Polynomial rings and their quotients

Given a ring R and an ideal I, we've seen many occurrences of the *quotient ring*

$$A = R/I.$$

Since R has in particular the structure of an abelian group and an ideal is a subgroup (which is automatically normal (why?)) the quotient group R/I has already been studied in group theory. The definition of an ideal in fact imposes on the subgroup I exactly the condition necessary to put a ring structure on R/I. That is to say, the quotient ring is just the quotient group, with a natural multiplication induced by the multiplication of R.

Among the very important examples of this construction are quotients of polynomial rings

$$B[x_1, x_2, \ldots, x_n]/(f_1, \ldots, f_m)$$

where the ideal

$$(f_1, \ldots, f_m)$$

is specified simply by a collection of generators $f_i \in B[x_1, \ldots, x_n]$. Polynomial rings of many variables have probably not been dealt with much in your courses so far, but we have, in this course, studied extensively the cases

$$\mathbb{Q}[x]/(f(x))$$

and

$$\mathbb{Z}[x]/(m(x))$$

coming from one variable.

The main point I wish to make in this note is that

it is often convenient to express a ring as a quotient of a polynomial ring

even when it's not a priori given that way. This is because the structure of a polynomial ring is rather transparent, so that expressing some other ring as its quotient can simplify many computations. Say we consider a number field like

$$\mathbb{Q}(\zeta_5)$$

where $\zeta_n = \exp(2\pi i/n)$. Because the minimal polynomial of ζ_5 is $m(x) = x^4 + x^3 + x^2 + x + 1$, we get

$$\mathbb{Q}(\zeta_5) \simeq \mathbb{Q}[x]/(m(x))$$

and we can use this fact, for example, to construct the multiplication table for the field in a clear cut manner. Try this out yourself. This presentation is quite important in computer programs that work with such an algebraic number field, in which the field $\mathbb{Q}(\zeta_5)$ would essentially be described as $\mathbb{Q}^4$ with a multiplication induced by the isomorphism

$$\mathbb{Q}^4 \simeq \mathbb{Q}[x]/(x^4 + x^3 + x^2 + x + 1)$$

I am calling this a presentation because it is entirely analogous to the procedure of writing a group as a quotient of a free group, except it's actually more useful.(One of the bitter but interesting lessons of sophisticated group theory is that free groups are rather complicated.)

The key point of Dedekind's factorization theorem is exactly that the rings of integers that occur in it are quotients of polynomial rings in a *single* variable. In fact, for $K = \mathbb{Q}(\zeta_5)$, the fact that $\mathcal{O}_K = \mathbb{Z}[\zeta_5]$ is exactly saying that $\mathcal{O}_K \simeq \mathbb{Z}[x]/(m(x))$. Let me pause here to clarify one point that came up in the questions on the blog. When we write

$$\mathbb{Z}[\zeta_5]$$

this refers to the subring of $\mathbb{C}$ generated by ζ_5. But when we write

$$\mathbb{Z}[x]$$

the x is an abstract variable, not a definite number. Of course, confusion can arise from the existence of an isomorphism

$$\mathbb{Z}[x]/(m(x)) \simeq \mathbb{Z}[\zeta_5]$$

that takes x to ζ_5. To see one aspect of the distinction, note that $m(x) \neq 0$ in $\mathbb{Z}[x]$, but $m(\zeta_5) = 0$ in $\mathbb{Z}[\zeta_5]$. So the ideal $m(\zeta_5)$ in $\mathbb{Z}[\zeta_5]$ is just the zero ideal.

