MS Algebra I/II Recitation Notes

Ethan Lu

Last Updated: November 30, 2021

Contents

1 Recitation 1: Preliminaries (8/31/21)

EXERCISE 1.1 **Associativity**

Show that, if $\circ$ is an associative operation, then any valid parenthesization of $g_1 \circ g_2 \circ \cdots \circ g_n$ is equal to

$$g_1 \circ (g_2 \circ \cdots (g_{n-1} \circ g_n))).$$

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 $g_1 \circ \cdots \circ g_n$ as above, and decompose it as

$$e_1 \circ e_2 := \underbrace{(g_1 \circ \cdots \circ g_k)}_{\text{parenthesized somehow}} \circ \underbrace{(g_{k+1} \circ \cdots \circ g_n)}_{\text{parenthesized somehow}}$$

for $k < n$. Then by hypothesis, we have

$$e_1 = g_1 \circ (g_2 \circ \cdots \circ (g_{k-1} \circ g_k)))$$

and hence

$$e_1 \circ e_2 = (g_1 \circ (\cdots \circ (g_{k-1} \circ g_k))) \circ e_2 = g_1 \circ (\cdots \circ (g_{k-1} \circ g_k)) \circ e_2)$$

by associativity. Applying the hypothesis again, we get the desired conclusion. ■

As just a quick reminder, some definitions discussed in class:

Definition 1. $(G, \cdot)$ is a **semigroup** if $\cdot : G \times G \to G$ is an associative operation.

Definition 2. $(G, \cdot)$ is a **monoid** if it's a semigroup and there exists $e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$.

Definition 3. $(G, \cdot)$ is a **group** if it's a monoid and for all $g \in G$, there exists $h \in G$ such that $gh = hg = e$.

EXAMPLE 1.2 **Semigroups, Monoids, and Groups**

Classify the following.

1. $(\{0, 1, \cdots, n-1\}, +)$.
2. $(\{1, \cdots, n-1\}, \times)$.
3. $(\mathbb{R}^{3\times3}, \times)$ (i.e. the set of 3×3 matrices).
4. $\{M \in \mathbb{R}^{3\times3} \mid \det(M) = 1\}$.
5. $\{M \in \mathbb{Z}^{3\times3} \mid \det(M) = 1\}$.
6. (Strings, +).

---

2 Recitation 2: Permutation Groups (9/7/21)

Below, X will be a fixed (possibly infinite) set and $\sigma : X \to X$ an arbitrary permutation.

Let $\sim$ be the binary relation on X such that $x \sim y \iff \exists k \in \mathbb{Z} \mid y = \sigma^k(x)$.

Exercise 2.1

Show that $\sim$ is an equivalence relation.

Let's call the equivalence classes "cycles."

Exercise 2.2

Show that for each $x \in X$ that its cycle $[x]$ is either a finite loop or an infinite "line."

Now let's say that X is finite, i.e. that up to relabeling, $X = \{1, 2, ..., n\}$.
The result we've proved above gives us a much more compact way of specifying σ: rather than writing out something like this:

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 just write $\sigma := (1, 2, 9)(3, 5, 7)$.

Exercise 2.3

Show any disjoint cycles commute.

Exercise 2.4

Show that the representation above is unique up to commuting cycles.

Exercise 2.5

Let $X = \{1, \cdots, 9\}$, $\sigma := (1, 2, 9)(3, 5, 7)$, and $\tau := (1, 3, 2)(4, 9)$. Compute $\sigma\tau$.

This next exercise has some connections to the **Orbit-Stabilizer** theorem, which we'll probably be talking about next week:

Exercise 2.6

Let $x \in X$. Show that $G := \{k \in \mathbb{Z} : \sigma^k(x) = x\}$ is a subgroup of $\mathbb{Z}$. By homework, this implies G is either trivial or $n\mathbb{Z}$ for $n \in \mathbb{N}$. What do these cases correspond to?

EXERCISE 2.7

Suppose $|X| < \infty$, and $\sigma, \tau \in S_X$. Show that σ, τ are conjugate to each other iff they have the same cycle decomposition.

