LECTURE 14: MORE POLYNOMIAL THEORY

E1

Example 4.6.7. *Consider $f(x) = x^4+14x^2+49 = (x^2+7)^2$ thus $f(x)$ is reducible over $\mathbb{R}$ yet $f(x)$ has no zeros in $\mathbb{R}$. At fourth order we lose the necessary connection between zeros and reducibility.*

The next few theorems we consider are probably new to most students in this course.

Definition 4.6.8. *The* **content** *of a nonzero polynomial $a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ is the $gcd(a_0, a_1, \ldots, a_n)$. If the content of $f(x) \in \mathbb{Z}[x]$ is 1 then we say $f(x)$ is a* **primitive polynomial**.

Gallian calls this Gauss's Lemma. That doesn't seem overly descriptive given Gauss's work.

Example 4.6.9. *Let $f(x) = 3x+6$ then the content of $f(x)$ is $gcd(3, 6) = 3$. Notice, $f(x) = 3(x+2)$ and $x+2$ is primitive as $gcd(1, 2) = 1$. Any monic polynomial is primitive, $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ has $gcd(1, a_{n-1}, \ldots, a_1, a_0) = 1$. The idea of the content is to find that integer which naturally factors out of a polynomial in $\mathbb{Z}[x]$. Of course, $3x^2 + 5x + 7$ is also primitive since its coefficients are relatively prime. We can't factor out an integer $n > 1$ from a primitive polynomial.*

Theorem 4.6.10. *The product of two primitive polynomials is primitive.*

Proof: we follow Gallian's argument on page 297. Suppose $f(x), g(x) \in \mathbb{Z}[x]$ are primitive and $f(x)g(x)$ is not primitive. If p is a prime divisor of the content of $f(x)g(x) = ph(x)$ then consider the polynomials $\overline{f(x)}, \overline{g(x)} \in \mathbb{Z}_p[x]$ formed by reducing the coefficients of $f(x), g(x)$ respective. Observe,

$$0 = \overline{ph(x)} = \overline{f(x)} \cdot \overline{g(x)}$$

Thus, as $\mathbb{Z}_p[x]$ is an integral domain, $\overline{f(x)} = 0$ or $\overline{g(x)} = 0$. It follows p divides $f(x)$ or $g(x)$ thus $f(x)$ or $g(x)$ is not primitive. Hence, by proof by contradiction, $f(x)g(x)$ is primitive. □

A concept is used in the proof above which merits some discussion. If $\phi : R \to S$ is a ring homomorphism then there is a natural homomorphism $\psi : R[x] \to S[x]$ induced by mapping the coefficients of R to corresponding coefficients of S. In particular,

$$\Psi(a_nx^n + \cdots + a_1x + a_0) = \phi(a_n)x^n + \cdots + \phi(a_1)x + \phi(a_0)$$

for each $a_nx^n + \cdots + a_1x + a_0 \in R[x]$. In the proof for the primitive product theorem we used the natural homomorphism $\phi(k) = [k]_p$ where $\phi : \mathbb{Z} \to \mathbb{Z}_p$ to induce $\psi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Our notation was $\overline{f(x)}$ for $\psi(f(x))$. We continue to use such induced homomorphisms of polynomials in many of the proofs and examples we soon consider, often without explicit mention.

Theorem 4.6.11. *Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$ then it is reducible over $\mathbb{Z}$.*

Proof: Let $f(x) \in \mathbb{Z}[x]$ be monic[7]. Also, suppose there exist $h(x), g(x) \in \mathbb{Q}[x]$ with $f(x) = h(x)g(x)$. Suppose a is the least common multiple of the denominators of the coefficients in $h(x)$ and let b be the least common multiple of the denominators in $g(x)$. It follows $ah(x), bg(x) \in \mathbb{Z}[x]$ and $abf(x) = ah(x) \cdot bg(x)$. If c_h is the content of $ah(x)$ and c_g is the content of $bg(x)$ then there are primitive polynomials $g_1(x), h_1(x)$ for which $bg(x) = c_gg_1(x)$ and $ah(x) = c_hh_1(x)$. Observe,

$$abf(x) = ah(x) \cdot bg(x) = c_gg_1(x) \cdot c_hh_1(x) = c_hc_gh_1(x)g_1(x)$$

note $h_1(x)g_1(x)$ is primitive as it is the product of primitive polynomials. Thus the content of $abf(x)$ precisely c_hc_g. But, $f(x)$ is monic thus ab is the content of $abf(x)$. Hence, $ab = c_hc_g$ and it follows

