M3P8 Algebra III

Lectured by Dr David Helm
Typeset by David Kurniadi Angdinata

Autumn 2018

Contents

Lecture 1
Friday
05/10/18

0 Introduction

This course is an introduction to ring theory. The topics covered will include ideals, factorisation, the theory of field extensions, finite fields, polynomial rings in several variables, and the theory of modules.

In addition to the lecture notes, the following will cover much of the material we will be studying.

1. M Artin, Algebra, 1991

Rings are contexts in which it makes sense to add and multiply. For example, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, polynomials, functions $\{0,1\} \to \mathbb{R}$, and $\mathbb{Z}/n\mathbb{Z}$ are rings. The goals of this course include

1. to unify arguments that apply in all of the above contexts, and
2. to study relationships between different rings.

The applications of rings include

1. number theory, by studying extensions of $\mathbb{Z}$ in which particular Diophantine equations have solutions, for example $n = x^2 + y^2 = (x + iy)(x - iy)$ to study solutions in $\mathbb{Z}\{i\}$ and pass to result about $\mathbb{Z}$,
2. algebraic geometry, by the study of zero sets of polynomials in several variables via rings of functions, and
3. topology, by cohomology classes of topological spaces.

1 Basic definitions and examples

1.1 Rings

Recall the definition of a commmutative ring.

Definition 1.1.1. A **commutative ring with identity** R is a set together with two binary operations $+_R, \cdot_R : R \times R \to R$, addition and multiplication, and two distinguished elements 0_R and 1_R such that the following holds.

1. The operation $+_R$ makes R into an abelian group with identity 0_R.
   (a) For all $r \in R$, $0_R +_R r = r +_R 0_R = 0_R$ (additive identity).
   (b) For all $r, s, t \in R$, $(r +_R s) +_R t = r +_R (s +_R t)$ (associativity of $+_R$).
   (c) For all $r, s \in R$, $r +_R s = s +_R r$ (commutativity of $+_R$).
   (d) For all $r \in R$, there exists $-r \in R$ such that $r +_R (-r) = (-r) +_R r = 0_R$ (additive inverses).
2. The operation $\cdot_R$ is associative and commutative with identity 1_R.
   (a) For all $r \in R$, $1_R \cdot_R r = r \cdot_R 1_R = 1_R$ (multiplicative identity).
   (b) For all $r, s, t \in R$, $(r \cdot_R s) \cdot_R t = r \cdot_R (s \cdot_R t)$ (associativity of $\cdot_R$).
   (c) For all $r, s \in R$, $r \cdot_R s = s \cdot_R r$ (commutativity of $\cdot_R$).
3. Multiplication distributes over addition.
   (a) For all $r, s, t \in R$, $r \cdot_R (s +_R t) = r \cdot_R s +_R r \cdot_R t$ and $(s +_R t) \cdot_R r = s \cdot_R r +_R t \cdot_R r$ (distributivity of $\cdot$ over $+$).

There is some redundancy here, of course. I have written things this way so that one obtains the definition of a noncommutative ring simply by removing the condition that multiplication is commutative. In this course, however, all rings will be commutative.

Proposition 1.1.2. Let R be a ring. Then for all $r \in R$, $r \cdot_R 0_R = 0_R$.

Proof. $r \cdot_R 0_R = r \cdot_R (0_R +_R 0_R) = r \cdot_R 0_R +_R r \cdot_R 0_R$. Thus $0_R = -(r \cdot_R 0_R) +_R (r \cdot_R 0_R) = -(r \cdot_R 0_R) +_R (r \cdot_R 0_R +_R r \cdot_R 0_R) = r \cdot_R 0_R$. $\square$

Some people require $0_R \neq 1_R$ in R.

Proposition 1.1.3. If $0_R = 1_R$, then $R = \{0_R\}$.

Proof. $0_R = r \cdot_R 0_R = r \cdot_R 1_R = r$. $\square$

When it is clear from the context what ring we are working with, we will write 0_R and 1_R as 0 and 1, $a +_R b$ as $a + b$ and $a \cdot_R b$ as ab.

Definition 1.1.4. A ring R is a **field** if $R \neq \{0_R\}$ and every nonzero element of R has a multiplicative inverse, that is for every $r \in R \setminus \{0_R\}$ there exists $r^{-1} \in R$ such that $rr^{-1} = r^{-1}r = 1_R$.

We do not consider the zero ring $\{0_R\}$ to be a field. We have seen many examples of rings at this point. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all rings with their usual notion of addition and multiplication. All of them but $\mathbb{Z}$ are in fact fields. As another example, we have the ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n. Let $n \in \mathbb{Z}_{>0}$, and recall that a and b are said to be congruent modulo n if $a - b$ is divisible by n. It is easy to check that this is an equivalence relation on $\mathbb{Z}$. Moreover, since any $a \in \mathbb{Z}$ can uniquely be written as $qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$, the set $\{[0]_n, \dots, [n-1]_n\}$ is a complete list of the equivalence classes under this relation, where $[a]_n$ denotes the set of all integers congruent to $a \mod n$. We denote this n-element set by $\mathbb{Z}/n\mathbb{Z}$, and we can define addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ by setting $[a]_n + [b]_n = [a + b]_n$ and $[a]_n [b]_n = [ab]_n$. This defines a ring structure on $\mathbb{Z}/n\mathbb{Z}$ once one checks that it is well-defined. This is the first example of a general construction of the quotient of a ring by an ideal we will define later.

Lecture 2
Monday
08/10/18

1.2 Polynomial rings

A very important class of rings that we will study are the polynomial rings. Let R be any ring. Then we can form a new ring $R[X]$, called the **ring of polynomials in X with coefficients in R**. Informally, a polynomial in $R[X]$ is a finite sum of the form $r_0 + \dots + r_n X^n$ for some $n \in \mathbb{Z}_{\geq 0}$ and $r_i \in R$. If $n > m$, we consider $r_0 + \dots + r_n X^n$ to represent the same polynomial of $R[X]$ as $s_0 + \dots + s_m X^m$ if $r_i = s_i$ for $i \leq m$ and $r_i = 0_R$ for $i > m$. That is, you can pad out a polynomial with terms of the form $0_R X^i$ without changing it. From a formal standpoint, it is better to define a polynomial to be an infinite sum $\sum_{n=0}^{\infty} r_i X^i$ for $r_i \in R$ in which all but finitely many r_i are zero. This makes it easier to define addition and multiplication. The **degree** of such an expression is the largest i such that r_i is nonzero. We add and multiply in $R[X]$ just as we would any other polynomials, by

$$\left(\sum_{i=0}^{\infty} r_i X^i\right) +_{R[X]} \left(\sum_{i=0}^{\infty} s_i X^i\right) = \sum_{i=0}^{\infty} (r_i +_R s_i) X^i,$$

$$\left(\sum_{i=0}^{\infty} r_i X^i\right) \cdot_{R[X]} \left(\sum_{i=0}^{\infty} s_i X^i\right) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} (r_j \cdot_R s_{i-j})\right) X^i.$$

What about polynomial rings in more than one variable? Since the construction of polynomial rings takes an arbitrary ring as input, one can iterate it. Start with a ring R, and consider first the ring $R[X]$ and then the ring $(R[X])[Y]$. An polynomial of this has the form $\sum_{i=0}^{\infty} \left(\sum_{j=0}^{\infty} r_{ij} X^j\right) Y^i$ for $r_{ij} \in R$. On the other hand, we can consider the ring $(R[Y])[X]$, whose polynomials have the form $\sum_{i=0}^{\infty} \left(\sum_{j=0}^{\infty} s_{ij} Y^j\right) X^i$ for $s_{ij} \in R$. Alternatively, we could consider the ring $R[X, Y]$ whose polynomials are formal expressions of the form $\sum_{i=0}^{\infty} \left(\sum_{i=0}^{\infty} r_{ij} X^i\right) Y^j$ with only finitely many nonzero coefficients r_{ij} and define addition and multiplication in the usual way. It is not hard to see that all three approaches yield the same ring. There is a bijection between these expressions. We will therefore primarily use notation like $R[X, Y]$ for polynomial rings in multiple variables, but we will occasionally need to know that this is the same as $(R[X])[Y]$ or $(R[Y])[X]$. The identification we have made here is an example of an isomorphism of rings, a notion we will make precise later.

1.3 Subrings and extensions

Definition 1.3.1. Let R be a ring. A subset S of R is a **subring** of R if

1. $0_R, 1_R, -1_R \in S$.
2. S is closed under $+_R$ and $\cdot_R$, so if $r, s \in S$, then so are $r +_R s$ and $r \cdot_R s$.

Subrings inherit the additive and multiplicative structures from the ring that contains them, and are thus themselves rings.

Example. $\mathbb{Z}$ is a subring of $\mathbb{R}$, which is itself a subring of $\mathbb{C}$.

It is easy to see that the intersection of two subrings of R, or even an arbitrary collection of subrings of R, is also a subring of R.

Definition 1.3.2. Let $S \subseteq R$ be a subring of a ring R, and let α be an element of R. We can then form a subring $S[\alpha]$ of R, called the **subring of R generated by α over** S, consisting of all elements of R that can be expressed as $r_0 + \cdots + r_n\alpha^n$ for some $n \in \mathbb{Z}^*$, and $r_i \in S$.

This operation is known as **adjoining** the element α to the ring S. An alternative way of defining the ring $S[\alpha]$ is to note that it is the smallest subring of R containing S and α. In one direction, any such subring contains every expression of the form $r_0 + \cdots + r_n\alpha^n$, with $r_i \in S$, so any subring of R containing S and α contains $S[\alpha]$. One can thus construct $S[\alpha]$ as the intersection of every subring of R containing S and α. Since the intersection of any collection of subrings of R is a subring of R it is clear that this intersection is equal to $S[\alpha]$ as defined above.

Example. Let i denote a square root of -1 in $\mathbb{C}$. $\mathbb{Z} \subseteq \mathbb{C}$ and i form $\mathbb{Z}[i]$. Note $-1 = i^2 = i^6 = i + i^3 + i^{10}$.

Proposition 1.3.3. Every element of $\mathbb{Z}[i]$ can be uniquely expressed as $a + bi$ for $a, b \in \mathbb{Z}$.

Example. Given $\sum_{n=0}^{\infty} a_n i^n$ with only finitely many a_n nonzero, set $a = a_0 - a_2 + \dots$ and $b = a_1 - a_3 + \dots$. Then $\sum_{n=0}^{\infty} a_n i^n = a + bi$. For uniqueness, if $a + bi = c + di$ in $\mathbb{C}$ for $a, b, c, d \in \mathbb{Z}$, then $a = c$ or $b = d$.

If α is more complicated then the elements of $R[\alpha]$ may well be harder to describe.

Example. If α is the real cube root of 2, then every element of $\mathbb{Z}[\alpha]$ can be uniquely expressed as $a + b\alpha + c\alpha^2$ for $a, b, c \in \mathbb{Z}$.

Example. In $\mathbb{Z}[\pi]$, any element has a unique expression in the form $\sum_{n=0}^{\infty} a_n\pi^n$ for all but finitely many a_n are zero. Suppose $\sum_{n=0}^{\infty} a_n\pi^n = \sum_{n=0}^{\infty} b_n\pi^n$, then $0 = \sum_{n=0}^{\infty} (a_n - b_n)\pi^n$. Since π is transcendental, this polynomial must be zero. Thus each $a_n = b_n$.

Example. The elements of $\mathbb{Z}\left[\frac{1}{2}\right]$ can be expressed uniquely as a/b, where b is a power of 2 and a is odd unless $b = 1$.

Example. Let α be a root of $x^2 - \frac{1}{2}x + 1$. Then $\alpha^2 \in \mathbb{Z}[\alpha]$ and $\alpha^2 = \alpha/2 - 1$. Can show that every element of $\mathbb{Z}[\alpha]$ can be expressed as $a + b\alpha$ for $a, b \in \mathbb{Z}\left[\frac{1}{2}\right]$, but not every $a + b\alpha$ arises $a, b \in \mathbb{Z}\left[\frac{1}{2}\right]$.

Lecture 3 Wednesday 10/10/18

1.4 Integral domains and rings of fractions

Definition 1.4.1. A **zero divisor** in a ring R is a nonzero element r of R such that there exists a nonzero $s \in R$ with $rs = 0$. A ring R in which there are no zero divisors is called an **integral domain**.

Example. $\mathbb{Z}$ is an integral domain and any subring of a field is an integral domain, but $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain, as $[2][3]$ is zero modulo 6 even though neither $[2]$ nor $[3]$ is zero modulo 6.

If R is an integral domain, then we can form the field of fractions of R in analogy to the way we build $\mathbb{Q}$ from $\mathbb{Z}$.

Definition 1.4.2. Let R be an integral domain. The **field of fractions** $K(R)$ is the set of equivalence classes of expressions of the form a/b for $a, b \in R$, $b \neq 0$, where $a/b \sim a'/b'$ iff $ab' = a'b$. We add and multiply elements of $K(R)$ just as we do for fractions, by

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \qquad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}, \qquad 0_{K(R)} = \frac{0_R}{1_R}, \qquad 1_{K(R)} = \frac{1_R}{1_R}.$$

If $a \neq 0$ in R, then $b/a \in K(R)$, so $(a/b) \cdot (b/a) = ab/ba \sim 1/1$.

Then $K(R)$ is a field, and it contains R in a natural way as a subring if we identify r with $r/1_R \in K(R)$. The field $K(R)$ is in some sense the smallest field containing R as a subring. When we talk about homomorphisms and isomorphisms, we will be able to state this more precisely. More generally, a subset S of R is a **multiplicative system** if $1 \in S$ and $0 \notin S$, and S is closed under multiplication, that is if a, b are in S then so is ab. For any integral domain R and any multiplicative system S, we can define $S^{-1}R \subseteq K(R)$ consisting of all fractions of the form a/b with $b \in S$. It is easy to see that his is closed under addition and multiplication, and defines a ring in between R and $K(R)$.

Example. If $R = \mathbb{Z}$ and S is the set of powers of 2, then $S^{-1}R = \mathbb{Z}\left[\frac{1}{2}\right]$. On the other hand, if S is the set of odd integers, then $S^{-1}R$ is the set of all rational numbers of the form a/b with b odd.

In general $S^{-1}R$ is the smallest subring of $K(R)$ containing R in which every element of S has a multiplicative inverse, that is $b^{-1} \in S$ for all $b \in S$. The process of obtaining $S^{-1}R$ from R is called **localisation** and is an extremely powerful tool. One can even make sense of it when R is not an integral domain, but one has to be more careful. The equivalence relation on fractions is tricker, for example. We will not discuss this in this course but it will be quite useful in future courses.

2 Homomorphisms, ideals, and quotients

2.1 Homomorphisms

Let R and S be rings. A ring homomorphism from R to S is, roughly, a way of interpreting elements of R as elements of S, in a way that is compatible with the addition and multiplication laws on R and S. More precisely is the following.

Definition 2.1.1. A function $f : R \to S$ is a **ring homomorphism** if

1. $f(1_R) = 1_S$,
2. for all $r, r' \in R$, $f(r +_R r') = f(r) +_S f(r')$, and
3. for all $r, r' \in R$, $f(r \cdot_R r') = f(r) \cdot_S f(r')$.

Note. If f is a homomorphism then $f(0_R) = f(0_R + 0_R) = f(0_R) +_S f(0_R)$ gives $f(0_R) = 0_S$. Thus we do not need to require this as an axiom. On the other hand we do need to require $f(1_R) = 1_S$. For certain R, S one can construct examples of maps $f : R \to S$ that satisfy properties 2 and 3 of the definition without satisfying property 1.

Example. If R is a subring of S, then the inclusion of R into S, such as $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, is a homomorphism. This is just a fancy way of saying that the addition and multiplication on R are induced from the corresponding operations on S.

Example. The composition of two homomorphisms is a homomorphism, as is easily checked from the definitions.

Example. The map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ that takes an integer m into its congruence class modulo n is also a homomorphism. In fact, this is a special case of the following construction.

Proposition 2.1.2. Let R be any ring. Then there is a unique ring homomorphism $f : \mathbb{Z} \to R$ such that

$$f(n) = \begin{cases} 1_R + \cdots + 1_R & n > 0 \\ -(1_R + \cdots + 1_R) & n < 0 \\ 0_R & n = 0 \end{cases}.$$

Proof. Let $f : \mathbb{Z} \to R$ be a homomorphism. Then, directly from the definition, we have $f(0) = 0_R$ and $f(1) = 1_R$. In particular for all $n > 0$, $f(n) = f(1 + \cdots + 1) = 1_R +_R \cdots +_R 1_R$, where there are n copies of 1_R in the sum. Moreover, $0_R = f(n + (-n)) = f(n) + f(-n)$, so $f(-n) = -(1_R +_R \cdots +_R 1_R)$. Thus $f(n)$ is determined, for all n, completely by the fact that f is a homomorphism. In the converse direction, it is not hard to check that the map defined above is in fact a homomorphism. □

Thus, for any ring R, we can regard an integer as an element of R via this homomorphism.

Definition 2.1.3. A bijective homomorphism $f : R \to S$ is called an **isomorphism**. Write $S \cong R$ for S is isomorphic to R.

In this case one verifies easily that the inverse map $f^{-1} : S \to R$ is also a bijective homomorphism.

2.2 Evaluation homomorphisms

Let R be a ring, and consider the ring $R[X]$ of polynomials in X with coefficients in R. If s is an element of R, then we can define a homomorphism $R[X] \to R$ by **evaluation at** s. More precisely, given an element of $R[X]$ of the form $P(X) = r_0 + \cdots + r_n X^n$ for some n and $r_i \in R$. Then $P(s)$ for $s \in R$ is defined to be $P(s) = r_0 + \cdots + r_n s^n \in R$. Consider the map $\phi_s : R[X] \to R$ that sends $\phi_s(P)$ to $P(s)$. In effect, it substitutes s for X. It is easy to check that this is in fact a ring homomorphism. More generally, if R and S are rings and $f : R \to S$ is a homomorphism, and s is an element of S, then we can define a map

$$\phi_{s,f} : R[X] \to S,$$

by setting

$$\phi_{s,f}(r_0 + \cdots + r_n X^n) = f(r_0) + \cdots + f(r_n) s^n.$$

That is, by appling f to the coefficients and substituting s for X. Again, this is clearly a homomorphism. The evaluation homomorphisms $\phi_{s,f}$ are a fundamental property of polynomial rings. In some sense, they are the reason polynomial rings are worth studying. In fact, the ring $R[X]$ is uniquely characterised by the fact that homomorphisms from $R[X]$ to S are in bijection with pairs (s, f), where $f : R \to S$ is a homomorphism and s is an element of S.

2.3 Images, kernels, and ideals

Definition 2.3.1. Let $f : R \to S$ be a homomorphism. The **image** of f is $Im(f) = \{f(r) \mid r \in R\} \subseteq S$. The **kernel** of f is $Ker(f) = \{r \in R \mid f(r) = 0\} \subseteq R$.

The image of a homomorphism $f : R \to S$ is easily seen to be a subring of S.

Example. If R is a subring of S, $f : R \to S$ is the inclusion and s lies in S, then the image of the map $\phi_{s,f} : R[X] \to S$ is precisely the subring $R[s]$ of S.

By contrast, the kernel of a homomorphism f is almost never a subring of R. For instance, subrings contain the identity. However, it is an ideal of R.

Lecture 4 Friday 12/10/18

Definition 2.3.2. A nonempty subset I of R is an **ideal** of R if I is closed under addition, that is for all $i, j \in I$, $i + j \in I$, and for all $i \in I$, $r \in R$, $ri \in I$.

Then one can verify, directly from the definition, that the kernel of any homomorphism $f : R \to S$ is an ideal of R.

Note. Any ideal of R contains 0_R, and conversely the subset $\{0_R\}$ of R is an ideal, called the **zero ideal**. A homomorphism $f : R \to S$ is injective iff its kernel is the zero ideal. Forward direction is easy. Conversely, if $f(x) = f(y)$, $f(x - y) = 0$, so $x - y \in Ker(f)$. If $Ker(f) = \{0\}$, $x = y$.

The kernel of the homomorphism $\mathbb{Z} \to R$ is either the zero ideal, or the ideal of multiples of n in $\mathbb{Z}$ for some positive n. We say that R has characteristic zero or characteristic n, respectively. If not zero, the **characteristic** of R is the smallest n such that the sum of n copies of 1_R is equal to zero.

2.4 Ideals: examples and basic operations

If r is an element of R, then any ideal containing R contains any multiple sr of R, for any r in S. Conversely, one checks easily that the set $\{sr \mid s \in R\}$ is an ideal of R. It is known as the **ideal of R generated by r**, and denoted $\langle r \rangle$. An ideal generated by one element in this way is called a **principal ideal**.

Note. The ideal generated by 1_R, or more generally by any element of R with a multiplicative inverse, is all of R. This ideal is called the **unit ideal** of R.

Proposition 2.4.1. R is a **field** iff the only ideals of R are the zero ideal $\{0\}$ and the unit ideal R.

Proof. If R is a field, let $I \subseteq R$ be a nonzero ideal. There exists $r \in I \neq 0$. Then for all $s \in R$, $\left(sr^{-1}\right)(r) \in I$, so $s \in I$ for all $s \in R$. Conversely, if R has only zero ideal, unit ideal, let $r \in R \neq 0$, let $I \{sr \mid s \in R\}$. This is an ideal not zero ideal, so it is all of R. In particular, $1 \in I$, so there exists $s \in R$ such that $sr = 1$. $\square$

More generally is the following.

Definition 2.4.2. If S is a subset of elements of R, then any ideal containing S consists of all elements of R the form $r_0 s_0 + \cdots + r_n s_n$ for some $n \in \mathbb{Z}_{\geq 0}$, $r_i \in R$, and $s_i \in S$. The intersection of all these ideals is an ideal of R, known as the **ideal of R generated by S**, and denoted $\langle S \rangle$. It is also the smallest ideal of R containing S.

If S has one element, $\langle S \rangle$ is a principal ideal. We will show soon that any ideal of $\mathbb{Z}$ is a principal ideal, as is any ideal of the ring $k[X]$ for any field k. On the other hand, there are rings in which not every ideal is principal.

Example. The ideal $\langle X, Y \rangle$ of $k[X, Y]$ is not a principal ideal.

Given ideals I and J there are several ways to create new ideals.

1. If I, J are ideals, then the intersection $I \cap J$ is an ideal. If I and J are given by generators, it might be hard to find generators for the intersection. Certainly it is not enough to intersect the generating sets.
2. The union of ideals is not usually an ideal. Taking $R = \mathbb{Z}$, $\langle 3 \rangle \cup \langle 5 \rangle$ contains $3, 5$ but not $3 + 5$.
3. If I, J are ideals, then the sum $I + J$ is an ideal, which are all expressions of the form $i + j$ for $i \in I$, $j \in J$. It is the smallest ideal containing both I and J, and also the ideal generated by $I \cup J$.
4. If I, J are ideals, the product $I \cdot J$ or IJ is the ideal generated by elements of the form ij for $i \in I$, $j \in J$. This may be strictly larger than the set of such products.

Example. Consider the product of the ideals $I = \langle X, Y \rangle$ and $J = \langle Z, W \rangle$ in $R = k[X, Y, Z, W]$ for k a field. The product $IJ = \langle XZ, XW, YZ, YW \rangle$ contains $XZ + YW$, but the latter is not a product of an element in I with an element in J.

Note. Let I, J be general ideals. The product of I and J is always contained in the intersection of I and J, but the two need not be equal, even in simple rings like $\mathbb{Z}$. $\langle 3 \rangle \cdot \langle 3 \rangle = \langle 9 \rangle \subseteq \mathbb{Z}$ and $\langle 3 \rangle \cap \langle 3 \rangle = \langle 3 \rangle$.

