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 $d \leq n$. For if $x^n - 1$ is in the ideal $\langle x^d - 1 \rangle$, then $d \leq n$ by degree considerations; conversely, if $d \mid n$, then $d \leq n$ 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

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

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. □

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

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

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

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

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 $\operatorname{char}(F) = p$. 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 $\binom{pn}{pi} = \binom{n}{i} \pmod{p}$. □

References

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

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

§13.4-5 Exercises

13.4 1,2,3,4; 13.5: 3,6,9

Lemma. Let $(\mathcal{P}, \leq)$ be a poset with $A \in \mathcal{P}$. Let $UC(A) = \{X \in \mathcal{P} : A \leq X\}$ and $LC(A) = \{X \in \mathcal{P} : X \leq A\}$ be the upper and lower cones on A (in $\mathcal{P}$).

... Isom Ext. Thm.

Prop. A Let k be a field and let k^a be its algebraic closure. Fix a collection of polynomials $\{f_i\}_I$ of $k[x]$. TFAE:

1. Where $\{\alpha_{i,j}\}$ is the collection of roots to the f_i over k^a, K is the field $k(\{a_{i,j}\})$.
2. Where, for each $i \in I$, K_i/k is a field extension s.th. f_i splits completely in K_i but does not split in any proper subfield of K_i, K is the compositum of the K_i.

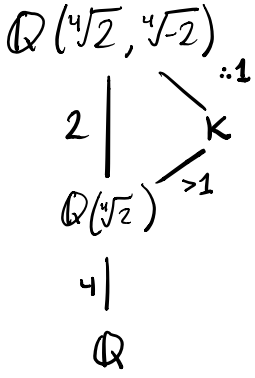
Pf. [Lang 2002; Ch. V, §3, Theorem 3.3].

1. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 - 2$.
2. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + 2$.
3. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + x^2 + 1$.
4. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^6 - 4$.

1] Given. x^4-2 as a polynomial over $\mathbb{Q}$ with splitting field K.

To prove. $K = \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{-2})$ and $[K:\mathbb{Q}] = 8$.

Proof. Consider the Hasse diagram of field extensions.



We'll justify.

over $\mathbb{Q}$
- x^4-2 is Eisenstein at 2, so irred. over $\mathbb{Z}$, thus by Gauss' lemma over $\mathbb{Q}$.
- Therefore $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.

over $\mathbb{Q}(\sqrt[4]{2})$:
- $x^4 - 2 = (x-\sqrt[4]{2})(x+\sqrt[4]{2})(x^2+\sqrt{2})$
- Since $x^2+\sqrt{2}$ has no roots over $\mathbb{R}$, $x^2+\sqrt{2}$ has no roots in $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$.
- Because $x^2+\sqrt{2}$ is quadratic without roots in $\mathbb{Q}(\sqrt[4]{2})$, $x^2+\sqrt{2}$ is irreducible over $\mathbb{Q}(\sqrt[4]{2})$.
- Adjoining the root $\sqrt[4]{-2}$ of $x^2+\sqrt{2}$, we see $[\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{-2}) : \mathbb{Q}(\sqrt[4]{2})] = 2$.

over $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{-2})$
- $x^4-2 = (x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-\sqrt[4]{-2})(x+\sqrt[4]{-2})$ splits completely.

By Prop A, $K = \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{-2}, -\sqrt[4]{-2})$. Observe $K \leq \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{-2})$.

But $\sqrt[4]{-2} \notin \mathbb{Q}(\sqrt[4]{2})$, so $\mathbb{Q}(\sqrt[4]{2}) \subsetneq K$. Since the extension $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{-2}) / \mathbb{Q}(\sqrt[4]{2})$ is simple, we conclude $K = \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{-2})$. □

21 Given. x^4+2 as a polynomial over $\mathbb{Q}$, with splitting field K.

To prove. $K = \mathbb{Q}(i, \sqrt[4]{2})$ and $[K:\mathbb{Q}] = 8$.