Proof. $\implies$: I kinda messed this up in recitation so I'll actually write up something that works here. Suppose that $\sigma = \pi\tau\pi^{-1}$, i.e. that π witnesses conjugacy of the two. Then for any $x \in X$,

$$[x]_\sigma = \bigcup_{k\in\mathbb{N}} \sigma^k(x) = \bigcup_{k\in\mathbb{N}} \pi\tau^k(\pi^{-1}x) = \pi[\pi^{-1}x]_\tau$$

where we write $[x]_\sigma, [x]_\tau$, to denote the cycle of x according to the respective permutations. Note then that applying π to any subset of X preserves it's cardinality, and hence we can identify any equivalence class according to τ with a corresponding equivalence class of π that has the same cardinality, so we're done!
$\impliedby$: Exercise!

■

3 Recitation 3: Group Actions (9/14/21)

As just a quick reminder, some definitions discussed in class:

Definition 4. A **group action** of the group G on the set X (denoted by $G \curvearrowright X$), is either (or equivalently)

- A homomorphism $G \to S_X$.
- A function $\cdot : G \times X \to X$ such that
  1. $e \cdot x = x \quad \forall x \in X$
  2. $g_1 g_2 \cdot x = g_1 \cdot (g_2 \cdot x) \forall g_1, g_2 \in G, x \in X$

THEOREM 3.1

Suppose that G is a group and $H \leq G$ with $[G : H] = n$. Then $\exists N \leq H$ normal in G with $[G : N]$ dividing $n!$ Hint: consider the action $G \curvearrowright G/H$ by left multiplication.

The next several exercises will build up to the following result.

THEOREM 3.2

Suppose G is a group such that $|G| = p^2$. Then either $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ or $G \cong \mathbb{Z}_{p^2}$.

Now we'll show some quick auxiliary results needed for the next result.

Definition 5. The **center** $Z(G)$ of a group G is the set

$$Z(G) := \{g \in G \mid gh = hg \quad \forall h \in G\}.$$

EXERCISE 3.3

Show that $Z(G)$ is a normal subgroup.

EXERCISE 3.4

Show if $G/Z(G)$ is cyclic, than it's trivial.

EXERCISE 3.5

Show that if G is a nontrivial p-group, then $Z(G) \neq \{e\}$.

EXERCISE 3.6

Use the previous 3 results to prove the theorem.

Recall for any two groups G, H, we can equip their Cartesian product $G \times H$ with the group structure of their **direct product** (i.e. the coordinate-wise product).

Exercise 3.7

Show that the direct product $G \times H$:

1. has subgroups isomorphic to G and H.
2. has quotients isomorphic to G and H.

Proposition 1. *The 5 subgroups of order 8 are:*

1. $\mathbb{Z}_8$.
2. $\mathbb{Z}_4 \times \mathbb{Z}_2$.
3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
4. D_8.
5. *The quaternions.*

Back to group action stuff:

Exercise 3.8

Show that if $H \leq G$, then $gHg^{-1} \leq G$ for all $g \in G$, and hence that we have a natural action $G \curvearrowright \{H \mid H \leq G\}$.

Recall the following:

Definition 6. The sign $\operatorname{sgn}(\sigma)$ of a permutation σ is $(-1)^{T(\sigma)}$, where $T(\sigma)$ is the number of 2-cycles in any valid decomposition of σ into two-cycles.

Definition 7. The **alternating group** A_n is the set

$$A_n := \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}$$

Exercise 3.9

Show that:

1. $\sigma \mapsto (1 + \operatorname{sgn}(\sigma))/2$ is a homomorphism from S_X to $\mathbb{Z}_2$, and hence that $A_n \leq S_n$.
2. 3-Cycles are always even.
3. Whenever $n > 4$ any two 3-cycles are conjugate in A_n.

4 Recitation 4: Sylow's Theorems and Friends (9/21/21)

Today we'll be reviewing Sylow's theorems with some applications. A quick reminder of what those are:

Definition 8. $H \leq G$ is a **Sylow p-subgroup** if it's a maximal p-subgroup.

THEOREM 4.1 **(Sylow's theorems)**

---

1. Sylow p-subgroups exist; that is, for all groups G, with $|G| = p^k m$, $\exists H \leq G$ with $|H| = p^k$.
2. Any two Sylow p-subgroups are conjugate to each other.
3. The number of Sylow p-groups $n_p(G)$ satisfies:
   - $n_p(G) = [G : N_G(H)]$ (in particular, $n_p(G)$ divides m).
   - $n_p(G) \equiv 1 \pmod{p}$.