2.5 Quotients

Let R be a ring and let I be an ideal of R. If x, y are elements of R, we say that x is **congruent to** y **modulo** I if $x-y$ is in I. This is an equivalence relation on R. We denote the equivalence class of r by $r+I$, or the alternative notations $[r]_I$, $\overline{r}$. It is the set $\{r+s \mid s \in I\}$. Let R/I denote the set of equivalence classes on R modulo I. This set has the natural structure of a ring. The additive and multiplicative identities are 0_R+I and 1_R+I, respectively, and addition and multiplication are defined by $(r+I)+(s+I) = (r+s)+I$ and $(r+I)\cdot(s+I) = (rs+I)$ respectively. One has to check that these are well-defined, but this is not difficult. The ring R/I is called the **quotient of** R **by the ideal** I.

Example. If $R = \mathbb{Z}$ and I is the ideal generated by n, then R/I is the ring $\mathbb{Z}/n\mathbb{Z}$ that we have already seen.

Note. There is a **reduction modulo** I or **natural quotient** homomorphism $R \to R/I$ defined by taking r to $r+I$. This homomorphism is surjective with kernel I.

We then have the following.

Proposition 2.5.1 (Universal property of the quotient)**.** Let $I \subseteq R$ be an ideal and let $f : R \to S$ be a homomorphism, and suppose that the kernel of f contains I. Then there is a unique homomorphism $\overline{f} : R/I \to S$ such that for all $r \in R$, $\overline{f}(r+I) = f(r)$.

Proof. $\overline{f}$ is necessarily unique, as every element of R/I has the form $r+I$ for some r. It thus suffices to show that it is well-defined and gives a homomorphism. If $r+I = r'+I$, then $r-r' \in I$, so $f(r-r') = 0$ gives $f(r) = f(r')$. Thus $\overline{f}$ is well-defined. Checking that it is a homomorphism follows from f is a homomorphism. ☐

Note. The kernel of $\overline{f}$ in the above proposition is just the image of the kernel of f in R/I. If the kernel of f is equal to I, this image is the zero ideal and $\overline{f}$ is injective. In particular, any homomorphism of R to S can be thought of as an isomorphism of some quotient of R with a subring of S.

Example. Let $R \subseteq S$ be a subring, $\alpha \in S$, and $\iota : R \to S$ be the inclusion map. Recall that we have an evaluation at α by $\phi_{\iota,\alpha} : R[X] \to S$. Image of this is $R[\alpha]$. Let $I = Ker(\phi_{\iota,\alpha})$. Then $\phi_{\iota,\alpha}$ descends to a map $\phi_{\iota,\alpha} : R[\alpha]/I \to S$ that is injective with image $R[\alpha]$. So $R[\alpha]$ is isomorphic to a quotient of $R[X]$.

Lecture 5
Monday
15/10/18

2.6 Prime and maximal ideals

Definition 2.6.1. An ideal I of R is **prime** if the quotient R/I is an integral domain. It is **maximal** if R/I is a field.

Note. As fields are integral domains, every maximal ideal is prime. The converse need not hold, of course. The zero ideal in $\mathbb{Z}$ is prime but not maximal.

Proposition 2.6.2. An ideal I is prime iff for every pair of elements s, r in R such that rs is in I, either r is in I or s is in I.

Proof. This is just a restatement of the definition. R/I integral domain iff for all whenever two elements $r+I$ and $s+I$ in R/I satisfy $(r+I)(s+I) = 0+I$ in R/I, either $r+I = 0+I$ or $s+I = 0+I$ in R/I. This is the same as saying rs lies in I iff either r or s lies in I. ☐

Proposition 2.6.3. An ideal I is maximal iff the only ideals of R containing I are I and the unit ideal R.

This justifies the name maximal for such ideals.

Proof. First suppose that R/I is a field. Recall that R/I is a field iff only ideals of R/I are $\{0\}$ and R/I. Given an ideal $J \subseteq R/I$, let $\tilde{J}$ be the preimage of J under $R \to R/I$. $\tilde{J}$ is an ideal containing I and contained in R. Then J is either the zero ideal of R/I, in which case $\tilde{J}$ is contained in, and thus equal to, I, or J is all of R/I, in which case $\tilde{J}$ contains I and an element of 1_R+I, so $\tilde{J}$ contains 1_R and is thus the unit ideal of R. Conversely, if the only ideals of R containing I are I and the unit ideal, then for any r in $R \setminus I$, the ideal of R generated by I and r contains 1_R. We can thus write $1_R = rs+i$, where $i \in I$ and $s \in R$. This means that $s+I$ and $r+I$ are multiplicative inverses of each other in R/I, so R/I is a field. ☐

3 Factorisation

In these notes R always denotes an integral domain.

3.1 Divisibility, units, associates, and irreducibles

Definition 3.1.1. Let r, s be elements of R. We say r **divides** s, written $r \mid s$, if there exists $r' \in R$ with $rr' = s$, or, equivalently, s lies in the principal ideal $\langle r \rangle$ generated by r. An element r that divides 1_R is called a **unit** of R, or, equivalently, $\langle r \rangle = R$.

The set of units in R forms a group under multiplication denoted R^*. For any element $r \in R$ and any unit u of R, both u and ur divide r.

Definition 3.1.2. The set of elements of R of the form ur, with $r \in R^*$ are called **associates** of R, that is r, r' are associates if $r = ur'$ for a unit $u \in R^*$.

This implies $r \mid r'$, that is there exists u' with $u'u = 1$ and $u'r = r'$.

Note. The principal ideals $\langle r \rangle$ and $\langle r' \rangle$ are equal iff r and r' are associates.

Definition 3.1.3. A nonzero element r of R is called **irreducible** if r is not a unit and the only elements of R that divide r are the units and the associates of r.

3.2 Unique factorisation domains

An interesting question is when elements of rings admit unique factorisations into irreducibles. To that end we define the following.

Definition 3.2.1. A **unique factorisation domain** (UFD) is a ring R in which

1. every nonunit, nonzero element $r \in R$ admits a factorisation as a finite product of irreducibles in R, and
2. if $r = p_1 \dots p_n = q_1 \dots q_m \in R$ are two factorisations of r as products of irreducibles p_i, q_i, then $n = m$ and, up to permuting the q_i, each q_i is an associate of p_i.

Example. Both conditions can fail.

1. There are certainly domains in which 1 can fail, although they are somewhat exotic. One example is to take the rational polynomial ring $R = \mathbb{C}\left[X^{\mathbb{Q}}\right]$ with coefficients in $\mathbb{C}$, whose entries are finite formal sums $\sum_{i=0}^{N} a_i X^{n_i}$ where the a_i are in $\mathbb{C}$ and the n_i are nonnegative rational numbers $\mathbb{Q}_{\geq 0}$. Any element of R is a polynomial in $X^{1/n}$ for some n. The element X of this ring is not a unit, and also not a finite product of irreducibles. In $\mathbb{C}\left[X^{1/n}\right]$, X factors as $\left(X^{1/n}\right)^n$. X has no factorisation into irreducibles in R. We will show later that a very mild finiteness condition on a domain R, the condition that R is Noetherian, actually guarantees that 1 holds.
2. Even if 1 holds, 2 often fails. The classic example of this is $R = \mathbb{Z}\left[\sqrt{-5}\right]$, in which $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are all irreducibles, none are associates of each other, yet $(2)(3) = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$.

Another way to interpret condition 2 is as follows.

Definition 3.2.2. We say an element r of R is **prime** if the principal ideal $\langle r \rangle$ of R is a prime ideal. In other words, for any s, s' in R, if r divides ss', then $r \mid s$ or $r \mid s'$.

Lemma 3.2.3. Prime elements are irreducible.

Proof. If r is prime and s divides r, we can write $r = ss'$. Then since r divides ss' we have that either r divides s, in which case $rs'' = s$, then $ss's'' = s$ and $s's'' = 1$, so r is an associate of s, or r divides s', in which case $s' = rs''$, then $r = srs''$ and $ss'' = 1$, so r is an associate of s' and s is a unit. $\square$

The converse is not necessarily true, but we have the following observation as a criteria for R to be a UFD.

Proposition 3.2.4. Let R be a domain in which condition 1 holds. Then condition 2 above holds for R iff every irreducible element of R is prime.

Proof. First suppose condition 2 holds, and let r be an irreducible element of R. If r divides ab, we can write $rs = ab$ for some $s \in R$. Expanding out s, a, b as products of irreducibles we see that r is an associate of some irreducible dividing a or b, so r is prime. Conversely, if every irreducible element of R is prime, and we have $p_1 \dots p_n = q_1 \dots q_m$ products of irreducibles, then, since p_1 is prime, it divides the product $q_1 \dots q_m$ and is thus an associate of some q_i. We can thus cancel p_1 from the left and q_i from the right after introducing a unit on one side. This is possible because R is an integral domain. Repeating the process we find that, up to reordering the terms and multiplying by units, the two expressions coincide. $\square$

3.3 Principal ideal domains

Definition 3.3.1. An integral domain R is a **principal ideal domain** (PID) if every ideal of R is a principal ideal.

Theorem 3.3.2. Every PID is a UFD.

We first show 1. It is true for units trivially.

Lemma 3.3.3. Let R be a PID. Then every nonzero nonunit $r \in R$ has a irreducible divisor.

Proof. Fix $r = r_0 \in R$. We first show r has an irreducible factor. If r_0 is irreducible we are done. Otherwise r_0 is not irreducible, we can choose an r_1, not a unit nor an associate of r_0, such that r_1 divides r_0, so $r_0 = r_1 s_1$ with r_1, s_1 not units. If r_1 is not irreducible we choose r_2 similarly, and repeat. If this process ever terminates we have found an irreducible divisor of r. Suffices to show this terminates. Suppose it does not terminate. We obtain an increasing tower of ideals

$$\langle r_0 \rangle \subsetneq \langle r_1 \rangle \subsetneq \dots.$$

Let I be the union of all these ideals generated by $r_0, r_1, \dots$. Then I is an ideal, so it is generated by some element $s \in I$. Thus s divides r_i for all i. On the other hand, s lives in some $\langle r_j \rangle$, so r_j divides s. Thus s is an associate of r_j, and therefore an associate of r_i for all $i > j$, that is $I \subseteq \langle r_j \rangle$. This contradicts our construction because $\langle r_{j+1} \rangle \subseteq I$ and $\langle r_{j+1} \rangle \neq \langle r_j \rangle$. $\square$

Thus r has an irreducible divisor s_0.

Lemma 3.3.4. Let R be a PID. Every nonzero nonunit $r \in R$ is a finite product of irreducibles.

Proof. Consider rs_0^{-1}. If this is a unit we are done. If not let s_1 be an irreducible divisor of rs_0^{-1}. If $r\left(s_0 s_1\right)^{-1}$ is a unit we are done, otherwise repeat. We obtain a sequence of irreducibles $s_0, s_1, \dots$ such that $s_0 \dots s_i$ divides r for all i, so $r = r_0 s_0 = r_0 r_1 s_1 = \dots$ with $r_0, r_1, \dots$ irreducible. If this process ever terminates we are done. Suppose it does not. Then we have a strictly increasing tower of ideals

$$\langle r \rangle \subsetneq \langle s_0 \rangle \subsetneq \langle s_1 \rangle \subsetneq \dots.$$

This cannot continue forever. Arguing as above we arrive at a contradiction. $\square$

Now we show 2.

Proof of Theorem 3.3.2. It suffices to show that in a PID every irreducible is prime. Let $r \in R$ be irreducible, and suppose that r divides st. Want $r \mid s$ or $r \mid t$. Let q be a generator of the ideal $\langle r, s \rangle$ of R, so $\langle r, s \rangle = \langle q \rangle$. Then q divides r, so either q is a unit or q is an associate of r. If q is an associate of r, then since q divides s, r divides s. on the other hand, if q is a unit, then the ideal generated by r and s is the unit ideal and $1 \in \langle r, s \rangle$, so we can write $1 = xr + ys$ for x, y elements of R. We then have $t = xrt + yst$, and since r divides both yst and xrt, r divides t. $\square$

Lecture 6
Wednesday
16/10/18

3.4 Euclidean domains

One technique for proving that rings are PIDs is Euclid's algorithm. We formalize this in an abstract setting as follows.

Definition 3.4.1. Let R be an integral domain.

