Example. $R[x, y]$ is a polynomial ring over R in two commuting indeterminates, x and y that satisfies

$$(x^i y^j)(x^k y^l) = x^{i+k} y^{j+l}$$

and distributivity.

Note. Noncommutative indeterminates version is denoted $R\langle x, y\rangle$.

We can thin of $R[x, y]$ as $(R[x])[y]$ or as $(R[y])[x]$. For example, in $\mathbb{Z}[x, y]$:

$$\begin{aligned} 5 + 6y - 3xy^2 + 2x^3y - 7x^2y^2 + 4x &\in \mathbb{Z}[x, y] \\ (5 + 4x) + (6 + 2x^3)y - (3x + 7x^2)y^2 &\in (\mathbb{Z}[x])[y] \\ (5 + 6y) + (4 - 3y^2)x - (7y^2)x^2 + 2y(x^3) &\in (\mathbb{Z}[y])[x] \end{aligned}$$

Theorem

$R = F[x]$, F is a field, $f(x), g(x) \in F[x]$. There exist unique $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r < \deg g$.

Proof

Uniqueness: Suppose

$$\begin{aligned} q_1(x)g(x) + r_1(x) &= q_2(x)g(x) + r_2(x) \\ (q_1(x) - q_2(x))g(x) &= r_2(x) - r_1(x) \end{aligned}$$

Notice the LHS is zero polynomial or has degree $\geq \deg g$, and the RHS is either zero polynomial or has degree $< \deg g$. The only way they can equal is to be both zero polynomial. Thus they are unique. □

Theorem: Factor Theorem

$f(x) \in F[x], a \in F$. a is a root of $f(x)$ if and only if $(x - a)$ is a factor of $f(x)$. That is,

$$f(x) = (x - a)h(x), h(x) \in F[x].$$

We have $\deg f = 1 + \deg h$.

Proof

Use division algorithm with $f(x)$ and with $g(x) = x - a$:

$$f(x) = q(x)(x - a) + r(x).$$

where $r(x) = 0$ or $\deg r < \deg(x - a)$ which means $r(x)$ is a nonzero constant.

Thus we get

$$f(x) = q(x)(x - a) + c.$$

Consider $\phi_a : F[x] \to F$. So

$$\phi_a(f(x)) = \phi_a(q(x)(x - a) + c)$$
$$f(a) = q(a)(a - a) + c$$

There are two cases.

Case. $c = 0$, then $f(a) = 0$ and $f(x) = q(x)(x - a)$.

Case. $c \neq 0$, then $f(a) \neq 0$ and $f(x) = q(x)(x - a) + c$. Here a is not a root and c is a nonzero remainder.

□

Corollary: 23.6

Let F be a field and F^* be its group of units. Any finite subgroup of F^* is cyclic.

Proof

Let G be a finite subgroup of F^*. Then $G \simeq \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r}$, where d_i are prime powers. Let $m = \operatorname{lcm}(d_1, \ldots, d_r)$, thus $m \leq d_1 \cdot \ldots \cdot d_r$. In $\mathbb{Z}_d, a_i^{d_i} = 1 \Rightarrow a_i^m = 1$ because d_i/m. This means $a^m = 1$ for any $a \in G$. So every element is a root of $x^m - 1 \in F[x]$, and there are at most m such roots by factor theorem and induction. Since $d_1 \cdot \ldots \cdot d_r$ is the order of G and every element of G is such root, and there are at most m of them in F, we have $d_1 \cdot \ldots \cdot d_r \leq m$. Hence, $m = d_1 \cdot \ldots \cdot d_r$. Since the d_i are relatively prime, then the direct product is cyclic. □

Note (important special case). If F is a finite field, then F^* is cyclic. For example, $\mathbb{Z}_{11}^*$ is cyclic of order 10. Q2 Section 20.

2 is a generator for $\mathbb{Z}_{11}^*$. Since $\mathbb{Z}_{11}^* \simeq (\mathbb{Z}_{10}, +_{10})$. Then the possible orders of elements are 1,2,5,10. Since 2 is not order 1,2,5, it must be order 10. Thus 2 is a primitive root.

How many generators does $\mathbb{Z}_{10}$ have? 1,3,7,9. They are pairs of inverses. So we start from 2 and find them: $2 \to 8 \to 7 \to 6$. 8 is cube of 2, 7 is inverse of cube, 6 is inverse of 2.

Example (23.4)**.** $x^4 + 3x^3 + 2x + 4 \in \mathbb{Z}_5[x]$. We can see that 1 is a root of $f(x) \in \mathbb{Z}_5$. To factor, we can do it by tacking the easy terms first. But this isn't always feasible.

We get $(x-1)(x^3+4x^2-x+1)$. Now does x^3+4x^2+4x+1 have any roots in $\mathbb{Z}_5$? We can find them exhaustively. So 1 is a root, and we get $(x-1)(x-1)(x+1)$. So

$$f(x) = (x-1)^3(x+1).$$

Definition: irreducible

Let R be a ring with 1. $f(x) \in R[x]$ is **irreducible** if

(i) $f(x)$ is not zero or a unit.

(ii) If $f(x) = g(x)h(x)$ then either $g(x)$ or $h(x)$ is a unit.

Note. $3x + 3 \in \mathbb{Z}[x]$ is not irreducible, since units in $\mathbb{Z}$ are ± 1 so we can factor $3(x + 1)$. This works because $\mathbb{Z}$ is not a field.