MATH 210B

Name: Quin Darcy **Due Date:** 2/19/20
Instructor: Dr. Shannon **Assignment:** Homework 4

1. Prove that $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\sqrt{i})$.

Proof. We begin by noting that a basis for $\mathbb{Q}(i, \sqrt{2})$ is $B_1 = \{1, i, \sqrt{2}, \sqrt{2}i\}$ and a basis for $\mathbb{Q}(\sqrt{i})$ is $B_2 = \{1, \sqrt{i}, i\}$. Now since $\mathbb{Q}(i, \sqrt{2})$ is a field, then both $1/\sqrt{2}$ and $i/\sqrt{2}$ are elements. Moreover, it is closed under addition and multiplication. With this in mind consider

$$\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)^2 = \left(\frac{1 + 2i - 1}{2}\right) = i.$$

From this is follows that

$$\sqrt{i} = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}} \in \mathbb{Q}(i, \sqrt{2}).$$

Thus, $B_2 \subseteq \mathbb{Q}(i, \sqrt{2})$ and hence $\mathbb{Q}(\sqrt{i}) \subseteq \mathbb{Q}(i, \sqrt{2})$. Similarly, we have shown that

$$\sqrt{i} - \frac{i}{\sqrt{2}} = \frac{1}{\sqrt{2}} \in \mathbb{Q}(\sqrt{i}),$$

and so this element has a multiplicative inverse, namely, $\sqrt{2} \in \mathbb{Q}(i)$. Lastly, since $\sqrt{2}(\sqrt{i})^2 = \sqrt{2}i \in \mathbb{Q}(\sqrt{i})$, then $B_1 \subseteq \mathbb{Q}(\sqrt{i})$ and thus $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\sqrt{i})$. Therefore, $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\sqrt{i})$. $\square$

3. The Möbious function, μ, is defined by the following: $\mu(1) = 1$; if $t > 1$, then let $t = p_1^{r_1} \cdots p_m^{r_m}$ be the prime factorization of t. $\mu(t) = (-1)^m$, if $r_i = 1$ for all i, $1 \leq i \leq m$, and $\mu(t) = 0$, if $r_i > 1$ for some i. Then

$$\Phi_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}.$$

Using this result, find Φ_3, Φ_4, Φ_5, Φ_6.

Solution. Using the given formula, we get:

$$\Phi_3(x) = \prod_{d|3} (x^{3/d} - 1)^{\mu(d)} = (x^3 - 1)(x - 1)^{-1} = x^2 + x + 1.$$

$$\Phi_3(x) = \prod_{d|4} (x^{4/d} - 1)^{\mu(d)} = (x^4 - 1)(x^2 - 1)^{-1} = x^2 + 1.$$

$$\Phi_5(x) = \prod_{d|5} (x^{5/d} - 1)^{\mu(d)} = (x^5 - 1)(x - 1)^{-1} = x^4 + x^3 + x^2 + x + 1.$$

$$\Phi_6(x) = \prod_{d|6} (x^{6/d} - 1)^{\mu(d)} = \frac{x^7 - x^6 - x + 1}{x^5 - x^3 - x^2 + 1}.$$

4. Assume that F is a finite field.

   (a) Explain (one sentence) why char(F) is a prime number, p, and why F contains a subfield that is isomorphic to $\mathbb{Z}_p$.

   Solution. Since F is a field, then it has no zero divisors and so if the characteristic were composite, say ab, then either $a1_F$ or $b1_F$ is zero, contradicting the definition of characteristic. Moreover, the set $\{a1_F \colon a \in \mathbb{Z}\}$ is a subfield of F with order p, and thus isomorphic to $\mathbb{Z}_p$.

   (b) By (a), F is a vector space over $\mathbb{Z}_p$. Assume that $[F \colon \mathbb{Z}_p] = n$. Determine (with proof) $|F|$.

   Proof. Let $\{r_0, \ldots, r_{n-1}\}$ be a basis for F over $\mathbb{Z}_p$ and consider any $w \in F$. Then for $a_0, \ldots, a_{n-1} \in \mathbb{Z}_p$, we have

   $$w = a_o r_0 + \cdots + a_{n-1} r_{n-1}.$$

   since there are n many basis elements and p many choices for each coefficient, then it follows that there are p^n many elements in F. Thus, $|F| = p^n$. $\square$

   (c) Give a field with 125 elements.