Proof. Over the algebraic closure $\mathbb{Q}^a$, where ζ is a primitive 8^{th} root of unity,

x^4+2 has the set of roots $\mathcal{A} = \{\zeta^m \sqrt[4]{2} : m = 1, 3, 5, 7\}$.

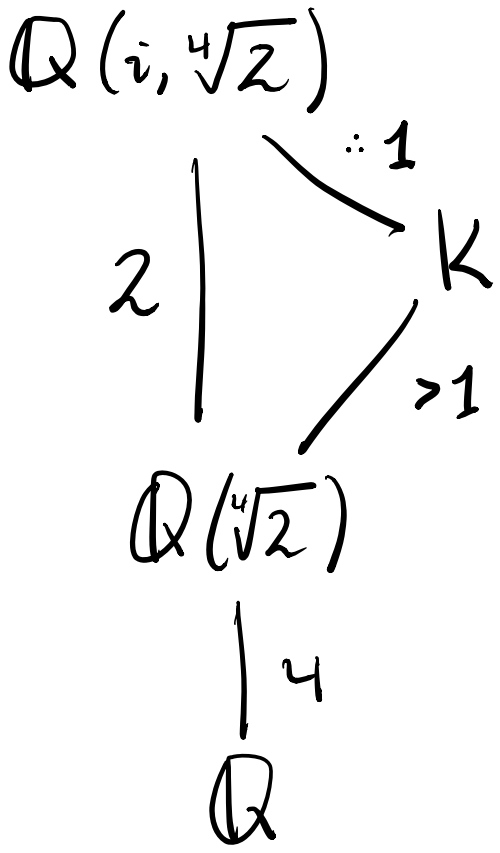
By prop A, $K = \mathbb{Q}\{\mathcal{A}\}$. Because $\operatorname{Im} \zeta \neq 0$, $\sqrt[4]{2} \cdot \zeta \notin \mathbb{Q}(\sqrt[4]{2})$. So $\mathbb{Q}(\sqrt[4]{2}) \subsetneq K$.

Because $\zeta = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \in \mathbb{Q}(i, \sqrt[4]{2})$, we see $\mathcal{A} \subset \mathbb{Q}(i, \sqrt[4]{2})$, so $K \subset \mathbb{Q}(i, \sqrt[4]{2})$.

By analogous argument to 13.4.1, $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 2$

(x^4-2 is irred. over $\mathbb{Q}$ and x^2+1 is irred. over $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$, to be explicit).

The conclusion follows from the Hasse diagram of field extensions:



□

3] Given. x^4+x^2+1 as a polynomial over $\mathbb{Q}$, with splitting field K.

To prove. $K = \mathbb{Q}(\zeta_6)$ and $[K:\mathbb{Q}] = 2$.

Proof. Over the alg. closure $\mathbb{Q}^a$, $y^2+y+1 = \Phi_3(y)$ is cyclotomic with roots $\{\zeta_3, \zeta_3^2\}$.

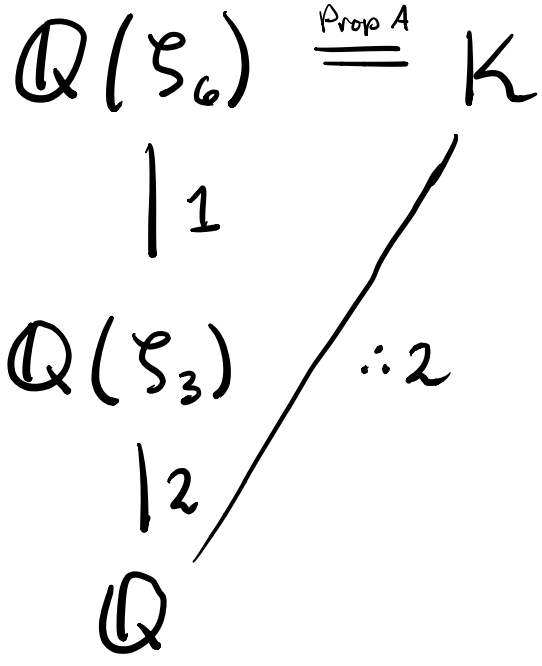
Let $x^2 = y$. Then over $\mathbb{Q}^a$, $x^4+x^2+1 = (x^2-\zeta_3)(x^2+\zeta_3)$ has roots $\{\zeta_6^m : m=1,2,4,5\}$.

Apply prop A and $K = \mathbb{Q}(\zeta_6)$ is the splitting field of x^4+x^2+1 over $\mathbb{Q}$,

where we've used that ζ_6 generates the cyclic group $C_6 \subset \mathbb{C}$. Computing degrees:

$[\mathbb{Q}(\zeta_3):\mathbb{Q}] = 2$, as the min poly $\Phi_3(y)$ for ζ_3 is cyclotomic hence irreduc. over $\mathbb{Q}$.

$[\mathbb{Q}(\zeta_6):\mathbb{Q}(\zeta_3)] = 1$, as $\{1, \zeta_3, \zeta_6\} = \left\{1, -\frac{1}{2}+i\frac{\sqrt{3}}{2}, \frac{1}{2}+i\frac{\sqrt{3}}{2}\right\}$ is $\mathbb{Q}$-linearly dependent.



□

Given. $x^6 - 4$ as a polynomial over $\mathbb{Q}$ and K its splitting field.

To prove. $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$; $[K:\mathbb{Q}] = 6$.

Proof. Over $\mathbb{Q}^a$, $x^6 - 4 = (x^3 - 2)(x^3 + 2)$. To list roots in $\mathbb{Q}^a$:

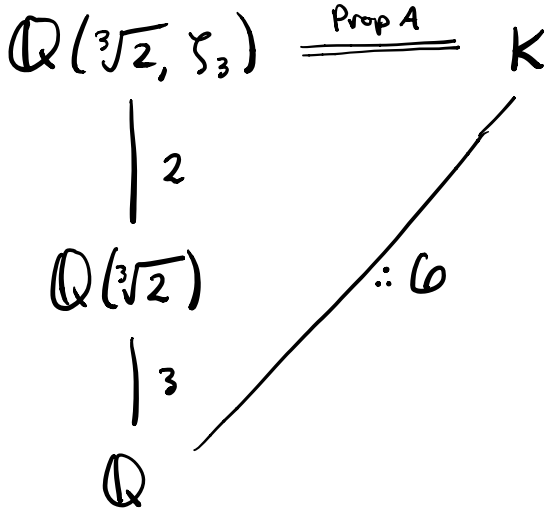
- The factor $x^3 - 2$ has roots $\{\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}\}$.
- The factor $x^3 + 2$ has roots $\{\zeta_6\sqrt[3]{2}, \zeta_6^5\sqrt[3]{2}, \zeta_6^3\sqrt[3]{2}\}$.

From 13.4.3, recall $\{1, \zeta_3, \zeta_6\}$ is $\mathbb{Q}$-linearly dep. Therefore, applying Prop A, $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is the splitting field of $x^6 - 4$ over $\mathbb{Q}$.

To compute degrees:

- $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2$ because $\sqrt[3]{2}$ is a root of $x^3 - 2$ and $x^3 - 2$ is Eisenstein at 2, thus irreduc. over $\mathbb{Q}$. (The min. poly of $\sqrt[3]{2}$ is $x^3 - 2$ over $\mathbb{Q}$.)
- $[\mathbb{Q}(\zeta_3, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 2$ as $\Phi_3(x)$ has roots $\{\zeta_3, \zeta_3^2\}$ with nonzero imaginary parts. Since $\Phi_3(x)$ has no roots in $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, $\Phi_3(x)$ is an irreduc. quadratic over $\mathbb{Q}(\sqrt[3]{2})$. (The min poly of ζ_3 is $x^2 + x + 1 = \Phi_3(x)$ over $\mathbb{Q}(\sqrt[3]{2})$.)

We have the Hasse diagram of extensions:



□