**MATH 437: Homework VII.**
**Due in class on Monday, March 29**

1. The field $\mathbb{Q}[e^{\frac{2\pi i}{p}}]$.
(a) Fix a field $k$. If $y = ax + b$ where $a, b \in k, a \neq 0$ then note $x = \frac{y-b}{a}$. Fix a polynomial $f(y) \in k[y]$. Show that $f(y)$ is an irreducible polynomial in $k[y]$ if and only if $f(ax + b)$ is an irreducible polynomial in $k[x]$.
(b) Let $p$ denote a prime number. Consider the $p$th cyclotomic polynomial

$$\Phi_p(y) = \frac{y^p - 1}{y - 1} = y^{p-1} + y^{p-2} + \cdots + y + 1$$

in $\mathbb{Z}[y]$. Since this is a polynomial with integer coefficients, it defines a polynomial in $k[y]$ for any field $k$.

Show using Eisenstein's Criterion (See Lang or Hungerford for a statement and proof) that $\Phi_p(x + 1)$ is irreducible in $\mathbb{Q}[x]$. Conclude that $\Phi_p(y)$ is irreducible in $\mathbb{Q}[y]$ and hence the $p$th cyclotomic polynomial is irreducible over $\mathbb{Q}$. (Hint: Consider $(x + 1)^p - 1$.)
(c) Show that $\Phi_p(y) = (y - 1)^{p-1}$ in $k[y]$ when $char(k) = p$ and hence $\Phi_p$ is not irreducible when $p = char(k) > 2$.
(d) Explain why the roots of $\Phi_p$ in a field $E$ of characteristic not equal to $p$ are exactly the primitive $p$th roots of unity in $E$, i.e., the set $\{e \in E | e^p = 1, e^k \neq 1 \text{ for } 1 \leq k < p\}$. What can you say about primitive $p$th roots of unity when $char(E) = p$? Find a factorization of $\Phi_p$ in $\mathbb{C}[x]$ in terms of $\zeta = e^{\frac{2\pi i}{p}} = cos(\frac{2\pi}{p}) + isin(\frac{2\pi}{p}) \in \mathbb{C}$.
(e) Explain why $\mathbb{Q}[\zeta] = \{p(\zeta) | p \in \mathbb{Q}[x]\}$ is a field where $\zeta = e^{\frac{2\pi i}{p}}$. Express $\frac{1}{\zeta}$ as a rational polynomial in $\zeta$.
Find a basis for $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$ and compute $|\mathbb{Q}[\zeta] : \mathbb{Q}|$. Use this basis to find a matrix representing the $\mathbb{Q}$-linear map $\lambda : \mathbb{Q}[\zeta] \to \mathbb{Q}[\zeta]$ given by $\lambda(x) = \zeta x$. What are the minimal polynomial and characteristic polynomials of this matrix?

2. **Linear algebra and field extensions** Let $k$ be a field and suppose $k \subseteq E$ where $E$ is an algebraically closed field. Let $\alpha \in E$ be algebraic over $k$ and let $Irr(\alpha, k)(x) = \sum_{k=0}^{n} a_k x^k$ be its irreducible polynomial over $k$.

Consider the $k$-linear map $\lambda_\alpha : k[\alpha] \to k[\alpha]$ given by $\lambda_\alpha(x) = \alpha x$ for all $x \in k[\alpha]$.
(a) If we give $k[\alpha]$ a $k[x]$-module structure via $q(x) \cdot \beta = q(\alpha)\beta$, explain

