Problem 1. a) Let R be a UFD and let K be the field of fractions of R. Let $f(x) = f_0 + f_1 x + ... + f_n x^n \in R[x]$. Suppose that $z \in K$ is a root of f. Write $z = a/b$ for some $a, b \in R$ such that $\gcd(a, b) = 1$. Prove that $a|f_0$ and $b|f_n$. Conclude that if f is monic then $z \in R$.

b) Prove that if $n \in \mathbb{Z}$ is not a $k-$th power of an integer then there are no rational numbers r such that $r^k = n$. (In other words, $\sqrt[k]{n}$ is irrational). Hint: Use a).

c) Which of the following polynomials have a root in $\mathbb{Q}$?

$$2x^5 + 7x^2 - 3,\ 3x^5 + 2x^4 + 6x^2 + x - 2,\ x^{2007} - 12x^{1974} - 2007x^{12} - 1.$$

Hint: Use a) to reduce to a finite number of cases and verify each case.

Solution: a) Multiplying the equation $f(z) = 0$ by b^n we get

$$f_n a^n + f_{n-1} a^{n-1} b + ... + f_1 a b^{n-1} + f_0 b^n = 0.$$

Note that all the summands on the left except the first one are divisible by b and all the summand except the last one are divisible by a. Since 0 is divisible by both a and b, we conclude that $b|f_n a^n$ and $a|f_0 b^n$. Since $\gcd(a, b) = 1$, we have $\gcd(b, a^n) = 1 = \gcd(a, b^n)$ (we proved in class that in UFD if $\gcd(x, y) = 1 = \gcd(x, z)$ then $\gcd(x, yz) = 1$; this and easy induction show that if $\gcd(a, b) = 1$ then $\gcd(a, b^n) = 1$ for all positive integrs n). We proved in class that in a UFD if $\gcd(x, y) = 1$ and $x|yz$ then $x|z$. In our situation this implies that $b|f_n$ and $a|f_0$.

If f is monic, then $f_n = 1$ and therefore $b|1$. This means that b is invertible in R so $z = ab^{-1} \in R$.

b) Consider the monic polynomial $x^k - n \in \mathbb{Z}[x]$. By a), if $r \in \mathbb{Q}$ is a root of this polynomial then $r \in \mathbb{Z}$, so $n = r^k$ is a $k-$th power of an integer. In other words, if n is not a $k-$th power of an integer then $x^k - n$ has no roots in $\mathbb{Q}$.

c) Suppose that $r \in \mathbb{Q}$ is a root of $2x^5 + 7x^2 - 3$. There are integers a, b such that $\gcd(a, b) = 1$, $b > 0$ and $r = a/b$. By part a) we have $a|3$ and $b|2$. Thus $a \in \{-3, -1, 1, 3\}$ and $b \in \{1, 2\}$. By direct computation we check that none of these work, so $2x^5 + 7x^2 - 3$ has no rational roots.

Similarly, a rational root of $3x^5 + 2x^4 + 6x^2 + x - 2$ must be of the form a/b where $a \in \{-2, -1, 1, 2\}$ and $b \in \{1, 3\}$. Direct computation shows that $-2/3$ is a root of $3x^5 + 2x^4 + 6x^2 + x - 2$.

A rational root of $x^{2007} - 12x^{1974} - 2007x^{12} - 1$ must be an integer which divides -1, so it is -1 or 1. But neither 1 nor -1 is a root, so $x^{2007} - 12x^{1974} - 2007x^{12} - 1$ has no rational roots.

Problem 2. Prove that the following polynomials are irreducible:

a)

$$\frac{1}{5}x^6 + 6x^5 - 3x^3 + \frac{6}{5}x - 24 \text{ in } \mathbb{Q}[x].$$

b) $x^4 - 5$ in $\mathbb{Q}[i][x]$.

c) $f(x) = [(x+2)^p - 2^p]/x$ in $\mathbb{Q}[x]$, where p is odd prime.

