Problems 2

1 Exercise from Homework 2

Show that the ring obtained from $\mathbb{Z}/12\mathbb{Z}$ by adjoining an inverse of 2 is isomorphic to $\mathbb{F}_3$.

2 More polynomials

1. Suppose that $P(x)$ is irreducible over a field $\mathbb{F}$ and let $a \in \mathbb{F}$. Show that $P(x+a)$ is irreducible as well.
2. Let $a \in \mathbb{F}_p$. Show that $x^p + a$ is reducible on $\mathbb{F}_p[x]$.
3. Let $f, g \in \mathbb{Q}[x]$, with f irreducible. Suppose that it exists α such that $f(\alpha) = g(\alpha) = 0$. Show that f divides g.
4. Show that the following polynomials are irreducible in $\mathbb{Q}[x]$:
   (a) $x^4 - 8x^3 + 12x^2 - 6x + 2$;
   (b) $x^5 - 12x^3 + 36x - 12$;
   (c) $x^4 - x^3 + 2x + 1$;
5. Let $(x^3 - x + 2)$ the principal ideal generated by $(x^3 - x + 2)$ in $\mathbb{Q}[x]$.
   (a) Show that the quotient ring $R = \mathbb{Q}[x]/(x^3 - x + 2)$ is a field.
   (b) Let y be the image of x in R. Compute y^{-1}.

3 Gauss Integers

Our goal is to show that a prime $p \in \mathbb{Z}$ is a sum of two squares if and only if $p = 2$ or $p \equiv 1[4]$.

1. We denote $S = \{p \in \mathbb{Z} \text{ prime}, \exists\, a, b \in \mathbb{Z},\ p = a^2 + b^2\}$. Show that $p \in S \iff p$ is reducible in $\mathbb{Z}[i]$.
2. Show that $\mathbb{Z}[i]/(p)$ is an integral domain if and only if -1 is a square in $\mathbb{F}_p$.
3. Deduce the result in the case where $p = 2$.
4. Case $p > 2$. Show that $x \in \mathbb{F}_p$ is a square if and only if $x^{\frac{p-1}{2}} = 1$. Deduce the result.