Now we'll show some auxiliary results that will be useful in showing simplicity of A_5.

EXERCISE 4.2

Any group with order 15 is cyclic.

EXERCISE 4.3

Any group with order 30 has a subgroup of order 15.

The counting type argument used above is pretty cool, and will be useful in the next result, but make sure that you're careful when using it! In particular, we're exploiting cyclicity to conclude that $H \cap K = \{e\}$ for any H, K both p-groups, but this doesn't necessarily work when $|H|, |K|$ are higher powers of p.

EXERCISE 4.4

Any group with order 60 and $n_5(G) > 1$ is simple. Hint: first show that $5 \nmid |H|$ for any proper $H \trianglelefteq G$, then do some quotient trickery.

COROLLARY 4.5

A_5 is simple. Hint: consider $\langle (1,2,3,4,5) \rangle$ and $\langle (1,3,2,4,5) \rangle$.

THEOREM 4.6

A_n is simple.

Proof. We didn't actually get to this in recitation, so see section 4.6 in Dummit and Foote. ■

COROLLARY 4.7

A_n is generated by 3-cycles. Hint: Use the results from last week to show that the group generated by 3-cycles is normal in A_n.

5 Recitation 5: Nilpotence and Solvability (9/28/21)

Recall the following definitions from class:

Definition 9. Given a group G, the **commutator** $[g, h]$ of any two elements $g, h \in G$ is defined via

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

and is extended to sets $A, B \subseteq G$ via

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

Definition 10. The **derived series** of a group G is the sequence of subgroups $\{G^{(i)}\}_{i\in\mathbb{N}}$ defined recursively via $G^{(0)} = G, G^{(i+1)} = [G^i, G^i]$. The **lower central series** of a group G is the sequence of subgroups $\{G^i\}_{i\in\mathbb{N}}$ defined recursively via $G^0 = G, G^{i+1} = [G, G^i]$.

Definition 11. A group is **solvable** if $G^{(i)} = \{e\}$ for some $i \in \mathbb{N}$. The smallest such i for which this happens is the solvable length of the group. A group is **nilpotent** if $G^i = \{e\}$ for some $i \in \mathbb{N}$. The smallest such i for which this happens is the nilpotency class of the group.

Exercise 5.1

Recall that D_{2n} is the dihedral group on n elements. Show that D_{2n} is generated by the elements $r := x \mapsto x + 1 \pmod n$, $s := x \mapsto -x \pmod n$ and further that we have the identities:

- $s^2 = r$.
- $sr = r^{-1}s$.
- $sr^k = r^{-k}s$.

Exercise 5.2

Show that D_{2n} is always solvable, and that it's nilpotent iff $n = 2^k$ for $k \in \mathbb{N}$.

Exercise 5.3

Let $D_{2\mathbb{N}}$ be the automorphism group of the bi-infinite graph on $\mathbb{Z}$; that is, the graph with edges between k and $k + 1$ for all $k \in Z$. Show that this group is generated by r, s as above and that the same identities hold. Classify the nilpotence and solvability of this group.

Definition 12. Recall that given two groups G, H where $G \curvearrowright H$ by automorphisms, we can define the **semidirect** product $H \rtimes G$ on $H \times G$ via

$$(g_0, h_0)(g_1, h_1) = (h_0(g_0 \cdot h_1), g_0g_1)$$

Exercise 5.4

Suppose that $A \in \mathbb{Z}^{2\times 2}$ with determinant ± 1. Show that $\mathbf{x} \mapsto A\mathbf{x}$ is an automorphism on $(\mathbb{Z}^2, +)$. Conclude that this naturally induces an action $\mathbb{Z} \curvearrowright \mathbb{Z}^2$ via $n \cdot \mathbf{x} = A^n\mathbf{x}$.

Exercise 5.5

Show that the semi-direct product above is always solvable. Show also that when $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ this group is nilpotent but when $A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ it's not.

6 Recitation 6: Midterm Review (10/5/21)

Not much to say here :)

7 Recitation 7: Rings and Category Stuff (10/12/21)

As per usual, let's start by recalling some definitions from class.

