MAT 150C - Homework 6

Markus Tran

1. Let R be a finite integral domain, and let $r \neq 0 \in R$. Since R is finite, there exist $n, m \in \mathbb{Z}$ such that $r^n = r^m$ and $m > n$. Thus

$$r^n - r^m = r^n(1 - r^{m-n}) = 0.$$

Since R is an integral domain, either $r^n = 0$ or $(1 - r^{m-n}) = 0$. But powers of r are nonzero because $r \neq 0$, and therefore

$$1 - r^{m-n} = 0 \implies r^{m-n} = r(r^{m-n-1}) = 1.$$

This means that r is invertible, and R is a field.

2. (a) Let $f(x) \in \mathbb{R}[x]$. Let z be a root of f so that $f(z) = 0$. Thus

$$f(\overline{z}) = \sum_n a_n (\overline{z})^n = \sum_n \overline{a_n z^n} = \overline{\sum_n a_n z^n} = \overline{0} = 0$$

and $\overline{z}$ is also a root of f.

(b) Let $f(x) \in \mathbb{R}[x]$ be a real polynomial of degree n. Then f has n complex roots, and

$$f(x) = \prod_{i=0}^{n} (x - z_i), \quad \text{where } z \in \mathbb{C}.$$

Since roots come in conjugate pairs, if z is a nonreal root of f, then $(x - z)(x - \overline{z}) = x^2 - (z + \overline{z})x + z\overline{z}$ divides f where $x^2 - (z + \overline{z})x + z\overline{z} \in \mathbb{R}[x]$. Therefore any real polynomial can be written as a product of real polynomials with degree at most 2, and any irreducible polynomial must have degree at most 2.

(c) Let $f(x) \in \mathbb{R}[x]$ be a real polynomial of odd degree. Let $f = p_1 p_2 \cdots p_n$ be a decomposition of f into irreducibles. Since $\deg(f) = \sum_i \deg(p_i)$, at least one of p_i must have odd degree. If p_i is an irreducible polynomial of odd degree, then it has degree 1 and is equal to $x - z$ where z is a real root of f.

3. Since $\mathbb{F} \subseteq \mathbb{F}(\alpha^2) \subseteq \mathbb{F}(\alpha)$, we have

$$[\mathbb{F}(\alpha) : \mathbb{F}] = [\mathbb{F}(\alpha) : \mathbb{F}(\alpha^2)][\mathbb{F}(\alpha^2) : \mathbb{F}].$$

Suppose $\mathbb{F}(\alpha^2) \neq \mathbb{F}(\alpha)$. Since α is a root of $x^2 - \alpha^2 \in \mathbb{F}(a^2)[x]$, then $[\mathbb{F}(\alpha) : \mathbb{F}(\alpha^2)] = 2$. But this is a contradiction because $[\mathbb{F}(\alpha) : \mathbb{F}(\alpha^2)]$ does not divide $[\mathbb{F}(\alpha) : \mathbb{F}]$.

4. We have the chain of field extensions $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{\mathrm{p}}) \subseteq \mathbb{Q}(\zeta_{\mathrm{p^r}})$, so

$$[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}(\zeta_p)][\mathbb{Q}(\zeta_p) : \mathbb{Q}].$$

ζ_{p^r} is a root of $x^{p^{r-1}} - \zeta_p$ over $\mathbb{Q}(\zeta_p)$, which means $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}(\zeta_p)] = p^{r-1}$ (and it is probably irreducible because of ζ_p). ζ_p has been shown to be a root of the irreducible polynomial $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$, which means $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. Thus

$$[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = p^{r-1} \cdot (p-1).$$

5. Suppose $\zeta_5 \in \mathbb{Q}(\zeta_7)$, so that $\mathbb{Q}(\zeta_5) \subseteq \mathbb{Q}(\zeta_7)$. Then $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ divides $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$ which is a contradiction.