1. A **Euclidean norm** on R is a function $N : R \to \mathbb{Z}_{\geq 0}$ such that for all $a, b \in R$, with $b \neq 0$, there exists $q, r \in R$ such that $a = qb + r$, and either $r = 0$ or $N(r) < N(b)$.
2. An integral domain R is called a **Euclidean domain** if there is a Euclidean norm on R.

Theorem 3.4.2. Any Euclidean domain is a PID.

Proof. Let R be a Euclidean domain, N be a Euclidean norm on R, and $I \subseteq R$ a nonzero ideal of R. Let $a \in I$ be a nonzero element such that $N(a)$ is minimal, that is if $b \in I$, $b \neq 0$, then $N(b) \geq N(a)$. Claim that $I = \langle a \rangle$. Let $b \in I$. Then there exists q, r such that $b = aq + r$, with either $r = 0$ or $N(r) \geq N(a)$. So $r = 0$ gives $b = aq$. Thus $I = \langle a \rangle$. $\square$

Proof. Let R be a Euclidean domain, N be a Euclidean norm on R, and $I \subseteq R$ be a nonzero ideal of R. Let n be the smallest integer such that there exists a nonzero element $a \in I$ with $N(a) = n$ minimal, that is if $b \in I$ and $b \neq 0$, then $N(b) < N(a)$. Claim that $I = \langle a \rangle$. Then for any $b \in I$, we can write $b = qa + r$ with $N(r) < N(a)$ unless $r = 0$. But since $N(a)$ is the smallest possible norm in I, we must have $r = 0$, so $b = qa$. Thus I is generated by a and we are done. $\square$

3.5 Examples

Example.

1. The classic example of a Euclidean domain is $\mathbb{Z}$, with $N(x) = |x|$ for $x \in Z$.
2. The ring $\mathbb{Z}[i]$ is a Euclidean domain, with $N(z) = z\overline{z} = |z|^2$, so $N(x + yi) = |x + yi|^2 = x^2 + y^2$. To see this, note that given a and b in $\mathbb{Z}[i]$ for $b \neq 0$, set $q' = a/b \in \mathbb{Q}[i]$. Write $q' = x' + iy'$ with $x', y' \in \mathbb{Q}$. Let x and y be the closest integers to x' and y', such that $|x - x'|, |y - y'| \leq 1/2$, and set $q = x + iy$ in $\mathbb{Z}[i]$ and $r = a - bq$. Then
$$N(r) = |r|^2 = |a - bq|^2 = \left|a - b\left(\frac{a}{b} + (q - q')\right)\right|^2 = |b(q - q')|^2 = |b|^2 |q - q'|^2 \leq \frac{N(b)}{2}.$$
Similar arguments can be used to prove that $\mathbb{Z}[\alpha]$ is a Euclidean domain for
$$\alpha = \sqrt{-2}, \qquad \alpha = \frac{-1 + \sqrt{-3}}{2}, \qquad \alpha = \frac{-1 + \sqrt{-7}}{2}.$$
Beyond this one needs other tricks and for most α unique factorization fails.
3. A critical example is the polynomial ring $K[X]$ for K a field. Here we can take $N(P(X))$ to be the degree of $P(X)$. Then, given polynomials $P(X), T(X) \in K[X]$ and $T(X) \neq 0$, we can use polynomial long division to write $P(X) = Q(X) T(X) + R(X)$ for some $Q(X)$ with the degree of R strictly less than that of T, unless T is constant, in which case we can make $R = 0$. To prove this, fix $T(X)$. If $\deg(T(X)) = 0$, $T(X)$ is constant, so $T(X) = c \neq 0 \in K$. Take $Q(X) = c^{-1} P(X)$, so $R(X) = 0$. Otherwise induct on $\deg(P(X))$. If $\deg(P(X)) < \deg(T(X))$, set $R(X) = P(X)$ and $Q(X) = 0$. Suppose the claim is true for polynomials of degree n and $P(X)$ has degree $n + 1$, so
$$P(X) = \sum_{i=0}^{n+1} a_i X^i, \qquad T(X) = \sum_{i=0}^{d} b_i X^i,$$
for $d < n + 1$. Then $S(X) = P(X) - (a_{n+1}/b_d) X^{n+1-d} T(X)$ has degree n. By inductive hypothesis there exists $Q(X)$, $R(X)$ with $\deg(R(X)) < \deg(T(X))$ such that
$$S(X) = Q(X) T(X) + R(X) \qquad \implies \qquad P(X) = \left(\frac{a_{n+1}}{b_d} X^{n+1-d} + Q(X)\right) T(X) + R(X).$$

Later, will show if R UFD, then $R[X]$ is also a UFD.

4 The Chinese remainder theorem

In elementary number theory, let $m_1, m_2 \in \mathbb{Z}$ be relatively prime and $a_1, a_2 \in \mathbb{Z}$. Then there exists $a \in \mathbb{Z}$ such that

$$a \equiv a_1 \mod m_1, \qquad a \equiv a_2 \mod m_2.$$

Moreover, a is unique up to congruence modulo $m_1 m_2$. Question is given ideals $I_1, \dots, I_r$ and $a_1, \dots, a_r \in \mathbb{R}$, when can we find a $a \in R$ with $a \in a_1 + I_1, \dots a_r + I_r$?

4.1 Products

Definition 4.1.1. Let $R_1, \dots, R_n$ be rings. The **direct product** $R \times \dots \times R_n$ is a ring whose elements are n-tuples $(r_1, \dots, r_n)$ with $r_i \in R_i$ for all i. The addition and multiplication are given componentwise.

$$(r_1, \dots, r_n) + (r_1', \dots, r_n') = (r_1 + r_1', \dots, r_n + r_n'), \qquad (r_1, \dots, r_n)(r_1', \dots, r_n') = (r_1 r_1', \dots, r_n r_n').$$

Note. The product comes with natural homomorphisms for all i, π_i, **projection** onto the i-th factor, defined by

$$\pi_i(r_1, \dots, r_n) = r_i : R_1 \times \dots \times R_n \to R_i,$$

and the following universal property.

Theorem 4.1.2 (Universal property of the product)**.** Let $S, R_1, \dots, R_n$ be any rings. For any homomorphisms $f_1 : S \to R_1, \dots, f_n : S \to R_n$, there exists a unique homomorphism $f : S \to R_1 \times \dots \times R_n$ such that $\pi_i \circ f = f$ for all i.

Proof. Given f_i, the homomorphism f is defined by $f(s) = (f_1(t), \dots, f_n(t))$. Then $(\pi_i \circ f)(s) = f_i(s)$. For uniqueness, if $(\pi \circ g)(s) = f_i(s)$ for all i, then $g(s) = (f_1(s), \dots, f_n(s)) = f(s)$. $\square$

More generally, if I is any index set, and for each $i \in I$ we have a ring R_i, we can define the product $\prod_i R_i$. An element r of this product is a choice, for each $i \in I$, of an element of R_i. We write such an element as $(r_i)_{i \in I}$. For each $j \in I$ we have a map $\pi_j : \prod_i R_i \to R_j$ given by $\pi_j\left((r_i)_{i \in I}\right) = r_j$. Such a product satisfies a very similar universal property. For any collection $f_i : S \to R_i$ of maps for each $i \in I$, we get a unique map $f : S \to \prod_i R_i$ such that $\pi_j \circ f = f_j$.

4.2 The Chinese remainder theorem

Let R be a ring, and let $I_1, \dots, I_r$ be a finite collection of ideals of R. We have the natural maps $R \to R/I_1, \dots, R \to R/I_r$, which are surjective with kernel I_j. Consider the product map

$$R \to \frac{R}{I_1} \times \dots \times \frac{R}{I_r}.$$

It is easy to see that the kernel of this map is the set of $r \in R$ such that r maps to zero in R/I_j for all j. That is, the kernel is the intersection $I_1 \cap \dots \cap I_r$. Call this ideal J. We thus have an injective embedding

$$\frac{R}{J} \hookrightarrow \frac{R}{I_1} \times \dots \times \frac{R}{I_r}.$$

A natural question to ask is, what can we say about the image? In other words, given congruence classes modulo $I_1, \dots, I_r$, when is there a single element of R that lives in all those congruence classes simultaneously?

Note. Because the above map is injective, if one such element exists, then there is a unique congruence class modulo J that satisfies all of the required congruences.

Of course, without further hypotheses we cannot expect this map to be surjective. Think about what happens when $I_1 = I_2$, for instance. Nonetheless, we have the following.

Definition 4.2.1. We will say $I_1, \dots, I_r$ are **pairwise relatively prime** if for each $i \neq j$, the sum $I_i + I_j$ is the unit ideal in R.

(TODO Exercise: if $R = \mathbb{Z}$, then $I_i = \langle n_i \rangle$, and $\{I_i\}$ is pairwise relatively prime iff for all $i \neq j$, n_i and n_j are relatively prime)

Theorem 4.2.2. Let R be a ring and $I_1, \dots, I_r$ be pairwise relatively prime ideals. Then the natural map

$$\frac{R}{J} \hookrightarrow \frac{R}{I_1} \times \dots \times \frac{R}{I_r}$$

is an isomorphism.

Proof. We have to prove it is surjective. Fix any tuple $(c_1, \dots, c_r)$ of elements of R. We need to find $c \in R$ such that $c \in c_i + I_i$ for all i. It suffices to construct, for each i, an element e_i of R such that $e_i \equiv 1 \mod I_i$ and $e_i \equiv 0 \mod I_j$ for $i \neq j$. Suppose we have such an element. Then the element $c = c_1 e_1 + \dots + c_r e_r$ is such that $c \equiv c_j \mod I_j$ for all j. Given i, j with $i \neq j$, we know that $I_i + I_j$ is the unit ideal. That is, we can write $a_{ij} + b_{ij} = 1$ with $a_{ij} \in I_i$ and $b_{ij} \in I_j$. Then $a_{ij} \equiv 1 \mod I_j$ and $a_{ij} \equiv 0 \mod I_i$ as an element of $R/I_1 \times \dots \times R/I_r$, so a_{ij} has zero in the i-th place and one in the j-th place. Then for any j we can take $e_j = \prod_{i \neq j} a_{ij}$ and $e_j \equiv 1 \mod I_j$ and $e_j \equiv 0 \mod I_i$ for all $i \neq j$, so e_j has one only in the j-th place. So $R \to R/I_1 \times \dots \times R/I_r$ is surjective. The result follows. $\square$

4.3 Examples

When $R = \mathbb{Z}$, then every ideal is principal, so we can write $I_j = \langle n_j \rangle$ for all j. The condition that $I_i + I_j$ is the unit ideal becomes the condition that $n_i \in \mathbb{Z}$ are pairwise relatively prime. In this case the ideal J is generated by the product n of the n_i. Specialising, we find the version of the Chinese remainder theorem from elementary number theory.

Theorem 4.3.1. If $\{n_j \in \mathbb{Z}\}$ is a finite collection of pairwise relatively prime integers, and n is their product, then for any $c_1, \dots, c_r \in \mathbb{Z}$, there exists $c \in \mathbb{Z}$ unique up to congruence modulo n such that c is congruent to c_i mod n_i for all i.

Now let K be a field and take $R = K[X]$. If $c_1, \dots, c_r \in K$ are distinct elements of K, the ideals $I_i = \langle X - c_i \rangle \subseteq R$ are such that $I_i + I_j = \langle X - c_i \rangle + \langle X - c_j \rangle$ contains $c_i - c_j \in K^*$, so contains 1. That is, $I_i + I_j$ is the unit ideal in R and the ideals I_i are pairwise relatively prime. Moreover, for each i, I_i is the kernel of the evaluation map $f_i : R \to K$ by that takes $P(X)$ to $P(c_i)$. Let $f : R \to K \times \dots \times K$ by $P(X) \mapsto (P(c_1), \dots, P(c_r))$. Then the following diagram commutes.

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, two heads] & K \times \dots \times K \\
\frac{R}{J} \arrow[r, "\sim"'] & \frac{R}{I_1} \times \dots \times \frac{R}{I_r} \arrow[u, "\sim"']
\end{tikzcd}$$

Chinese remainder theorem gives that f is surjective. We thus have an isomorphism of R/I_i with K that takes $P(X)$ to $P(c_i)$ for all polynomials P. We thus obtain the following.

