Math 30820 Honors Algebra 4
Homework 7

Andrei Jorza

Due Wednesday, 3/8/2017

Do 6 of the following questions. Some questions may be obligatory. Artin a.b.c means chapter a, section b, exercise c. You may use any problem to solve any other problem.

Throughout this problem set $\Phi_n(X)$ is the n-th cyclotomic polynomial.

1. Let p be a prime number. Show that a polynomial $P(X) \in \mathbb{F}_p[X]$ is irreducible if and only if $P(X) \mid X^{p^n} - X$ but $(P(X), X^{p^d} - X) = 1$ for all $d \mid n$, $d < n$.

   Proof. Since $X^{p^n} - X$ is a product of irreducible polynomials of degree $\mid n$, if P is irreducible of degree n then $P \mid X^{p^n} - X$ and certainly $P \nmid X^{p^d} - X$ as $n > d$ so $n \nmid d$.

   Now suppose P is reducible and Q is an irreducible factor of P of degree $d < n$. Then $Q \mid P \mid X^{p^n} - X$ so necessarily $d = \deg Q \mid n$. But then also $Q \mid X^{p^d} - X$ so $Q \mid (P, X^{p^d} - X)$. Therefore if P satisfies $(P, X^{p^d} - X) = 1$ for all $d < n$, $d \mid n$ we deduce that P is irreducible. □

2. For an integer n write $\omega(n)$ be the number of distinct prime divisors of n, i.e., if $n = p_1^{a_1} \cdots p_k^{a_k}$ is the prime factorization then $\omega(n) = k$. Show that

$$\sum_{n \geq 1} \frac{2^{\omega(n)}}{n^s} = \frac{\zeta^2(s)}{\zeta(2s)}$$

   [Hint: Use the product formula for $\zeta(s)$ from class.]

   Proof. First

$$\frac{\zeta(s)}{\zeta(2s)} = \prod_p \frac{\frac{1}{1-\frac{1}{p^s}}}{\frac{1}{1-\frac{1}{p^{2s}}}} = \prod_p \left(1 + \frac{1}{p^s}\right) = \sum_{n \text{ squarefree}} \frac{1}{n^s}$$

   Next,

$$\frac{\zeta^2(s)}{\zeta(2s)} = \left(\sum_{n \text{ squarefree}} \frac{1}{n^s}\right)\left(\sum_{m=1}^{\infty} \frac{1}{m^s}\right) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

   and from class $a_n = \sum_{d \mid n, d \text{ squarefree}} 1$ is the number of squarefree divisors of n. But if $\omega(n) = k$ so n has k distinct prime factors then every squarefree divisor d of n is a product of these prime factors to the exponent 0 or 1. Therefore there are $2^k = 2^{\omega(n)}$ choices and so $a_n = 2^{\omega(n)}$ as desired.

   Another solution, due to Nick. Since $\omega(mn) = \omega(m) + \omega(n)$ when (m, n) it follows that you can factor the LHS over primes as

$$\sum \frac{2^{\omega(n)}}{n^s} = \prod_p \sum_{n=0}^{\infty} \frac{2^{\omega(p^n)}}{p^{ns}}$$

But $\displaystyle\sum_{n=0}^{\infty} \frac{2^{\omega(p^n)}}{p^{ns}} = 1 + \frac{2}{p^s} + \frac{2}{p^{2s}} + \cdots = \frac{1+p^{-s}}{1-p^{-s}}$ and as in the first solution we see that

$$\frac{\zeta(s)^2}{\zeta(2s)} = \prod_p \frac{1+p^{-s}}{1-p^{-s}}$$

□

3. Show that the probability that a monic polynomial of degree n in $\mathbb{F}_p[X]$ is irreducible is $\frac{1}{n} + \varepsilon$ where $|\varepsilon| \le \frac{1}{p^{n/2}}$.

