1) Let \( f(x) \) and \( g(x) \) be polynomials in \( F[x] \) such that \( (f(x), g(x)) = 1 \). Prove that if \( h(x) = f(x)g(x) \), then \( F[x]/(h(x)) \cong F[x]/(g(x)) \oplus F[x]/(f(x)) \).

**Proof.** Let \( \phi : F[x] \rightarrow F[x]/(g(x)) \oplus F[x]/(f(x)) \) be the homomorphism defined by \( \phi(p(x)) = [p(x) + (f(x)), p(x) + (g(x))] \). By the First Homomorphism Theorem, it suffices to show that \( \ker(\phi) = (h(x)) \) and \( \phi \) is surjective.

The inclusion \( \ker(\phi) \supseteq (h(x)) \) is immediate. Suppose that \( p(x) \in \ker(\phi) \), then \( p(x) + (f(x)) = 0 + (f(x)) \) and \( p(x) + (g(x)) = 0 + (g(x)) \) so that \( p(x) \in (f(x)) \) and \( p(x) \in (g(x)) \). Thus \( f(x) \) and \( g(x) \) divide \( p(x) \). But as \( f(x) \) and \( g(x) \) are coprime, \( h(x) = f(x)g(x) \) divides \( p(x) \), so that \( p(x) \in (h(x)) \) as required.

To prove surjectivity, we must show that for any \( [p(x) + (f(x)), q(x) + (g(x))] \in F[x]/(g(x)) \oplus F[x]/(f(x)) \), there exists \( r(x) \in F[x] \) such that \( [r(x) + (f(x)), r(x) + (g(x))] = [p(x) + (f(x)), q(x) + (g(x))] \). Since \( (f(x), g(x)) = 1 \), we have such that \( 1 = f(x)\alpha(x) + g(x)\beta(x) \) for some \( \alpha(x), \beta(x) \in F[x] \). Thus \( p(x) - q(x) = f(x)\alpha'(x) + g(x)\beta'(x) \) where \( \alpha'(x) = \alpha(x)(p(x) - q(x)) \) and \( \beta'(x) = \beta(x)(p(x) - q(x)) \). Let \( r(x) = p(x) - f(x)\alpha'(x) = q(x) + g(x)\beta'(x) \), then \( \phi(r(x)) = [p(x) + (f(x)), q(x) + (g(x))] \) as required. \( \square \)

2) Let \( I \subset R \) be an ideal in a commutative ring with 1. Show that \( I \) is maximal if and only if \( R/I \) is a field.

**Proof.** If \( I \) is maximal and \( r + I \in R/I \) is non-zero, then \( r \not\in I \) so that \( (r, I) = R \) and hence \( ar + bi = 1 \) for some \( a, b \in R \) and \( i \in I \). But then \( (a + I)(r + I) = ar + I = (1 - bi) + I = 1 + I \). Thus all elements in \( R/I^* \) are invertible, and so \( R/I \) is a field.

Conversely, suppose that \( R/I \) is a field and let \( I \subset J \subset R \) be an ideal. We must show that \( J = I \) or \( J = R \). If \( I \not= J \), then pick \( j \in J \setminus I \) so that \( j + I \not= 0 + I \). Since \( R/I \) is a field, there is an element \( k \in R \) such that \( (j + I)(k + I) = 1 + I \). It follows that \( jk - 1 = i \in I \). But then \( 1 = jk - i \in J + I = J \) and so \( J = R \). \( \square \)

3) Let \( F \subset K \) be an inclusion of fields. Prove that \( k \in K \) is algebraic over \( F \) if and only if \( F(k) \cong F[x]/(f(x)) \) where \( f(x) \in F[x] \) is an irreducible polynomial. (Note, that the isomorphism is assumed to fix \( F \))

1
Proof. Suppose that \( k \) is algebraic over \( F \), then there is an irreducible polynomial \( f(x) \in F[x] \) such that \( f(k) = 0 \). We may assume that \( f(x) \) has minimal degree amongst all non-zero polynomials such that \( f(a) = 0 \). Let \( \phi : F[x] \to F(a) \) be the homomorphism defined by \( \phi(g(x)) = g(a) \). We claim that \( \text{Ker}(\phi) = (f(x)) \). Since \( f(a) = 0 \), we have the inclusion \( \text{Ker}(\phi) \supseteq (f(x)) \). Suppose on the other hand that \( \phi(g(x)) = 0 \) so that \( g(a) = 0 \). Write \( g(x) = g(x)q(x) + r(x) \) where \( \deg(r(x)) < \deg(f(x)) \). We have \( r(a) = g(a) - f(a)q(a) = 0 \) and so \( r(x) = 0 \), i.e. \( g(x) \in (f(x)) \). Finally, the image of \( \phi \) is a subfield of \( F(a) \) containing \( F \) and \( a \), hence \( \phi \) is onto and by the FHT, \( F(a) \cong F[x]/(f(x)) \).

Suppose now that \( F(k) \cong F[x]/(f(x)) \), then \( \dim_F F(k) = n \) where \( n = \deg f(x) \). But then \( 1, k, k^2, \ldots, k^n \) are linearly dependent so that \( \sum_{i=0}^{n} a_i k^i = 0 \) for some \( a_i \in F \). But then \( k \) is a zero of the polynomial \( \sum_{i=0}^{n} a_i x^i \).

4) Let \( \overline{\mathbb{Q}} \) be the algebraic closure of \( \mathbb{Q} \) in \( \mathbb{C} \). Show that \( [\overline{\mathbb{Q}} : \mathbb{Q}] \) is infinite.

Proof. Let \( a_p \) be a complex root of \( x^p - 2 \). By Eisenstein’s Criterion, this polynomial is irreducible and so \( [\mathbb{Q}(a_p) : \mathbb{Q}] = p \). Since \( \overline{\mathbb{Q}} \supseteq \mathbb{Q}(a_p) \supseteq \mathbb{Q} \), we have \( [\overline{\mathbb{Q}} : \mathbb{Q}] \geq p \) for all \( p \) and hence \( [\overline{\mathbb{Q}} : \mathbb{Q}] \) is infinite.

5) Show that \( x^3 + 2x + 2 \) an irreducible polynomial of degree 3 in \( \mathbb{Z}_3[x] \). Find a generator of the multiplicative group \( (\mathbb{Z}_3[x]/(x^3 + 2x + 2))^* \). How many generators does this group have?

Proof. Since \( x^3 + 2x + 2 \) has no roots and has degree 3, it is irreducible. Thus \( \mathbb{Z}_3[x]/(x^3 + 2x + 2) \) is the finite field with \( 3^3 \) elements and \( (\mathbb{Z}_3[x]/(x^3 + 2x + 2))^* \) is a cyclic group of order 22. There are \( \phi(26) = \phi(2)\phi(13) = 12 \) generators.

We have \((2x + 1)^3 = x^3 + x + 1\), \((2x + 1)^4 = x^2 + 2x = x + 2\), \((2x + 1)^5 = 2x^2 + x + 2\), \((2x + 1)^8 = 2x^2 + 2x + 1\), \((2x + 1)^{13} = 2\) and so the order of \( 2x + 1 \) is 26.

6) Show that \( x^4 + x^3 + x^2 + x + 1 \) is irreducible in \( \mathbb{Q}(\sqrt[3]{3})[x] \).

Proof. \( \phi_4(x) = x^4 + x^3 + x^2 + x + 1 \) is irreducible in \( \mathbb{Q}[x] \) (as seen in class). Let \( \theta \) be a root of \( \phi_4(x) \). Then \( [\mathbb{Q}(\theta) : \mathbb{Q}] = 4 \). Since \( x^5 - 3 \) is irreducible (Eisenstein’s Criterion), we have \( [\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 5 \). Since 4 and 5 are coprime, \( [\mathbb{Q}(\theta, \sqrt[3]{3}) : \mathbb{Q}] = 20 \). But then \( 20 = [\mathbb{Q}(\theta, \sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{3}) \cdot \mathbb{Q}(\sqrt[3]{3})] = 4 \), and hence \( x^4 + x^3 + x^2 + x + 1 \) is irreducible in \( \mathbb{Q}(\sqrt[3]{3})[x] \).

7) Prove that \( [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4 \).
Proof. Let \( a = \sqrt{2} + \sqrt{3} \), then \( a^2 = 5 + 2\sqrt{6} \) and \( a^3 = 5a + 4\sqrt{3} + 3\sqrt{2} = 8a + \sqrt{3} \). But then \( \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \) and hence \( \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \) so that \( \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \). It follows that \( [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] | [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \leq 4 \). To show equality, it suffices to show that \( \sqrt{2} \not\in \mathbb{Q}(\sqrt{3}) \). Suppose \( \sqrt{2} = a + b\sqrt{3} \) where \( a, b \in \mathbb{Q} \), then \( 2 = a^2 + 3b^2 + 2ab\sqrt{3} \) and so \( \sqrt{3} = \frac{2-a^2-3b^2}{2ab} \in \mathbb{Q} \) which is impossible (if \( ab \neq 0 \), \( \sqrt{3} \in \mathbb{Q} \) which is impossible; if \( ab = 0 \) then either \( b = 0 \) so that \( \sqrt{2} = a \) or \( a = 0 \) so \( \sqrt{2} = b\sqrt{3} \) and both cases are easily seen to be impossible). \( \square \)

8) Show that if \( n \geq 3 \), then \( A_n \) is generated by 3-cycles.

Proof. Let \( t = (i, j) \) and \( t' = (i', j') \) be transpositions. We may assume \( i < j \) and \( i' \leq j' \). We claim that if \( t \neq t' \), then \( tt' \) is a product of two 3-cycles. If \( i, i', j, j' \) are all distinct, then \( (i, j)(i', j') = (i, i')(i', j', j) \).

If \( i = i' \), then \( (i, j)(i, j') = (i, j', j) = (i, j, j') \).

If \( g \in A_n \), then \( g = t_1 \cdots t_{2k} \) where \( t_i \) are transpositions. So the first claim follows since by what we have shown above, we have \( t_2t_{2i+1} = g_{2i}g_{2i+1} \) where \( g_{2i} \) and \( g_{2i+1} \) are 3-cycles. \( \square \)