27. Fields from quotient rings

In Lecture 26 we have shown that the quotient ring $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ is isomorphic to $\mathbb{C}$, so, in particular, it is a field, while $\mathbb{R}[x]/(x^2-1)\mathbb{R}[x]$ is not a field. The reason we did not get a field in the second case is clear: the polynomial x^2-1 is reducible, that is, has a non-trivial factorization $x^2-1=(x-1)(x+1)$, and we have seen in the proof from Example 3 that the existence of factorization $(x-1)(x+1)$ is what prevents $\mathbb{R}[x]/(x^2-1)\mathbb{R}[x]$ from being a field. On the other hand, x^2+1 is irreducible, although it is not clear how to deduce that $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ is a field just from the irreducibility of x^2+1.

In this lecture we will settle the latter issue: we will show that if F is any field and $p \in F[x]$ is a polynomial, the the quotient ring $F[x]/pF[x]$ is a field $\iff$ p is irreducible.

27.1. **Basic definitions.**

Definition. Let F be a field and $p \in F[x]$ a polynomial with coefficients in F. Then p is called <u>irreducible</u> if

(i) p is non-constant, or, equivalently, $\deg(p) > 0$;
(ii) p does not have non-trivial factorizations, that is, p cannot be written as $p = gh$ where $g, h \in F[x]$ and both g and h are non-constant.

Remark: Irreducible polynomials are direct counterparts of prime integers. The convention not to consider constant polynomials as irreducible corresponds to the convention not to consider 1 as a prime number. As we will see shortly, the analogy between prime integers and irreducible polynomials goes well beyond the definition.

Definition. Let F be a field and $p \in F[x]$ a polynomial with coefficients in F. Then p is called <u>monic</u> if the leading coefficient of p is equal to 1.

Next we define the greatest common divisor for polynomials.

Definition. Let F be a field and $f, g \in F[x]$ two polynomials. A polynomial $d \in F[x]$ is called the greatest common divisor (gcd) of f and g if the following conditions hold:

(i) d is monic
(ii) d divides both f and g

(iii) If $h \in F[x]$ is another polynomial which divides both f and g, then h divides d.

Remark: If $u, v \in F[x]$ are two polynomials, we say that v divides u if $u = vw$ for some polynomial $w \in F[x]$.

27.2. **Main theorems.**

Theorem 27.1 (GCD Theorem for polynomials)**.** *Let F be a field and $f, g \in F[x]$ two polynomials, not both of which are equal to 0. The following hold:*

(1) *The greatest common divisor of f and g exists and unique. It is denoted by $gcd(f, g)$*
(2) *There exist $u, v \in F[x]$ s.t. $gcd(f, g) = fu + gv$.*
(3) *Let $I = \{p \in F[x] : p = fu + gv \text{ for some } u, v \in F[x]\}$. Then $gcd(f, g)$ is the unique monic polynomial in I of smallest possible degree.*
(4) *The set I from (3) is an ideal of $F[x]$ and coincides with $gcd(f, g)F[x]$, the principal ideal generated by $gcd(f, g)$.*

Proof. The proof is analogous to the proof of GCD theorem for integers. The key tool in the proof is Theorem 26.1 (long division of polynomials). □

Theorem 27.2. *Let F be a field and $f \in F[x]$. Let $R = F[x]$ and $I = fF[x]$. Then the quotient ring R/I is a field $\iff$ f is irreducible.*

Remark: Theorem 27.2 is a direct analogue of the following theorem we proved in Lecture 8: if n is an integer, then $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ is a field $\iff$ n is prime.

Proof. As in the previous lecture, we use the shortcut notation $[k] = k + I$ for $k \in F[x]$.

The quotient ring R/I is always commutative and has unity (since $R = F[x]$ is commutative and has unity). Therefore, R/I is a field if and only if

(a) every nonzero element of R/I is invertible and
(b) $[0] \neq [1]$ in R/I.

"$\Leftarrow$" Suppose that f is irreducible. Any nonzero element of R/I is equal to $[k]$ for some $k \in F[x]$ which is not divisible by f. Since f is irreducible and f does not divide k, we must have $gcd(f, k) = 1$, and therefore, by Theorem 27.1(2) there exist $u, v \in F[x]$ s.t. $fu + kv = 1$.

Since $fu \in I$, we have $[fu] = [0]$. Therefore,

$$[k][v] = [kv] = [1 - fu] = [1] - [fu] = [1] - [0] = [1],$$

which shows that $[v]$ is the inverse of $[k]$, so $[k]$ is invertible. Thus, we verified condition (a).

Condition (b) is clear (by contradiction): if $[0]$ was equal to $[1]$, then 1 would have been a multiple of f, which is impossible since f is non-constant.

"$\Rightarrow$" We prove this by contrapositive. Suppose that f is not irreducible. Then by definition either f is constant or f is a product of two non-constant polynomials.
Case 1: $f = 0$. Then $I = \{0\}$, so $R/I \cong R = F[x]$, which is clearly not a field.
Case 2: f is a nonzero constant. Then it is easy to see that $I = R$, so $R/I = R/R$ is the zero ring, consisting of just one element (which is both $[0]$ and $[1]$). Therefore, $[0] = [1]$, so condition (b) does not hold and R/I is not a field.
Case 3: $f = gh$ where g and h are non-constant polynomials. Then $\deg(g) < \deg(f)$ and $\deg(h) < \deg(f)$, so g and h are not multiples of f and therefore $[g] \neq [0]$ and $[h] \neq [0]$. On the other hand, $[g][h] = [gh] = [f] = [0]$. Therefore, R/I has a zero divisor, namely $[g]$, and therefore cannot be a field. □

27.3. **Constructing finite fields of non-prime order.** So far we only know how to construct finite fields of prime order: we know that if p is any prime, then $\mathbb{Z}_p$ is a field of order p. Using quotients rings of the form discussed above, one can construct finite fields of any prime-power order, that is, order p^k where p is a prime and $k \geq 1$ is an arbitrary integer.
We shall explain in detail how to construct fields of order p^2 and then briefly state how to get fields of order p^k for any k.

Lemma 27.3. *Let F be a field and $q \in F[x]$ a quadratic polynomial, that is, $q = ax^2 + bx + c$ where $a, b, c \in F$ and $a \neq 0$. Let $R = F[x]$ and $I = qR$. Then*

(i) *For every element $[f] \in R/I$ there exist unique $a, b \in F$ s.t. $[f] = [ax + b]$.*
(ii) *Assume that $F = \mathbb{Z}_p$ for some prime p. Then $|R/I| = p^2$.*

Proof. (i) is proved by the same argument as Lemma 26.1 from last time.

(ii): by part (i), $|R/I|$ is equal to the number of polynomials $ax + b$, with $a, b \in \mathbb{Z}_p$. There are p choices for a and p choices for b, so overall there are p^2 choices. □

Combining Theorem 27.2 and Lemma 27.3, we deduce the following:

Corollary 27.4. *Let p be a prime, and let $q = ax^2 + bx + c \in \mathbb{Z}_p[x]$ be a quadratic polynomial with coefficients in $\mathbb{Z}_p$. Assume that q is irreducible. Then $\mathbb{Z}_p[x]/q\mathbb{Z}_p[x]$ is a field of order p^2.*

So, to construct a field of order p^2 it suffices to find a quadratic irreducible polynomial in $\mathbb{Z}_p[x]$.

Lemma 27.5. *Let F be a field and $q = ax^2 + bx + c \in F[x]$ a quadratic polynomial which does not have any roots in F. Then q is irreducible.*

Proof. Assume that q is not irreducible. Since $\deg(q) = 2 > 0$, q is non-constant, so q has a factorization $q = gh$ with g and h non-constant. Then $\deg(g) + \deg(h) = \deg(q) = 2$. Thus we must have $\deg(g) = \deg(h) = 1$, so $g = \alpha x + \beta$ and $h = \gamma x + \delta$ for some $\alpha, \beta, \gamma, \delta \in F$, with $\alpha, \gamma \neq 0$. Then

$$q(-\alpha^{-1}\beta) = g(-\alpha^{-1}\beta)h(-\alpha^{-1}\beta) = 0 \cdot h(-\alpha^{-1}\beta) = 0,$$

so q has a root $-\alpha^{-1}\beta \in F$, contrary to our assumption. □

Thus, we are now reduced to showing that for every prime p, there exists an irreducible quadratic polynomial in $\mathbb{Z}_p[x]$.

Case 1: $p > 2$. As we proved in Lecture 9, there are precisely $\frac{p+1}{2}$ elements of $\mathbb{Z}_p$ which are representable as a square. Since $\frac{p+1}{2} < p$, there exists $[d] \in \mathbb{Z}_p$, which is not a square. Hence $x^2 - [d]$ is a quadratic polynomial with no roots we were looking for.

Case 2: $p = 2$. We claim that $q = x^2 + x + [1] \in \mathbb{Z}_2[x]$ has no roots – indeed, $\mathbb{Z}_2$ has only two elements $[0]$ and $[1]$, and by direct check we have $q([0]) = [1] \neq [0]$ and $q([1]) = 3 \cdot [1] = [1] \neq [0]$.

Summarizing, we proved the following:

Theorem 27.6.

(1) *Let p be a prime, and let $[d] \in \mathbb{Z}_p$ be any element which is not a square. Then the quotient ring $\mathbb{Z}_p[x]/(x^2 - [d])\mathbb{Z}_p[x]$ is a field of order p^2.*

(2) *The quotient ring $\mathbb{Z}_2[x]/(x^2 + x + [1])\mathbb{Z}_2[x]$ is a field of order 4.*

Exercise: Find a suitable value of $[d]$ for $p = 3, 5$ and 7.

Finally, we briefly comment on the construction of a field of order p^k. By the same logic as above if $q = a_k x^k + \ldots + a_0 \in \mathbb{Z}_p[x]$ is an irreducible polynomial of degree k with coefficients in $\mathbb{Z}_p$, then $\mathbb{Z}_p[x]/q\mathbb{Z}_p[x]$ is a field of order p^k.

Even though there is no simple recipe which produces an irreducible polynomial of degree k in $\mathbb{Z}_p[x]$ for every prime p and integer $k \geq 1$, using a clever counting argument, one can show that such polynomial always exists (for every p and k). Thus, for every p and k there exists a field of order p^k.

Using some basic tools from linear algebra, one can show that these are the only possible orders of finite fields, that is, every finite field has order p^k for some prime p. For instance, there is no field of order 6.

Finally, using more advanced tools from field theory one shows that for every prime p and $k \geq 1$, a field of order p^k is unique up to isomorphism.