why $k[\alpha]$ is a cyclic $k[x]$-module. List the invariant factor(s) and elementary divisor(s) for this module.
(b) If $\mathbb{A} \in Mat_n(k)$ is a $k$-matrix representing $\lambda_\alpha$ in some $k$-basis, explain why the set of eigenvalues of $\mathbb{A}$ (in $E$) is exactly the set of roots of $Irr(\alpha, k)$ (in $E$).
(c) Show that $Tr(\lambda_\alpha) = -a_{n-1}$ and $det(\lambda_\alpha) = (-1)^n a_0$.
(d) Let $\beta \in k[\alpha]$ be **nonzero**. Explain why $\beta = q(\alpha)$ where $q(x) \in k[x]$ is relatively prime to $Irr(\alpha, k)(x)$. If $Irr(\alpha, k)(x) = \prod_{j=1}^{n}(x - \lambda_j)$ in $E[x]$ show that $Irr(\beta, k) | \prod_{j=1}^{n}(x - q(\lambda_j))$ in $E[x]$ with equality if and only if $k[\alpha] = k[\beta]$. (Hint: Consider $\lambda_\beta : k[\alpha] \to k[\alpha]$ given by multiplication by $\beta$. Note that $\lambda_\beta = q(\lambda_\alpha)$ and consider the Cayley-Hamilton Theorem.)
(e) If $|k[\alpha] : k|$ is a prime number. Show that for all $\beta \in k[\alpha]$, either $\beta \in k$ or $k[\beta] = k[\alpha]$.

3. **Irreducible polynomials** Let $k$ be a field and let $\alpha, \beta$ be algebraic over $k$. Set $f(x) = Irr(\alpha, k)(x), g(x) = Irr(\beta, k)(x) \in k[x]$ and $h(x) = Irr(\beta, k[\alpha])(x) \in k[\alpha][x]$.
(a) Show that $h | g$ in $k[\alpha][x]$ and use this to show

$$|k[\alpha, \beta] : k| = deg(f)deg(h) \leq |k[\alpha] : k||k[\beta] : k|$$

with equality if and only if $Irr(\beta, k)$ stays irreducible over $k[\alpha]$.
(b) Show that $deg(g(x))$ divides $|k[\alpha, \beta] : k|$. Use this to prove that

$$|k[\alpha, \beta] : k| = |k[\alpha] : k||k[\beta] : k|$$

when $|k[\alpha] : k|$ and $|k[\beta] : k|$ are relatively prime.
(c) Let $E$ be a finite extension of $k$. Explain why $E = k[\alpha_1, \ldots, \alpha_n]$ for some finite set of $\alpha_i \in E$.
(d) If $E$ is a finite extension of $k$ and $g(x)$ is an irreducible polynomial of $k[x]$ with degree relatively prime to $|E : k|$, show that $g(x)$ is still irreducible in $E[x]$.

4. $n$**th roots** (a) Use Eisenstein's criterion to show that $x^n - p$ is irreducible in $\mathbb{Q}[x]$ for all primes $p$ and integers $n \geq 1$.
(b) From real analysis, is it shown there exists a unique positive real number denoted $\sqrt[n]{p}$ with $(\sqrt[n]{p})^n = p$. Write down a factorization of $x^n - p$ in $\mathbb{C}[x]$ using $\sqrt[n]{p}$ and $\zeta_n = e^{\frac{2\pi i}{n}}$.
(c) Explain why $deg(Irr(\zeta_n, \mathbb{Q})) \leq n - 1$ and use this to show that $x^q - p$ is irreducible over $\mathbb{Q}[\zeta_q]$ when $p, q$ are primes. Use this to calculate

$|\mathbb{Q}[\zeta_q, \sqrt[q]{p}] : \mathbb{Q}|$ when $p, q$ are primes. Show that $\mathbb{Q}[\zeta_q, \sqrt[q]{p}]$ is the smallest subfield of $\mathbb{C}$ over which $x^q - p$ factors into a product of linear factors. It is because of this that $\mathbb{Q}[\zeta_q, \sqrt[q]{p}]$ is called the splitting field of $x^q - p$ over $\mathbb{Q}$. (d) Describe the splitting field $E$ of $x^4 - 2$ over $\mathbb{Q}$ (smallest subfield of $\mathbb{C}$ in which it factors into linear factors) and calculate $|E : \mathbb{Q}|$. (Hint: $i \notin \mathbb{R}$.)