[7] a polynomial is monic if it has a leading coefficient of 1

$f(x) = h_1(x)g_1(x)$ where $h_1(x), g_1(x) \in \mathbb{Z}[x]$. In summary, for monic $f(x) \in \mathbb{Z}[x]$ if $f(x) = h(x)g(x)$ for some $h(x), g(x) \in \mathbb{Q}[x]$ then there exist $h_1(x), g_1(x) \in \mathbb{Z}[x]$ for which $f(x) = h_1(x)g_1(x)$ with $\deg(h(x)) = \deg(h_1(x))$ and $\deg(g(x)) = \deg(g_1(x))$. If $f(x) \in \mathbb{Z}[x]$ is not monic then we can factor out the content c of $f(x)$ to write $f(x) = cf_1(x)$ where $f_1(x)$ is primitive. If $f(x)$ is reducible over $\mathbb{Q}$ then it follows $f_1(x)$ is reducible hence by our argument for primitive polynomials $f_1(x)$ is reducible over $\mathbb{Z}$ and consequently $f(x) = cf_1(x)$ is reducible over $\mathbb{Z}$ as well. □

E2

Example 4.6.12. *Consider,* $f(x) = 6x^2 + 19x - 7$ *notice*

$$f(x) = 6x^2 + 19x - 7 = 6(x^2 + (19/6)x - 7/6) = 6(x + 7/2)(x - 1/3)$$

hence $f(x) = (2x + 7)(3x - 1)$. *If we can reduce* $f(x) \in \mathbb{Z}[x]$ *using* $\mathbb{Q}$ *then the reduction transfers nicely back to* $\mathbb{Z}[x]$. *Pragmatically, in this example, it's way easier to just see that* $f(x) = (2x + 7)(3x - 1)$ *from the outset.*

Gauss taught us that modular arithmetic gives great insight into ordinary integer arithmetic. Here is a prime example of such indirect reasoning. Notice p could be any prime.

Theorem 4.6.13. *Let* $p \in \mathbb{Z}$ *be prime and suppose* $f(x) \in \mathbb{Z}[x]$ *has* $deg(f(x)) \geq 1$. *Consider* $\overline{f(x)}$ *the corresponding polynomial in* $\mathbb{Z}_p[x]$ *formed from* $f(x)$ *by reducing the coefficients of* $f(x)$ *modulo* p. *If* $\overline{f(x)}$ *is irreducible over* $\mathbb{Z}_p$ *and* $deg(f(x)) = deg(\overline{f(x)})$ *then* $f(x)$ *is irreducible over* $\mathbb{Q}$.

Proof: suppose $f(x) \in \mathbb{Z}[x]$ with $\deg(f(x)) \geq 1$. Furthermore, suppose $\overline{f(x)}$ is irreducible over $\mathbb{Z}_p$ and $\deg(f(x)) = \deg(\overline{f(x)})$ but $f(x)$ is reducible over $\mathbb{Q}$. Hence, by Theorem 4.6.11 there exist $g(x), h(x) \in \mathbb{Z}[x]$ with $f(x) = g(x)h(x)$ and $\deg(g(x)), \deg(h(x)) < \deg(f(x))$. Using the homomorphism of $\mathbb{Z}[x]$ and $\mathbb{Z}_p[x]$ given by $f(x) \mapsto \overline{f(x)}$ we find

$$\overline{f(x)} = \overline{g(x)} \cdot \overline{h(x)}$$

Note, since the leading coefficient might be divisible by p the degree of the induced polynomials could be smaller; $\deg(\overline{g(x)}) \leq \deg(g(x))$ and $\deg(\overline{h(x)}) \leq \deg(h(x))$. However, $\deg(f(x)) = \deg(\overline{f(x)})$ hence

$$\deg(\overline{g(x)}) \leq \deg(g(x)) < \deg(f(x)) = \deg(\overline{f(x)})$$

and

$$\deg(\overline{h(x)}) \leq \deg(h(x)) < \deg(f(x)) = \deg(\overline{f(x)})$$

hence $\overline{f(x)} = \overline{g(x)} \cdot \overline{h(x)}$ shows $\overline{f(x)}$ is reducible thus contradicting the irreducibility of $\overline{f(x)}$. Thus $f(x)$ must be irreducible given the conditions of the Theorem. □