Solution: a) The polynomial $\frac{1}{5}x^6 + 6x^5 - 3x^3 + \frac{6}{5}x - 24$ is associated to the monic (hence primitive) polynomial $f = x^6 + 30x^5 - 15x^3 + 6x - 120$. We know that $x^6 + 30x^5 - 15x^3 + 6x - 120$ is irreducible in $\mathbb{Q}[x]$ iff it is irreducible in $\mathbb{Z}[x]$. Consider the ideal $P = 3\mathbb{Z}$. Note that all assumptions of the Eisenstein criterion are satisfied for this choice of P and our polynomial f. Thus f is irreducible in $\mathbb{Z}[x]$, hence in $\mathbb{Q}[x]$.

b) Recall that $\mathbb{Z}[i]$ is a PID with field of fractions $\mathbb{Q}[i]$. Since $x^4 - 5$ is primitive, it is irreducible in $\mathbb{Q}[i][x]$ iff it is irreducible in $\mathbb{Z}[i][x]$. Now the irreducible factorization of 5 in $\mathbb{Z}[i]$ is $5 = (2+i)(2-i)$. The ideal $P = (2+i)\mathbb{Z}[i]$ is prime (since $2+i$ is irreducible and $\mathbb{Z}[i]$ is a UFD). Clearly $2 + i \in P$ and $2 + i \notin P^2 = (2+i)^2\mathbb{Z}[i]$. Thus the assumptions of Eisenstein criterion hold for P and $x^4 - 5$. Thus $x^4 - 5$ is irreducible in $\mathbb{Z}[i][x]$ and hence in $\mathbb{Q}[i]$.

c) Using the binomial formula we have

$$f(x) = x^{p-1} + \binom{p}{1} \cdot 2 \cdot x^{p-2} + \binom{p}{2} \cdot 2^2 \cdot x^{p-3} + ... + \binom{p}{p-1} \cdot 2^{p-1}.$$

Since $p | \binom{p}{i}$ for $i = 1, 2, ..., p-1$, f is a monic polynomial whose all coefficients except the leading belong to the prime ideal $P = p\mathbb{Z}$. The constant term $\binom{p}{p-1} \cdot 2^{p-1} = p \cdot 2^{p-1}$ is not divisible by p^2 so it does not belong to P^2. Thus all assumptions of the Eisenstein criterion are satisfied and therefore f is $\mathbb{Z}[x]$, hence also in $\mathbb{Q}[x]$.

Problem 3. Let R be UFD with field of fractions K and let $f = f_0+f_1x+...+f_nx^n \in R[x]$. Suppose that there is a prime ideal P of R such that $f_n \notin P$, $f_0, ..., f_{n-1} \in P$ and $f_0 \notin P^2$. Prove that f is irreducible in the ring $K[x]$. Hint: Use Problem 2b) from homework 28.

Solution: Let d be a greatest common divisor of all the coeffcients if f. Write $f_i = dg_i$ and let $g = g_0+g_1x+...+g_nx^n$. Then g is primitive and g is accociated to f in $K[x]$. Thus f is irreducible in $K[x]$ iff g is irreducible in $R[x]$. Since $f_n = dg_n \notin P$ and P is an ideal, neither d nor g_n belong to P. Since P is prime and $f_i = dg_i \in P$ for $i = 0, 1, ..., n-1$ and $d \notin P$, we conclude that $g_i \in P$ for $i = 0, 1, ..., n-1$. Finally, since $f_0 = dg_0 \notin P^2$, also $g_0 \notin P^2$. Thus the assuptions of Eisenstein criterion are satisified for g and the prime ideal P. If $g = pq$ for some $p, q \in R[x]$, then one of p, q is constant by Eisenstein criterion. We may assume $p = c$ is a constant. But then c divides all coefficients of $cq = g$. Since g is primitive, c must be invertible in R. Thus whenever $g = pq$ then p or q is invertible, i.e. g is irreducible in $R[x]$. Consequently, f is irreducible in $K[x]$.