

Day 1: Primer on Field Extensions

Tom Gannon

August 14, 2017

1 Introduction

Today we'll show that the *separable closure* of a field extension K/F (i.e. the set of elements separable over F) is a field. We will further show that this separable closure L has the property that K/L is a *purely inseparable extension*, which we'll define shortly. A good reference for this is Keith Conrad's blurb *Separable Extensions*, which you can find by googling it.

1.1 Primer on Separability

For the whole day, we'll fix a field F , which we'll refer to the "base" or the "ground" field whenever I feel like changing it up and typing more letters out than just typing the letter F . Moreover, we'll fix an algebraic closure $\overline{F}$ that all the action of today is going to be taking place in—meaning that any field extension we refer to is implicitly assumed to be a subset of $\overline{F}$. If you want a proof that such a thing exists, it's in Dummit and Foote. We'll start off with some basics regarding this:

Definition 1.1. We say that an element $\alpha \in \overline{F}$ is **separable** over F if the minimal polynomial of α over F , say $q(x)$, does not have α as a multiple root—that is, $(x - \alpha)^2 \nmid q(x)$. We say a field extension K/F is **separable** if every element in K is separable over F .

It isn't too hard to check whether a given element is separable once you know its minimal polynomial:

Exercise 1.2. Assume $p(x) \in F[x]$ has root α . Show $p(x)$ has a multiple root α (that is, $(x - \alpha)^2 \mid p(x)$) if and only if the (formal) derivative $p'(x)$ has α as a root. (Hint: Show that the product rule formally holds and write $p(x) = q(x)(x - \alpha)$).

For a topic that is not analysis, the derivative comes up a lot more than you might think. For example:

Exercise 1.3. Fix $\alpha \in \overline{F}$, and let $q(x) \in F[x]$ denote the minimal polynomial of α . Show that $q(x)$ has α as a multiple root if and only if $q'(x) = 0$. Conclude that no irreducible polynomial over a field of characteristic zero has a multiple root, and classify those polynomials with coefficients in a field of characteristic p which have derivative zero.

In particular, every polynomial over $\mathbb{Q}$ is separable.

1.2 Primer on Morphisms of Fields

Morphisms of fields $F_1 \rightarrow F_2$ are just ring morphisms—that is, maps that preserve the addition and multiplication structure of the ring. By convention, we'll require our ring maps send $1 \rightarrow 1$. With this convention, we have an interesting phenomenon:

Exercise 1.4. Show that any map of fields is an embedding/injection.

We'll use the two terms embedding and injection interchangeably. This result suggests that field embeddings are the things we should look closer at. One natural question is, if K/F is a finite dimensional field extension, how many different ways can we embed K in a different way into some subfield of $\overline{F}$ (meaning, for example, that the identity and conjugation maps $\mathbb{C} \rightarrow \mathbb{C}$ represent distinct maps)?

2 Primer on Separable Closure

Exercise 2.1. (Bound on Embeddings) Let K/F be an $n \in \mathbb{N}^{>0}$ dimensional extension of fields. Show that there are at most n distinct embeddings $K \hookrightarrow \bar{F}$ which fix F pointwise. (Hint: Let $K = F(\alpha_1, \dots, \alpha_n)$ and proceed by induction on n , noting that $n = [K : F] = [F(\alpha_1, \dots, \alpha_n) : F(\alpha_1, \dots, \alpha_{n-1})] \dots [F(\alpha_1) : F]$. Most of the work should be done in the base case.)

Exercise 2.2. (Separability Maximizes Embeddings) Let K/F be an $n \in \mathbb{N}^{>0}$ dimensional extension of fields. Show that there are **exactly** n distinct embeddings $K \hookrightarrow \bar{F}$ which fix F pointwise if and only if K/F is separable. (Hint: Most of the work you did in the last exercise—argue wherever you wrote " $\leq$ ", you should argue why equality holds.)

Exercise 2.3. (Sneakily proving that a field is separable if and only if some set of generators is separable, except it's not that sneaky because I'm putting it in these parenthesis) Let K/F be an $n \in \mathbb{N}^{>0}$ dimensional extension of fields. Show that there are **exactly** n distinct embeddings $K \hookrightarrow \bar{F}$ which fix F pointwise if and only if $K = F(\alpha_1, \dots, \alpha_n)$ and each α_i is separable over F . (Again, you did of the work you did in the last exercise. For "only if," argue by contrapositive and argue why "<" needs to occur somewhere).