   Solution. By HW3, $x^3 + x + 1$ is irreducible over $\mathbb{Z}_5$. Thus, $\mathbb{Z}_5/(x^3 + x + 1)_i$ is a field. We know that $\{I + 1, I + x, I + x^2\}$ is a basis and so $I + (a + bx + cx^2)$ represents any elements of this field. There are 5 choices for a, b and c. Thus, there are $5^3 = 125$ elements in this field.

5. Factor $x^3 - 2$ into irreducible factors over $\mathbb{Q}$, over $\mathbb{R}$, over $\mathbb{C}$, over $\mathbb{Z}_3$, and over $\mathbb{Z}_5/(x^2 + 3x + 4)_i$.

   Solution.

   $\mathbb{Q}$: $x^3 - 2$;
   $\mathbb{R}$: $(x - 2^{1/3})(x^2 + 2^{1/3}x + 2^{2/3})$;
   $\mathbb{C}$: $(x - 2^{1/3})(x + \frac{1 - i\sqrt{3}}{2^{2/3}})(x + \frac{1 + i\sqrt{3}}{2^{2/3}})$;
   $\mathbb{Z}_3$: $(x - 2)^2(x + 1)$;
   $\mathbb{Z}_5/(x^2 + 3x + 4)_i$: $(I + 3)(I + x)(I + 4x + 2)$.

6. Assume that E is a field and F is a subfield of E. Let $K = \{a \in E \colon a \text{ is algebraic over } F\}$. Prove that K is a subfield of E that contains F.

   Proof. To begin we note that for any $a \in F$, a is algebraic over F since a is a root of $x - a \in F[x]$. Thus, $F \subseteq K$. Now let $a, b \in K$. Then $x - a \mid f(x)$ and $x - b \mid g(x)$ for some $f(x), g(x) \in F[x]$. Thus, for $q_1(x), q_2(x) \in F[x]$, we have that

   $$f(x) = q_1(x)(x - a) \quad \text{and} \quad g(x) = q_2(x)(x - b).$$

Since $F[x]$ is a ring, then the addition and multiplication of any of the nonzero polynomials in $F[x]$ will result in another element of $F[x]$. From this we can first show that $-g(x) + 2xq_2(x) = q_2(x)(x+b)$ and so $-b \in K$. Furthermore, it follows that

$$f(x) + g(x) + q_1(x)a - q_2(x)b + (q_1(x) + q_2(x))(-a+b) = (q_1(x) + q_2(x))(x - (a-b)).$$

Thus, there is some polynomial in $F[x]$ for which $(x - (a-b))$ is a factor. Hence, $a - b \in K$. Now we must show that $ab^{-1} \in K$. First, we observe that if $g(x) = c_0 + c_1x + \cdots + c_nx^n$, then $g(b) = c_0 + c_1b + \cdots + c_nb^n = 0$. Multiplying both sides by b^{-n}, we get $c_0b^{-n} + c_1b^{-n+1} + \cdots + c_n = 0$. Hence, for the polynomial $g(x)b^n \in F[x]$, b^{-1} is a root and thus $b^{-1} \in K$. Finally, since ab^{-1} is a root of $bx - a \in F[x]$, then $ab^{-1} \in K$. It also follows that since E is a field and $K \subseteq E$, then K has no zero divisors. Thus, K is a commutative ring with identity, no zero divisors and every nonzero element has a multiplicative inverse. Therefore, K is a subfield of E. □

7. Prove that if $[E\colon F]$ is finite, then every element of E is algebraic over F.

   Proof. By Theorem 2, for all $c \in E$, c is algebraic over F iff $[F(c)\colon F]$ is finite. Thus, since $F(c) \subseteq E$ for all $c \in E$, then $[F(c)\colon F]$ is finite for all $c \in E$. Therefore, for all $c \in E$, c is algebraic over F. □

8. Find the minimal polynomial over $\mathbb{Q}$ of each of the following:

   (a) $3 + \sqrt{2}$.