E3

Example 4.6.14. *Consider* $f(x) = 29x^3 + 5x^2 + 2x + 1$. *Modulo 2,* $\overline{f(x)} = x^3 + x^2 + 1$ *hence*

$$\overline{f}(0) = 1 \qquad \& \qquad \overline{f}(1) = 1 + 1 + 1 = 1$$

hence $\overline{f(x)}$ *is irreducible in* $\mathbb{Z}_2[x]$ *from which we find* $f(x)$ *is irreducible over* $\mathbb{Q}$.

I used a combination of Theorems 4.6.6 and 4.6.13 to guide my logic in the above Example. I'll use Gallian's example from the paragraph on page 299.

E4

Example 4.6.15. *Consider* $f(x) = 21x^3 - 3x^2 + 2x + 8$. *Over* $\mathbb{Z}_2$ *we can factor* $\overline{f(x)} = x^3 + x^2 = x^2(x+1)$. *However, if we study the polynomial induced from* $f(x)$ *in* $\mathbb{Z}_5(x)$ *we can calculate modulo 5,* $\overline{f(x)} = x^3 + 2x^2 + 2x + 3$ *hence*

$$\overline{f}(0) = 3, \quad \overline{f}(1) = 1 + 2 + 2 + 3 = 3, \quad \overline{f}(2) = 8 + 2(4) + 2(2) + 3 = 23 = 3,$$

$$\overline{f}(3) = \overline{f}(-2) = -8 + 8 - 4 + 3 = -1, \quad \overline{f}(4) = \overline{f}(-1) = -1 + 2 - 2 + 3 = 2.$$

But, sometimes, no choice of p reveals the irreducibility. Theorem 4.6.13 only affirms irreducibility over $\mathbb{Q}$, it does not deny it.

SIDE QUEST! +10

Example 4.6.16. *Let $f(x) = x^4 + 1$. We can show that $\overline{f(x)}$ is reducible in $\mathbb{Z}_p[x]$ for* **any** *prime p. Yet, $f(x) = x^4 + 1$ is irreducible over $\mathbb{Q}$. (proof of these claims is the content of Exercise 29, which it seems likely I assign)*

There is an obvious way to trade a polynomial in $\mathbb{Q}[x]$ for a corresponding polynomial in $\mathbb{Z}[x]$. After making this correspondence we are free to use the tools at our disposal for irreducibility over $\mathbb{Q}$ for polynomials in $\mathbb{Z}[x]$.

E5

Example 4.6.17. *Let $f(x) = (3/7)x^4 - (2/7)x^2 + (9/35)x + 3/5$ the contruct the corresponding $h(x) = 35f(x) = 15x^4 - 10x^2 + 9x + 21$. It should be clear that irreducibility of $h(x)$ over $\mathbb{Q}$ is naturally tied to irreducibility of $f(x)$. Working modulo 2, $\overline{h(x)} = x^4 + x + 1$ and $\overline{h}(0) = 1$ and $\overline{h}(1) = 1 + 1 + 1 = 1$ thus $\overline{h(x)}$ has no linear factors. To search for possible quadratic factors we need only consider $x^2, x^2 + 1$, $x^2 + x$ and $x^2 + x + 1$ as there are no other quadratic factors possible in $\mathbb{Z}_2[x]$. Since x^2 and $x^2 + 1$ and $x^2 + x$ have zeros in $\mathbb{Z}_2$ it follows they cannot be factors of $\overline{h(x)}$. To see why $x^2 + x + 1$ is not a factor consider the following:*

