Homework 6, Math 401

due on March 2, 2020

Before you start, please read the syllabus carefully.

1. Consider the field extension $\mathbb{Z}_3 \subset F = \mathbb{Z}_3[x]/\langle x^2 - 2\rangle$.
   (a) Write down the elements in F.
   (b) Write down the multiplication table for the group of units F^*.
   (c) Find all ring homomorphism from F to F.
2. Consider the field extension $\mathbb{Z}_5 \subset F = \mathbb{Z}_5[x]/\langle x^2 - 2\rangle$. Is $f(T) = T^2 - 3$ irreducible in F? What is the splitting field of $f(T) \in F[T]$?
3. Consider the field $F = \mathbb{Z}_5$. How many monic irreducible quadratic polynomials (meaning leading coefficient 1) are there in $F[x]$?
4. Consider $f(x) = x^3 - x + 1 \in \mathbb{Z}_3[x]$.
   (a) Is $f(x)$ irreducible?
   (b) Prove that if $f(\alpha) = 0$, then $f(\alpha + 1) = 0$.
   (c) **Bonus**: What is the splitting field of $f(x)$?
5. Let $g_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1} \in \mathbb{Q}[x]$.
   (a) Write down $g_p(x+1)$ via the quotient $\frac{(x+1)^p - 1}{x+1-1}$.
   (b) Prove that the number $\binom{p}{k} \equiv 0 \mod p$ for $1 \le k \le p - 1$.
   (c) Prove that the polynomial $g_p(x)$ is irreducible for every p.
   (d) What is the degree $[K : \mathbb{Q}]$ where $K = \mathbb{Q}[x]/\langle g_p(x)\rangle$?
   (e) Prove that if $g_p(\alpha) = 0$, then $g_p(\alpha^r) = 0$ for every $1 \le r \le p - 1$.
   (f) Prove that $\alpha \neq \alpha^r$ for any $1 < r < p$.
6. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$.
   (a) Prove that $f(x)$ is irreducible.
   (b) Prove that $\mathbb{Q}[x]/\langle f(x)\rangle \simeq \mathbb{Q}[\beta]$ where $\beta \in \mathbb{C}$ is a root of $f(x)$.
   (c) Show that if $\beta \in \mathbb{C}$ is a root of $f(x)$, then $\alpha\beta$ is also a root of $f(x)$. Here $\alpha \in \mathbb{C}$ is one root of $g_3(x)$ in the last question.
   (d) Denote $K \subset \mathbb{C}$ to be the smallest subfield of $\mathbb{C}$ such that $f(x)$ splits into product of linear factors, i.e., degree 1 polynomials. Prove that $\alpha, \beta \in K$.
   (e) **Bonus**: Prove that $2|[K : \mathbb{Q}]$ and $3|[K : \mathbb{Q}]$. Hint: In order to prove $2|[K : \mathbb{Q}]$, look for some subfield $\mathbb{Q} \subset M \subset K$ where $[M : \mathbb{Q}] = 2$.