Debra Griffin
Field Extensions, Part III, Handout
Supplement to Section 3.8
Worksheet #1 - 4

---

1. *Prove that* $\mathbb{Z}_3[x]/(x^3 - x^2 + 1) \cong \mathbb{Z}_3[x]/(x^3 - x^2 + x + 1)$.

Proof:
Let $f(x) = x^3 - x^2 + 1$. Then $f(0) = 1, f(1) = 1, f(2) = 2$.

Let $g(x) = x^3 - x^2 + x + 1$. Then $g(0) = 1, g(1) = 2, g(2) = 1$.

Thus, $f(x)$ and $g(x)$ have no linear factors, and since each has degree 3, then

each is irreducible over $\mathbb{Z}_3$.

By Kronecker's Them, Lecture Notes 3/17/10 (If F is a field and $f(x) \in F[x]$ such that $f(x)$ is not constant, then there is an extension, E of F, that contains a root of $f(x)$.)

$\exists$ E and E' such that $f(x)$ has a root a in E and $g(x)$ has a root a' in E'.

By Lecture Notes 3/10/10 (If E/F is an extension, $a \in E$, and a is algebraic over F, then $F(a) \cong F[x](p(x))$ where $p(x)$ is an irreducible polynomial in $F[x]$ such that a is a root.)

we have $\mathbb{Z}_3(a) \cong \mathbb{Z}_3[x]/(x^3 - x^2 + 1)$ and $\mathbb{Z}_3(a') \cong \mathbb{Z}_3[x]/(x^3 - x^2 + x + 1)$.

By Lecture Notes 3/10/10, (If E/F is an extension, $a \in E$ where a is algebraic over F, $p(x)$ is an irreducible polynomial in $F[x]$ such that a is a root, deg $p(x) = n$, then … $[F(a):F] = n$.) and Vector Space HW #9 (If V is a vector space over $\mathbb{Z}_p$ with dim $V = n$, then $|V| = p^n$)
$|\mathbb{Z}_3(a)| = |\mathbb{Z}_3(a')| = 3^3 = 27$.

And by Lecture Notes 3/24/10 (Any 2 fields of order p^n are isomorphic.) we have

$\mathbb{Z}_3(a) \cong \mathbb{Z}_3[x]/(x^3 - x^2 + 1) \cong \mathbb{Z}_3[x]/(x^3 - x^2 + x + 1) \cong \mathbb{Z}_3(a')$.

---

2. *Write addition and multiplication tables for $\mathbb{F}_8$, the field with 8 elements.*

+	0	1	a	a^2	a^3	a^4	a^5	a^6
0	0	1	a	a^2	a^3	a^4	a^5	a^6
1	1	0	a^3	a^6	a	a^5	a^4	a^2
a	a	a^3	0	a^4	1	a^2	a^6	a^5
a^2	a^2	a^6	a^4	0	a^5	a	a^3	1
a^3	a^3	a	1	a^5	0	a^6	a^2	a^4
a^4	a^4	a^5	a^2	a	a^6	0	1	a^3
a^5	a^5	a^4	a^3	a^6	a^2	1	0	a
a^6	a^6	a^2	a^5	1	a^4	a^3	a	0

×	0	1	a	a^2	a^3	a^4	a^5	a^6
0	0	0	0	0	0	0	0	0
1	0	1	a	a^2	a^3	a^4	a^5	a^6
a	0	a	a^2	a^3	a^4	a^5	a^6	a^5
a^2	0	a^2	a^3	a^4	a^5	a^6	1	a
a^3	0	a^3	a^4	a^5	a^6	1	a	a^2
a^4	0	a^4	a^5	a^6	1	a	a^2	a^3
a^5	0	a^5	a^6	1	a	a^2	a^3	a^4
a^6	0	a^6	1	a	a^2	a^3	a^4	a^5

Proof:

Since $\mathbb{F}_8^*$ is cyclic, by Extension Field Part II HW #3, then $\mathbb{F}_8^* = \{1, a, a^2, a^3, a^4, a^5, a^6\}$. From this, the multiplication table for $\mathbb{F}_8$ is straightforward.

To determine the addition table, let $f(x) = x^3 + x + 1$, and note the following:

$f(x)$ is irreducible over $\mathbb{Z}_2$ as $f(0) = 1$, $f(1) = 1$, and $\deg f(x) = 3$.

By Kronecker's Them, Lecture Notes 3/17/10 (If F is a field and $f(x) \in F[x]$ such that $f(x)$ is not constant, then there is an extension, E of F, that contains a root of $f(x)$.)

$\exists$ E such that $f(x)$ has a root a in E.