$$(x^2 + x + 1)(x^2 + ax + b) = x^4 + x + 1$$

then $x^4 + (a + 1)x^3 + (b + a + 1)x^2 + (a + b)x + b = x^4 + x + 1$ from which we would require

$$a + 1 = 0, \quad b + a + 1 = 0, \quad a + b = 0, \quad b = 1$$

these equations are inconsistent as the first two provide $b = 0$ whereas the last gives $b = 1$. Thus $x^2 + x + 1$ does not factor $\overline{h(x)}$ and we deduce $\overline{h(x)}$ is irreducible in $\mathbb{Z}_2[x]$ thus $h(x)$ is irreducible over $\mathbb{Q}$ and hence $f(x) = \frac{1}{35}h(x)$ is irreducible over $\mathbb{Q}$.

To decide irreduciblility of quartics in a given $\mathbb{Z}_p[x]$ we can enumerate the possible quadratics and test if they factor the given quartic via long-division or the algebraic technique I used in the Example above. This is illustrated for $p = 3$ in Example 8 of Gallian on page 299-300 and is motivation for Problems 15 and 16 on page 308. Given the effort required for such an example, the criterion below is amazing:

Theorem 4.6.18. Eisenstein's Criterion: *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. If there is a prime p such that $p \nmid a_n$ but $p \mid a_j$ for $j = n - 1, \ldots, 0$ and $p^2 \nmid a_0$ then $f(x)$ is irreducible over $\mathbb{Q}$.*

Proof: I'll postpone proof until a bit later, I found the argument given in Example 4 on page 321 of Gallian far more interesting than the proof by contradiction given on page 300. □

E6

Example 4.6.19. *Consider $f(x) = 13x^7 + 2x^6 + 4x^3 + 18x + 2$. Observe $p = 2$ is such that $2 \nmid 13$ and $2^2 = 4 \nmid 2$ but 2 does divide $2, 4, 18$ and 2 (and the zero coefficients, note $p \mid 0$ for any p since $0 = p(0)$) thus by Eisenstein's Criterion with $p = 2$ we find $f(x)$ is irreducible over $\mathbb{Q}$.*

Consider, if $S = 1 + x + \cdots + x^{p-1}$ then $xS = x + x^2 + \cdots + x^p$ then

$$S - xS = (x + x^2 + \cdots + x^p) - (1 + x + \cdots + x^{p-1}) = x^p - 1$$

thus, formally, solving for S yields $1 + x + \cdots + x^{p-1} = \frac{x^p - 1}{1 - x}$. Perhaps you remember this algebra from the derivation of the geometric series. In any event, the polynomial $\Phi_p(x) = 1 + x + \cdots + x^{p-1}$ is **defined** to be the p-th *cyclotomic polynomial.*

Theorem 4.6.20. *For $p \in \mathbb{Z}$ prime $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$.*

Proof: the proof in Gallian you'll find in many books, and, my notes: let $f(x) = \Phi_p(x+1)$ thus

$$f(x) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{1}{x}\left(x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-1}x + 1 - 1\right)$$

Cleaning things up a bit,

$$f(x) = x^{p-1} + px^{p-2} + \cdots + p$$

where we may observe every coefficient except the leading coefficient is divided by p and the constant term is not divisible by p^2 hence $f(x)$ is irreducible by Eisenstein's Criterion. Suppose $\Phi_p(x)$ is reducible over $\mathbb{Q}$. In particular, suppose there exist $g(x), h(x) \in \mathbb{Q}[x]$ of degree less than $p-1$ where $\Phi_p(x) = g(x)h(x)$. Then $\Phi_p(x+1) = f(x) = g(x+1)h(x+1)$ shows $f(x)$ is reducible since $g(x+1), h(x+1) \in \mathbb{Q}[x]$ is easily seen with a little algebra. But, this contradicts the irreducibility of $f(x)$ hence $\Phi_p(x)$ is irreducible over $\mathbb{Q}$. □

Irreducible polynomials are useful for building new fields. This is seen in the Corollary to the Theorem below:

Theorem 4.6.21. *Let F be a field and suppose $p(x) \in F[x]$. Then $\langle p(x)\rangle$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over F.*

Proof: suppose that F is a field and $p(x) \in F[x]$. If $\langle p(x)\rangle$ is a maximal ideal in $F[x]$ then $\langle p(x)\rangle$ is a nonzero proper ideal hence $p(x) \neq 0$ and $p(x)$ is nonconstant. Suppose $p(x) = g(x)h(x)$ is a factorization of $p(x)$ over F. If $j(x) \in \langle p(x)\rangle$ then $j(x) = p(x)k(x) = g(x)h(x)k(x)$ thus $j(x) \in \langle g(x)\rangle$ and we find $\langle p(x)\rangle \subseteq \langle g(x)\rangle \subseteq F[x]$. Thus, by maximality, $\langle p(x)\rangle = \langle g(x)\rangle$ or $\langle g(x)\rangle = F[x]$. If $\langle p(x)\rangle = \langle g(x)\rangle$ then we have $g(x) \in \langle p(x)$ hence $g(x) = q(x)p(x)$ and $p(x) = g(x)h(x)$ so $\deg(g(x)) \geq \deg(p(x))$ and $\deg(p(x)) \geq \deg(g(x))$ from which we find $\deg(g(x)) = \deg(p(x))$. On the other hand, if $\langle g(x)\rangle = F[x]$ then each $f(x) = g(x)k(x)$ for some $k(x) \in F[x]$ for each $f(x) \in F[x]$. It follows that $g(x) \in F^\times$ hence $\deg(g(x)) = 0$. In summary, if $p(x) = g(x)h(x)$ then neither of the factors may have nontrivial degree smaller than that of $p(x)$. That is, $p(x)$ is irreducible over F.

Conversely, suppose $p(x)$ is irreducible. Suppose I is an ideal of $F[x]$ for which $\langle p(x)\rangle \subseteq I \subseteq F[x]$. Recall from Theorem 4.5.17 we know $F[x]$ is a PID hence $I = \langle g(x)\rangle$ for some $g(x) \in F[x]$. Note $p(x) = p(x)1 \in \langle p(x)\rangle \subseteq \langle g(x)\rangle$ hence there exists $k(x) \in F[x]$ for which $p(x) = k(x)g(x)$. However, irreducibilty of $p(x)$ implies either $\deg(k(x)) = 0$ or $\deg(g(x)) = 0$. If $\deg(k(x)) = 0$ then $\langle p(x)\rangle = \langle g(x)\rangle$. If $\deg(g(x)) = 0$ then $\langle p(x)\rangle = F[x]$. Thus $\langle p(x)\rangle$ is a maximal ideal in $F[x]$. □

Corollary 4.6.22. *Let F be a field and $p(x) \in F[x]$ is irreducible over F. Then $F[x]/\langle p(x)\rangle$ is a field.*

Proof: if F is a field and $p(x)$ is an irreducible polynomial then $\langle p(x)\rangle$ is maximal by Theorem 4.6.21. Thus $F[x]/\langle p(x)\rangle$ if a field by Theorem 4.3.7. □

Corollary 4.6.23. *Let F be a field and $p(x), a(x), b(x) \in F[x]$. If $p(x)$ is irreducible over F and $p(x) \mid a(x)b(x)$ then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.*

Proof: suppose $p(x) \in F[x]$ is irreducible over a field F. Then $\langle p(x) \rangle$ is a maximal ideal hence a prime ideal as $F[x]/\langle p(x) \rangle$ is a field and thus an integral domain which implies primality of $\langle p(x) \rangle$ via Theorem 4.3.6. If $a(x), b(x) \in F[x]$ an $p(x) \mid a(x)b(x)$ then $a(x)b(x) = p(x)k(x)$ hence $a(x)b(x) \in \langle p(x) \rangle$ hence $a(x) \in \langle p(x) \rangle$ or $b(x) \in \langle p(x) \rangle$ as $\langle p(x) \rangle$ is a prime ideal. But, $a(x) \in \langle p(x) \rangle$ implies $p(x) \mid a(x)$ and $b(x) \in \langle p(x) \rangle$ implies $p(x) \mid b(x)$. The Corollary follows. □.

The Theorem above is important in the proof that $\mathbb{Z}[x]$ forms a *Unique Factorization Domain*. In particular, the uniqueness stems from this Theorem.

E7

Example 4.6.24. *Consider $F = \mathbb{Z}_2$ and the polynomial $x^3 + x + 1$. Notice $x^3 + x + 1 \neq 0$ for $x = 0, 1$ thus $x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$ and hence $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ is a field. See page 302-303 for further calculations in this field with eight elements. Another way we can understand this field is to work directly with indeterminants. The essential rule is that $x^3 = -x - 1 = x + 1$ in $\mathbb{Z}_2$. So, we can look at elements of the field as $a + bx + cx^2$ where $a, b, c \in \mathbb{Z}_2$ and we multiply as usual subject the interesting rule $x^3 = x + 1$. For example,*

$$x(e + fx + gx^2) = ex + fx^2 + gx^3 = ex + fx^2 + g(x + 1) = g + (e + 1)x + fx^2$$

Or, to focus on the interesting part,

$$x(x^2) = x^3 = x + 1 \qquad \& \qquad x^2(x^2) = xx^3 = x(x + 1) = x^2 + x$$

Consider, always working modulo 2,

$$(x + 1)(x^2 + x) = x^3 + x^2 + x^2 + x = x + 1 + x = 1$$

Of course this field is less fun if we write the coset and not just the representative. In practice, we just write the representative when we do a lot of calculation in a particular context. For example, $\mathbb{C} = \mathbb{R}[x]/\langle x^2+1 \rangle$ has typical element $a+bx+\langle x^2+1 \rangle$, but, we usually just write $a+bi$ where $i^2 = -1$.

I'll include another of Gallian's excellent examples here:

E8

Example 4.6.25. *The polynomial $x^2 + 1 \in \mathbb{Z}_3$ can be shown to be irreducible. Thus*

$$\mathbb{Z}_3[x]/\langle x^2 + 1 \rangle \cong \{a + bx + \langle x^2 + 1 \rangle \mid a, b \in \mathbb{Z}_3\}$$

forms a field with nine elements. At the level of representatives, $(a+bx)(c+dx) = ac-bd+(ad+bc)x$ so you can see this is isomorphic to $\mathbb{Z}_3[i]$ which Gallian gave as Example 12 in Chapter 14.

We begin to understand the interplay between ideals in rings and the structure of polynomials. The next feature to explore is the polynomial analog of the prime factorization of integers. Any integer $z \in \mathbb{Z}$ can be expressed as $z = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes. This decomposition is unique upto reordering of the primes.

Theorem 4.6.26. *Every nonzero, non-unit polynomial $f(x)$ in $\mathbb{Z}[x]$ can be written as:*

$$f(x) = b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x)$$

where $b_1, b_2, \ldots, b_s$ are irreducible polynomials of degree 0 and $p_1(x), p_2(x), \ldots, p_m(x)$ are irreducible polynomials of positive degree. This decomposition is unique up to reordering in the sense that if

$$f(x) = c_1 c_2 \ldots c_t q_1(x) q_2(x) \cdots q_n(x)$$

then $t = s$ and $m = n$ and for each j there exists k such that $c_j = \pm b_k$ for $j = 1, \ldots, t$ for each $j' = 1, \ldots, n$ there exists k' such that $p_{j'}(x) = \pm q_{k'}(x)$.

Proof: I'll let you read the proof in Gallian. The argument has three stages. First, we peel off the content which is factored via the prime factorization of integers. This leaves a primitive polynomial which we are able to factor into irreducible factors using a simple induction argument. Finally, the unique factorization centers around the use of the analog of Gauss' lemma for polynomials paired with the fact that the units of $\mathbb{Z}$ are just ± 1. □

Remark 4.6.27. How do we find the **units** in a given unital ring R? We have to solve $xy = 1$ for all possible $x, y \in R$. For $\mathbb{Z}$ a bit of common sense immediately reveals that $x, y = \pm 1$ is all that can be done since otherwise either x or y is forced outside $\mathbb{Z}$. For example, 2 needs $\frac{1}{2} \in \mathbb{Q}$ for a multiplicative inverse. We learn in the next Lecture that many interesting examples are paired with a **norm** and this new calculational tool allows us deeper insight into the structure of units.