Theorem 4.3.2. For any $c_1, \dots, c_n \in K$, there is a polynomial $P(X)$ in R, unique up to congruence modulo $(X - a_1) \dots (X - a_n)$ such that $P(a_i) = c_i$ for all i.

Lecture 7
Friday
19/10/18

5 Fields and field extensions

Next we will use $K[X]$ is a PID for K a field to study fields systematically.

5.1 Prime fields

Let K be a field. We have a unique ring homomorphism $\iota : \mathbb{Z} \to K$ by $n \geq 0 \mapsto n_K = 1_K + \dots + 1_K$. Let I be the kernel. Then $\mathbb{Z}/I \hookrightarrow K$ so $\mathbb{Z}/I$ is an integral domain, so I is a prime ideal. Thus I is either the zero ideal $\{0\}$, if K has characteristic zero, or the ideal $\langle p \rangle$ for some prime p of $\mathbb{Z}$. In the former case $I = \{0\}$, the injection $\mathbb{Z} \hookrightarrow K$ extends to an inclusion $\mathbb{Q} \hookrightarrow K$ sending $a/b \mapsto (\iota a)\left(\iota b^{-1}\right) = a_K/b_K$. In the latter case $I = \langle p \rangle$, we get an injection $\mathbb{Z}/p\mathbb{Z} \hookrightarrow K$, which we often denote $\mathbb{F}_p$ when we think of it as a field. Upshot is that every field K contains exactly one of $\mathbb{Q}$, $\mathbb{F}_p$, for p prime, in exactly one way depending on its characteristic. This field is called the **prime field** of K, and it is contained in K in a unique way.

5.2 Field extensions

The prime fields are in some sense the smallest possible fields. Once we know they exist, it makes sense to study fields by studying pairs K, L of fields such that $K \subseteq L$ of fields, trying to relate L to K.

Definition 5.2.1. A **field extension** is a pair of fields K, L with $K \subseteq L$, and is often denoted L/K.

Note. Such an inclusion of fields L/K makes L into a K-vector space, that is a vector space over K.

Definition 5.2.2. We say that a field extension L/K is **finite** if L is finite-dimensional as a K-vector space. If this is the case, the **degree** of such an extension is the dimension of L as a K-vector space $\dim_K L$, and is denoted $[L : K]$.

Proposition 5.2.3. Let $K \subseteq L \subseteq M$ be fields. Then M/K is finite iff M/L and L/K are both finite. If this is the case then $[M : K] = [M : L]\,[L : K]$.

Proof. First suppose that M/K is finite. Then L is a K-subspace of M, so finite dimensional as a K-vector space. Moreover, there exists a K-basis $m_1, \dots, m_r$, and this basis spans M over K and thus also over L. Thus M is finite-dimensional as an L-vector space, so M/L is finite. Conversely, suppose L/K, M/L are finite. Let $e_1, \dots, e_n$ be a K-basis for L, and let $f_1, \dots, f_n$ be an L-basis for M. Then claim that

$$e_1 f_1, \dots, e_1 f_m, \dots, e_n f_1, \dots, e_n f_m$$

is a K-basis for M. Every element x of M can be expressed uniquely as $c_1 f_1 + \dots + c_m f_m$ with $c_i \in L$. Each c_i in turn can be expressed as $d_{1,i} e_1 + \dots + d_{n,i} e_n$ with $d_{j,i} \in K$. Thus we can express x as

$$d_{1,1} e_1 f_1 + \dots + d_{n,1} e_n f_1 + \dots + d_{1,m} e_1 f_m + \dots + d_{n,m} e_n f_m.$$

In particular the set $\{e_i f_j\}$ for $1 \leq i \leq n$ and $1 \leq j \leq m$ spans M over K. In this case the degree of L over K is n and the degree of M over L is m, so it remains to show that $\{e_i f_j\}$ is linearly independent over K. Suppose we have elements $d_{i,j}$ of K such that $\sum_{i,j} d_{i,j} e_i f_j = 0$. Then, regrouping, we find that $\sum_j \left(\sum_i d_{i,j} e_i\right) f_j = 0$ is an L-linear combination of the f_j that is zero. Since the f_j are linearly independent over L we must have $\sum_i d_{i,j} e_i = 0$ for all j. Since the e_i are linearly independent over K we must have $d_{i,j} = 0$ for all i, j. ☐

Lecture 8
Monday
22/10/18

5.3 Extensions generated by one element

Let L/K be a field extension, and let α be an element of L.

Definition 5.3.1. We let $K(\alpha)$ denote the subfield of L consisting of all elements of L that can be expressed in the form $P(\alpha)/Q(\alpha)$, where P and Q are polynomials with coefficients in K and $Q(\alpha)$ is not zero. This is the smallest subfield of L containing K and α.

Recall that if R, S are rings, $f : R \to S$ is a homomorphism, and $\alpha \in S$, then have $\phi_{f,a} : R[X] \to S$ by $\phi_{f,a}\left(\sum_{i=1}^{n} r_i X^i\right) = \sum_{i=1}^{n} f(r_i)\,\alpha^i$. We have a natural map $K[X] \to K(\alpha) \subseteq L$., inclusion on K, that takes a polynomial $P(X)$ to $P(\alpha)$. It is a ring homomorphism. Let I be the kernel of this homomorphism. We then get an injection of $K[X]/I$ into the field $K(\alpha)$. Thus $K[X]/I$ is an integral domain, so I is a prime ideal of $K[X]$. Since $K[X]$ is a PID, every nonzero prime ideal is maximal. (TODO Exercise) There are thus two cases. In the first I is the zero ideal that is not maximal. That is, there is no nonzero polynomial Q in $K[X]$ such that $Q(\alpha)$ is zero in L. We say that α is **transcendental** over K in this case. In the second I is an ideal $\langle Q \rangle$ for $Q \in K[X]$ a nonzero irreducible polynomial that is a maximal ideal of $K[X]$. In this case we say α is **algebraic** over K.

Definition 5.3.2. $K(X)$ is the **field of rational functions** on X,

$$K(X) = \left\{ \frac{P(X)}{Q(X)} \;\middle|\; P, Q \in K[X],\ Q \neq 0 \right\} / \sim .$$

Assume first that α is transcendental over K, that is $I = \{0\}$. Recall $I = \{P(X) \in K[X] \mid P(\alpha) = 0\}$. So in this case there is no nonzero polynomial $P \in K[X]$ with $P(\alpha) = 0$. In this case the map taking $P(X)$ to $P(\alpha)$ is an injection of $K[X]$ into $K(\alpha) \subseteq L$. In particular every nonzero element of $K[X]$ gets sent to a nonzero, hence invertible, element of L. Thus the map from $K[X]$ to L extends to an injective map from the field of fractions of $K[X]$, which we denote $K(X)$, to L. This map takes $P(X)/Q(X)$ to $P(\alpha)/Q(\alpha)$. By definition of $K(\alpha)$, this map is surjective so the image of this map is $K(\alpha)$. In particular $K(X)$ and $K(\alpha)$ are isomorphic. Thus the following diagram holds.

$$\begin{tikzcd} & L \\ K(X) \arrow[r, "\sim", "g"'] & K(\alpha) \arrow[u, hook, "\subseteq"'] \\ K[X] \arrow[u, hook, "\subseteq"] \arrow[ur, hook, "f"'] & \end{tikzcd} \qquad f : P(X) \mapsto P(\alpha) \qquad g : \frac{P(X)}{Q(X)} \mapsto \frac{P(\alpha)}{Q(\alpha)}$$

Note. In this case $K(\alpha)$ is infinite dimensional as a K-vector space. It contains a subspace isomorphic to $K[X]$, for instance.

If α is algebraic over K, then I is a nonzero maximal ideal of the PID $K[X]$, so it is generated by a single irreducible polynomial $Q(X)$ in $K[X]$. As a consequence, since the units in $K[X]$ are just the constant polynomials, the polynomial $Q(X)$ is well-defined up to a constant factor. It is called the **minimal polynomial** of α. By definition, it divides every polynomial $P(X)$ such that $P(\alpha) = 0$. Since $\langle Q(X) \rangle$ is maximal, the ring $K[X] / \langle Q(X) \rangle$ is a field. Recall that for any $P \in K[X]$, can write $P(X)$ uniquely as $A(X)Q(X) + R(X)$ with $\deg(R) < \deg(Q)$. So $1, \dots, X^{\deg(Q)-1}$ are a K-basis of $K[X] / \langle Q(X) \rangle$. So its dimension as a K-vector space is equal to the degree of $Q(X)$. The map $K[X] \to K(\alpha) \subseteq L$ descends to an injection of $K[X] / \langle Q(X) \rangle$ into L. Since its image is a subfield of $K(\alpha)$ containing K and α, this map is an isomorphism of $K(\alpha)$ with $K[X] / \langle Q(X) \rangle$. Thus in this case the extension $K(\alpha)/K$ is a finite extension, of degree equal to the degree of $Q(X)$. Thus the following diagram holds.

$$\begin{tikzcd} K[X] \arrow[dr, two heads, "f"] & L \\ \dfrac{K[X]}{\langle Q(X) \rangle} \arrow[u, hook, "\subseteq"] \arrow[r, "g", "\sim"'] & K(\alpha) \arrow[u, hook, "\subseteq"'] \end{tikzcd} \qquad f : P(X) \mapsto P(\alpha) \qquad g : [R(X)]_{\langle Q(X) \rangle} \to R(\alpha)$$

To summarise, extend K by a single element by

1. building $K[X]$, and
2. either passing to field of fractions $K(X)$ to form a transcendental extension, or choosing an irreducible polynomial Q to form an algebraic extension $K[X] / \langle Q(X) \rangle$.

Slightly informally, instead of $K[X] / \langle Q(X) \rangle$, we sometimes write $K(\alpha)$, where α is a root of $Q(X)$.

Definition 5.3.3. An extension L/K is **algebraic** if every element of L is algebraic over K.

An observation is that if L/K is finite, then L/K is algebraic. Suppose not. Let $\alpha \in L$ be transcendental over K. $K[X]$ is a polynomial ring in $K(\alpha)$ contained in L, so L/K is not finite.

Corollary 5.3.4. Let L/K be a field extension for $\alpha, \beta \in L$ algebraic over K. Then $\alpha + \beta$, $\alpha\beta$ are algebraic over K.

Proof. $[K(\alpha) : K] = \deg(\alpha)$ and $[K(\alpha, \beta) : K(\alpha)] \le \deg(\beta)$, so $[K(\alpha, \beta) : K] \le (\deg(\alpha))(\deg(\beta))$. Now $K \subseteq K(\alpha + \beta) \subseteq K(\alpha, \beta)$, so $\deg(\alpha + \beta)$ over K is at most $(\deg(\alpha))(\deg(\beta))$. Similarly for $\alpha\beta$. ☐

Corollary 5.3.5. If L/K, then the subset L^{alg} of elements of L algebraic over K is a field.

Proof. If $a_0 + \dots + a_n\alpha^n = 0$ then $a_0\left(\alpha^{-1}\right)^n + \dots + a_n = 0$. ☐

Example. $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ is the subfield of elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$.

5.4 Example

Example. Consider the polynomial $X^2 + X + 1$ in $\mathbb{F}_2[X]$. It has no roots in $\mathbb{F}2$, so it is irreducible, as a polynomial of degree 2 any nontrivial factor would be linear. The other polynomials of degree two are X^2, $X^2 + X = X(X + 1)$, $X^2 + 1 = (X + 1)^2$, so $X^2 + X + 1$ is the unique irreducible polynomial of degree two. Let $\mathbb{F}_4 = \mathbb{F}_2[X] / \left\langle X^2 + X + 1\right\rangle$. Thus the quotient $\mathbb{F}_2[X] = \left\langle X^2 + X + 1\right\rangle$ is a field extension of degree two of $\mathbb{F}_2$, which is denoted $\mathbb{F}_4$. Its four elements are $0, 1, X, X + 1$, or more precisely, their classes modulo $\left\langle X^2 + X + 1\right\rangle$.

$\cdot$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

Note that $X^2 = -X - 1 = X + 1$, $X^2 + X + 1 = 0$, $(X + 1)^2 = X$, and $X^3 = X(X + 1) = 1$ in $\mathbb{F}_4$. In particular the multiplicative group of $\mathbb{F}_4$ is cyclic of order three. This is not particularly surprising, as all groups of order three are cyclic. We will see later, though, that the multiplicative group of any finite field is cyclic.