   Solution. To begin we let $x = 3 + \sqrt{2}$ and so $(x-3)^2 = 2$. Thus, $x^2 - 6x + 7 = 0$. Letting $p = 3$, then by the $\mathbb{Z}_p$ test, we see that $\varphi(x^2 - 6x + 7) = x^2 + [1]$. This does not have a root in $\mathbb{Z}_3$ and is therefore irreducible over $\mathbb{Z}_3$ and therefore over $\mathbb{Q}$. Thus, $x^2 - 6x + 7$ is the minimal polynomial.

   (b) $\sqrt{-1 + \sqrt{2}}$.

   Solution. Letting $x = \sqrt{-1 + \sqrt{2}}$, we get that $x^4 + 2x - 1 = 0$. Using the $\mathbb{Z}_p$ test, with $p = 3$ we get that $\varphi(x^4 + 2x - 1) = x^4 + 2x + 2$. It is clear that this has no linear factors since no element of $\mathbb{Z}_3$ is a root for the polynomial. Thus, if it is reducible, then for some $a, b, c, d, e, f \in \mathbb{Z}_3$ we have

   $$x^4 + 2x + 2 = (ax^2 + bx + c)(dx^2 + ex + f).$$

   This yields the following conditions

   i. $ad = 1$
   ii. $ae + bd = 0$
   iii. $af + be + cd = 2$
   iv. $bf + ce = 0$
   v. $cf = 2$

With some calculation we can determine that there are 8 possible polynomials in $\mathbb{Z}_3$ that satisfy the first three conditions, namely (when written as an ordered 6-tuples e.g $2x+1$ is $(2,1)$), are $(1,2,2,1,1,1),(1,2,0,1,1,0),(1,0,0,1,0,2)$,$(1,0,1,1,0,1),(2,2,2,2,1,1),(2,2,0,2,1,0),(2,0,1,2,0,0),(2,0,2,2,0,2)$. However, all of these polynomials either fail conditions iv. or v. Therefore, there is no factors of x^4+2x+2 in $\mathbb{Z}_3$. Thus, the polynomial is irreducible in $\mathbb{Z}_3$ and therefore irreducible in $\mathbb{Q}$. Thus, x^4+2x-1 is the minimal polynomial of $\sqrt{-1+\sqrt{2}}$.

10. Prove that $\mathbb{Q}(\sqrt{3},\sqrt{5}) = \mathbb{Q}(\sqrt{3}+\sqrt{5})$.

Proof. It follows immediately that $\mathbb{Q}(\sqrt{3}+\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3},\sqrt{5})$. Thus we must show that $\sqrt{3},\sqrt{5} \in \mathbb{Q}(\sqrt{3}+\sqrt{5})$. Since $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ is a field, then $(\sqrt{3}+\sqrt{5})^{-1}$ is an element of this field. Thus,

$$\begin{aligned}
(\sqrt{3}+\sqrt{5})^{-1} &= \frac{1}{\sqrt{3}+\sqrt{5}} \\
&= \frac{1}{\sqrt{3}+\sqrt{5}}\frac{(\sqrt{3}-\sqrt{5})}{(\sqrt{3}-\sqrt{5})} \\
&= -\frac{1}{2}\sqrt{3}+\frac{1}{2}\sqrt{5}.
\end{aligned}$$

And so $-\frac{1}{2}(\sqrt{3}-\sqrt{5}) \in \mathbb{Q}(\sqrt{3}+\sqrt{5})$. $(-2)(-\frac{1}{2}(\sqrt{3}-\sqrt{5})) = \sqrt{3}-\sqrt{5} \in \mathbb{Q}(\sqrt{3}+\sqrt{5})$. This implies $\sqrt{3}-\sqrt{5}+\sqrt{3}+\sqrt{5} = 2\sqrt{3} \in \mathbb{Q}(\sqrt{3}+\sqrt{5})$ and so $\sqrt{3} \in \mathbb{Q}(\sqrt{3}+\sqrt{5})$. A similar argument shows that $\sqrt{5} \in \mathbb{Q}(\sqrt{3}+\sqrt{5})$. Therefore, $\mathbb{Q}(\sqrt{3},\sqrt{5}) = \mathbb{Q}(\sqrt{3}+\sqrt{5})$. $\square$