Proof. From class the probability is

$$\frac{1}{n} \frac{p^n - \sum_{q_1 \mid n} p^{n/q_1} + \sum_{q_1 \neq q_2 \mid n} p^{n/(q_1 q_2)} - \cdots}{p^n}$$

where the sums are over distinct prime divisors of n. Therefore

$$|\varepsilon| = \left| \frac{-\sum_{q_1 \mid n} p^{n/q_1} + \sum_{q_1 \neq q_2 \mid n} p^{n/(q_1 q_2)} - \cdots}{np^n} \right| \le \sum_{d \mid n, d \text{ squarefree}} \frac{p^{n/d}}{np^n} \le \sum_{d \mid n, d \text{ squarefree}} \frac{1}{np^{n/2}}$$

$$= \frac{2^{\omega(n)}}{np^{n/2}} \le \frac{1}{p^{n/2}}$$

because if $n = p_1^{a_1} \cdots p_k^{a_k}$ then $n \ge 2^k$. □

4. Show that $\Phi_{2n}(X) = \Phi_n(-X)$ for any odd $n > 1$.

Proof. If n is odd then ζ is a primitive n-th root of 1 if and only if $-\zeta$ is a primitive $2n$-th root of 1. Indeed, $-e^{2\pi i k/n} = e^{2\pi i(n+2k)/(2n)}$ and k is coprime to n if and only if $2k+n$ is coprime to $2n$ (for this last part you need that n is odd). This implies that $\Phi_{2n}(X)$ and $\Phi_n(-X)$ have the same roots. Finally, it suffices to check that $\Phi_n(-X)$ is monic. But the leading coefficient is $(-1)^{\varphi(n)}$ and we know from last semester that if $n > 1$ is odd then $\varphi(n)$ is even. □

5. Let $a \in \mathbb{Z}$. Show that if p is an odd prime divisor of $\Phi_n(a)$ then either $p \mid n$ or $n \mid p-1$.

Proof. Recall that $\Phi_n(X) \mid X^n - 1$ so if $p \mid \Phi_n(a)$ then $p \mid a^n - 1$. Suppose $p \nmid n$. We need to show that $n \mid p-1$. For this it would suffice to show that $a \mod p$ has multiplicative order n as $a^{p-1} \equiv 1 \pmod{p}$.

Suppose that k is the order of $a \mod p$. Since $a^n \equiv 1 \pmod{p}$ we deduce $k \mid n$. Since $p \mid a^k - 1 = \prod_{d \mid k} \Phi_d(a)$ we'd have that $\Phi_d(a) \equiv 0 \pmod{p}$ for some $d \mid k \mid n$. But then a is a root of $\Phi_n(X) \mod p$ and of $\Phi_d(X) \mod p$ so necessarily a double root of $X^n - 1 = \Phi_n(X) \prod_{d \mid n, d < n} \Phi_d(X)$. However $X^n - 1$ is separable in $\mathbb{F}_p[X]$ as $p \nmid n$.

□

6. Suppose $f : \mathbb{R} \to \mathbb{R}$ is a field automorphism.
   (a) Show that $f|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$.
   (b) Show that if $x > 0$ then $f(x) > 0$ and conclude that f is increasing.

(c) Show that if $|x-y| < \dfrac{1}{n}$ then $|f(x)-f(y)| < \dfrac{1}{n}$ and conclude that f is continuous.

(d) Show that $f = \mathrm{id}_{\mathbb{R}}$.

Proof. (a): From last semester $f|_{\mathbb{Z}} = \mathrm{id}_{\mathbb{Z}}$ as f is a ring homomorphism. Next, $f(a/b) = f(a)/f(b) = a/b$ for $a/b \in \mathbb{Q}$ as f is also a field homomorphism.