Definition 13. A **ring** is a structure $(R, +, \times)$ where $+, \times$ are binary operations on R such that $(R, +)$ is an abelian group, $(R, \times)$ is a semigroup, and for all $a, b, c \in R$:

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

Definition 14. A **ring homomorphism** between rings R, S is a function $\varphi : R \to S$ such that $\varphi(r + s) = \varphi(r) + \varphi(s)$ and $\varphi(rs) = \varphi(r)\varphi(s)$ for all $r, s \in R$. In the case R, S have 1, it's called **unital** if $\varphi(1_R) = 1_S$.

Exercise 7.1

Suppose R is a ring with 1. Show that there exists a unique unital ring hom $\varphi : \mathbb{Z} \to R$.

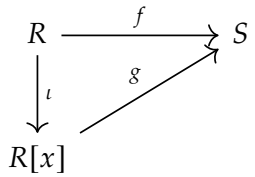
Recall also that given any commutative ring with 1 R, we can form the polynomial ring $R[x]$ by "adding in x" and having it commute with everything. (Technically the assumptions of commutativity and the existence of a unit aren't necessary, but they make things slightly nicer so for the purposes of this handout we'll assume it).

Exercise 7.2

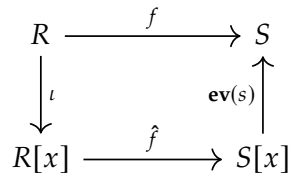
Show that $\iota : R \to R[x]$ via $\iota(r) = r$ is an injective ring homomorphism.

Exercise 7.3

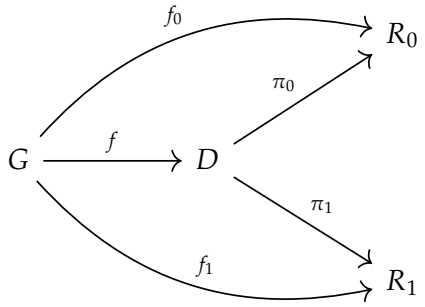
Let R, S be commutative rings with 1, $f : R \to S$ be a homomorphism, and $s \in S$. Show that there exists a unique ring hom $g : R[x] \to S$ such that $g \circ \iota = f$ and $g(x) = s$. (e.g. that the following diagram commutes).



Remark. This is **the universal property of polynomial rings**, and can actually be used as a defining property for $R[x]$. What's really going on in our construction is the following.



Definition 15. Suppose R_0, R_1 are algebraic structures. We call D a **direct product** of R_0, R_1 if D is also a structure (of the same type) and there exists $\pi_i : D \to R_i$ homomorphisms such that for any other structure G and homomorphisms $f_i : G \to R_i$, there exists a unique $f : G \to D$ such that the following diagram commutes.



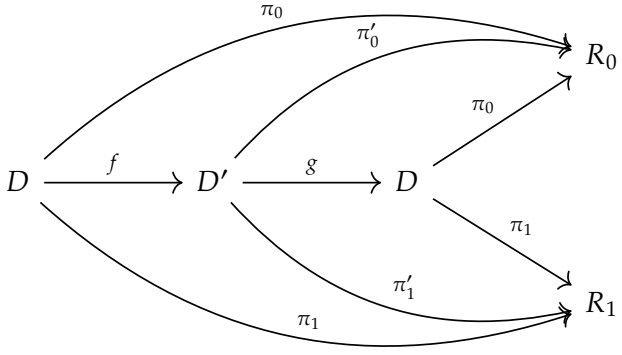
EXERCISE 7.4 **The direct product is a direct product**

Show that $R_0 \otimes R_1$ as defined in class is a direct product.

EXERCISE 7.5

Show that the direct product is unique up to isomorphism.

Proof. Let D, D' be any two direct products with associated homomorphisms π_i, π_i'. Take a moment to reflect on the following diagram:



where f, g are the (unique!) homomorphisms guaranteed by the universal property. By the universal property of D on itself, we see that we must have $f \circ g = \mathbf{Id}_D$, and hence by symmetric logic, $g \circ f = \mathbf{Id}_{D'} \implies f$ is an isomorphism.

■

Remark. The same construction above generalizes to direct products of arbitrarily many algebraic structures, though the exact numerology gets a bit more subtle when you're dealing with infinite products.

