# Third problem set

1. In class we proved that, for any $a \in \mathbb{Z}_p$, we have $a^p = a$. (where $p$ is prime). Use this result to show

$$x^p - x = x(x-1)\cdot \cdots \cdot (x-(p-1))$$

in $\mathbb{Z}_p[x]$. Use this result to deduce $(p-1)! = -1$ in $\mathbb{Z}_p$.
(Hint. Think about zeros of $x^p - x$ in $\mathbb{Z}_p$.)

2. (a) Show that $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ where $\omega = \frac{-1+\sqrt{-3}}{2}$.
(b) Show that the field of fractions of $\mathbb{Z}[\omega]$ is $\mathbb{Q}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Q}\}$.
(Hint. Use $\omega^2 + \omega + 1 = 0$; and compute $(a+b\omega)(a+b\bar{\omega})$ where $\bar{\omega} = \frac{-1-\sqrt{-3}}{2}$. (Notice $\omega + \bar{\omega} = -1$ and $\omega\bar{\omega} = 1$.))

3. Find all the primes $p$ such that $x+2$ is a factor of $x^6 - x^4 + x^3 - x + 1$ in $\mathbb{Z}_p[x]$.

4. Find a zero of $x^3 - 2x + 1$ in $\mathbb{Z}_5$ and express it as a product of a degree 1 and a degree 2 polynomial.

5. How many degree 2 and degree 3 polynomials with no zeros in $\mathbb{Z}_2[x]$ are there?

# Third problem set

1. Prove that the following polynomials are irreducible in $\mathbb{Q}[x]$.

   ⓐ $x^3-3x^2+3x+4$.

   ⓑ $x^n-12$ where $n\in\mathbb{Z}^+$.

   ⓒ $x^5-10x^3+25x^2-51x+2017$

   (Only in this part of the problem you are allowed to use the following (advance) theorem:

   Let $p$ be a prime and $a\in\mathbb{Z}_p\setminus\{0\}$. Then $x^p-x+a$ is irreducible in $\mathbb{Z}_p[x]$.)

2. ⓐ Prove that $f_0(x)=x^5-3x^3+6x^2+9x-21$ is irreducible in $\mathbb{Q}[x]$. (Hint. Think about a useful criterion!)

   ⓑ Let $\alpha$ be a real zero of $f_0(x)$. Suppose $\phi_\alpha:\mathbb{Q}[x]\longrightarrow\mathbb{R}$ is the evaluation homomorphism; that means $\phi_\alpha(f(x))=f(\alpha)$. Prove that

$$\ker\phi_\alpha=\langle f_0(x)\rangle.$$

   (Hint. Use the fact that $\mathbb{Q}[x]$ is a PID and partⓐ).

# Third problem set

3. (a) Prove that $\left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \,\middle|\, a,b \in \mathbb{Q} \right\}$ is a subring of $M_2(\mathbb{Q})$.

(b) Prove that $f: \mathbb{Q}[\sqrt{2}] \longrightarrow \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \,\middle|\, a,b \in \mathbb{Q} \right\}$,

$$f(a+b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$$

is a ring isomorphism.