24 Fields

24.1 Review — Noetherian Rings

Recall the definition of Noetherian rings:

Definition 24.1
A ring is Noetherian if every ideal is finitely generated.

This definition has a useful reformulation, in terms of chains.

Proposition 24.2
A ring is Noetherian if and only if every increasing chain of ideals stabilizes — in other words, given any chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$, from some point on we must have $I_n = I_{n+1} = \cdots$.

Example 24.3
In the case $R = \mathbb{Z}$, a chain of ideals amounts to a list of integers d_1, d_2, ... where $d_i \mid d_{i-1}$ for all i. This chain clearly has to stabilize, since it's a nonincreasing sequence of positive integers.

Proof of Proposition 24.2. First suppose R is Noetherian, and we have a chain $I_1 \subseteq I_2 \subseteq \cdots$. Then their union $I = I_1 \cup I_2 \cup \cdots$ is an ideal. Since R is Noetherian, then I is finitely generated, so we can write $I = (a_1, \ldots, a_n)$. Then for each i, a_i must be contained in some ideal (since it's in their union). But there's finitely many a_i, so some I_m must contain all of them (since $I_k \subseteq I_{k+1}$, once a_i appears in one ideal, it appears in all following ones). So then $I_m = I$, and the sequence must stabilize at I_m — we must have $I_m = I_{m+1} = \cdots = I$.

For the other direction, suppose R is *not* Noetherian, and let $I \subset R$ be an ideal that's not finitely generated. Pick $a_1 \in I$, and define a_n inductively such that $a_n \in I$ but $a_n \notin (a_1, \ldots, a_{n-1})$ — this is possible because otherwise I would be generated by a_1, ..., a_{n-1}. Now we can take $I_n = (a_1, \ldots, a_n)$, which gives an infinite non-stabilizing chain of ideals. □

Note 24.4
Sometimes the chain condition is given as the *definition* of Noetherian rings.

This has an application to unique factorization in PIDs. Previously, we proved uniqueness but not existence — in our specific examples we had a concept of a norm that we could use to prove that the factorization process always terminates, but it's nontrivial to prove existence of a factorization in an abstract PID. But now we do have the tools to prove that the factorization process terminates in general.

Corollary 24.5
In a PID, every element can be factored as a product of irreducibles.

Proof. Start with the element, and keep on factoring terms until stuck. If we get stuck, then all factors must be irreducible; so assume that the factorization process is infinite instead. Then we can organize the factorization process into an infinite chain of ideals — attempting to factor an element will give a chain d_1, d_2, d_3, ... where $d_{i+1} \mid d_i$ for all i, and then $(d_1) \subset (d_2) \subset \cdots$. This would contradict the chain condition, so factorization must terminate. □

Similarly, we can also revisit a statement we made earlier about maximal ideals:

Proposition 24.6
In a Noetherian ring, every (non-unit) ideal is contained in a maximal ideal.

This is actually true in *any* ring, but the proof requires set theory. But we're mostly interested in several concrete rings, which are all Noetherian; so this proposition covers all such cases.

Proof. Let $I \subset R$ be an ideal, and assume I is not contained in a maximal ideal. Set $I_1 = I$. Now find $I_2 \supset I$ (not equal to I or R), which is possible since I is not maximal. But I_2 is not maximal either, so we can similarly construct $I_3 \supset I_2$, and inductively build a chain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \subsetneq R$ — this is possible at every step because if we couldn't choose I_{n+1}, then I_n would be a maximal ideal containing I. This contradicts chain termination. □

Note 24.7
As a final remark on modules: one important tool in studying modules is an upgrade on the presentation with generators and relations. The idea is that once we have generators and relations, we can also look at the relations between relations, and so on. First construct a surjective map $R^n \to M$ by fixing generators. This map has a kernel K_1, and we can construct a surjective map $R^m \to K_1$ by fixing its generators. This map has a kernel K_2, and we can construct a surjective map $R^\ell \to K_2$, and so on. This is called the **sygyzy** or **free resolution**, and it tells you a lot about the structure of the module.

24.2 Introduction to Fields

Definition 24.8
A **field** is a ring where all nonzero elements are units.

Definition 24.9
A **field extension** is a pair of fields $L \supset K$. The extension is written as L/K.

The theory of field extensions developed from trying to understand how to systematically solve polynomial equations — an important example of a field extension is $L = K(\alpha)$ where α is a root of an irreducible polynomial. We know a formula for solving quadratics; people were interested in understanding more general formulas. One result we'll get to in a few weeks is that if P is a generic polynomial in $\mathbb{Q}[x]$ of degree at least 5, and $K = \mathbb{Q}(\alpha)$ for a root α of P, then K is not contained in any field $\mathbb{Q}(\beta_1, \ldots, \beta_n)$ such that $\beta_i^{d_i} \in \mathbb{Q}(\beta_1, \ldots, \beta_{i-1})$ for each i (for some positive integers d_i) — you can't build the field by repeatedly taking roots. It then follows that there's no expression for the roots of P in terms of arithmetic operations and radicals.

Another application is to compass and straightedge constructions — let $\zeta_n \in \mathbb{C}$ be a primitive nth root of unity.

Guiding Question
When is $\mathbb{Q}(\zeta_n)$ contained in a field of the form $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ for all i?

In other words, we want to find out whether we can obtain ζ_n by the regular operations along with extracting square roots. This is interesting because it happens if and only if a regular n-gon can be constructed by a compass and straightedge. We'll see how to get a complete answer (as Gauss did) — for example, the answer is yes for $n = 17$ and no for $n = 19$. (In fact, a 17-gon appeared on Gauss's tombstone — this was an achievement he was proud of.)

24.3 Field Extensions

Definition 24.10
An extension L/K is **finite** if L is finite-dimensional as a vector space over K.

Essentially, what this means is that if we forget that we can multiply by elements of L, but remember that we can add them and multiply by elements of K, then that turns L into a vector space over K; the extension is finite when this vector space has finite dimension.

We've already seen how to construct examples of finite extensions: if $P \in K[x]$ is an irreducible polynomial, then we saw that $K[x]/(P)$ is a field. (This is because $K[x]$ is a PID, so (P) is a maximal ideal.) In this case, the dimension of the vector space is $d = \deg P$, since we saw the monomials $\overline{1}$, $\overline{x}$, …, $\overline{x^{d-1}}$ form a basis.

Definition 24.11
The **degree** of the extension L/K, denoted $[L : K]$, is the dimension of L as a vector space over K.

On the other hand, suppose we start with an extension L/K, and pick an element $\alpha \in L$. We say α is **algebraic** over K if it satisfies a polynomial equation — meaning that $P(\alpha) = 0$ for some nonzero $P \in K[x]$.

If α is algebraic, then we can take its minimal polynomial P (the monic polynomial of smallest degree with $P(\alpha) = 0$ — this is unique because all polynomials with $P(\alpha) = 0$ form an ideal, and since $K[x]$ is a PID, all ideals are principal and generated by their minimal-degree element). The minimal polynomial has to be irreducible — if $P = P_1P_2$, then $P(\alpha) = P_1(\alpha)P_2(\alpha) = 0$, but since we're in a field, this would imply $P_1(\alpha)$ or $P_2(\alpha)$ is 0, contradicting minimality.

Then we have a homomorphism $K[x]/(P) \to L$ sending $x \mapsto \alpha$. But any homomorphism of fields is injective (alternatively, the kernel of the map $f : K[x] \to L$ sending $x \mapsto \alpha$ is exactly the set of polynomials P with $P(\alpha) = 0$, which is generated by the minimal polynomial of α; so this homomorphism is injective). So we have an isomorphism $K[x]/(P) \cong K(\alpha)$, where $K(\alpha)$ is the subfield of L generated by α.

Note 24.12
This isomorphism is important: later we'll look at automorphisms of fields, and this is the trick that will let us build such maps. For example, start with $K = \mathbb{Q}$ and $L = \mathbb{C}$, and take $\alpha = \sqrt[3]{2}$ and $\beta = \sqrt[3]{2}\omega$ for a primitive third root of unity ω. Then α and β are both roots of the irreducible polynomial $x^3 - 2$. So $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta)$, since both extensions are isomorphic to the abstract construction $\mathbb{Q}[x]/(x^3 - 2)$.

Lemma 24.13
If we have a field extension L/K, then $\alpha \in L$ is algebraic if and only if $K(\alpha)$ is finite-dimensional over K.

Proof. We've already seen that if α is algebraic, then $K(\alpha)$ is finite-dimensional (since it's isomorphic to $K[x]/(P)$ for some irreducible P, which is finite). Meanwhile, a polynomial relation can be thought of as a linear relation between the powers of α. If $m > \dim_K K(\alpha)$, then $1, \alpha, \ldots, \alpha^m$ must be linearly dependent; that linear dependence corresponds to a polynomial over K, giving a polynomial P such that $P(\alpha) = 0$. □

Corollary 24.14
If L/K is finite, then every $\alpha \in L$ is algebraic over K.

24.4 Towers of Extensions

Proposition 24.15
Suppose that we have a tower of field extensions $K \supset E \supset F$, where K/E and E/F are finite. Then K/F is finite, and

$$[K : F] = [K : E] \cdot [E : F].$$

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a basis for E as a vector space over F, and $\beta_1, \ldots, \beta_m$ a basis for K as a vector space over E. Then we'll show that the terms $\alpha_i\beta_j$ form a basis for K/F.

This becomes clear just by substituting notation. First, in order to see that this is a generating set, every $x \in K$ can be written as $x = \sum \lambda_i\beta_i$, while each $\lambda_i \in E$ can be written as $\lambda_i = \sum a_{ij}\alpha_j$, which gives

$$x = \sum a_{ij}\alpha_j\beta_i.$$

Similarly, to prove independence, if we have $\sum a_{ij}\alpha_j\beta_i = 0$, we can collect terms into

$$\sum \left(\sum a_{ij}\alpha_j \right) \beta_i = 0.$$

If the a_{ij} are not all 0, then one of the terms $\sum a_{ij}\alpha_j$ must be nonzero (since the α_j are linearly independent), and therefore the entire sum must be nonzero (since the β_i are linearly independent), contradiction. □

Example 24.16
Find $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$, where $\alpha = \sqrt[3]{2}$ and $\beta = \sqrt[3]{2}\omega$.

Proof. We saw α and β both have minimal polynomial $x^3 - 2$. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Meanwhile, $x^3 - 2$ factors in $\mathbb{Q}(\alpha)$ as $(x - \alpha)(x^2 + \alpha x + \alpha^2)$. The second factor is irreducible (as otherwise, β would lie in $\mathbb{Q}(\alpha)$), so $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$, which means $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 6$. □

Resource: Algebra II Student Notes

Spring 2022

Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng