

Mathematics GU4042 Modern Algebra II

Assignment # 7

Benjamin Church

February 16, 2020

Page 193.

Problem 1.

Over \mathbb{C} , the polynomial $P(X) = X^3 - 2 = \left(\frac{X}{\sqrt[3]{2}}\right)^3 - 1$ thus, any solution to $P(X) = 0$ must be a 3rd root of unity times $\sqrt[3]{2}$. The third roots of unity are generated by $\zeta_3 = \frac{-1+\sqrt{3}}{2}$ so every root can be written in the form $\zeta_3^n \sqrt[3]{2}$. Also, $(\zeta_3^2 \sqrt[3]{2})/2 = \zeta_3$ so we know that both ζ_3 and $\sqrt[3]{2}$ must be in the splitting field and clearly every root is generated by these elements. Thus, the splitting field is $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$.

Problem 2.

Consider the polynomial $P(X) = X^4 + 5X^2 + 6$. Over \mathbb{Q} this polynomial can be factored as $(X^2 + 3)(X^2 + 2)$ so the roots in \mathbb{C} are $\pm i\sqrt{3}$ and $\pm i\sqrt{2}$. The splitting field must contain both $i\sqrt{3}$ and $i\sqrt{2}$ and these two elements plus \mathbb{Q} generate all the roots. Thus, the splitting field is $\mathbb{Q}(i\sqrt{3}, i\sqrt{2})$.

Problem 3.

The polynomial $f = X^2 + X + 1$ has no roots in \mathbb{F}_2 . This is easily checked because \mathbb{F}_2 is finite: $f(0) = 0^2 + 0 + 1 = 1$ and $f(1) = 1^2 + 1 + 1 = 1$. From problem # 9 on assignment # 3, we know that any degree two polynomial over \mathbb{F}_2 is irreducible iff it has no roots in \mathbb{F}_2 . Thus, f is irreducible over \mathbb{F}_2 and therefore, $E = \mathbb{F}_2[X]/(X^2 + X + 1)$ is a field. We know that $[E : F] = 2$ because $\deg f = 2$ with $\{1, X\}$ forming a basis of E over F . Since F contains 2 elements, E contains 4 elements, namely, $0, 1, X, 1 + X$. By the classification of finite fields, there is a unique field extension of \mathbb{F}_2 of degree 2 or equivalently of order 4. Thus, $E \cong \mathbb{F}_{2^2}$ which is the splitting field of $X^4 - X = X(X - 1)(X^2 + X + 1)$ over \mathbb{F}_2 . This can be seen explicitly because \mathbb{F}_2 already contains every root of X and $X - 1$ so we need only extend by the roots of $X^2 + X + 1$. We explicitly exhibit the addition and multiplication tables below.

+	0	1	X	1 + X	·	0	1	X	1 + X
0	0	1	X	1 + X	0	0	0	0	0
1	1	0	1 + X	X	1	0	1	X	1 + X
X	X	1 + X	0	1	X	0	X	1 + X	1
1 + X	1 + X	X	1	0	1 + X	0	1 + X	1	X

$(\mathbb{F}_{2^2}, +) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $(\mathbb{F}_{2^2}^\times, \cdot) \cong \mathbb{Z}/3\mathbb{Z}$.

Problem 5.

Let K be a field of characteristic $p > 0$. Then suppose that K contains a subfield, F , of order p^n . Then $F^\times = F \setminus \{0\}$ is a finite subgroup of K^\times and thus cyclic of order $p^n - 1$. By Lagrange, $\forall r \in F^\times : r^{p^n-1} = 1$. Thus, every $r \in F$ satisfies $r^{p^n} - r = 0$ (zero also satisfies this polynomial). Therefore, K contains p^n distinct roots of $X^{p^n} - X$ which has order p^n so the polynomial $X^{p^n} - X$ must split over K . Conversely, suppose that $X^{p^n} - X$ splits over K . Then, $\exists \alpha_1, \dots, \alpha_{p^n} \in K$ such that,

$$X^{p^n} - X = (X - \alpha_1) \cdots (X - \alpha_{p^n})$$

K has characteristic p so K contains a prime subfield isomorphic to \mathbb{F}_p . The subfield $\mathbb{F}_p(\alpha_1, \dots, \alpha_{p^n})$ is the splitting field of $X^{p^n} - X$ over \mathbb{F}_p . By the classification of finite fields, $\mathbb{F}_p(\alpha_1, \dots, \alpha_{p^n}) \cong \mathbb{F}_{p^n}$. Thus, K contains an isomorphic copy of \mathbb{F}_{p^n} . This is the unique subfield of order p^n because every element of $F \subset K$ with order p^n must be a root of $X^{p^n} - X$ but all p^n roots are contained in $\mathbb{F}_p(\alpha_1, \dots, \alpha_{p^n})$ so $F \subset \mathbb{F}_p(\alpha_1, \dots, \alpha_{p^n})$ however, they both have order p^n so $F = \mathbb{F}_p(\alpha_1, \dots, \alpha_{p^n})$.

Problem 7.

Let K be a field and let L, M be finite subfields of order p^l and p^m respectively. Now, $L \cap M$ is a finite field and it is a subfield of both L and M therefore, it is a subgroup of both so by Lagrange, its order divides p^l and p^m so $|L \cap M| = p^d$ for some $d \leq \max\{l, m\}$. By Lemma ??, since $|L \cap M|$ is a subfield of both L and M with order p^d we must have that $d \mid l$ and $d \mid m$. Suppose that $c \mid l$ and $c \mid m$ then by Lemma ??, there exist subfields of L and of M with order p^c . However, by problem 5, K contains at most one subfield of order p^c so there is a single subfield, F contained in both L and M with order p^c . Thus, $F \subset L \cap M$ so, by Lemma ??, $c \mid d$. Therefore, $d = \gcd(l, m)$.

Lemmas

Lemma 0.1. There exists a subfield of order p^m in \mathbb{F}_{p^n} if and only if $m \mid n$.

Proof. \mathbb{F}_{p^n} has characteristic p and therefore contains an isomorphic copy of \mathbb{F}_p . Suppose that K is a subfield of \mathbb{F}_{p^n} then $[\mathbb{F}_{p^n} : K][K : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ thus $[K : \mathbb{F}_p] \mid n$ so $K = p^m$ with $m \mid n$. Suppose that $m \mid n$ then let $n = mr$,

$$P(X) = X^{p^n} - X = (X^{p^m} - X)(X^{p^{n-m}} + X^{p^{n-2m}+1} + \dots + X^{p^{m+r-1}} + X^r)$$

We can show that this division must be possible by modular arguments. Because $m \mid n$ we have $p^m - 1 \mid p^n - 1$ by Lemma ?? so,

$$\text{mod } X^{p^m-1} 1 (X^{p^m-1} - 1) \implies \text{mod } X^{p^n-1} 1 (X^{p^m-1} - 1) \implies X^{p^m-1} - 1 \mid X^{p^n-1} - 1$$

However, $X^{p^n} - X$ splits over \mathbb{F}_{p^n} and thus, $X^{p^m} - X$ splits over \mathbb{F}_{p^n} . Since \mathbb{F}_{p^n} has characteristic p , by problem 5, there exists a unique subfield of order p^m . \square

Lemma 0.2. $\gcd(a^r - 1, a^s - 1) = a^{\gcd(r,s)} - 1$ and in particular, $a^r - 1 \mid a^s - 1 \iff r \mid s$

Proof. Let $d = \gcd(r, s)$ so there exist integers x, y s.t. $ax + by = d$. Now, let $g = a^d - 1$ then,

$$\text{mod } a^d 1 g \implies \text{mod } a^r 1 g \text{ and } \text{mod } a^s 1 g$$

Therefore, $g \mid a^r - 1$ and $g \mid a^s - 1$. Suppose that $c \mid a^r - 1$ and $c \mid a^s - 1$ then,

$$\text{mod } a^s 1c \text{ and } \text{mod } a^r 1c \implies \text{mod } a^{ax+by} = a^d 1c \implies c \mid a^d - 1 = g$$

Thus, $g = \gcd(a^r - 1, a^s - 1)$. We need not worry about taking a^r or a^s to negative powers because they are invertible modulo c . \square