MATD01 Fields and Groups

Assignment 6

Due Saturday March 7 at 10:00 pm
(to be submitted on Crowdmark)

Notes: Please write your solutions neatly and clearly. Note that due to time limitations, only some questions will be graded.

1. Textbook, Exercise # 71 parts (i), (iii), (iv)

2. Recall from Assignment 5, Question 4(e) that the minimal polynomial of a primitive complex n-th root of unity over $\mathbb{Q}$ has degree no greater than $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$. The goal of this question is to show that that in fact, the degree of this polynomial is equal to $\varphi(n)$.

For any $\zeta \in \mathbb{C}^\times$, let $|\zeta|$ denote the order of ζ as an element of the group $\mathbb{C}^\times$. For each $n \geq 1$, define

$$\phi_n(x) \ := \prod_{\zeta \in \mathbb{C}^\times,\, |\zeta| = n} (x - \zeta) \ \in \mathbb{C}[x].$$

Thus $\phi_n(x)$ is the monic element of $\mathbb{C}[x]$ whose roots are the primitive n-th roots of unity (and are all of multiplicity one). We call $\phi_n(x)$ the *n-th cyclotomic polynomial*. Since the group μ_n of n-th complex roots of unity is cyclic, there are $\varphi(n)$ primitive n-th roots of unity. Thus $\deg(\phi_n(x)) = \varphi(n)$.

You will prove in this question that:

- $\phi_n(x)$ has coefficients in $\mathbb{Z}$ (note that *a priori*, we only know that $\phi_n(x)$ has coefficients in a field that contains all the n-th roots of unity);
- $\phi_n(x)$ is irreducible over $\mathbb{Q}$.

It will then follow that all primitive n-th roots of unity have the same minimal polynomial over $\mathbb{Q}$ (namely $\phi_n(x)$).

(a) Show that,

$$x^n - 1 = \prod_{d|n} \phi_d(x),$$

where the product is over the positive divisors of n. (Hint: Put the factors of $x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta)$ into appropriate groups. Does the order of every element of μ_n divide n?)

(b) Use strong induction to show that $\phi_n(x)$ has coefficients in $\mathbb{Z}$.
(Hint: By the uniqueness of quotient and remainder in the division algorithm, if $f(x), g(x) \in \mathbb{Q}[x]$ and $g(x) \mid f(x)$ in $\mathbb{C}[x]$, then we have $g(x) \mid f(x)$ in $\mathbb{Q}[x]$ as well: if $q(x), r(x) \in \mathbb{Q}[x]$ are the quotient and remainder of $f(x)$ in division by $g(x)$ in $\mathbb{Q}[x]$, then $q(x)$ and $r(x)$ also satisfy the properties of the quotient and remainder of $f(x)$ in division by $g(x)$ in $\mathbb{C}[x]$ (do you agree?); in particular, if $g(x) \mid f(x)$ in $\mathbb{C}[x]$, then $r(x) = 0$. Remember the version of the division algorithm which allows polynomials with coefficients in an integral domain (Exercise 17 of Rotman).)

(c) You now prove that $\phi_n(x)$ is irreducible over $\mathbb{Q}$ in the following three steps.

Step One: Use Gauss lemma (Theorem 39) to argue that $\phi_n(x) = f(x)g(x)$ for some monic $f(x), g(x)$ with integral coefficients, with $f(x)$ irreducible in $\mathbb{Q}[x]$ (and hence of positive degree).

The goal of the rest of the proof is now to show that $\phi_n(x) = f(x)$.

Step Two: This is the main step. In (i)-(iv) below you will prove that if ζ is a root of $f(x)$ and p is a prime number which does not divide n, then ζ^p is also a root of $f(x)$.

(i) Suppose $f(\zeta) = 0$ and p is prime with $p \nmid n$. Suppose $f(\zeta^p) \neq 0$. Does it follow that $g(\zeta^p) = 0$? Why? Conclude that $f(x) \mid g(x^p)$ in $\mathbb{Z}[x]$.