Oh but look! If you put those last two exercises together in the obvious way, you get:

Corollary 2.4. A finite dimensional field extension K/F is separable if and only if some generating set of K/F contains only separable elements.

Exercise 2.5. Show that if $\alpha, \beta \in \bar{F}$ are separable over F , then $\alpha \pm \beta$, $\alpha\beta$ and α^{-1} are also separable over F . (If you want some algebra fun, you can argue α^{-1} is separable over F directly, but the others are not so easy to do directly).

Corollary 2.6. The **separable closure** K_{sep} of a field extension K/F , defined to be the set of all elements of K separable over F , is a field.

Definition 2.7. We define the **separability degree** of an extension K/F to be the degree of $[K_{\text{sep}} : F]$.

3 Primer on Purely Inseparable Extensions

Definition 3.1. A field extension E/L is said to be **purely inseparable** over L if $p := \text{char}(L)$ is nonzero¹ and for all $\alpha \in E$, α raised to the power p^n for some n is in L (written more normally, this means there is some $n \in \mathbb{N}^{>0}$ such that $\alpha^{p^n} \in L$, but I always would misread that as $(\alpha^p)^n \in L$, which isn't the same thing) or $E = L$.²

Exercise 3.2. (Alternate Definition of Purely Inseparable Extensions) Show that equivalently a purely inseparable extension E/L with $p := \text{char}(L) > 0$ is an extension where for all $\alpha \in E$, the minimal polynomial of α over E is $x^{p^n} - \alpha^{p^n}$ (again "alpha raised to a power that is itself a power of p ") for some $n \in \mathbb{N}$.

Exercise 3.3. (Alternate Definition of Purely Inseparable Extensions) Show that equivalently a purely inseparable extension E/L is an extension where for all $\alpha \in E$, if α is separable over E then $\alpha \in L$.

To close this fun off, you should prove the below theorem (which is actually just one finishing step):

Theorem 3.4. (Field Extensions Split into Separable and Purely Inseparable Extensions) Given any finite dimensional extension K/F , then there exists an intermediate field L with $F \subset L \subset K$ where L/F is separable and K/L is purely inseparable.

This idea will be used a lot. Want to prove something is true for all field extensions? Can you prove it for a separable field extension and a purely inseparable one and then show that if your statement is true for L/F and K/L then it's true for K/F .

¹Fun fact! One way to view the characteristic of a field L is to view it as number n such that $n\mathbb{Z}$ is the kernel of the unique map $\mathbb{Z} \rightarrow L$. This explains why the characteristic of $\mathbb{Q}$ is said to be 0 instead of what you might have thought would be natural at first, "characteristic ∞ ".

²This is a technical condition you don't really need to worry about—it's just stated to make the last theorem of this paper sound more clean. Also, two footnotes in one definition! How cool is that?!

Day 2: Galois Theory

Tom Gannon

August 15, 2017

1 Introduction

We'll review the basics of Galois Theory and prove a theorem which determines the structure of a composite of two fields when the Galois group of the two subfields are known.

1.1 Primer on Galois Theory

As always, let F be a field, and any field extension mentioned will take place a fixed algebraic closure of F .

Recall that the term "**Galois group**" is just the group of automorphisms of K fixing F pointwise for certain, specific field extensions K/F called *Galois Extensions*. Roughly, a "Galois Extension" means that there are as many automorphisms as there can be.

Definition 1.1. A field extension K/F is **algebraic** if for all $\alpha \in K$, there exists an $f(x) \in F[x]$ such that $f(\alpha) = 0$. An extension K/F is **normal** if it is the splitting field of some collection of polynomials (i.e. the smallest¹ field containing all the roots of those polynomials), and K/F is **Galois** if it is a normal, separable, algebraic extension.

This doesn't always happen:

Exercise 1.2. (Finite, Separable Extension That Isn't a Galois Extension): Show that the field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has trivial automorphism group, meaning there is exactly one embedding $\mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{Q}(\sqrt[3]{2})$. Find a field K where there are 3 distinct embeddings $\mathbb{Q}(\sqrt[3]{2}) \hookrightarrow K$. If you looked at the "separability" sheet, you can prove this is the maximal number of extensions.

Exercise 1.3. (Finite, Normal Extension That Isn't Galois) Show that if $F := \mathbb{F}_2(x)$ and $K := F[t]/(t^2 - x)$ (i.e. adjoining a square root of x), then $\text{Aut}(K/F)$ is trivial.

