......

Summaries, March 9 and 10

We reviewed the mapping property of quotient ring, which is in the previous summary.

Next, the **Correspondence Theorem.** Let $R \xrightarrow{\varphi} R'$ be a *surjective* homomorphism with kernel K. (So $R' \approx R/K$.) There is a bijective correspondence between these two sets:

$$\{\text{ideals of } R \text{ that contain } K\} \quad \leftrightarrow \quad \{\text{ideals of } R'\}$$

If I is an ideal of R that contains K, the corresponding ideal of R' is the image $\varphi(I)$ in R'. If J is an ieal of R', the corresponding ideal of R is the inverse image $\varphi^{-1}(J)$.

If the ideal I of R corresponds to the ideal I' of R', then the quotient rings R/I and R'/I' are isomorphic.

Example. Let $R = \mathbb{Z}$, $R' = \mathbb{Z}/12\mathbb{Z}$, and let φ the canonical map. Ideals of R' correspond to ideals of $\mathbb{Z}$ that contain $12\mathbb{Z}$. They are generated by the divisors of 12: $1, 2, 3, 4, 6, 12$. So $\mathbb{Z}/12\mathbb{Z}$ contains six ideals.

Using the notation (a) for the principal ideal generated by an element a, the six ideals are: $(\overline{1}), (\overline{2}), (\overline{3}), (\overline{4}), (\overline{6})$, and $(\overline{12})$, which is the zero ideal.

adding a relation to a ring.

Given an element a of a ring R, one can ask to force the relation $a = 0$ in R. This is the way that the ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n is defined.

If we want to have $a = 0$, we must accept some consequences, including that $ra = 0$ for all elements r of R. So killing a fores us to kill all elements of the principal ideal $I = Ra$. Then we can form the quotient ring $\overline{R} = R/Ra$. The surjective homomorphism $R \xrightarrow{\pi} \overline{R}$ that sends an element r to the coset $r + I$ has kernel I. So $\overline{R}$ is the ring obtained by killing a. Killing a has no consequences other than $ra = 0$.

adjoining an element to a ring.

Next, we consider the problem of adding a new element to a given ring R. The model for this procedure is the construction of the complex numbers $\mathbb{C}$ from the real numbers $\mathbb{R}$ by adjoining an element i. The element i has no properties other than the equation $i^2 + 1 = 0$, and the ones implied by the ring axioms,

We can identify $\mathbb{C}$ with the quotient ring $\mathbb{R}[x]/I$ where I is the principal ideal of $\mathbb{R}[x]$ generated by $x^2 + 1$. The canonical homomorphism $\mathbb{C}[x] \xrightarrow{\pi} \mathbb{C}$ that maps x to i is surjetive, and its kernel is the principal ideal I generated by $x^2 + 1$. o if $\overline{R}$ denotes the quotient ring $\mathbb{R}[x]/I$, then π defines an isomorphism $\overline{R} \approx \mathbb{C}$. This tells us how to make such a construction more generally.

Let R be a ring, and let $f(x)$ be a polynomial in $R[x]$ with coefficients in R. To adjoin an elmeent α to R with the equation $f(\alpha) = 0$, one forms the quotient $R' = R[x]/(f)$ of the polynomial ring $R[x]$, modulo the principal ideal $(f) = Rf$ generated by f. The residue of x is the new element α.

Does the residue of x in $R' = R[x]/(f)$ does satisfy the relation $f(\alpha) = 0$? Say that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. The canonical map $R[x] \xrightarrow{\pi} R'$ has $f(x)$ in its kernel, and it is a homomorphism. Let's write the image $\pi(z)$ of an element z of $R[x]$ as $\overline{z}$. So in particular, $\overline{x} = \alpha$. Then $\overline{f} = 0$, and

$$\overline{a}_n\alpha^n + \overline{a}_{n-1}\alpha^{n-1} + \cdots + \overline{a}_0 = \overline{a}_n\overline{x}^n + \overline{a}_{n-1}\overline{x}^{n-1} + \cdots + \overline{a}_0 = \overline{f} = 0$$

are $\overline{a}_i$ are the images of the coeficients a_i in R', and if we are able to identify R with its image in R', i.e., if the restriction of π to the constant polynomials is injective, we will have

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

as desired. This will work in most cases of interest, though it is possible that the desired equation $f(\alpha) = 0$ is so bad that it kills some constant polynomials.