One application of this view is when computing (further) quotient rings. If we have

$$a_1, a_2, \ldots, a_n \in A$$

and $A = R/I$ where I is the ideal generated by $r_1, \ldots, r_m$, then we can express the quotient

$$A/(a_1, a_2, \ldots, a_n)$$

as a quotient ring of R. The formula is

$$A/(a_1, a_2, \ldots, a_n) \simeq R/(\tilde{a}_1, \tilde{a}_2, \ldots, \tilde{a}_n, r_1, r_2, \ldots, r_m)$$

where the $\tilde{a}_i$ are 'lifts' of the a_i, that is, $\tilde{a}_i$ is any element of R such that its class in $A = R/I$ is a_i. At first glance, this may seem to complicate the problem. But when R is a relatively easy ring like a polynomial ring, the problem may actually simplify considerably. The point is that we are relating the ideal $(a_1, a_2, \ldots, a_n)$ to the more complicated-looking ideal $(\tilde{a}_1, \tilde{a}_2, \ldots, \tilde{a}_n, r_1, r_2, \ldots, r_m)$, but which lies inside a ring R that we can sometimes choose to be simpler than A.

We've seen many examples of this nature, but let's repeat one for the sake of review. Suppose $K = \mathbb{Q}(i)$ so that $\mathcal{O}_K = \mathbb{Z}[i]$. Let J be the ideal $(5, 1+i)$. How can we compute $N(J)$? Of course we need to analyze the ring $\mathcal{O}_K/J$. But

$$\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(x^2+1).$$

This isomorphism is induced by the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}[i]$ that takes $f(x)$ to $f(i)$. So a lift of $1+i$ is $1+x$ while $5 \in \mathbb{Z}[x]$ is a lift of $5 \in \mathbb{Z}[i]$. Hence,

$$\mathbb{Z}[i]/(5, 1+i) \simeq \mathbb{Z}[x]/(5, 1+x, x^2+1)$$

But we can then take the quotient by (5) first so that

$$\mathbb{Z}[x]/(5, 1+x, x^2+1) \simeq \mathbb{F}_5[x]/(1+x, x^2+1)$$

Now taking the quotient by $(1+x)$ first, we find that

$$\mathbb{F}_5[x]/(1+x) \simeq \mathbb{F}_5$$

by the map that takes $f(x)$ to $f(-1)$. This map takes x^2+1 to $2 \in \mathbb{F}_5$. So we get

$$\mathbb{F}_5[x]/(1+x, x^2+1) \simeq \mathbb{F}_5/(2) = 0$$

since $2 \in \mathbb{F}_5$ is invertible. This tells us that

$$\mathbb{Z}[i]/(5, 1+i) = 0$$

and $N(J) = 1$.

Similarly, we can compute $N(I)$ for $I = (1+i)$:

$$\mathbb{Z}[i]/(1+i) \simeq \mathbb{Z}[x]/(1+x, x^2+1) \simeq \mathbb{Z}/(1+1) = \mathbb{Z}/2$$

so that $N(I) = 2$. (Explain to yourself the second isomorphism.)

In Dedekind's factorization theorem, we have a situation where $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some algebraic integer α. This means

$$\mathcal{O}_K \simeq \mathbb{Z}[x]/(m(x))$$

where $m(x)$ is the minimal polynomial of α. We compute the factorization of the ideal (p) is $\mathcal{O}_K$ by using the factorization

$$m(x) \equiv m_1(x)^{e_1} \cdots m_s(x)^{e_s} \qquad \mod p$$

of $m(x)$ in $\mathbb{F}_p[x]$ into irreducible polynomials $m_i(x)$. Then we get

$$(p) = P_1^{e_1} \cdots P_s^{e_s}$$

with $P_i = (p, \tilde{m}_i(\alpha))$, where $\tilde{m}_i(x) \in \mathbb{Z}[x]$ are any polynomials lifting the $m_i(x)$ in $\mathbb{F}_p[x]$. (In practice, we tend, somewhat confusingly but naturally, to use the same notation for $\tilde{m}_i$ and m_i because, for example, the polynomial

$$x^2 + 5x + 1$$

would be denoted the same way in $\mathbb{Z}[x]$ or $\mathbb{F}_{11}[x]$.) Anyways, to check that the P_i are indeed maximal ideals we compute

$$\mathcal{O}_K/P_i = \mathbb{Z}[\alpha]/P_i \simeq \mathbb{Z}[x]/(p, \tilde{m}_i(x)) \simeq \mathbb{F}_p[x]/(m_i(x))$$

and note that the last ring is a field since $m_i(x) \in \mathbb{F}_p[x]$ is assumed to be irreducible.