Exercise 1.4. (Finite Extension Implies Algebraic Extension) Show that if K/F is a finite extension (that is K is a finite dimensional vector space over $F \subset K$) then K/F is an algebraic extension. (Hint: If $\alpha \in K$, consider the set $\{1, \alpha, \alpha^2, \dots\}$). Conclude that any finite, normal, separable extension is a Galois extension.

This is good for us in particular because for finite, normal, separable extensions we have an easy to remember relation between the dimension of the field and the order of the Galois group.

Theorem 1.5. If K/F is a finite Galois extension with $G := \text{Gal}(K/F)$, then $|G| = [K : F]$.

Exercise 1.6. Prove the above theorem! You will probably want all of the results covered on "separability" day, and also to prove that if K/F is a Galois extension, then any field embedding $i : K \rightarrow \overline{F}$ actually sends $K \rightarrow K$.

Exercise 1.7. (Galois Groups aren't necessarily finite) Construct a Galois extension with infinite Galois group. Note that $\mathbb{C}/\mathbb{Q}$ doesn't satisfy this criterion— $\mathbb{C}$ has some elements that are not algebraic, i.e. **transcendental** over $\mathbb{Q}$. (Hint: It's "close" to being Galois, though. You'll have to use ideas from the last day to solve this, depending on the route you take. This is definitely the hardest exercise of the day, and least important for the course.)

¹We'll be working in a fixed algebraic closure of any field we talk about, which always exists. So if you had some technical worry, don't.

2 Primer on Using Galois Theory in Non Galois Extensions

Recall that the **Fundamental Theorem of Galois Theory** says that given any finite Galois extension K/F (one for which $[K : F]$ finite, or equivalently $|G|$ finite) with Galois group G , there is a bijective correspondence $\{\text{subgroups of } G\} \leftrightarrow \{\text{intermediate subfields } F \subseteq L \subseteq K\}$ given by taking a subgroup and mapping to the set of elements fixed pointwise by every element of that subgroup and taking an intermediate field to the group of elements fixing that field pointwise. But we can get even more out of this theorem:

Exercise 2.1. (*Distinct Field Embeddings*) Let L/F be a finite separable field extension, not necessarily Galois. Show that there is a finite Galois extension K/F containing L . Let $G := \text{Gal}(K/F)$ and let H denote the set of elements fixing L pointwise. Show that any field embedding of L fixing F must map into K . Show that the **distinct** embeddings are given by picking a representative of each coset in G/H . Can two distinct embeddings map into the same field? Determine a condition on H and G which determines when L/F is Galois, and prove it.

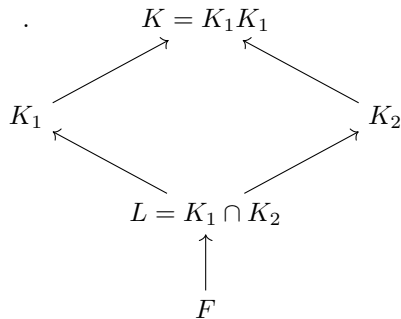
3 Primer on The "Sliding Lemma"

The "Sliding Lemma" is a term I made up to describe a lemma which describes the Galois group of the composite of two fields when the automorphism groups of the two fields are known. Maybe once these Primer Exercises achieve world class fame, everyone will call it the sliding lemma one day! But until then, here's the lemma:

Exercise 3.1. Define the "composite" of two fields $K_1, K_2 \subset \bar{F}$ if you haven't heard the term yet. Informally, it is the union of the two fields, but closed under all of the field operations.

Lemma 3.2. Assume that K_1, K_2 are finite extensions of F and K_1/F is Galois. Then if $K := K_1 K_2$ denotes the composite field, then K/K_2 (for emphasis, over K_2 —not over F) is Galois, and if $L := K_1 \cap K_2$, then $\text{Gal}(K/K_2) \cong \text{Gal}(K_1/L)$.

A good reference for this is section 14.4 of Dummit and Foote. Here's a picture taken from that section that I use a lot, where the arrows denote "inclusion" and also denote "I couldn't figure out how to get rid of them."



Exercise 3.3. Show that, with the above setup, that K/K_2 is Galois.

Exercise 3.4. Let $G := \text{Gal}(K/K_2)$ and $H := \text{Gal}(K_1/L)$. Define a map $\psi : G \rightarrow H$ that seems like a good candidate for an isomorphism. Show it is an injective group homomorphism.