The simplest case is that the; polynomial $f(x)$ is monic, i.e., that $a_n = 1$. In that case, R' will have an R-basis $1, \alpha, ..., \alpha^{n-1}$. Every element of R' can be written in a unique way as a combination of this basis with coefficients in R. In particular, the map $R \to R'$ is injective.

Things become more complicated when f isn't monic. For example, let $f(x) = ax - 1$. In this case, we will have $a\alpha = 1$, i.e., α is an inverse of the element a. The ring R' can be described as the ring obtained by adjoining an inverse of the element a. So far, so good. However, there doesn't seem to be any restriction on the element a. We seem to be able to adjoin an inverse of the element 0, though we are told never to invert 0.

What happens is that the equation $f(\alpha) = 0$ becomes $0\alpha - 1 = 0$, which simplifies to $1 = 0$. The resulting ring R' is $R[x]/(1)$. However, the principal ideal (1) generated by 1 is the whole ring. Therefore $R' = R/(1) = \{0\}$. Yes, we can invert 0, but doing so gives us the zero ring.

Some terminology.

A *zero divisor* a in a ring R is a nonzero element such that, for some other nonzero element b, the product ab is zero.

A nonzero ring that has no zero divisors is called a *domain*, or elsewhere, an *integral domain*.

An ideal P of a ring R is a *prime ideal* if it satisfies any one of the following three equivalent conditions:

(1) If a and b are elements o R, and if the produt ab is in P, then a is in P or b is in P (or both).

(2) If A and B are ideal of R, and if the product ideal AB is contained in P, then $A \subset P$ or $B \subset P$.

(3) The quotient ring $\overline{R} = R/P$ is a domain.

Let's check that (1) implies (2). Say ideals A and B are given, and that $AB \subset P$. If $B \subset P$, OK. Else there is an element $b \in B$ that isn't in P. But $Ab \subset AB \subset P$. Therefore ab is in P for every a in A. By (1), a or b is in P, and since b isn't in P, $a \in P$ for every a in A. So

A *maximal ideal* M of a ring R is an ideal that satisfies one of th following equivalent conditions:

(1) M isn't the unit ideal, $M < R$, but such that there is no ideal I such that $M < I < R$.

(2) The quotient ring $\overline{R} = R/M$ is a field.

So, M is a maximal element among ideals different from the unit ideal.

The fact that these conditions are equivalent follows from the next, rather trivial, lemma:

Lemma. A ring R is a field if and only if it contains exactly two ideals, the zero ideal and the unit ideal.

proof. If R is a field, and if I is any nonzero ideal of R, then I contains a nonzero element a, which will have an inverse in the field. Then I contains $1 = a^{-1}a$, so I is the unit ideal. Conversely, suppose that R contains precisely two ideals. Those ideals are the zero ideal and the unit ideal R. Then if a is a nonzero element, the principal ideal Ra isn't zero, so it is the unit ideal, which means that there is an r in R such that $ra = 1$. That element is the inverse of a. So every nonzero element has an inverse, and R is a field. □

The nonzero prime ideals of the ring $\mathbb{Z}$ of integers are also the maximal ideals, the ones generated by prime integers. The same is true of the polynomial ring $F[x]$, when F is a field. However, in the ring $R = \mathbb{C}[x, y]$ the prime ideals are the ones generated by irreducible polynomials such as $y^2 - x^3 + x$, polynomials that cannot be factored. Thse are not maximal ideals.

The maximal ideals are described by Hilbert's Nullstellensatz.