E9 Show $P(x) = x^4 + x + 1$ is irreducible over $\mathbb{Z}_2$. Then if $\beta = x + \langle P(x) \rangle$ find multiplication table for the field $\mathbb{Z}_2[x]/\langle P(x) \rangle$

Notice $P(0) = 0+0+1 = 1 \neq 0$ and $P(1) = 1+1+1 = 1 \neq 0$ thus $P(x)$ has no linear factor. Hence we need only consider irreducible quadratic factors.

Good news for $x^2 + ax + b$ with $a, b \in \mathbb{Z}_2$ clearly x^2, $x^2 + x$ have zero of 0 and $\underbrace{x^2+1}_{g(x)}$ has $g(1) = 1+1 = 0$ $\therefore$ x^2+x+1 is only possible irreducible quadratic over $\mathbb{Z}_2$ and indeed $h(x) = x^2 + x + 1$ has $h(0) = 1 = h(1)$ $\therefore$ x^2+x+1 irred.

$$
\begin{array}{r}
x^2 - x \\
\hline
x^2+x+1 \;\big)\; x^4 + x + 1 \\
x^4 + x^3 + x^2 \\
\hline
x + 1 - x^3 - x^2 \\
-x^3 - x^2 - x \\
\hline
1
\end{array}
$$

$\therefore$ $x^2+x+1 \nmid P(x)$

$\Rightarrow$ $P(x)$ irreducible.

$$x^4 + x + 1 = (x^2+x+1)(x^2-x) + 1.$$

$$\frac{\mathbb{Z}_2[x]}{\langle x^4+x+1 \rangle} = \left\{ \overline{ax^3 + bx^2 + cx + d} \;\middle|\; a, b, c, d \in \mathbb{Z}_2 \right\}$$

where $\overline{f(x)} = f(x) + \langle x^4 + x + 1 \rangle$

$$\frac{\mathbb{Z}_2[x]}{\langle x^4+x+1 \rangle} = \left\{ a\beta^3 + b\beta^2 + c\beta + d \;\middle|\; a, b, c, d \in \mathbb{Z}_2 \right\}$$

E9 continued

$$\frac{\mathbb{Z}_2[x]}{\langle x^4+x+1\rangle} = \{0, 1, \beta, 1+\beta, \beta^2, 1+\beta^2, \beta^3, 1+\beta^3,$$
$$\beta+\beta^2, \beta+\beta^3, 1+\beta+\beta^2, 1+\beta+\beta^3, 1+\beta+\beta^2+\beta^3,$$
$$\text{——}, \text{——}, \text{——}, \}$$

We have $\beta^4+\beta+1 = 0$

$\beta^4+\beta = 1$

$\beta(\beta^3+1) = 1 \quad \therefore \underline{\beta^{-1} = 1+\beta^3}$

$\underline{(\beta^3+1)^{-1} = \beta}.$

What's the inverse of β^2?

$$\beta^2(\underline{\quad ? \quad}) = 1$$

$\beta^4 = 1+\beta \Rightarrow \beta^2 \cdot \beta^2 = 1+\beta$

$\Rightarrow \beta^2 \cdot \beta^2(1+\beta^3) = 1(1+\beta^3) + \beta(1+\beta^3)$

$\Rightarrow \beta^2(\beta^2(1+\beta^3)) = 1+\beta^3+1 = \beta^3$

$\Rightarrow \beta^2 \beta^2(1+\beta^3) = \beta^3$

$\Rightarrow \beta^2[1+\beta^3]\beta^{-1} = 1$

$\Rightarrow \beta^2[1+\beta^3][1+\beta^3] = 1$

$\Rightarrow \beta^2(1+\beta^3+\beta^3+\beta^6) = 1$

$\Rightarrow \beta^2(1+\beta^2 \cdot \beta^4) = 1$

$\Rightarrow \beta^2(1+\beta^2(\beta+1)) = 1$

$\Rightarrow \beta^2(1+\beta^3+\beta^2) = 1$ $\boxed{(\beta^2)^{-1} = 1+\beta^2+\beta^3}$