8 Recitation 8: Ideals and Zorn's Lemma (10/19/21)

As per usual recall that:

Definition 16. An **ideal** I of a ring R is a subset $I \subseteq R$ such that $I \leq R$ and $IR, RI \subseteq I$. Given arbitrary $A \subseteq I$, we write (A) to denote the ideal generated by A; that is:

$$(A) := \cap\{I \subseteq R \mid A \subseteq I, I \text{ is an ideal}\}.$$

When $A = \{a\}$, we may occasionally drop the parentheses and just write (a) to mean $(\{a\})$. In the case above, when an ideal is generated by a single element, we call the ideal **principal**.

Definition 17. A commutative ring F with a 1 is a **field** if the zero ideal is maximal; that is, $I \supsetneq (0) \implies I = R$ if I is an ideal. This differs from the usual definition of "you can divide by stuff," but as we'll show now these definitions are actually equivalent.

Exercise 8.1

Suppose that F is a C1 ring. Show that F is a field iff $(F \setminus \{0\}, \times)$ is a group.

Now we'll show some results on how the divisibility structure can be lifted to $F[x]$.

Exercise 8.2

Let $f \in F[x] \setminus \{0\}$, and $g \in F[x]$ with degree at least that of f. Then there exists $\hat{g} \in F[x]$ of strictly lower degree such that $g - \hat{g} \in (f)$.

Theorem 8.3 **Division in Polynomial Rings**

Let $f \in F[x] \setminus \{0\}$, $g \in F[x]$. Show that there exists a unique $r \in F[x]$ such that the degree of r is less than that of g and $g - r \in (f)$.
Conclude that $F[x]/(f) = \{r + (f) \mid \text{the degree of } r < \text{the degree of f}\}$.

Exercise 8.4

Show that every ideal in $F[x]$ is principle (i.e. that $F[x]$ is a PID).

For the rest of today's recitation, we'll be going through some useful examples on how Zorn's lemma can be used when reasoning about ideals/rings in general.

Exercise 8.5

Let I, R be such that $I \subseteq R$ is a nonprincipal ideal. Show that R has a maximal nonprincipal ideal.

Recall that a ring is **Noetherian** if every chain of ideals is finite (alternatively, that for any sequence $I_0 \subseteq I_1 \subseteq \cdots$, there exists N such that $I_n = I_{n+1}$ for all $n \geq N$).

Exercise 8.6

Let R be a non-Noetherian ring. Show that R has a maximal ideal that is not generated by any finite $A \subseteq R$.

Exercise 8.7

Let R be a C1 ring. Show that

$$\bigcup_{n \in \mathbb{N}} \{r \in R \mid r^n = 0\} = \bigcap \{I \subseteq R \mid I \text{ is a prime ideal}\}$$

9 Recitation 9: Factorization and Stuff (10/26/21)

Today, all rings will be integral domains (i.e. commutative with 1 such that $\{0\}$ is a prime ideal).

Definition 18. Let $D \subseteq R$ be a multiplicatively closed subset of R such that $1 \in R$ and $0 \notin R$. We define the **localization** of D to be the ring

$$D^{-1}R := \{[a/b]_\sim \mid a \in R, b \in D\}$$

where $a/b \sim c/d \iff ad = bc$, and the ring operations are given by

$$\left[\frac{a}{b}\right]_\sim + \left[\frac{c}{d}\right]_\sim = \left[\frac{ad+bc}{bd}\right]_\sim \qquad \left[\frac{a}{b}\right]_\sim \times \left[\frac{c}{d}\right]_\sim = \left[\frac{ac}{bd}\right]_\sim$$

Exercise 9.1

Check that $\sim$ is an equivalence relation and that these operations are well-defined, making $D^{-1}R$ into a ring.

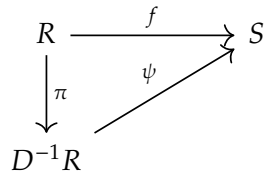
Exercise 9.2

Show that $\pi : R \to D^{-1}R$ via $\pi(r) = [r/1]_\sim$ is an injective ring homomorphism, and hence we have a canonical inclusion $R \subseteq D^{-1}R$.

Theorem 9.3 **Universal Property of Localization**

Suppose that $f : R \to S$ is a unital homomorphism such that $f(d)$ is a unit for all $d \in D$. Then there exists a unique $\psi : D^{-1}R \to S$ such that $f = \psi \circ \pi$.