By Lecture Notes 3/10/10 (If E/F is an extension, $a \in E$, and a is algebraic over F, then $F(a) \cong F[x](p(x))$ where $p(x)$ is an irreducible polynomial in $F[x]$ such that a is a root.)

we have $\mathbb{Z}_2(a) \cong \mathbb{Z}_2[x]/(x^3 + x + 1)$

By Lecture Notes 3/10/10, (If E/F is an extension, $a \in E$ where a is algebraic over F, $p(x)$ is an irreducible polynomial in $F[x]$ such that a is a root, $\deg p(x) = n$, then … $[F(a):F] = n$.)

and Vector Space HW #9 (If V is a vector space over $\mathbb{Z}_p$ with $\dim V = n$, then $|V| = p^n$)

$|\mathbb{Z}_2(a)| = 2^3 = 8 = |\mathbb{F}_8|$.

Thus $a^3 + a + 1 = 0$. From this we have

$a^3 + a + 1 = 0$; $a^4 + a^2 + a = 0$; $a^5 + a^3 + a^2 = 0$; and $a^6 + a^4 + a^3 = 0$

By substitution and the fact that the order of any nonzero element of $\mathbb{F}_8$ is 2, we can determine the rest of the table. Observe.

$a + 1 = a^3$ $a^2 + 1 = a^4 + a + 1 = a^4 + a^3 = a^6$ $a^3 + 1 = a$ $a^4 + 1 = a^2 + a + 1 = a^3 + a^2 = a^5$ $a^5 + 1 = a^3 + a^2 + 1 = a + a^2 = a^4$ $a^6 + 1 = a^4 + a^3 + 1 = a^4 + a = a^2$	$a^2 + a = a^2 + a^3 + 1 = a^5 + 1 = a^4$ $a^3 + a = a^3 + a^3 + 1 = 1$ $a^4 + a = a^4 + a^3 + 1 = a^6 + 1 = a^2$ $a^5 + a = a^5 + a^3 + 1 = a^2 + 1 = a^6$ $a^6 + a = a^6 + a^3 + 1 = a^4 + 1 = a^5$	$a^3 + a^2 = a^5$ $a^4 + a^2 = a$ $a^5 + a^2 = a^3$ $a^6 + a^2 = a^4$
$a^4 + a^3 = a^6$ $a^5 + a^3 = a^2$ $a^6 + a^3 = a^4$	$a^5 + a^4 = a^5 + a^2 + a = a^3 + a = 1$ $a^6 + a^4 = a^3$	$a^6 + a^5 = a^6 + a^3 + a^2 = a^4 + a^2 = a$

See Gallian for an alternative addition and multiplication table.

---

3. *Is $\mathbb{F}_4$ a subfield of $\mathbb{F}_8$? (Prove or disprove).*

No. $\mathbb{F}$ is not a subfield of $\mathbb{F}_8$.

Proof:

If $|\mathbb{F}_4| = 4 = 2^2$, then $\text{char}(\mathbb{F}_4) \neq 0$, hence $\text{char}(\mathbb{F}_4) = 2$

by Lecture Notes 3/8/10 (If F is a field, then char $(F) = 0$ or char $(F) = p$ for some prime p.)

So then $\mathbb{F}_4$ contains a subfield isomorphic to $\mathbb{Z}_2$

by Lecture Notes 3/8/10 (Let F be a field… If char $(F) = p$, then F contains a subfield isomorphic to $\mathbb{Z}_p$.)

And by Vector Space HW #9 $[\mathbb{F}_8:\mathbb{Z}_2] = 3$.

Similarly, $[\mathbb{F}_4:\mathbb{Z}_2] = 2$.

If $\mathbb{F}_4$ a subfield of $\mathbb{F}_8$, then by Extension Fields HW #14(a) (Let F be a field and let E and E' be two extension fields of F with $E \subseteq E'$, then $[E':F] \geq [E:F]$.)

we have $[\mathbb{F}_8: \mathbb{F}_4] \leq [\mathbb{F}_8:\mathbb{Z}_2] = 3$

So then Lecture Notes 3/15/10 (If K is an extension of E, E is an extension of F, and $[K:E]$ and $[E:F]$ are both finite, then $[K:F] = [K:E][E:F]$.) gives us that

$3 = [\mathbb{F}_8:\mathbb{Z}_2] = [\mathbb{F}_8: \mathbb{F}_4][\mathbb{F}_4:\mathbb{Z}_2] = m \bullet 2$ for some positive integer m, a contradiction.

$\therefore$ $\mathbb{F}_4$ is not a subfield of $\mathbb{F}_8$.

---

4. *For any prime p, prove that if F_{p^n} is a subfield of F_{p^m}, then $n|m$.*

Proof:

By proof parallel to $[F_4:\mathbb{Z}_2] = 2$ in #3 above, $[F_{p^n}:\mathbb{Z}_p] = n$ and $[F_{p^m}:\mathbb{Z}_p] = m$.

So $m = [F_{p^m}:\mathbb{Z}_p] = [F_{p^m}: F_{p^n}][F_{p^n}:\mathbb{Z}_p] = rn$ for some positive integer r.

$\therefore$ $n|m$.