(b): If $x > 0$ then $f(x) = f(\sqrt{x}^2) = f(\sqrt{x})^2 > 0$ because $f(\sqrt{x}) \in \mathbb{R}$ and if $x \neq 0$ then $f(\sqrt{x}) \neq 0$ by the injectivity of f. If $x > y$ then $f(x) - f(y) = f(x-y) > 0$ so f is increasing.

(c): By part (b) if $-1/n < x - y < 1/n$ we deduce that $-1/n = f(-1/n) < f(x) - f(y) = f(x-y) < f(1/n) = 1/n$ as desired. Therefore $\lim_{x\to y} f(x) = f(y)$ so f is continuous.

(d): If $x \in \mathbb{R}$ consider a sequence $(q_n) \subset \mathbb{Q}$ with $\lim q_n = x$. By continuity

$$f(x) = f(\lim q_n) = \lim f(q_n) = \lim q_n = x$$

□

7. Artin 15.7.5 on page 474.

Proof. From class $X^{3^n} - X$ factors as a product of all monic irreducible polynomials in $\mathbb{F}_3[X]$ of degree $\mid n$. We need to do this for $n = 2$ and $n = 3$ so we need to list monic irreducible polynomials of degrees 1, 2 and 3.

Degree 1: X, $X \pm 1$.

Degree ≥ 2: the constant term cannot be 0 or else the polynomial would be divisible by X. Also, if $P(X)$ of degree 2 or 3 is reducible then it has a linear factor and therefore a root in $\mathbb{F}_3$. So we only need to list $X^2 + aX + b$ with $b \neq 0$ and $X^3 + cX^2 + dX + e$ with $e \neq 0$ that don't vanish at ± 1.

Degree 2: The possibilities are $X^2 + (0, 1, -1)X \pm 1$. There are 6 polynomials in total of which $X^2 + 1$, $X^2 \pm X - 1$ don't have ± 1 as roots so are irreducible. Alternatively we need to eliminate products of linear factors so $(X \pm 1)(X \pm 1)$ which are $X^2 - 1$, $X^2 + X + 1$ and $X^2 - X + 1$.

Degree 3: Again it's easier to eliminate products of three linears and linear times irreducible quadratic. So we need to eliminate $(X \pm 1)^3 = X^3 \pm 1$ and $(X \pm 1)^2(X \mp 1) = X^3 \pm X^2 - X \mp 1$. We also need to eliminate products of $X \pm 1$ and $X^2 + 1$ or $X^2 \pm X - 1$. The former products are $X^3 \pm X^2 + X \pm 1$ and the latter products are $X^3 + (a+b)X^2 + (ab-1)X - a$ where $a, b = \pm 1$ so we are eliminating $X^3 \pm X^2 \pm 1$, $X^3 + X \pm 1$ as well. We are left with $X^3 \pm X^2 \mp 1$, $X^3 \pm X^2 + X \mp 1$, $X^3 \pm X^2 - X \pm 1$ and $X^3 - X \pm 1$. □

8. Artin 15.7.12 on page 474.

Proof. Write $P_q(X) = x^q - x$. Suppose $P_{q'} \mid P_q$ in $\mathbb{Z}[x]$. This is then also true in $\mathbb{F}_p[x]$ and so $\mathbb{F}_{q'}$, the set of roots of $P_{q'} \mod p$, is a subset of $\mathbb{F}_q$, the set of roots of $P_q \mod p$. Therefore $k \mid r$ from class.

Now suppose $r = kl$. Then $p^r - 1 = p^{kl} - 1 = (p^k - 1)(p^{k(l-1)} + \cdots + p^k + 1) = (p^k - 1)N$ and so

$$\frac{x^q - x}{x^{q'} - x} = \frac{x^{p^r - 1} - 1}{x^{p^k - 1} - 1} = \frac{x^{(p^k-1)N} - 1}{x^{p^k - 1} - 1} = x^{(p^k-1)(N-1)} + \cdots + x^{p^k - 1} + 1$$

so $P_{q'} \mid P_q$ in $\mathbb{Z}[x]$. □