Remark. As in the previous recitations, the above can actually be used as a defining property for $D^{-1}R$, and is equivalent to the following diagram commuting.



As before, it can easily be checked that uniquely defines the localization up to isomorphism.

Definition 19. Whenever D is the complement of a prime ideal, we can easily see that D satisfies the criteria above, and hence can be localized. In particular, when $D := R \setminus \{0\}$, we define $F_R := D^{-1}R$ to be R's **field of fractions**.

Recall the following now:

Definition 20. An integral domain R is a **unique factorization domain** if, for all $r \neq 0, (r) \neq R$, the ideal (r) factors uniquely as

$$(r) = \prod_k (p_k)$$

with each p_k irreducible.

Definition 21. Given a finite collection $r_1, \cdots r_n \in R$, we call $d \in R$ a GCD for $r_1, \cdots, r_n$ if $d \mid r_i$ for all $i \in [n]$ and $d' \mid r_i$ for all $i \implies (d') \supseteq (d)$.

Exercise 9.4

Show that GCDs exist in a UFD (and hence also in a PID).

Exercise 9.5

Suppose that R is an integral domain where every finitely generated ideal is principle. Show that GCDs always exist.

Recall the following theorem from class:

Theorem 9.6 **(Gauss)**

Suppose that $f \in R[x]$ is irreducible. Then f remains irreducible in $F_R[x]$.

Today, we'll prove the converse:

Theorem 9.7

Suppose $f \in R[x]$ is irreducible as a polynomial in $F_R[x]$. Then there exists $r \in R$, $g \in R[x]$ such that $f = rg$ and g is irreducible.

---

10 Recitation 10: Polynomial Factorization and Gröbner Bases (11/2/21)

Definition 22. Suppose that F is a field, and $F[x]$ is it's polynomial ring. We define the **formal derivative** $' : F[x] \to F[x]$ to be the linear operator extending $x^n \mapsto nx^{n-1}$ (recall we have a canonical homomorphism $\mathbb{Z} \to F$).

Exercise 10.1 **Product Rule**

Show that $(fg)' = f'g + g'f$.

Exercise 10.2

Let $r \in R$. Show that $f(r) = f'(r) = 0$ iff $(x - r)^2$ divides f.

Theorem 10.3 **Eisenstein**

Suppose that p is prime and that $f = x^n + \sum_{i<n} a_i x^i \in \mathbb{Z}[x]$ where p divides a_i for all i. Then if p^2 doesn't divide a_0, then f is irreducible.

Exercise 10.4

$x^4 + 1 \in \mathbb{Z}[x]$ is irreducible.

Exercise 10.5

Given p prime, we define the n**th cyclotomic polynomial** to be

$$\frac{x^p - 1}{x - 1} \in \mathbb{Z}[x].$$

Show that this polynomial is irreducible.

Now we'll turn to a proof of Hilbert's basis theorem. We'll begin by collecting some auxiliary results:

Exercise 10.6

Let $\{a_n\} \subseteq \mathbb{R}$. Then there exists a subsequence $\{a_{n_k}\} \subseteq \{a_n\}$ that is either nondecreasing or nonincreasing.

Exercise 10.7

Let $<$ be the partial order on $\mathbb{N}^n$ where $a := (a_1, \cdots, a_n) < b := (b_1, \cdots, b_n)$ iff $a \neq b$ and $a_i \leq b_i$ for all i, and write $a \sim b$ iff $a \not< b$ and $b \not< a$.
Now let $X \subseteq \mathbb{N}^n$ be such that $x \sim y$ for all $x, y \in X$. Then $|X| < \infty$.