Proposition 5.4.1. Let K be a field with four elements. Then $K \cong \mathbb{F}_4$.

Proof. Let $\alpha \in K$ with $\alpha \ne 0$ and $\alpha \ne 1$. Consider $1, \alpha, \alpha^2$. Since K has dimension two over $\mathbb{F}_2$, there is a linear dependence. So there exists a polynomial P in $\mathbb{F}_2[X]$ of degree at most two such that $P(\alpha) = 0$. In fact P must be irreducible of degree two. If it is divisible by something of degree one, then a polynomial of degree one vanishes on α, so $\alpha = 0$ or $\alpha = 1$. So $\alpha^2 + \alpha + 1 = 0$. The map $\mathbb{F}_2[X] \to K$ sending X to α descends to $\mathbb{F}_2[X] / \left\langle X^2 + X + 1\right\rangle \to K$. So $\mathbb{F}_4$ embeds in K. Thus the following diagram holds and $K \cong \mathbb{F}_4$.

$$\begin{tikzcd}
\mathbb{F}_2[X] \arrow[drr, two heads, "P(X)\mapsto P(\alpha)"] & & \\
\dfrac{\mathbb{F}_2[X]}{\langle X^2+X+1\rangle} \arrow[u, hook, "\subseteq"] \arrow[rr, "\sim"'] & & K
\end{tikzcd}$$

☐

Lecture 9 Wednesday 24/10/18

6 Finite fields

6.1 Finite fields

Let K be a finite field. That is, a field with only finitely many elements. Then K has characteristic p for some prime p, and is in particular a finite dimensional $\mathbb{F}_p$ vector space. Thus its order is a power p^r of p for $r > 0 \in \mathbb{Z}$. If we fix a particular prime power p^r, then two questions naturally arise. Does there exist a field of order p^r? If so, can we classify fields of order p^r up to isomorphism? We will see that in fact, up to isomorphism, there is a unique field $\mathbb{F}_{p^r}$ of order p^r.

6.2 The Frobenius automorphism

Let p be a prime. For any ring R, the map $x \mapsto x^p$ on R certainly satisfies $(xy)^p = x^p y^p$ for all $x, y \in R$. On the other hand,

$$(x+y)^p = x^p + \binom{p}{1} x y^{p-1} + \dots + \binom{p}{p-1} x^{p-1} y + y^p.$$

Now the binomial coefficients satisfy

$$p \;\Bigg|\; \binom{p}{i} = \frac{p!}{i!\,(p-i)!},$$

for $1 \le i \le p-1$, so if R has characteristic p, we have $(x+y)^p = x^p + y^p$. So $x \mapsto x^p : R \to R$ is a ring homomorphism from R to R, called the **Frobenius endomorphism** of R. If R is a field of characteristic p, then the Frobenius endomorphism is injective. If in addition R is finite, then any injective map from R to R is surjective. In particular the Frobenius endomorphism is a bijective and an isomorphism from R to R when R is a finite field of characteristic p. In this case we call the map $x \mapsto x^p$ the Frobenius **automorphism**. Composing the Frobenius endomorphism with itself, we find that for any r, $x \mapsto x^{p^r}$ is also an endomorphism of any ring R of characteristic p.

Example. Let $R = \mathbb{F}_4$. $y \to y^2$ gives $0 \mapsto 0$, $1 \mapsto 1$, $X \mapsto X+1$, and $X+1 \mapsto X$.

Note. Let K be a field of p^r elements. Then $\alpha^{p^r} = \alpha$ for all $\alpha \in K$. If $\alpha = 0$, clear. Otherwise $\alpha \in K^*$, K^* is an abelian group of order $p^r - 1$. Lagrange's theorem gives $\alpha^{p^r-1} = 1$, so $\alpha^{p^r} = \alpha$.

We have the following.

Proposition 6.2.1. Let K be a field of characteristic p, such that $\alpha^{p^r} = \alpha$ for all $\alpha \in K$. Let $P(X) \in K[X]$ be an irreducible factor of $X^{p^r} - X$ over $K[X]$. Then every element β of $K[X] / \langle P(X) \rangle$ satisfies $\beta^{p^r} = \beta$.

Proof. Let $d = \deg(P)$. Can write $\beta = c_0 + \dots + c_{d-1} X^{d-1}$. Moreover, since $P(X) = 0$ in $K[X] / \langle P(X) \rangle$ and $P(X)$ divides $X^{p^r} - X$, we have $X^{p^r} = X$ in $K[X] / \langle P(X) \rangle$. Thus

$$\beta^{p^r} = c_0^{p^r} + \dots + c_{d-1}^{p^r} \left(X^{p^r}\right)^{d-1} = c_0 + \dots + c_{d-1} \left(X^{p^r}\right)^{d-1} = c_0 + \dots + c_{d-1} X^{d-1} = \beta.$$

∎

Corollary 6.2.2. There exists a field K of characteristic p such that

1. $\alpha^{p^r} = \alpha$ for all $\alpha \in K$, and
2. the polynomial $X^{p^r} - X$ of $K[X]$ factors into linear factors over $K[X]$.

Proof. Let $K_0 = \mathbb{F}_p$. K_0 satisfies 1. We construct a tower of fields $K_0 = \mathbb{F}_p \subsetneq K_1 \subsetneq \dots$ all satisfying 1 as follows. Suppose we have constructed K_i satisfying 1. If $X^{p^r} - X$ factors into linear factors over $K_i[X]$, we are done. Otherwise, choose a nonlinear irreducible factor $P_i(X)$ of $X^{p^r} - X$ in $K_i[X]$ of degree at least two, and set $K_{i+1} = K_i[X] / \langle P_i(X) \rangle$. Then K_{i+1} is strictly larger than K_i and still satisfies 1. On the other hand, in any field K_i satisfying 1, every element is a root of $X^{p^r} - X$, so $\# K_i \le p^r$ for all i. Since this polynomial can have at most p^r roots, this process must eventually terminate. ∎

Since $X^{p^r} - X$ has degree p^r, we expect the field K constructed above to have p^r elements. So it suffices to show that over any field K of characteristic p, $X^{p^r} - X$ has no repeated roots. To prove this we need an additional tool.

6.3 Derivatives

Definition 6.3.1. Let R be a ring, and let $P(X) = r_0 + \cdots + r_d X^d$ be an element of $R[X]$. The **derivative** $P'(X)$ of $P(X)$ is the polynomial $r_1 + \cdots + d r_d X^{d-1}$.

Note. Just as for differentiation in calculus, we have a Leibniz rule. For $P, Q \in R[X]$, $(PQ)'(X) = P(X) Q'(X) + P'(X) Q(X)$, by reducing to P, Q monomials.

From this we deduce the following.

Lemma 6.3.2. Let K be a field, and let $P(X)$ be a polynomial in $K[X]$ with a multiple root in K. Then $P(X)$ and $P'(X)$ have a common factor of degree greater than zero.

Proof. Let $\alpha \in K$ be the multiple root. Then we can write $P(X) = (X - \alpha)^2 Q(X)$. Applying the Leibniz rule we get $P'(X) = 2(X - \alpha) Q(X) + (X - \alpha)^2 Q'(X)$ and it is clear that $X - \alpha$ divides both $P(X)$ and $P'(X)$. ☐

Corollary 6.3.3. Let K be a field of characteristic p. Then $X^{p^r} - X$ has no repeated roots in K.

Proof. Let $P(X) = X^{p^r} - X$. Then $P'(X) = -1$, so $P(X)$ and $P'(X)$ have no common factor. ☐

Corollary 6.3.4. There exists a finite field of p^r elements.

Proof. The field K we constructed has p^r elements. ☐

Lecture 10
Friday
26/10/18

6.4 The multiplicative group

Rather than show immediately that there is a unique finite field of p^r elements, we make a detour to study the multiplicative group of a finite field. This is not strictly necessary to prove uniqueness, but will simplify the proof, and is of interest in its own right. Let K denote a field of p^r elements. The goal of this section is to show that K^* is cyclic.

Note. As a multiplicative group, K^* is an abelian group of order $p^r - 1$, so by Lagrange's theorem, we have $\alpha^{p^r - 1} = 1$ for all $\alpha \in K^*$.

Recall for an abelian group A, operation written additively, that the order of an element a of A is the smallest $d \in \mathbb{Z}_{>0}$ such that $da = 0$.

1. The order of an element a of A divides the order of A.
2. If $d'a = 0$ for some $d' \in \mathbb{Z}$ then the order of a divides d'.

The order of an element a of K^* is the smallest $d \in \mathbb{Z}_{>0}$ such that $a^d = 1$. Since $a^{p^r - 1} = 1$, the order of a is a divisor of $p^r - 1$. On the other hand, if d is a divisor of $p^r - 1$, then any element of order dividing d is a root of the polynomial $X^d - 1$. Since K is a field, this polynomial has at most d roots, and we find that there are at most d elements of K^* of order dividing d. Order of any element divides $p^r - 1$. Know $X^{p^r - 1} - 1$ has $p^r - 1$ distinct roots in K. For $d \mid p^r - 1$, $X^d - 1 \mid X^{p^r - 1} - 1$, so $X^d - 1$ has exactly d roots in K. That is, for all $d \mid p^r - 1$, K^* has exactly d elements of order dividing d. In fact, we have the following.

Proposition 6.4.1. Let A be a finite abelian group of order n, and suppose that A has exactly d elements of order dividing d, for all d dividing n. Then A is cyclic.

In particular K^* is cyclic. The remainder of this section will be devoted to proving this proposition. As a corollary, we deduce that the multiplicative group of any finite field is cyclic. Consider the cyclic group $\mathbb{Z}/n\mathbb{Z}$. The order of any element in this group is a divisor of n.

Definition 6.4.2. For $n \in \mathbb{Z}$, we let $\Phi(n)$ denote the number of elements in $(\mathbb{Z}/n\mathbb{Z}, +)$ of exact order n. This equals to the number of elements $t \in \mathbb{Z}$ for $1 \le t \le n$ such that $(t, n) = 1$.

Note. Since $[1]$ in $\mathbb{Z}/n\mathbb{Z}$ has order n, $\Phi(n)$ is nonzero for all n.

Lemma 6.4.3. For any d dividing n, the cyclic group $\mathbb{Z}/n\mathbb{Z}$ contains a unique subgroup of order d, and any element of $\mathbb{Z}/n\mathbb{Z}$ of order dividing d is contained in this subgroup.

Proof. The cyclic subgroup C of $\mathbb{Z}/n\mathbb{Z}$ generated by n/d is clearly a subgroup of order d. This has d elements $[0], \dots, (d-1)[n/d]$. Conversely, if x is an element of a subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d, then the order of x divides d, so dx is divisible by n, and hence by unique factorisation x is divisible by n/d. Thus x is in C and the claim follows. $\square$

As a consequence, we deduce the following.

Corollary 6.4.4. For any d dividing n, $\Phi(d)$ is the number of elements of $\mathbb{Z}/n\mathbb{Z}$ of order d.

Corollary 6.4.5. For any $n \in \mathbb{Z}$, we have

$$\sum_{d \mid n} \Phi(d) = n.$$

Proof. Since every element of $\mathbb{Z}/n\mathbb{Z}$ has order d for some d dividing n, the sum over all possible d dividing n of the number of elements of order d is just the number of elements of $\mathbb{Z}/n\mathbb{Z}$, which is n. $\square$

Proof of Proposition 6.4.1. Let A be as in the proposition. We must show that A contains an element of order n. In fact, we will show, by induction on d, that A contains exactly $\Phi(d)$ elements of order d for all $d \mid n$. In particular, A has $\Phi(n) > 0$ elements of order n, so it is cyclic. If $d = 1$, the only element of order one is the identity of A. Since $\Phi(1) = 1$ the base case holds. Assume the claim is true for all $d' < d$. A has

1. d elements of order dividing d, and
2. $\Phi(d)$ elements of order d' for $d' \mid d$ and $d' < d$,

so the number of elements of exact order d is $d - \sum_{d' \mid d,\ d' < d} \Phi(d')$. By the corollary, this is precisely $\Phi(d)$. $\square$

6.5 Uniqueness

We now turn to the question of showing that any two fields of p^r elements are isomorphic. Let K be such a field. The cyclicity of K^* immediately shows.