Exercise 3.5. Show that ψ above is surjective by arguing that if $K_1^{\psi(G)}$ denotes the elements in K_1 fixed by $\psi(G)$, then $K_1^{\psi(G)} = L$. (Hint: $K_2 \subset K_1^{\psi(G)} K_1 \subset K$. Use the fundamental theorem of Galois Theory.)

Exercise 3.6. Show that given two extensions K_1, K_2 over a field F such that at least one is Galois, then $[K_1 K_2 : K_1 \cap K_2] = [K_1 : K_1 \cap K_2][K_2 : K_1 \cap K_2]$. Show that this conclusion need not hold if neither extension is Galois. (Hint: I like to use $\mathbb{Q}[\sqrt[3]{2}]$ for all of my "Galois hypothesis is necessary" needs.) Conclude that if two extensions $K_1/F, K_2/F$ are **linearly disjoint**—i.e. $K_1 \cap K_2 = F$, then $[K_1 K_2 : F] = [K_1 : F][K_2 : F]$.

This idea comes up because one basic question you can ask in number theory is "given the integral closure of a Dedekind² ring in two fields, what does the integral closure in the composite field look like?"

²Dedekind rings are rings in which every ideal factors into a product of prime ideals, a generalization of UFDs. They're one of the first things in Algebraic Number Theory that make you think, "Woah! This is cool."

Day 3: Primer on Noetherian Stuff

Tom Gannon

August 17, 2017

1 Introduction

Today we'll deal with everything regarding the finitely generated and Noetherian properties. A lot of times finitely generated things turn out to be the right thing to work with in algebra, and we'll show why this is with a few strange pathologies. We'll also prove a property we'll need to use tomorrow that any submodule of R^n is free and of rank $\leq n$ if R is a PID.

1.1 Motivation from Principal Ideal Domains

Recall that a *Principal Ideal Domain* R is an integral domain R such that any ideal $I \subset R$ can be written $I = Ra$ for some element $a \in R$, and specifically recall a part of the proof that principal ideals are unique factorization domains:

Exercise 1.1. (*PIDs Are Factorization Domains*): Show that if R is a PID, then any nonzero element $r \in R$ has some factorization $r = s_1 \dots s_n$ where s_i are not necessarily distinct irreducible elements of R . (Hint: If $r_i = r_{i+1}t_{i+1}$ was reducible, then $(r_i) \subsetneq (r_{i+1})$. Let $I = \cup_i (r_i)$.)

1.2 The Initial Definition

The definition of a Noetherian ring generalizes the above proof technique we used:

Definition 1.2. We say a ring A is **Noetherian** if any chain of ideals $I_1 \subset I_2 \subset \dots \subset A$ stabilizes¹ at some point—that is, there exists an $n \in \mathbb{N}$ such that $m \geq n$ implies that $I_m = I_n$.

Another (equivalent) way to think of Noetherian rings is that the chain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$ can't happen for ideals $I_k \subset A$. This is called the **ascending chain condition** on ideals. Also, note that ideals of A are just A modules that *just so happen* to be a submodule of the A module A . In particular, it is possible to define the concept of a **Noetherian Module**, and you should do so. Feel free to do so before I tell you to in this next exercise. That way, you can feel like you're ahead of the game.

Exercise 1.3. Define what it means for an A module M to be **Noetherian** using the ascending chain condition on submodules. Show that equivalently, an A module M is Noetherian if and only if each submodule of M is finitely generated as an A module. Determine what this condition specifically means in terms of rings and ideals.

Exercise 1.4. (*A Non-Noetherian Ring/Module*) Show that the ring $\mathbb{R}[x_i]_{i \in \mathbb{N}_{>0}} = \mathbb{R}[x_1, x_2, \dots]$ is not a Noetherian ring.

If you ever come across something with "Noetherian" in the hypothesis, it's a good idea to throw the above ring in the theorem and see if it still holds.

2 Primer on Stock Results on Noetherian Modules that I Like To Keep Around

Exercise 2.1. (*Submodules/Quotients of Noetherian modules are Noetherian*) Show that if $N \subset M$ is a submodule of an A module M , then N and M/N are Noetherian.

¹A word on notation. " $\subset$ " and " $\subseteq$ " will mean the same thing—"is a subset of" and " $\subsetneq$ " means that the two sets aren't equal.

Exercise 2.2. (*Finitely Generated Module with Non Finitely Generated Submodule*) Let $R := \mathbb{R}[x_i]_{i \in \mathbb{N}^{>0}} = \mathbb{R}[x_1, x_2, \dots]$. Show that R is a finitely generated R module, but R has a submodule which is not finitely generated as an R module.

