MATH 435 ASSIGNMENT 11

ARNOLD JIADONG YU

1. Extension Fields

1.1. 4. Find the splitting field of x^4+1 over Q.
proof: Let E be an extension field of F and let $f(x)=x^4+1\in Q[x]$ splits in E. By inspection, $e^{i\pi}=-1 \implies e^{i\frac{\pi}{4}}$ is a zero. Moreover, it has four roots in C. They are $e^{i\frac{\pi}{4}}, e^{i\frac{3\pi}{4}}, e^{i\frac{5\pi}{4}}, e^{i\frac{7\pi}{4}}$. Notice that $e^{i\frac{\pi}{4}}$ generates other roots, i.e. $Q(e^{i\frac{\pi}{4}}, e^{i\frac{3\pi}{4}}, e^{i\frac{5\pi}{4}}, e^{i\frac{7\pi}{4}})=Q(e^{i\frac{\pi}{4}})$ and $(e^{i\frac{\pi}{4}})^{-1}=e^{i\frac{7\pi}{4}}\in Q(e^{i\frac{\pi}{4}})$, so $Q(e^{i\frac{\pi}{4}})$ is the splitting field.

1.2. 20. Let F be a field, and let a and b belong to F with $a\neq 0$. If c belongs to some extension of F, prove that $F(c)=F(ac+b)$. (F "absorbs" its own elements.
proof: ($\supseteq$). Let E be an extension of F, then $F\subset E$, $c\in E, a, b\in F$. i.e. $ac\in F(c)$ and $b\in F \implies ac+b\in F(c)$. Hence $F(c)\supseteq F(ac+b)$.
($\subseteq$) Given $a\neq 0$, then $(ac+b)\cdot\frac{1}{a}+(-\frac{b}{a})=c\in F(ac+b)$ since $ac+b\in F(ac+b), \frac{1}{a}, -\frac{b}{a}\in F$. Hence $F(c)\subseteq F(ac+b)$.
As a result, $F(c)\supseteq F(ac+b)$.

1.3. Let F be a field. Prove that F is an extension of Q, or F is an extension of $\mathbb{Z}_p$ for some prime p. (In the former case, we say the fields has characteristic zero, and in the latter case, we say it has characteristic p.)
proof: Let F be a field, then F is also integral domain. By characteristic of an integral domain, the characteristic of F is 0 or prime. If F is a infinite field, its characteristic is 0, if F is a finite field, its characteristic is prime. Assume F is a infinite field, then its characteristic is 0 and the smallest subfield denoted S of F must contain $0, 1$. i.e. S must contain Z. Moreover, S is a field and contain Z, then it must contain quotient field of Z which is Q. i.e. $S\cong Q$. Hence Q is a subfield of F, i.e. F is an extension of Q.
Assume F is a finite field, then by Fundamental Theorem of Finite Abelian Groups,

$$F\cong Z_{p_1^{n_1}}\oplus ...\oplus Z_{p_k^{n_k}}$$

where p_i are primes where $1 \leq i \leq k$. As a result, F is an extension of Z_p for some prime p. To be more precise, $F \cong Z_{p^n}$ since F has characteristic p.
Hence F is an extension of Q, or F is an extension of $\mathbb{Z}_p$ for some prime p.

1.4. 24*

1.5. 16. Suppose that β is a zero of $f(x) = x^4+x+1$ in some extension field E of Z_2. Write $f(x)$ as a product of linear factors in $E[x]$.
proof: $\beta \in E, Z_2(\beta) \subseteq E$ and $f(\beta) = \beta^4 + \beta + 1 = 0$, then $\beta^4 = -\beta - 1 = \beta + 1$. Moreover, we notice $f(x+y) = (x+y)^4 + (x+y) + 1 = x^4 + y^4 + x + y + 1 = f(x) + f(y) + 1$, and $f(1) = 1$. Then

$$f(\beta + 1) = f(\beta) + f(1) + 1 = 0 + 1 + 1 = 0$$

i.e. $\beta + 1$ is a zero of $f(x)$ and $\beta + 1 \in E$. Moreover,

$$f(x^2) = x^8+x^2+1 = x^8+x^5+x^4+x^5+x^2+x+x^4+x+1 = (x^4+x+1)^2 = f(x)^2$$

$$f(\beta^2) = (f(\beta))^2 = 0$$

i.e. β^2 is a zero of $f(x)$ and $\beta^2 \in E$. Therefore, $\beta^2 + 1$ is also a zero of $f(x)$ and $\beta^2 + 1 \in E$. As a result,

$$f(x) = (x + \beta)(x + \beta + 1)(x + \beta^2)(x + \beta^2 + 1) \in E[x]$$