MATH 435 ASSIGNMENT 10

ARNOLD JIADONG YU

1. Extension Fields

1.1. 2. Show that $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$.
proof: ($\subseteq$).

$$(\sqrt{2} + \sqrt{3})^{-1} = \frac{1}{\sqrt{2} + \sqrt{3}} \cdot \frac{\sqrt{2} - \sqrt{3}}{\sqrt{2} - \sqrt{3}} = -\sqrt{2} + \sqrt{3} \in Q(\sqrt{2} + \sqrt{3})$$

i.e.

$$[(\sqrt{2} + \sqrt{3}) + (-\sqrt{2} + \sqrt{3})]/2 = \sqrt{3} \in Q(\sqrt{2} + \sqrt{3})$$
$$[(\sqrt{2} + \sqrt{3}) - (-\sqrt{2} + \sqrt{3})]/2 = \sqrt{2} \in Q(\sqrt{2} + \sqrt{3})$$

Therefore, $Q(\sqrt{2}, \sqrt{3}) \subseteq Q(\sqrt{2} + \sqrt{3})$
($\supseteq$).

$$\sqrt{2} \in Q(\sqrt{2}, \sqrt{3}), \sqrt{3} \in Q(\sqrt{2}, \sqrt{3})$$
$$\implies \sqrt{2} + \sqrt{3} \in Q(\sqrt{2}, \sqrt{3})$$

Therefore, $Q(\sqrt{2}, \sqrt{3}) \supseteq Q(\sqrt{2} + \sqrt{3})$
Hence, $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$.

1.2. 8. Let $F = Z_2$, and let $f(x) = x^3 + x + 1 \in F[x]$. Suppose that a is a zero of $f(x)$ in some extension of F. How many elements does $F(a)$ have? Express each member of $F(a)$ in terms of a. Write out a complete multiplication table for $F(a)$.
proof: $Z_2 = \{0, 1\}$, then $f(0) = 1, f(1) = 1$ which is nonzero. Hence $f(x)$ doesn't have root in Z_2, i.e. $f(x)$ is irreducible in $Z_2[x]$. By Fundamental Theorem of Field Theorem, and Theorem 20.3 $F(a) \cong F[x]/\langle p(x)\rangle$,

$$F(a) \cong F[x]/\langle f(x)\rangle = Z_2[x]/\langle x^3 + x + 1\rangle$$
$$\implies Z_2[x]/\langle x^3 + x + 1\rangle = c_2x^2 + c_1x + c_0 \; c_2, c_1, c_0 \in Z_2$$
$$\implies F(a) = c_2a^2 + c_1a + c_0 \; c_2, c_1, c_0 \in Z_2$$

and $|F(a)| = 2 \cdot 2 \cdot 2 = 8$. i.e. $F(a)$ has 8 elements and they are

$$0, 1, a, a + 1, a^2, a^2 + 1, a^2 + a, a^2 + a + 1$$

and the multiplication table is

	0	1	a	$a+1$
0	0	0	0	0
1	0	1	a	$a+1$
a	0	a	a^2	a^2+a
$a+1$	0	$a+1$	a^2+a	a^2+1
a^2	0	a^2	$a+1$	a^2+a+1
a^2+1	0	a^2+1	1	a^2
a^2+a	0	a^2+a	a^2+a+1	1
a^2+a+1	0	a^2+a+1	a^2+1	a

	a^2	a^2+1	a^2+a	a^2+a+1
0	0	0	0	0
1	a^2	a^2+1	a^2+a	a^2+a+1
a	$a+1$	1	a^2+a+1	a^2+1
$a+1$	a^2+a+1	a^2	1	a
a^2	a^2+a	a	a^2+1	1
a^2+1	a	a^2+a+1	$a+1$	a^2+a
a^2+a	a^2+1	$a+1$	a	a^2
a^2+a+1	1	a^2+a	a^2	$a+1$

1.3. 10. Let $F(a)$ be the field described in Exercise 8. Show that a^2 and a^2+a are zeros of x^3+x+1.
proof:

$$f([a^2]) = [a^2]^3 + [a^2] + [1] = [a^6 + a^2 + 1]$$

$$f([a^2+a]) = [a^2+a]^3 + [a^2+a] + [1] = [a^6 + a^5 + a^4 + a^3 + a^2 + a + 1]$$

Moreover,

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

Hence

$$f([a^2]) = [2a^2+2] = 0$$

$$f([a^2+a]) = [4a^2+4a+4] = 0$$

i.e. a^2 and a^2+a are zeros of x^3+x+1.

1.4. 59.* Let D be an integral domain and let F be the field of quotients of D. Show that if E is any field that contains D, then E contains a subfield that is ring-isomorphic to F. (Thus, the field of quotients of an integral domain D is the smallest field containing D.)
proof: