Math 121, Winter 2023, Homework 4 Solutions

Section 13.5

Problem 3. *Prove that d divides n if and only if $x^d - 1$ divides $x^n - 1$.*

Solution. Using the hint, if $n = qd + r$ with $0 \le r < d$, then $x^n - 1 = (x^{qd+r} - x^r) + x^r - 1$. Unless $r = 0$, $x^d - 1$ can't divide $x^r - 1$ since $r < d$, so the result follows since $x^d - 1$ divides $x^{qd+r} - x^r = x^r(x^d - 1)(x^{(q-1)d} + x^{(q-2)d} + \cdots + 1)$.

(Alternatively, the roots of $x^n - 1$ are the nth roots of 1, while the roots of $x^d - 1$ are the dth roots of 1, so the latter divides the former if and only if nth roots are dth roots, so if and only if $d|n$.)

Problem 6. *Prove that $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times}(x - \alpha)$. Conclude that $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$ so the product of the nonzero elements of a finite field is $+1$ if $p = 2$ and -1 if p is odd. For p odd and $n = 1$ derive Wilson 's Theorem: $(p-1)! = -1(\mod p)$.*

Solution. The degrees of both sides match up, so for the first part we only need to show that if $\alpha \in \mathbb{F}_p^\times$ that $\alpha^{p^n-1} = 1$. $\mathbb{F}_{p^n}^\times$ is a group under multiplication with order $p^n - 1$, so by Lagrange's Theorem the order of every element divides $p^n - 1$, so $\alpha^{p^n-1} = 1$ for all $\alpha \in \mathbb{F}_{p^n}$, and the first statement holds.

The statements in the second sentence follow from the specialization $x = 0$. Finally, Wilson's Theorem is just a reinterpretation of the second sentence: up to a multiple of p, $(p-1)!$ is the product of all nonzero elements of $\mathbb{F}_p$.

Section 13.6

Problem 2. *Let ζ_n be a primitive nth root of unity and let d be a divisor of n. Prove that ζ_n^d is a primitive (n/d)th root of unity.*

Solution. ζ_n^d is an (n/d)th root of unity since $(\zeta_n^d)^{n/d} = \zeta_n^n = 1$. Furthermore, if $m < n/d$ and $(\zeta_n^d)^m = 1$, then $md < n$ and $\zeta_n^{md} = (\zeta_n^d)^m = 1$, so the primitivity of ζ_n as an nth root implies the primitivity of ζ_n^d as an (n/d)th root.

Problem 3. *Prove that if a field contains the nth roots of unity for n odd then it also contains the $2n$th roots of unity.*

Solution. Direct method: Let ζ_n be a primitive nth root of unity. Then $(-\zeta_n)^{2n} = (-1)^{2n}\zeta^{2n} = 1$, so $-\zeta_n$ is a $2n$-th root of unity. Conversely, if $(-\zeta_n)^a = 1$, then either a is even and $\zeta_n^a = 1$, in which case a is a multiple of $2n$ or a is odd and $\zeta_n^a = -1$. But no power of ζ_n can equal -1; otherwise let $b \geq 1$ be minimal with $\zeta_n^b = -1$, and ζ_n^{2b} must be a multiple of n, but since n is odd, this would mean that b is a multiple of n.

Indirect method: The map

$$a \mapsto \begin{cases} a, & \text{if } a \text{ is odd} \\ a+n, & \text{if } a \text{ is even} \end{cases}$$

is a bijection between integers $1, \ldots, n$ that are coprime to n and integers $1, \ldots, 2n$ that are coprime to $2n$. This means that $\phi(n) = \phi(2n)$, so the cyclotomic extensions $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ and $\mathbb{Q}(\zeta_{2n})/\mathbb{Q}$ have the same degree. Since $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{2n})$, the fields must be equal.

Problem 7. *Use the Mobius Inversion formula indicated in Section 14.3 to prove*

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Solution. Note that we don't need to know anything about the Mobius Inversion formula except the formula itself:

$$\text{if } F(n) = \sum_{d|n} f(d), \quad \text{then} \quad f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

We use the formula $x^n - 1 = \prod_{d|n} \Phi_d(x)$; to turn multiplication into addition set $F(n) := \log(x^n - 1)$ and $f(n) := \log(\Phi_d(x))$. Plugging these into the Mobius Inversion formula produces

$$\log(\Phi_n(x)) = \sum_{d'|n} \mu(d) \log(x^{n/d'} - 1),$$

so

$$\Phi_n(x) = \prod_{d'|n} (x^{n/d'} - 1)^{\mu(d')},$$

and the substitution $d = n/d'$ gives the desired formula.

Section 14.1

Problem 3. *Determine the fixed field of complex conjugation on $\mathbb{C}$.*

Solution. If $z \in \mathbb{C}$, z can be written uniquely as $z = a + bi$. (You already know this from long ago, but it also follows from Theorem 13.4 using the polynomial $x^2 + 1$). The complex comjugate $\overline{z} = a - bi$, and by uniqueness, that equals $a + bi$ precisely if $b = 0$ i.e. $z \in \mathbb{R}$.

Problem 5 *Determine the automorphisms of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ explicitly.*

Solution. By the Tower Law, this is a degree 2 field extension, so by Proposition 14.5 we have at most 2 automorphisms of $\mathbb{Q}(\sqrt[4]{2})$ fixing $\mathbb{Q}(\sqrt{2})$. The identity is such an automorphism, and for the other, we let $a \mapsto a$ for any $a \in \mathbb{Q}$ and let $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$. (How do we guess this? It must be one of $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$, and choosing one of the latter pair would give a map of order > 2). The powers of $\sqrt[4]{2}$ give us a basis of $\mathbb{Q}(\sqrt[4]{2})$, so our automorphism is

$$a + b\sqrt[4]{2} + c\sqrt{2} + d(\sqrt[4]{2})^3 \mapsto a - b\sqrt[4]{2} + c\sqrt{2} - d(\sqrt[4]{2})^3.$$

We see this fixes $\sqrt{2}$, so it is indeed an element of $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2}))$.

Problem 10. *Let K be an extension of the field F. Let $\phi : K \to K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K'. Prove that the map $\sigma \mapsto \phi\sigma\phi^{-1}$ defines a group isomorphism $Aut(K/F) \to Aut(K'/F)$.*

Solution. If $\sigma \in \mathrm{Aut}(K/F)$, then we first need to show that $\sigma' := \phi\sigma\phi^{-1}$ is indeed an element of $\mathrm{Aut}(K'/F')$. Since σ is the composition of three isomorphisms, it is itself an isomorphism, hence in $\mathrm{Aut}(K')$. Since σ fixes F, if $a \in F'$, then $\phi^{-1}(a) \in F$, so $\sigma'(a) = \phi(\sigma(\phi^{-1}(a))) = a$, and $\sigma' \in \mathrm{Aut}(K'/F')$.

Now, if $\sigma, \tau \in \mathrm{Aut}(K/F)$, then $\sigma\tau \mapsto \phi\sigma\tau\phi^{-1} = \phi\sigma\phi^{-1} \cdot \phi\tau\phi^{-1}$, so this map is a homomorphism. It is injective since if $\phi\sigma\phi^{-1} = \phi\tau\phi^{-1}$, $\sigma = \phi^{-1}\phi\sigma\phi^{-1}\phi = \phi^{-1}\phi\tau\phi^{-1}\phi = \tau$. Finally, for surjectivity, suppose that $\sigma' \in \mathrm{Aut}(K'/F')$. Then setting $\sigma := \phi^{-1}\sigma'\phi$, we have $\sigma \mapsto \phi\sigma\phi^{-1} = \phi\phi^{-1}\sigma'\phi\phi^{-1} = \sigma'$.