Proof. Suppose not, i.e. that $|X| = \infty$, and let $\pi_i : \mathbb{N}^n \to \mathbb{N}$ be the natural projection onto the ith coordinate.
Since we have a natural injection from X to $\prod_{i\in[n]} \pi_i[X]$, we see that there must be i with $\pi_i[X]$ infinite. WLOG, let this $i = 1$.
Then we can construct a sequence $\{x_i\}_{i\in\mathbb{N}} \subseteq X$ such that $\{x_{i,1}\}$ is strictly increasing.
Now suppose first that the set $\{x_{i,j}\}_{i\in\mathbb{N},j>1}$ is bounded.
Then by pigeonhole, there must exist $i < i'$ with $x_{i,j} = x_{i',j}$ for all $j > 1$. This in turn implies $x_i < x_{i'}$, which violates our hypothesis.
Otherwise, this set is unbounded, hence infinite, so we can apply the same argument again to find i_0 with $\pi_{i_0}[\{x_i\}]$ infinite. Again assuming WLOG $i_0 = 2$, we can apply the same argument to extract a further subsequence (not relabeled) $\{x_i\}_{i\in\mathbb{N}} \subseteq X$ such that $\{x_{i,1}\}, \{x_{i,2}\}$ is strictly increasing.
Iterating this argument, we eventually reach a contradiction, as it cannot be the case that there exists a sequence in X with all coordinates increasing.

■

Exercise 10.8

Let $M \subseteq F[x]$ be a set of monic monomials, and set $M_0 := \{m \in M \mid m' \nmid m \quad \forall m' \in M \setminus \{m\}\}$. Show that $(M_0) = (M)$ and further that M_0 is finite.

Exercise 10.9

Combine the above to deduce that Gröbner bases exist.

Theorem 10.10 **Buchberger's Criterion**

Let $I = (g_1, \ldots, g_m)$ be a nonzero ideal in $F[x_1, \cdots x_n]$, and let $S(f, g)$ be "the polynomial obtained by cancelling the leading terms of f, g". Then $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for I if and only if $S(g_i, g_j)$ has remainder 0 after dividing by $g_1, \cdots, g_m$ for all $1 \leq i < j \leq m$.

Proof. See proposition 9.6.26 in Dummit and Foote. ■

Exercise 10.11

Compute a Gröbner basis for $(x^3y - xy^2 + 1, x^2y^2 - y^3 - 1) \subseteq \mathbb{Q}[x, y]$ with the lexicographic order extending $x > y$.

11 Recitation 11: Modules and Field Extensions (11/9/21)

Today, we'll start off with some set theoretic black boxes.

THEOREM 11.1 **Schröder-Bernstein**

Suppose that A, B are two sets such that there exist injective functions $f : A \to B, g : B \to A$. Then there exists a bijection from A to B.

THEOREM 11.2

Suppose A is an infinite set. Then there exists a bijection between A and A^2.

Now recall the following result from previous recitations:

THEOREM 11.3

Suppose V is an F vector space. Then there exists $B \subseteq V$ such that B is a basis for V.

Today, we'll be proving the following.

THEOREM 11.4

Suppose B_1, B_2 are two bases for the F vector space V. Then $|B_1| = |B_2|$.

THEOREM 11.5

Any two vector spaces of the same dimensional and over the same field are isomorphic.

THEOREM 11.6

The dimension of $\mathbb{R}$ as a $\mathbb{Q}$-vector space is $|\mathbb{R}|$.

EXERCISE 11.7

Show that the same holds for $\mathbb{R}^2$, and hence that $\mathbb{R} \cong \mathbb{R}^2$ as vector spaces and additive groups.

EXERCISE 11.8

Suppose $F \subseteq K$ is a field extension, and that $[K : F] = n < \infty$. Then for all $\alpha \in K$, there exists a polynomial $p \in F[x]$ of degree at most n such that $p(\alpha) = 0$ in K.

12 Recitation 12: More Field Extensions (11/16/21)

We'll start today by reviewing some results from class: throughout, $F \subseteq K$ will be a field extension with $\alpha \in K$.

Definition 23. Given $\alpha \in K$, if there exists $f \in F[x]$ with $f(\alpha) = 0$ (in K), we call α **algebraic** over F. (There's a couple equivalences to this that I'm too lazy to write). It can then be checked that

$$\{f \in F[x] \mid f(\alpha) = 0\} \subseteq F[x]$$

is an ideal, and is hence principally generated by a unique monic polynomial m_α, called the **minimal polynomial** of α.

As part of the equivalent definitions of being algebraic, we have the following result:

Exercise 12.1

$F[\alpha] = F(\alpha) \iff \alpha$ is algebraic, where the left hand side is the ring generated by adding α, and the right is the corresponding field generated by α.

Exercise 12.2

$[F(\alpha) : F] = \deg m_\alpha$.

