HOMEWORK 1
SOLUTIONS

Problem 1 [13.1.5] Suppose α is a rational root of a monic polynomial in $\mathbb{Z}[X]$. Prove that $\alpha \in \mathbb{Z}$.

Proof. By the rational root theorem (Prop. 11, Ch.9) if $\alpha = \frac{p}{q} \in \mathbb{Q}$ is a root of the monic polynomial and $(p, q) = 1$ then $q \mid 1$ and therefore $\alpha \in \mathbb{Z}$. $\square$

Problem 2 [13.1.8] Prove that $x^5 - ax - a \in \mathbb{Z}[X]$ is irreducible unless $a = 0, 2$ or -1.

Proof. Let $f(x) = x^5 - ax - 1$. If f is reducible, there are two possible cases: it has a linear factor or it factors as the product of an irreducible quadratic with an irreducible cubic.

In the first case it follows that f has a root $r \in \mathbb{Z}$. By the rational root theorem we know that r divides the constant term, so $r = \pm 1$. Now $f(1) = 0$ implies $a = 0$, and $f(-1) = 0$ implies $a = 2$.

For the second case, assume that

$$f(x) = (Ax^2 + bx + c)(Bx^3 + dx^2 + ex + g).$$

Since f is monic we must have $A = B = 1$ or $A = B = -1$. WLOG, we'll assume that $A = B = 1$:

$$f(x) = x^5 + (b + d)x^4 + (c + e + bd)x^3 + (g + cd + be)x^2 + (bg + ce)x + cg.$$

Therefore $d = -b,\ c + e = b^2,\ b(c - e) = g,\ bg + ce = -a,\ cg = -1.$

If $c = -1$, then $g = 1$ and thus $-b(e + 1) = 1$, implying $e = 0$ or $e = -2$. In either case, $b^2 = c + e < 0$, which is a contradiction.

If $c = 1$, then $g = -1$ and thus $b(e - 1) = 1$, implying $e = 2$ or $e = 0$. If $e = 2$ then $b^2 = 3$, which is a contradiction. So $e = 0$ and hence $b = -1$ and $a = -1$, giving the factorization:

$$f(x) = (x^2 - x + 1)(x^3 + x^2 - 1).$$

$\square$

Problem 3 [13.2.3] Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + i$.

Solution. Clearly $1 + i \in \mathbb{Q}(i)$ and since $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ we see that the degree of the minimal polynomial should be 2. Notice that $(i + 1)^2 - 2(i + 1) + 2 = 0$ and the polynomial $x^2 - 2x + 2$ is irreducible by the Eisenstein's criterion, therefore it is the minimal polynomial of $i + 1$.

$\square$

Problem 4 [13.2.13] Suppose $F = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$. Prove that $\sqrt[3]{2} \notin F$.

Proof. Observe that each α_i satisfies $x^2 - \alpha_i^2 \in \mathbb{Q}[x]$, hence

$$[\mathbb{Q}(\alpha_1, \ldots, \alpha_i) : \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})] = 1 \text{ or } 2.$$

Therefore, $[F : \mathbb{Q}] = 2^t$, for some natural number $t \leq n$. If $\sqrt[3]{2} \in F$, then $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subseteq F$, so

$$2^t = [F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \cdot [F : \mathbb{Q}(\sqrt[3]{2})],$$

implying $3|2^t$, which is a contradiction. Thus, $\sqrt[3]{2} \notin F$.

$\square$

Problem 5. Let $m, n \geq 1$ be positive integers such that $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is an extension of finite fields. Show that $m|n$.

Proof. We shall use the following result.

Lemma 1. *Let F/K be a finite field extension such that K has q elements. Then F has q^n elements, where $n = [F : K]$.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a basis of F (as a vector space) over K. Then each element of F can be written as a linear combination $c_1\alpha_1 + \ldots + c_n\alpha_n$, where $c_i \in K$. Since each c_i can take q possible values, it follows that F has q^n elements. $\square$

Now, if $d = [F_{p^n} : F_{p^m}]$ then by the lemma it follows that $p^n = (p^m)^d$, showing that $m|n$.

$\square$