Proposition 6.5.1. Any finite field K of characteristic p is generated over $\mathbb{F}_p$ by a single element $\alpha \in K$.

Proof. Let α be an element of K, that generates K^* as an abelian group. Then $\mathbb{F}_p(\alpha)$ is contained in K, but contains α^n for all n so contains K^*, hence $K = \mathbb{F}_p(\alpha)$. $\square$

As a corollary, we deduce the following.

Proposition 6.5.2. For any prime p and any $r \in \mathbb{Z}_{>0}$, there exists an irreducible polynomial $P(X) \in \mathbb{F}_p[X]$ of degree r in $\mathbb{F}_p[X]$.

Proof. Let K be a finite field of p^r elements, α be an element of K that generates K over $\mathbb{F}_p$, and P the minimal polynomial of α over $\mathbb{F}_p$. We then have a surjective map $\mathbb{F}_p[X] \to K$ taking X to α. It is kernel is generated by irreducible P of degree $\deg(P) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = r$. Thus the following diagram holds.

$$\begin{tikzcd}
\mathbb{F}_p[X] \arrow[rrd, twoheadrightarrow, "Q(X)\mapsto Q(\alpha)"] & & \\
\dfrac{\mathbb{F}_p[X]}{\langle P(X)\rangle} \arrow[u, hook, "\subseteq"] \arrow[rr, "\sim"'] & & K = \mathbb{F}_p(\alpha)
\end{tikzcd}$$

$\square$

We thus have the following.

Lemma 6.5.3. Every irreducible polynomial $P(X)$ of degree r in $\mathbb{F}_p[X]$ is a divisor of $X^{p^r-1}-1$.

Proof. Let $K = \mathbb{F}_p(\alpha)$ where α is a root of P. $\#K = p^r$ so $\alpha^{p^r} - \alpha$ is zero in K. So $P(X) \mid X^{p^r} - X$. $\square$

Corollary 6.5.4. Any two finite fields K, K' of cardinality p^r are isomorphic.

Proof. Choose $\alpha \in K$ such that α generates K over $\mathbb{F}_p$. We can then write $K = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[X] / \langle P(X) \rangle$, where $P(X)$ is the minimal polynomial of α over $\mathbb{F}_p$. In particular $P(X)$ is irreducible of degree r. Since $P(X)$ divides $X^{p^r-1}-1$ in $\mathbb{F}_p[X]$, it also divides $X^{p^r-1}-1$ in $K'[X]$. Since in $K'[X]$, $X^{p^r-1}-1$ factors into linear factors, $P(X)$ also factors into linear factors over K'. In particular there exists a root $\alpha' \in K'$ of $P(X)$ in $K'[X]$ such that $P(\alpha') = 0$. Then the map $\mathbb{F}_p[X] \to K'$ that sends X to α' has kernel $\langle P(X) \rangle$ and induces a map

$$K \xrightarrow[\sim]{Q(\alpha) \mapsto Q(X)} \frac{\mathbb{F}_p[X]}{\langle P(X) \rangle} \xhookrightarrow{Q(X) \mapsto Q(\alpha')} K'$$

Since this is map of fields from K to K' that takes α to α' it is injective. Since both fields K, K' have the same cardinality p^r, it is also surjective and an isomorphism. $\square$

If $k = \mathbb{Q}$, $\mathbb{Q}[X] / \langle X^2 - p \rangle$ are pairwise nonisomorphic extensions of degree α for every prime p. Lecture 11 Monday 29/10/18

Lecture 11 is a problem class.

Lecture 12 Wednesday 31/10/18

7 R-modules

7.1 Definitions

Definition 7.1.1. An R-module M is a set, together with two operations $+ : M \times M \to M$ and $\cdot : R \times M \to M$, such that

1. $(M, +)$ makes M into an abelian group with identity 0_M,
2. $r(m + m') = rm + rm'$ for all $r \in R$, $m, m' \in M$,
3. $(r + r') = rm + r'm$ for all $r, r' \in R$, $m \in M$,
4. $(rr')m = r(r'm)$ for all $r, r' \in R$, $m \in M$, and
5. $1_R \cdot m = m$ for all $m \in M$.

Note. For an abelian group M, let $End(M)$ denote the set of homomorphisms $M \to M$ of abelian groups. $End(M)$ is a noncommutative ring. 2 iff for all $r \in R$, $\cdot r : M \to M$ lives in $End(M)$. 3, 4, and 5 iff the map $R \to End(M)$ given by 2 is a homomorphism of rings.

Example. The usual addition and multiplication on R naturally makes R into an R-module. More generally, any ideal of R is an R-module with the usual addition and multiplication.

Example. If $f : R \to S$, then f makes S into an R-module, where the addition $+$ is the usual addition in S, and the multiplication law is defined by $r \cdot s = f(r) \cdot_S s$ for all $r \in S$, $s \in S$. In particular any quotient R/I is an R-module. More generally, if $f : R \to S$ is a homomorphism, and M is any S-module, then M is also an R-module via $r \cdot m = f(r) \cdot m$. In particular, $R \to R/I$ lets us treat any R/I-module M as an R-module. Note that if M is an R/I-module, then for all $r \in I$, $m \in M$, $r \cdot m = 0$. We say that I **annihilates** M in this situation. Conversely, if M is an R-module and $r \cdot m = 0$ for all $r \in I$, $m \in M$, then M naturally has the structure of an R/I-module. Given $r + I \in R/I$, $m \in M$, we define $(r + I) \cdot m = rm$. If $r + I = r' + I$, then $r - r' \in I$, so $rm - r'm = (r - r')m = 0$ by assumption.

Example. Let $R = \mathbb{Z}$, and let M be an abelian group. Then M has the unique natural structure of $\mathbb{Z}$-module, as follows. Property 3 from the module axioms shows that

$$n \cdot m = \begin{cases} m + \dots + m & n > 0 \\ 0 & n = 0 \\ (-m) + \dots + (-m) & n < 0 \end{cases}.$$

Thus the multiplication law $\mathbb{Z} \times M \to M$ is forced on us, and one checks that it does satisfy properties 2 to 5 above. Informally, we say that abelian groups are $\mathbb{Z}$-modules.

Example. If R is a field, then R-modules are just R-vector spaces.

Example. Let S be a set, and let M_S be the set of R-valued functions $f : S \to R$. We add and multiply pointwise. For $f, g \in M_S$, we can define $f + g$ as the function that takes $s \in S$ to $f(s) + g(s)$, and rf as the function that takes s to $r \cdot f(s)$. M_S is clearly an R-module. Also of interest is the R-submodule F_S of M_S that consists of functions $f : S \to R$ such that $f(s) = 0_R$ for all but finitely many s. The R-module F_S is called the **free R-module** on the set S and will be very important for us.

7.2 Submodules, quotients, and direct sums

Definition 7.2.1. Let M be an R-module. A subset N of M is an **R-submodule** of M if N is closed under addition and multiplication by elements of R. That is, N is an additive subgroup of M, and for all $n \in N$, $r \in R$, we have $rN \subseteq N$.

In particular, the ideals of R are just the R-submodules of R.

Definition 7.2.2. If S is any subset of M, we define the **R-submodule of M generated by S** to be the set of all elements of M of the form $r_1 s_1 + \cdots + r_n s_n$, where the r_i are elements of R and the s_i are elements of S. It is the smallest R-submodule of M containing S.

Definition 7.2.3. An R-module M is a **finitely generated** R-module if M admits a finite subset S of M such that the R-submodule of M generated by S is all of M. We say S is a **generating set** for M.

Definition 7.2.4. Let M be an R-module and N be an R-submodule of M. We say two elements m, m' of M are **congruent modulo** N if their difference $m - m'$ lies in N. This is easily seen to be an equivalence relation, and the equivalence classes are the cosets of the form $m + N$, for $m \in M$. The set of equivalence classes is denoted M/N. It has the natural structure of an R-module, where $(m + N) + (m' + N) = (m + m') + N$ and $r \cdot (m + N) = rm + N$. This R-module is called the **quotient of M by N**.

If $m + N = m' + N$, then $m - m' \in N$, so $rm - rm' = r(m - m') \in N$. So well-defined. Have a natural map $M \to M/N$ taking m to $m + N$.

Definition 7.2.5. Given two R-modules M_1 and M_2, the **direct sum** $M_1 \oplus M_2$ is the set of ordered pairs (m_1, m_2) with $(m_1, m_2) + (m_1', m_2') = (m_1 + m_1', m_2 + m_2')$ and $r(m_1, m_2) = (rm_1, rm_2)$ for $m_1, m_1' \in M_1$, $m_2, m_2' \in M_2$, and $r \in R$.

Definition 7.2.6. Let M be an R-module and I an ideal of R. Then we can form the R-submodule IM of M consisting of all elements of M of the form $i_1 m_1 + \cdots + i_r m_r$ where the i_r are in I and the m_r are in M. This is an R-submodule of M, so we can form the quotient M/IM. Then M/IM is certainly an R-module, but it is also an R/I-module. One can define multiplication $R/I \times M/IM \to M/IM$ by $(r + I)(m + IM) = rm + IM$. As always one has to check that this is well-defined, but this is straightforward. We need that if $r - r'$ lies in I, and $m - m'$ lies in IM, then $rm - r'm'$ lies in IM. But $rm - r'm' = (r - r')m + r'(m - m')$ which is clearly in IM.

7.3 Module homomorphisms, kernels, and images

Definition 7.3.1. A map $f : M \to N$ of R-modules is called a **homomorphism of R-modules** if

1. f is a homomorphism of the underlying abelian groups, and
2. $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$.

Warning that a ring homomorphism $R \to R$ satisfies $f(rr') = f(r) f(r')$, but an R-module homomorphism $R \to R$ satisfies $f(rr') = rf(r')$.

Definition 7.3.2. The kernel of $f : M \to N$ is the set $\{m \in M \mid f(m) = 0\}$, an R-submodule of M. The image of $f : M \to N$ is the set $\{n \in N \mid \exists m \in M,\ f(m) = n\}$, an R-submodule of N.

It is easy to see that the kernel and image of a homomorphism of R-modules $f : M \to N$ are R-submodules of M and N, respectively.

Note. In particular there is a natural homomorphism from M to M/N, taking m to $m + N$. This homomorphism has the following universal property, exactly analogous to the universal property of the quotient construction for rings.

Proposition 7.3.3 (Universal property of the quotient)**.** Let N be an R-submodule of M, and let $f : M \to M'$ be an R-module homomorphism whose kernel contains N. Then there is unique homomorphism $\overline{f} : M/N \to M'$ such that $f(m+N) = f(m)$ for all $m \in M$. In particular the kernel of $\overline{f}$ is the image of $Ker(f)$ in M/N.

Proof. The proof is identical to that for quotient rings, and will be omitted. ☐

7.4 Free modules

Definition 7.4.1. Let M be an R-module. A subset S of M is a **basis** for M if the following two conditions hold.

1. S **spans** M **over** R. For all $m \in M$, there exists $s_1, \dots, s_n \in S$ finite and $r_1, \dots, r_n \in R$ such that $m = r_1 s_1 + \dots + r_n s_n$, that is the R-submodule of M generated by S is all of M.
2. S is R**-linearly independent**. For any collection $s_1, \dots, s_n$ of distinct elements of S, and any $r_1, \dots, r_n \in R$, $r_1 s_1 + \dots + r_n s_n = 0$ is nonzero in M unless all r_i are zero.

Definition 7.4.2. An R-module M that has a basis S is called a **free** R-module. The cardinality n of the basis S is called the **rank** of the free R-module M over R.

Lecture 13 Friday 02/11/18

Remark 7.4.3. If R is a field, then the notion of a basis for an R-module coincides with the usual notion for vector spaces. In this case, at least if one assumes the axiom of choice, every R-module has a basis. When R is not a field only very special modules have bases. For instance any quotient R/I of R, for I a nonzero ideal, has no basis.