We also have the following corollary of the homework:

Theorem 12.3

Suppose $\{\alpha_i\}_{i\in[n]} \subseteq K$, where $[F(\alpha_i) : F]$ are all relatively prime. Then $[F(\alpha_1, \cdots, \alpha_n) : F] = \prod[F(\alpha_i) : F]$.

Now we'll do some computational examples.

Exercise 12.4

Show $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$.

Exercise 12.5

Compute the splitting fields of $(x^p - 1)/(x - 1)$ and $x^p - 2$ as polynomials in $\mathbb{Q}[x]$ as a subset of $\mathbb{C}$.

---

13 Recitation 13: Automorphism Groups and Transcendence Bases (11/23/21)

It's the penultimate recitation! Today should be relatively light; the transcendence base stuff is more of a bonus topic since Thanksgiving is right around the corner.

We'll start by reviewing some explicit examples of automorphism groups; recall that given a field extension $F \subseteq K$, we denote by $\mathrm{Aut}_F(K)$ the set of automorphisms of K that fix F. When F isn't specified explicitly, assume it to be the isomorphic copy of $\mathbb{Z}\backslash p\mathbb{Z}$ or $\mathbb{Q}$ in K.
Also recall that given any irreducible $p \in F[x]$, if K is the splitting field of p, then $\mathrm{Aut}_F(K)$ acts transitively on the roots of p. Now we'll just go through the following:

Exercise 13.1

Compute the following automorphism groups:

1. $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$.
2. $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}))$.
3. $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \rho))$, where ρ is a third root of unity.
4. $\mathrm{Aut}(\mathbb{R})$.

Now we'll talk about transcendence base stuff!

Definition 24. Given fields F, K, a finite sequence $s_i \in K$ is **algebraically dependent** over F if there is a nonzero multivariate polynomial $f \in F[x_i]$ with $f(s_i) = 0$.
A set B is called **algebraically independent** if no injective sequence from B is algebraically dependent. Any maximal such B is called a **transcendence basis**.

First we'll establish some basic properties of transcendence bases:

Exercise 13.2

Show that if B is a transcendence base of K over F, then K is algebraic over $F(B)$.

Exercise 13.3

Show that this implies any base B for $\mathbb{C}$ over $\mathbb{Q}$ has cardinality equal to $|\mathbb{C}|$.

Exercise 13.4

Show that any $\sigma \in S_B$ extends to an element of $\mathrm{Aut}(\mathbb{C})$, and conclude that $|\mathrm{Aut}(\mathbb{C})| = 2^{2^\omega}$.

---

14 Recitation 14: Cyclotomic Polynomials! (11/30/21)

It's the last recitation! Today, we'll be discussing cyclotomic polynomials. We begin with the following definition.

Definition 25. For $n \in \mathbb{N}$, let $\mu_n \subseteq \mathbb{C}$ be the set of nth roots of unity: that is,

$$\mu_n := \{e^{2\pi i m/n} \mid m \in \mathbb{N}\}.$$

Today, we'll be interested in analyzing $\mathbb{Q}(\mu_n)$. Towards this end, we start with the following.

Definition 26. Say $\rho \in \mu_n$ is **primitive** if it has order n. We define

$$\Phi_n := \prod_{\rho \text{ primitive} \in \mu_n} (x - \rho) = \prod_{\gcd(i,n)=1, i<n} (x - \rho^i).$$

Exercise 14.1

Show that

$$x^n - 1 = \prod_{d|n} \Phi_n(x) \implies n = \sum_{d|n} \varphi(d).$$

This furnishes us with an explicit way to compute Φ_n through just polynomial division.

Exercise 14.2

Compute Φ_n for some some values of n.

Now we show some other interesting properties of Φ_n.

Exercise 14.3

Show:

- $\Phi_n \in \mathbb{Z}[x]$.
- Φ_n is irreducible. Hint: suppose $\Phi_n = fg$ for f, g monic and f irreducible. Using separability of $x^n - 1$ in $\mathbb{Z}/p\mathbb{Z}$, show that the roots of f are precisely the roots of Φ_n.

Exercise 14.4

Suppose $p \nmid n$, $m \mid n$ with $m < n$. Then $\Phi_n, x^m - 1$ have no common roots in $\mathbb{Z}/p\mathbb{Z}$.

Theorem 14.5

For any $n \in \mathbb{N}$, there exists infinitely many primes that are 1 mod n.
