq 0$ by the $v \neq 0$ assumption, so there are clearly only finitely many $n \in \mathbb{N}$ that work. □

Now suppose that $\mathbb{Z}^{\mathbb{N}}$ admits some basis $B = \{b_s : s \in S\}$ for some index set S. Consider the canonical basis elements of $\oplus_{i=1}^{\infty}\mathbb{Z}$, the e_i with 1 in the ith position and 0 everywhere else. Then $\forall i \in \mathbb{N}$, there is some finite set $S_i \subseteq S$ s.t.

$$e_i = \sum_{s \in S_i} \lambda_{i,s} b_s$$

is the finite basis representation of e_i. The key is then to consider the submodule $N \leq \mathbb{Z}^{\mathbb{N}}$ generated by $B_1 = \{b_s : s \in \cup_{i=1}^{\infty} S_i\}$. Let $B_1 \sqcup B_2 = B$, $M = \mathbb{Z}^{\mathbb{N}}/N$, and we see that $\mathbb{Z}^{\mathbb{N}} \cong M \oplus N$ where

$$N = \text{span}(B_1) = \text{span}(\{b_s : s \in \cup_{i=1}^{\infty} S_i\}) \text{ and } M \cong \text{span}(B_2) = \text{span}(B \setminus B_1).$$

In other words, we can extract the submodule N of $\mathbb{Z}^{\mathbb{N}}$ that contains $\oplus_{i=1}^{\infty}\mathbb{Z}$ and mod out by it to generate some new free $\mathbb{Z}$-module M. To finish the proof, you can use counting arguments to generate a $v \in M$ s.t. $v \neq 0$, but there are infinitely many $n \in \mathbb{N}$ s.t. $v = nw$ has a solution for $w \in M$. This violates the previous lemma, and subsequently M and therefore $\mathbb{Z}^{\mathbb{N}}$ cannot admit a basis.

13.2 Subgroups of $\mathbb{Z}^2$

Problem 67. Show that every subgroup of $\mathbb{Z}^2$ is isomorphic to $0, \mathbb{Z}$, or $\mathbb{Z}^2$.

Proof. Assume $G \leq \mathbb{Z}^2$ with $G \neq 0$ (this case is trivial). Let $p_1 : \mathbb{Z}^2 \to \mathbb{Z}$ denote the x-projection homomorphism, and consider $p_1(\mathbb{Z}) \leq \mathbb{Z}$. We know that $p_1(\mathbb{Z}) \cong m\mathbb{Z}$ for some $m \in \mathbb{N}^{\geq 0}$, so we have two cases.

Case 1: $m = 0$. Here we just have that the x-coordinate of every $(a, b) \in G$ is $a = 0$. Taking $n = \min_{(0,b) \in G, b > 0} b$, it becomes clear that $G = (0, n)\mathbb{Z} \cong \mathbb{Z}$.

Case 2: $m > 0$. Suppose that $u = (a, b) \in G$, so that $m | a$ with $a = mk$, as $p_1(G) = m\mathbb{Z}$. Fix an arbitrary $v \in G$ s.t. $p_1(v) = m$. Then we have that

$$p_1(u - kv) = 0 \implies u - kv \in G \cap (0 \times \mathbb{Z}).$$

In other words, we can write any $u \in G$ as the sum of kv and an element in $G \cap (0 \times \mathbb{Z})$. But clearly $G \cap (0 \times \mathbb{Z}) = 0 \times n\mathbb{Z}$ for some $n \geq 0$, so letting $w = (0, n)$ we see that

$$\forall u \in G, u - kv \in 0 \times n\mathbb{Z} \implies u = kv + lw$$

for some $l \in \mathbb{Z}$. In the case that $n = 0$, we simply get that $G = v\mathbb{Z} \cong \mathbb{Z}$, but when $n > 0$, we see that

$$G = v\mathbb{Z} + w\mathbb{Z} \cong \mathbb{Z}^2$$

via the homomorphism that sends $(1, 0) \to v$ and $(0, 1) \to w$. In any case we have $G \cong 0, \mathbb{Z}$, or $\mathbb{Z}^2$. □

13.3 Cyclotomic Polynomials

Definition 13.1 (nth roots of unity)**.** For $n \in \mathbb{N}$, we can define the set μ_n of nth roots of unity as the n distinct roots of $x^n - 1$, or

$$\mu_n = \{e^{\frac{2\pi ik}{n}} : k \in \mathbb{Z}, 0 \leq k < n\}.$$

We say that $\rho \in \mu_n$ is primitive if it has multiplicative order n. Since

$$\left(e^{\frac{2\pi ik}{n}}\right)^m = 1 \iff n|km$$

it turns out that $\gcd(k, n) = 1$ is a sufficient and necessary condition for $e^{\frac{2\pi ik}{n}}$ to be primitive. This tell us that in general, there are $\phi(n)$ distinct nth roots of unity, where ϕ is defined as follows.

Definition 13.2 (Euler Phi Function)**.** For $n \in \mathbb{N}$, we define the Euler phi function as

$$\phi(n) = |\{m \in \mathbb{N} : m \leq n, \gcd(m, n) = 1\}|.$$

Last week, for p prime we defined the pth cyclotomic polynomial as $\Phi_p(x) = \prod_{k=1}^{p-1}\left(x - e^{\frac{2\pi ik}{p}}\right)$ and showed that it was irreducible. In general, we can define the nth cyclotomic polynomial similarly.

Definition 13.3 (nth Cyclotomic polynomial)**.** For $n \in \mathbb{N}$, we define the nth cycltomic polynomial as the polynomial with the $\phi(n)$ primitive roots of unity as its roots, or

$$\Phi_n(x) = \prod_{1 \leq k \leq n, \gcd(k,n)=1} \left(x - e^{\frac{2\pi ik}{n}}\right).$$

Problem 68. Show that for $n \in \mathbb{N}$, we have that

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Use this to conclude that $n = \sum_{d|n} \phi(d)$.

Proof. We'll show the first part by bijecting roots between the LHS and RHS of the equation, noting that both polynomials are monic since the Φ_d terms are all individually monic. First note that if $\Phi_d(\alpha) = 0$, then it must be that

$$\alpha = e^{\frac{2\pi ik}{d}} \implies \alpha^n = e^{2\pi ik\frac{n}{d}} = 1$$

since $k \cdot \frac{n}{d} \in \mathbb{Z}$. This shows that the roots of the RHS are a subset of μ_n. We now show that if $\alpha \in \mu_n$, then $\Phi_d(\alpha) = 0$ for some $d|n$. Then for some $k \in \mathbb{Z}$ with $0 \leq k < n$, we can write

$$\alpha = e^{\frac{2\pi ik}{n}} = e^{\frac{2\pi i\frac{k}{\gcd(k,n)}}{\frac{n}{\gcd(k,n)}}}.$$

Clearly $\gcd\left(\frac{k}{\gcd(k,n)}, \frac{n}{\gcd(k,n)}\right) = 1$, so since $\frac{n}{\gcd(k,n)}|n$, it follows that by setting $d = \frac{n}{\gcd(k,n)}$ we have that $\Phi_d(\alpha) = 0$. As such, $\alpha \in \mu_n \implies$ it is a root of the RHS, so the polynomials have the same roots.

It remains to show that the roots (elements of μ_n) have the same cardinality on the LHS and RHS. Clearly each element of μ_n is a root exactly once in $\Phi_n(x)$, so it suffices to show that if $\alpha = e^{\frac{2\pi ik}{n}} \in \mu_n$, then it is a root of only one $\Phi_d(x)$, where $d|n$. We have that

$$\Phi_d(\alpha) = 0 \implies \alpha = e^{\frac{2\pi il}{d}}, \gcd(l, d) = 1 \implies e^{\frac{2\pi ik}{n}} = e^{\frac{2\pi il}{d}}, \gcd(l, d) = 1 \implies \frac{k}{n} = \frac{l}{d}, \gcd(l, n) = 1.$$

This is possible only when $\frac{l}{d}$ is the reduced form of $\frac{k}{n}$, or $d = \frac{n}{\gcd(k,n)}$, so d is uniquely defined and α appears only once as a root of the RHS. It follows that $x^n - 1 = \prod_{d|n} \Phi_d(x)$, as desired.

Now to show that $n = \sum_{d|n} \phi(d)$, we can just use additivity of the degree, noting that

$$n = \deg(x^n - 1) = \deg\left(\prod_{d|n} \Phi_d(x)\right) = \sum_{d|n} \deg(\Phi_d(x)) = \sum_{d|n} \phi(d).$$

□