Example. The ring R is a free module of rank one over R, with basis $\{1_R\}$. More generally any unit $u \in R^*$ gives a basis of R as an R-module.

Recall that the free module F_S on a set S was defined to be the set of functions $f : S \to R$ such that $f(s) = 0$ for all but finitely many $s \in S$. For each $s \in S$, we have an element e_s of F_S defined by $e_s(t) = 0$ for all $t \in S$ with $t \neq s$, $e_s(s) = 1$. Claim that the e_s form a basis for F_S. In particular, given $f : R \to S$ with $f(s) = 0$ for all but finitely many s, let $s_1, \dots, s_n$ be the set of elements in S on which $f(s_i)$ is nonzero. Set $r_i = f(s_i)$. Claim that $f = r_1 e_{s_1} + \dots + r_n e_{s_n}$. If $f(s) \neq 0$, then $s \in \{s_1, \dots, s_n\}$ so $e_{s_i}(s) = 0$ for all i. For any i, $e_{s_i}(s_j) = 0$ if $i \neq j$ and $e_{s_i}(s_i) = 0$, so $\left(\sum_{i=1}^n r_i e_{s_i}\right)(s_j) = r_j = f(s_j)$. Then f can be written as $r_1 e_{s_1} + \dots + r_n e_{s_n}$, so the e_s span F_S. On the other hand, for all $s_1, \dots, s_n \in S$ distinct with $\sum_{i=1}^n r_i e_{s_i} = 0$, $\sum_{i=1}^n r_i e_{s_i}$ takes the value r_i by evaluating at s_i for all i, and thus is only the zero function when all r_i are zero for all i, so we do have R-linear independence. Thus F_S is free, justifying its name.

Proposition 7.4.4. Let F_1, F_2 be free modules with basis S_1, S_2. Then $F_1 \oplus F_2$ is free with basis

$$\{(s, 0) \mid s \in S_1\} \cup \{(0, s') \mid s' \in S_2\}.$$

Moreover, if F_1 and F_2 are free of finite ranks n_1 and n_2 respectively, then $F_1 \oplus F_2$ is free of rank $n_1 + n_2$.

Proof. For linear independence, let $s_1, \dots, s_m \in S_1$ and $s'_1, \dots, s'_l \in S_2$ be distinct. Suppose we have $r_1, \dots, r_m, r'_1, \dots, r'_l \in R$ such that $r_1(s_1, 0) + \dots + r_m(s_m, 0) + r'_1(0, s'_1) + \dots + r'_l(0, s'_l) = 0$. Then $r_1 s_1 + \dots + r_m s_m = 0$ in M_1 and $r'_1 s'_1 + \dots + r'_l s'_l = 0$ in M_2 gives all r_i, r'_i are zero. For spanning set, let $(m, m') \in M_1 \oplus M_2$. Write $m = r_1 s_1 + \dots + r_m s_m$ for $s_i \in S_1$ and $m' = r'_1 s'_1 + \dots + r'_l s'_l$ for $s'_i \in S_2$, then $(m, m') = r_1(s_1, 0) + \dots + r_n(s_n, 0) + r'_1(0, s'_1) + \dots + r'_l(0, s'_l)$. Thus $S_1 \cup S_2$ is a basis for $F_1 \oplus F_2$, which immediately proves the claim. ☐

Free modules have the following universal property.

Proposition 7.4.5 (Universal property of free modules)**.** Let F_S be a free R-module on a set S. Then for any R-module M, and any map of sets $f : S \to M$, there is a unique homomorphism of R-modules $\phi_f : F_S \to M$ such that $\phi_f(e_s) = f(s)$ for all $s \in S$.

Proof. Define ϕ_f by $\phi_f(g) = \sum_{s \in S,\ g(s) \neq 0} g(s) f(s)$. Note that this is a finite sum since all by finitely many s have $g(s) = 0$. Then it is clear that this is a homomorphism of R-modules. On the other hand suppose ϕ is any other map $F_S \to N$ with $\phi(e_s) = f(s)$ for all s. Then we can write $g = \sum_{s \in S,\ g(s) \neq 0} g(s) e_s$, again a finite sum, so

$$\phi(g) = \sum_{s \in S,\ g(s) \neq 0} g(s) \phi(e_s) = \sum_{s \in S,\ g(s) \neq 0} g(s) f(s),$$

so uniqueness is clear. ☐

The image of ϕ_f is the submodule of N generated by the elements $f(s)$, for $s \in S$.

Corollary 7.4.6. Let M be a free R-module with a basis T for M. Let S be any set of the same cardinality as T, and let $g : T \to S$ be any bijection. Then the map $\phi_f : F_S \to M$ is an isomorphism. In particular, any two free R-modules of the same rank are isomorphic.

Proof. The map $\phi_f : F_S \to M$ is such that $\phi_f(e_s) = g(s)$. Since elements of T are linearly independent, this map is injective. Suppose $\phi_f(g) = 0$. Can write $g = \sum r_i e_{s_i}$ for s_i distinct, then $\phi_f(g) = \sum r_i f(s_i)$. Since s_i are distinct, $f(s_i)$ are distinct elements of T, so $\sum r_i f(s_i) = 0$ gives all r_i are zero, so $g = 0$. Since elements of T span M, this map is surjective. Given $m \in M$, write $m = \sum r_i t_i$. For all i, find s_i, with $f(s_i) = t_i$. Then $\phi_f\left(\sum r_i e_{s_i}\right) = \sum r_i t_i = m$. Thus M is isomorphic to F_S. Since M was arbitrary, any module of rank equal to the cardinality of S is isomorphic to F_S and the result follows. ☐

Note. It is also true, but harder to prove, that if M, N are free of different ranks, then $M \ncong N$.

7.5 Generators and relations

Now let M be any R-module, and let $S = \{m_1, \dots, m_t\}$ be a finite subset of M generating M. Then we have a natural map $F_S \to S$ taking e_i to m_i for all $m_i \in S$, and this map is surjective. In particular, let K be the kernel of this map, then $M \cong F_S/K$. Elements of the kernel K are called **relations** among S. Lecture 14 Monday 05/11/18

Explicitly, an element of K is a map $f : S \to R$ such that $f(s) = 0$ for all but finitely many s, and $\sum_{s \in S} f(s) s = 0$. In other words, each element of K encodes a linear relation among the elements of S. It is a measure of how far the elements of S are from being linearly independent. Let $T = \{k_1, \dots, k_s\}$ be a subset of K that generates K. Then in the same way as above, we get a surjection $F_T \twoheadrightarrow K$ taking e_i to k_i, with F_T a free module of rank s. Composing with the inclusion of K in F_S gives us a map $\phi : F_T \to F_S$ whose image is K. The map ϕ determines M up to isomorphism with the quotient F_S/K, and hence with $F_S/\phi(F_T)$. A description of a module as a quotient of a free module by the image of a map of free modules is called a **presentation** of M. If both modules have finite rank the presentation is called **finite**. A module that has a finite presentation is called **finitely presented**. Put another way, a presentation is a description of a module M in terms of

1. a generating set S for M, and

2. a generating set T for the linear relations satisfied by S.

When S and T are finite we can encode a presentation in a matrix, called the **presentation matrix**. Write $S = \{e_1, \dots, e_t\}$ and $T = \{f_1, \dots, f_s\}$. Then ϕ is determined by $\phi(f_1), \dots, \phi(f_s)$. For each i we can write $\phi(f_i)$ as a sum $\sum_{j=1}^{t} r_{ij} e_{s_j}$, and let A be the s by t matrix whose i, j entry is r_{ij}. Then A gives a map from R^t to R^s, and the quotient of R^s by the submodule AR^t of R^s is isomorphic to M.

Example. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$ generated by $[1]_n$. Map $\mathbb{Z} \to M$ is the quotient map with kernel $\langle n \rangle$. So presentation matrix is just (n).

Example. Let $R = \mathbb{Z}\left[\sqrt{-5}\right]$ and $I = \left\langle 2, 1 + \sqrt{-5}\right\rangle$. $R^2 \twoheadrightarrow I$ by $e_1 \mapsto 2$ and $e_2 \mapsto 1 + \sqrt{-5}$. $2e_2 - \left(1 + \sqrt{-5}\right) e_1 \mapsto 0$ in I, and since $(2)(3) = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$, $3e_1 - \left(1 - \sqrt{-5}\right) e_2 \mapsto 0$ in I. Claim that the two relations $\left(1 + \sqrt{-5}\right) e_1 - 2e_2$ and $3e_1 - \left(1 - \sqrt{-5}\right) e_2$ generate K. Let $ae_1 + be_2$ be a relation, so $a, b \in R$ and $2a + \left(1 - \sqrt{-5}\right) b = 0$, that is $a = \left(\left(1 + \sqrt{-5}\right)/2\right) b$. Question is for which b does $\left(\left(1 + \sqrt{-5}\right)/2\right) b$ lie in R. Claim that the set of such b is an ideal J of R. $2 \in J$ and $1 - \sqrt{-5} \in J$ so J contains $\left\langle 2, 1 - \sqrt{-5}\right\rangle$. $1 \notin J$, since $\left\langle 2, 1 - \sqrt{-5}\right\rangle$ is maximal, $J = \left\langle 2, 1 - \sqrt{-5}\right\rangle$. So we have a map $R^2 \to R^2$ with matrix

$$\begin{pmatrix} 1 + \sqrt{-5} & 3 \\ -2 & -1 + \sqrt{-5} \end{pmatrix}$$

presenting I.

General idea is if we have a presentation matrix $A : R^t \to R^s$ for M, with s rows and t columns, then BAC is also a presentation matrix for M, where B is $s \times s$ and C is $t \times t$, and B and C are invertible matrices with inverse matrix entries in R.

8 Noetherian rings and modules

8.1 Definitions and basic properties

Definition 8.1.1. Let R be a ring and let M be an R-module. We say M is **Noetherian** if every increasing infinite chain

$$M_1 \subseteq M_2 \subseteq \dots$$

of R-submodules M_i of M is **eventually constant**. That is, for any such chain, there exists N such that we have $M_i = M_N$ for all $i \geq N$. A ring R is Noetherian if R is Noetherian as an R-module over itself. Since the R-submodules of R are just the ideals of R, a ring R is Noetherian if every increasing infinite chain

$$I_1 \subseteq I_2 \subseteq \dots$$

of ideals I_j of R is eventually constant.

The following result about Noetherian R-modules is fundamental.

Proposition 8.1.2. An R-module M is Noetherian iff every R-submodule N of M is finitely generated.

Proof. Suppose first that M is Noetherian, and let N be an R-submodule of M. Choose an element n_0 of N, and let N_0 be the R-submodule of N generated by n_0. If N_0 is all of N, then N is finitely generated. Otherwise, choose n_1 in $N \setminus N_0$, and let N_1 be the R-submodule of N generated by n_0 and n_1. If N is not finitely generated, we may continue this process indefinitely, choosing for each i an n_i in $N \setminus N_{i-1}$, which is nonempty since N is not finitely generated, and letting N_i be generated by $n_0, \dots, n_i$. In this way we obtain a strictly increasing infinite chain

$$N_0 \subsetneq N_1 \subsetneq \dots$$

of submodules of M, contradicting the fact that M is Noetherian. Conversely, suppose that every R-submodule of M is finitely generated, and let

$$M_0 \subseteq M_1 \subseteq \dots$$

be an increasing chain. We must show that this chain is eventually constant. Let N be the union of the submodules M_i. Note that N is an R-submodule of M. Thus N is finitely generated, say by $n_1, \dots, n_s$. If $n_1, n_2 \in N$, then there exists i, j with $n_1 \in M_i$, $n_2 \in M_j$. If $d \geq i, j$, $n_1, n_2 \in M_d$, so $n_1 + n_2 \in M_d$ gives $n_1 + n_2 \in N$. Since N is the union of the M_j, there exists $i_1, \dots, i_s$ such that n_j is in M_{i_j} for all j. Let d be the largest of the i_j. Then M_d contains $n_1, \dots, n_s$ so it contains N. In particular for any $d' \geq d$ we have $N \subseteq M_d \subseteq M_{d'} \subseteq N$, so $N = M_d = M_{d'}$ for all such d' and the chain is constant after M_d. $\square$