(ii) Let $\pi : \mathbb{Z} \to \mathbb{F}_p$ be reduction mod p and $\pi^* : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ the induced map on polynomial rings (which applies π to the coefficients of any element of $\mathbb{Z}[x]$, see page 38 of Rotman). Explain why the following is true:

$$\pi^*(f(x)) \mid \pi^*(g(x^p)) = (\pi^*(g(x)))^p.$$

(iii) Conclude that $\pi^*(f(x))$ and $\pi^*(g(x))$ have a common irreducible factor. Does this imply that $x^n - 1 \in \mathbb{F}_p[x]$ has repeated roots? Why?

(iv) Use the hypothesis $p \nmid n$ to argue that $x^n - 1 \in \mathbb{F}_p[x]$ actually has no repeated roots. Deduce that $f(\zeta^p) = 0$, as desired.

Step Three: Show that if ζ is a root of $f(x)$ and m is a positive integer with $gcd(m, n) = 1$, then ζ^m is also a root of $f(x)$. Conclude that $f(x) = \phi_n(x)$.

(d) Why did we first need to argue that ϕ_n has coefficients in $\mathbb{Z}$? Would it have been enough for the proof in (c) if we just knew that ϕ_n has coefficients in $\mathbb{Q}$?

3. Let $K/\mathbb{F}_p$ be a field extension. Let $Fr : K \to K$ be the Frobenius map (defined by $Fr(\alpha) = \alpha^p$).

(a) Show that

$$\mathbb{F}_p = \{\alpha \in K : Fr(\alpha) = \alpha\}.$$

(b) Suppose K is finite. Show that Fr is an automorphism of K.

4. Let R be any integral domain. The goal of this question is to construct a field $Frac(R)$, called the *field of fractions of* R, which naturally contains R as a subring. The construction is modelled on how one gets $\mathbb{Q}$ from $\mathbb{Z}$.

(a) Consider the set

$$R \times (R - \{0\}) = \{(a, b) : a, b \in R; b \neq 0\}.$$

Define a relation $\sim$ on $R \times (R - \{0\})$ as follows:

given (a, b) and (c, d) in $R \times (R - \{0\})$, set $(a, b) \sim (c, d)$ if $ad = bc$.

Show that $\sim$ is an equivalence relation.

(b) Let $Frac(R)$ be the set of equivalence classes of $\sim$. For any $(a, b) \in R \times (R - \{0\})$, denote the equivalence class of (a, b) by $\frac{a}{b}$. Define operations on $Frac(R)$

as follows:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}\,, \qquad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}\,.$$

Show that these operations are well-defined. (Note that since R is a domain, $bd \neq 0$ if b and d are nonzero.)

(c) Show that $Frac(R)$ with operation defined above is a field, and that the map $\iota : R \to Frac(R)$ defined by $\iota(a) = \frac{a}{1}$ is an injective ring homomorphism. (We identify every element of R with its image under this map, and hence think of R as a subring of $Frac(R)$.)

(d) Let F be a field. The field $Frac(F[x])$ is called *the field of rational functions with coefficients in* F, and is denoted by $F(x)$. Note that we have $F \subset F[x] \subset F(x)$. Show that $F(x)$ is a transcendental extension of F.

(e) Suppose K/F is any field extension. Let $\alpha \in K$ be transcendental over F. Show that $F(\alpha) \simeq F(x)$.

5. (a) Show that $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[10]{2})$.

(b) Find $[\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}(\sqrt{2})]$.

(c) Show that $x^5 - \sqrt{2}$ is irreducible in $\mathbb{Q}(\sqrt{2})[x]$.

6. (a) Find the degree of $\mathbb{Q}(\sqrt{5 + 2\sqrt{2}})$ over $\mathbb{Q}$.

(b) Find the degree of $\mathbb{Q}(\sqrt{3 + 2\sqrt{2}})$ over $\mathbb{Q}$.

Extra Practice Problems: The following problems are for your practice. They are not to be handed in for grading.

1. Galois Theory by J. Rotman, second edition: Exercises # 68-77
2. Let K/F be a field extension. Let $\alpha, \beta \in K$ be algebraic over F with $[F(\alpha) : F] = m$ and $[F(\beta) : F] = n$. Show that $[F(\alpha, \beta) : F] \leq mn$. Moreover, show that if $gcd(m, n) = 1$, then $[F(\alpha, \beta) : F] = mn$. Give an example that shows that if m and n are not relatively prime, then $[F(\alpha, \beta) : F]$ may be strictly less than mn.