This shows that the hypothesis of a ring/module being Noetherian is stronger than requiring it to be finitely generated, because any Noetherian ring/module is finitely generated.

But on the other hand:

Exercise 2.3. Show that any finitely generated module of a Noetherian ring R is a Noetherian module. (Easy mode: Assume that R^n is Noetherian. Hard Mode: Prove it.)

We also have a very helpful:

Theorem 2.4. (*Hilbert's Basis Theorem*) If A is a Noetherian ring, so is $A[x]$.

Exercise 2.5. Prove this theorem. (Hint: Don't actually try to prove this theorem, just go look it up in a book somewhere. Like Dummit and Foote. To check if you really understand the proof, modify the idea of the proof slightly to show that if A is a Noetherian ring, then the ring of formal power series of A , $A[[x]]$, is a Noetherian ring.)

3 Primer on the Module R^n

Note that in the world of being "well behaved", modules are just the absolute worst. We have above that a finitely generated module can have a not finitely generated submodule. Also even if the submodules are finitely generated (i.e. the module is Noetherian), we don't have any good rank bounds:

Exercise 3.1. Show that the ring $R := \mathbb{Q}[x, y]$ has **rank** 1—that is, there is a subset of R consisting of one linearly independent element over R but no set of two linearly independent elements over R . However, construct a submodule (ideal) of R with rank 2.

Definition 3.2. An A -module M is free on generators $m_1, \dots, m_k \in M$ if $r_1 m_1 + \dots + r_k m_k = 0$ implies $r_i = 0$ for all i .

Exercise 3.3. (Rank one submodule that isn't a free submodule) Let $R = \mathbb{Z}[x]$ and let I denote the submodule/ideal $(2, x)$. Show that any two elements are linearly dependent and no single element spans.

This sort of tomfoolery² doesn't happen when you restrict to PIDs. In particular,

Theorem 3.4. If R is a PID, then any submodule of R^n is a free submodule³ of rank $\leq n$.

Exercise 3.5. Prove the above theorem. (Hint: Let $M_i := (Re_1 + \dots + Re_i) \cap M$, where M is the submodule and $\{e_i\}$ is the standard basis of R^n . For the inductive hypothesis at step k , let I denote the set of all elements r_k that have the form $r_1 e_1 + \dots + r_k e_k$ and are in M . Pick some v whose last coordinate is a generator of I , and show that $M_k \cong M_{k-1} \oplus Rv$).

We'll use this theorem tomorrow to help us prove that there's only one quality that a module M over a PID R can have, called *torsion*, that stops M from looking like R^n for some $n \in \mathbb{N}$.

²Side note. If you can think of a good adjective to describe a person that has the word "Tom" in it, I'd love to hear it. Currently there are only bad ones (e.g. "Peeping Tom")

³It could also be the zero submodule, by the way. You can think of R^0 as the zero module. But note that for a general ring, R^0 isn't the *only* module of rank zero!

Day 4: Modules over a PID

Tom Gannon

August 17, 2017

1 Introduction

Today we'll show that given any principal ideal domain R , any torsion free R module M is isomorphic to a free module R^m for some m . This comes up a lot in working over *Discrete Valuation Rings*, the natural setting where a lot of number theory occurs.

1.1 Primer on Principal Ideal Domains

Recall that a *Principal Ideal Domain* R is an integral domain R such that any ideal $I \subset R$ can be written $I = Ra$ for some element $a \in R$. One of the reasons we like to work with principal ideal domains is that is that if we can show that the set of all elements of a ring that satisfy a property $\mathcal{P}$ is an ideal, then we are guaranteed an element $a \in R$ such that a given $r \in R$ has property $\mathcal{P}$ if and only if $a|r$. The other reason we work with PIDs are that we have a *Bézout Identity*:

Exercise 1.1. (*PIDs Satisfy Bézout Identity*): Assume $a_1, \dots, a_n$ are elements of a PID R . Determine a notion of a greatest common divisor of $\{a_1, \dots, a_n\}$, and let d denote this greatest common divisor. Show that if $e \in R$ such that $e|a_i$ for all i , $e|d$. Moreover, show that the **Bézout Identity** holds, that is, there exist $r_i \in R$ such that $r_1a_1 + \dots + r_na_n = d$.

Exercise 1.2. (*UFDs Don't Satisfy Bézout Identity*) Determine the notion of a greatest common divisor in a unique factorization domain. Let $S := k[x, y]$ where k is some field. Then S is a UFD. Show that for all $r, s \in S$, $rx + sy \neq \gcd(x, y)$.

1.2 Primer on Modules

Recall that a *module* M over a ring R is a definition you can Google, and that we say M is *torsion free* if $r \in R, m \in M$ and $rm = 0$ implies either $r = 0$ or $m = 0$.

Exercise 1.3. (*Torsion Free Hypothesis is Necessary*) Show that if M is a non torsion free module over a principal ideal domain R , then for all $k \in \mathbb{N}$, $M \not\cong R^k$.

2 Primer on Modules over a Principal Ideal Domain

Theorem 2.1. Let M be a torsion free module over a principal ideal domain R that can be generated with n elements and cannot be generated by any fewer number of elements. Then $M \cong R^k$.

Proof. Induction on n . For the inductive step, assume $n > 1$ and that if N is a torsion free module over a R that can be generated with $n - 1$ elements and cannot be generated by any fewer number of elements, $N \cong R^{n-1}$. Let $m_1, \dots, m_n$ be a set of minimal generators for M . Then there is a "natural" map $\phi : R^n \rightarrow M$.

Exercise 2.2. Determine what ϕ should be, and argue why this immediately implies that ϕ is a module morphism (i.e. an R - "linear" map) and that ϕ is surjective. Conclude $M \cong R^n / \ker(\phi)$.

Thus it suffices to show that $W := \ker(\phi)$ is trivial. Assume it isn't.

Let's set up some notation. Let $\pi_i : R^n \rightarrow R$ be projection onto the i^{th} coordinate, and $\zeta_i : W \rightarrow R$ defined to be the composite of inclusion $W \hookrightarrow R^n$ with π_i . We claim that $W = Rm$ for some $m \in M$.

Exercise 2.3. (*Kernel Has Rank ≤ 1*) Show there exists an i such that ζ_i is not the zero map. Swapping generators if necessary, we assume that $\zeta := \zeta_n \neq 0$. Show there exists a nonzero $x \in R^n$ such that $W = Rx$. (Hint: Show that if the last coordinate of two elements of W agree, then the vectors themselves agree. Then let I denote the set of all elements $r_n \in R$ with $r_1e_1 + \dots + r_ne_n \in W$.)

Exercise 2.4. (*Almost basis completion*) Show that given any element nonzero¹ $x \in M$, there exists a $b \in R$ and a basis of R^n , say, $\{y_1, \dots, y_n\}$ such that $by_1 = x$. (Hint: Let $x = (x_i)$ componentwise and let $b := \gcd(x_1, \dots, x_n)$, $y_1 = \frac{1}{b}x$. Then there exists r_i such that $r_1 \frac{x_1}{d} + \dots + r_n \frac{x_n}{d} = 1$. Let $\Phi : R^n \rightarrow R$ via $\Phi(b_1, \dots, b_n) = r_1 b_1 + \dots + r_n b_n$. Then $x = \Phi(x)y_1 + (x - \Phi(x)y_1)$ to show $R^n \cong Ry_1 \oplus \ker(\Phi)$.)

Exercise 2.5. Combine the last two exercises to contradict the assumption that our generating set was minimal. (Hint: What assumption haven't we used yet?)

□

This result is the result that is used a lot in the specific applications of Discrete Valuation Rings and the like, which will be covered on like, day one of the course. But in the meantime, know that there's a stronger version of the theorem that gives a lot more power, whose proof isn't that much harder than this proof and can be found in Dummit and Foote:

Theorem 2.6. (*Fundamental Theorem of Modules over a Principal Ideal Domain*) Let M be a finitely generated module over a principal ideal domain R . Then there exists a unique $n \in \mathbb{N}$ (including the possibility of $n = 0$) such that $M \cong R^n \oplus R/(a_1) \oplus \dots \oplus R/(a_m)$ for some $a_1 | a_2 | \dots | a_m$ in R .

Exercise 2.7. (*Finite Generation Hypothesis is Necessary*) Determine a torsion free R module that is not a direct sum (even of infinite index!) of copies of R . (Hint: You learned the specific example you need in high school or before).

Exercise 2.8. (*Finite Fields Are Cyclic*) Assuming the Fundamental Theorem of Modules over a Principal Ideal Domain, show that the multiplicative group of a finite field is a cyclic group.

¹This also trivially holds for $x = 0$, but a hint is that the proof is different if x is nonzero.