Let R be the polynomial ring $\mathbb{C}[x_1, ..., x_n]$ in n variables, and let $p = (a_1, ..., a_n)$ be a point of complex n-space $\mathbb{C}^n$. One can evaluate polynomials at p. This gives us a homomorphism $R \xrightarrow{\pi_p} \mathbb{C}$: $\pi_p(f(x_1, ..., x_n)) = f(p) = f(a_1, ..., a_n)$, evaluation at p. Its kernel, the set of polynomials such that $f(a_1, ..., a_n) = 0$, is the ideal thatg we denote by $\mathfrak{m}_p$ that is generated by the linear polynomials $x_1 - a_1, ..., x_n - a_n$. Every polynomial $f(x)$ such that $f(a) = 0$ can be written as a combination of those linear polynomials, with polynomial coefficients. You can check this by writing down the Taylor's expansion of $f(x)$, which is a polynomial.

Since π_p is obviously surjective, we have an isomorphism isomorphism $\overline{R} = R/\mathfrak{m}_p \approx \mathbb{C}$. Since $\mathbb{C}$ is a field, $\mathfrak{m}_p$ is a maximal ideal. Hilbert's Nullstellensatz asserts that the ideal $\mathfrak{m}_p$ are all of the maximal ideals of $\mathbb{C}[x_1, ..., x_n]$.

It tells us, among other things, that there are no other "secret" points at which one can evaluate a polynomial.

Nullstellensatz. The maximal ideals of $R = \mathbb{C}[x_1, ..., x_n]$ are the kernels $\mathfrak{m}_p$ of the evaluation maps, for $p \in \mathbb{C}^n$.

proof. Let M be a maximal ideal of R, let F be the field R/M, and let $R \xrightarrow{\varphi} F$ be the canonical map from R to its quotient ring F. The restriction of φ to the field $\mathbb{C}$ of constant polynomials is injective because $\mathbb{C}$ is field. It maps $\mathbb{C}$ isomorphically to a subfield of F that we enote by $\mathbb{C}$ too.

We plan to show that $\mathbb{C} = F$. If so, then the images of the variables x_i will be complex numbers a_i, and $x_i - a_i$ will be in the kernel of φ. Since the polynomials $x_i - a_i$ generate the maximal ideal $\mathfrak{m}_p$ described above, we will have $M = \mathfrak{m}_p$.

We choose an index i, and relabel the variable x_i as x. Then we restrict the homomorphism φ to the subring $\mathbb{C}[x]$, obtaining a homomorphism $\mathbb{C}[x] \xrightarrow{\psi} F$. The image of this map is a subring of F, so it is a domain, and therefore the kernel of ψ is a prime ideal of $\mathbb{C}[x]$. The prime ideals are: the zero ideal, and the maximal ideals generated by linear polynomials $x - a$. If we show that the kernel isn't the zero ideal, it will follow that x is mapped to some complex number a. Then all the variables are mapped to elements of $\mathbb{C}$, and therefore the image of φ is simply $\mathbb{C}$, as we wanted to show.

Suppose that the kernel of ψ is the zero ideal, so that $\mathbb{C}[x]$ is mapped isomorphically to its image, a subring of F, Then F contains $\mathbb{C}[x]$, and since F is a field, it contains inverses of all polynomials, in particular it contains $1/(x - a)$ for every a

Now: As a runs over the complex numbers, the polynomials $1/(x - a)$ are linearly independent. You will be able to check that there is no nontrivial relation $\sum_1^n c_i/(x - a_i) = 0$ with distinct complex numbers a_i and with complex coefficients c_i. A simple reason is this: Near to one of the points a_i, $1/(x - a_i)$ gets large, while $1/(x - a_j)$ remains bounded for all $a_j \neq a_i$.

On the other hand, the field F is the image of the polynomial ring $\mathbb{C}[x_1, ..., x_n]$, and that polynomial ring has a countable basis consisting of the monomials: $1; x_1, ..., x_n; x_1^2, x_1x_2, ...$ So F is spanned by the images of the monomials, a countable set. A vector space that is spanned by a countable set cannot contain uncountably many independent elements. Thus it is impossible that $\mathbb{C}[x]$ is mapped injectively to F, and this completes the proof. $\square$