ASSIGNMENT 10 (§13.5)

COLTON GRAINGER (MATH 6140 MODERN ALGEBRA 2)

[1, No. 13.5.3]. *Given.* Suppose $n, d \in \mathbf{N}$. (If either n or d is 0, this problem is trivial.) Fix a field F of characteristic 0.

To prove. In $\mathbf{Z}$, d divides n if and only if, in $F[x]$, $x^d - 1$ divides $x^n - 1$.

Proof. Immediately note $d \le n$. For if $x^n - 1$ is in the ideal $\langle x^d - 1 \rangle$, then $d \le n$ by degree considerations; conversely, if $d \mid n$, then $d \le n$ by assumption that $n, d \in \mathbf{N}$. In either case, in the Euclidean domain $\mathbf{Z}$, there exist unique (here non-negative) $q, r \in \mathbf{N} \cup \{0\}$ such that

$$n = qd + r \quad \text{where} \quad 0 < r \le d.$$

And so the proposition is concerned with whether or not the polynomial

$$x^n - 1 = x^{qd+r} - 1 = (x^{qd} - 1)x^r + x^r - 1 \quad \text{is in the ideal} \quad \langle x^d - 1 \rangle. \tag{1}$$

Recall the factorization [2, No. VI.3]

$$x^d - 1 = \prod_{\zeta} (x - \zeta)$$

where the product is taken over all d-th roots of unity. Since these roots are closed under multiplication, they form a *subgroup* of $F^\times$. Because this subgroup (along with any finite subgroup of $F^\times$) is cyclic, we may group together all the terms belonging to the d-th roots of unity having the same order. Defining

$$\Phi_m(x) = \prod_{\text{order } \zeta = m} (x - \zeta),$$

we obtain

$$x^d - 1 = \prod_{m \mid d} \Phi_m(x). \tag{2}$$

To finish the proof. ($\Rightarrow$) If $d \mid n$, then (2) implies

$$x^d - 1 = \prod_{m \mid d} \Phi_m(x) \quad \text{divides} \quad \prod_{\ell \mid n} \Phi_\ell(x) = x^n - 1 \tag{3}$$

because

- each divisor m of d corresponds to a factor $\Phi_m(x)$ on the LHS of (3), and
- each divisor m of d is also some divisor ℓ of n, so
- each factor $\Phi_m(x)$ on the LHS of (3) also appears as a factor $\Phi_\ell(x)$ on the RHS of (3).

($\Leftarrow$) Conversely, suppose $x^n - 1$ is contained in $\langle x^d - 1 \rangle$. Consider the form of $x^n - 1$ in (1). Because $r < d$, by degree considerations, $x^r - 1$ cannot be in $\langle x^d - 1 \rangle$ unless $r = 0$. But $d \mid qd$ implies

$$x^{qd} - 1 = \prod_{\ell \mid qd} \Phi_\ell(x) \quad \text{is contained in} \quad \left\langle \prod_{m \mid d} \Phi_m(x) \right\rangle = \langle x^d - 1 \rangle. \tag{4}$$

Then (4) with our supposition that $x^n - 1 \in \langle x^d - 1 \rangle$ forces the difference

$$0 = x^r - 1 + (x^{qd} - 1)x^r - \langle x^d - 1 \rangle = x^r - 1 - \langle x^d - 1 \rangle.$$

and we conclude the remainder r of the integer division of n by d is 0. $\square$

Date: 2019-04-03.

[1, No. 13.5.6]. *Given.* Fix a field F of characteristic 0, a prime $p \geq 2$, and a nonnegative integer n. Consider the polynomial $x^{p^n-1} - 1$ over F.

To prove.

(i) $x^{p^n-1} - 1 = \prod_{\zeta \in \mathbf{F}_{p^n}^\times} (x - \zeta)$.

(ii) $\prod_{\zeta \in \mathbf{F}_{p^n}^\times} \zeta = (-1)^{p^n}$.

(iii) $(p-1)! \equiv -1 \pmod{p}$.

Proof.

First to establish $x^{p^n-1} - 1$ is separable. The derivative

$$D\left(x^{p^n-1} - 1\right) = (p^n - 1)x^{p^n-2} \quad \text{has root 0 of multiplicity } p^n - 2$$

but no roots in common with $x^{p^n-1} - 1$. Thus $x^{p^n-1} - 1$ is separable, with $p^n - 1$ distinct roots of unity. Recall [1, No. 13.5.3] the factorization

$$x^{p^n-1} - 1 = \prod_{\zeta} (x - \zeta) \tag{5}$$

where the product is taken over all $p^n - 1$-th roots of unity. In particular, the $p^n - 1$-th roots of unity form a cyclic group of order $p^n - 1$ that's (non-canonically) isomorphic to the cyclic group $\mathbf{F}_{p^n}^\times$ of the same order. Embedding $\mathbf{F}_{p^n}^\times$ in F, with (5) we have proved (i).

The evaluation map $\mathrm{ev}_0 \colon F[x] \to F$ produces

$$-1 = \mathrm{ev}_0\left(x^{p^n-1} - 1\right) = \mathrm{ev}_0\left(\prod_{\zeta \in \mathbf{F}_{p^n}^\times} (x - \zeta)\right) = (-1)^{p^n-1}\left(\prod_{\zeta \in \mathbf{F}_{p^n}^\times} \zeta\right),$$

which proves (ii).

Lastly, fix $n = 1$ and identify $\mathbf{F}_{p^1}$ with $\mathbf{Z}/(p)$ (against geometric intuition). Then the result of part (ii) forces

$$(p-1)! \pmod{p} = \prod_{\zeta \in (\mathbf{Z}/(p))^\times} \zeta = (-1)^p = -1$$

for any odd prime p. If $p = 2$, then $1 = 1! = -1 \pmod{2}$ trivially. We've proven (iii), *Wilson's theorem.* $\square$

[1, No. 13.6.9]. *Given.* $1, x$ in the polynomial ring $F[x]$ over the field F.

To prove.

(i) $\binom{pn}{pi}$ is the coefficient of x^{pi} in the binomial expansion $(1+x)^{pn} = \sum_{k=0}^{pn} \binom{pn}{k} 1^k x^{pn-k}$.

(ii) $\binom{pn}{pi} = \binom{n}{i} \pmod{p}$

Proof. For (i), observe that the coefficient of x^{pi} in the binomial expansion

$$(1+x)^{pn} = \sum_{k=0}^{pn} \binom{pn}{k} x^k$$

is found to be

$$\binom{pn}{k} \quad \text{such that } k = pi$$

because k is strictly increasing as an index on $\{0, \ldots, pn\}$.

For (ii), suppose $\mathrm{char}(F) = p$. Because

$$p \quad \text{divides} \quad \frac{p!}{\ell!(p-\ell)!} \quad \text{for } 0 < \ell < p$$

and

$$\binom{p}{\ell} = \frac{p!}{\ell!(p-\ell)!}$$

we have that

$$(1+x)^p = \sum_{\ell=0}^{p} \binom{p}{\ell} x^\ell = 1 + \underbrace{0 + \cdots + 0}_{p-1 \text{ terms}} + x^p.$$

From one perspective,

$$(1+x^p)^n = \sum_{\ell=0}^{n} \binom{n}{\ell} (x^p)^\ell.$$

Yet from another

$$(1+x^p)^n = (1+x)^{pn} = \sum_{k=0}^{pn} \binom{pn}{k} x^k.$$

Therefore whenever $k = p\ell$, we have $\binom{pn}{pi} = \binom{n}{i} \pmod{p}$. $\square$

References

[1] D. Dummit and R. Foote, *Abstract algebra.* Prentice Hall, 2004.

[2] S. Lang, *Algebra.* 2002.