11.1 Prove that all numbers of the form $a + bi$, for each $a, b \in \mathbb{Q}$ are algebraic over $\mathbb{Q}$

Given any numbers $a, b \in \mathbb{Q}$, we can construct

$(x - (a + bi))(x - (a - bi))$

Which is equal to $x^2 - (a + bi)x - (a - bi)x + (a^2 + b^2)$

$= x^2 - 2ax + (a^2 + b^2) \in \mathbb{Q}[x]$, with root $a + bi$

So numbers in the form $a + bi$ for $a, b \in \mathbb{Q}$ are algebraic of $\mathbb{Q}$

11.7 Let n be an integer greater than 1. Prove that $x^n - 2$ is irreducible in $\mathbb{Q}[x]$ by proceeding as follows.

1. Suppose that $x^n - 2 = g(x)h(x)$, where $g(x), h(x)$ are polynomials in $\mathbb{Z}[x]$ of degrees $k, l, k < n, l < n$. We wish to obtain a contradiction. Write out explicit expressions for $g(x), h(x)$.

So there must be integers in $\mathbb{Z}$ for coefficients of $g(x), h(x)$

Then $g(x) = a_k x^k + ...a_0 x^0, h(x) = b_l x^l + ... + b_0 x^0$

2) Show that 2 divides the constant coefficent of $g(x)$ or the constant coeffcient of $h(x)$, but not both. Make a choice, suppose that 2 divides the constant coefficient of $g(x)$, but not the constant coefficient of $h(x)$

The coefficient of x^0 terms for $g(x), h(x)$ are a_0, b_0 respectively.

The coefficient for x^0 for $f(x)$ is -2.

Then $a_0 * b_0 = -2$

So 2 divides exactly of a_0, b_0, since $a_0, b_0 \in \mathbb{Z}$

Without loss of generality, assume $2|a_0$, but $2 \not| b_0$

3) Now look at the degree one coefficient of $g(x)h(x)$, written in terms of the coefficients of $g(x), h(x)$, and use this to prove that 2 divides the degree one coefficients of $g(x)$.

The degree 1 coefficients of the product must be the degree 0 of $g(x)$ multiplied by the degree 1 of $h(x)$, and deg 1 term of $g(x)$ multiplied by the degree 0 term of $h(x)$. So degree one term is sum of $a_0 * b_1 + a_1 * b_0$

Comparing the coefficient of the x^1 term, the coefficient for $f(x)$ is 0, while the coefficient for the degree one term on the product is $a_0 * b_1 + a_1 * b_0$

So $0 = a_0 * b_1 + a_1 * b_0$

Since $2|0, 2|a_0 * b_1$, then $2|a_1 * b_0$

But b_0 is not divisible by 2, from part 2

Then $2|a_1$

4) Similarly, show that 2 divides the degree 2 coefficient of $g(x)$ and the degree 3 coefficient of $g(x)$

Degree 2 of $f(x) = 0$

Degree 2 of $g(x)h(x) = a_1 * b_1 + a_2 * b_0 + a_0 * b_2$

So $0 = a_1 * b_1 + a_2 * b_0 + a_0 * b_2$

2 divides 0, 2 divides all a_1, a_0, terms so 2 must divide a_2

Degree 3 of $f(x) = 0$

Degree 3 of $g(x)h(x) = a_3 * b_0 a_2 * b_1 + a_1 * b_2 + a_0 * b_3$

So $0 = a_3 * b_0 a_2 * b_1 + a_1 * b_2 + a_0 * b_3$

2 divides 0, 2 divides all terms with a_0, a_1, a_2, so 2 must divide a_3

5) The last two parts are just a warmup, so you can see what is going on. now start over again and use the fact that 2 divides the constant coefficient of $g(x)$ along with induction to show that for every i from 0 to k, we have that 2 divides the degree i coefficient of $g(x)$. Conclude from this that in particular, 2 divides the degree k coefficient of $g(x)$

By induction

Base case: done in part previous part

Inductive step

Inductive Hypothesis

Assume that 2 divides the first $m-1$ terms of $g(x)$, and not b_0

Need to show that 2 divides the m^{th} term.

The degree m coefficient of $f(x)$ is 0

The degree m coefficient of the product is the sum $a_m b_0 + a_{m-1} b_1 + ... a_0 b_m$

So $0 = a_m b_0 + a_{m-1} b_1 + .. a_0 b_m$

We know 2 divides 0, and we know that 2 divides all products involving a_i for $i < m$

And we know 2 does not divide b_0,

Then 2 must divide a_m

So 2 divides every coefficient of $g(x)$.

6) Show that this implies that 2 divides the degree-n coefficient of the product $g(x)h(x)$. Observe that this is a contradiction, and conclude that $g(x), h(x)$ as assumed cannot exist.

We know the degree n term of $g(x)h(x)$ is found by multiplying the highest terms of $g(x)$ and $h(x)$, which have coefficents $a_k b_l$

2 divides all coefficients of $g(x)$, so $2|a_k$

Then 2 divides the product $a_k b_l$

but $1 = a_k b_l$

2 divides rhs, but does not divide lhs, contradiction

Then $g(x), h(x)$ cannot exist, as assumed.

Then by corollary 11.5, since $f(x)$ has no factorization as a product of lower degree polynomials in $\mathbb{Z}[x]$, then $f(x)$ is irreeducible in $\mathbb{Q}[x]$

So $f(x) = x^n - 2$ is irreducible in $\mathbb{Q}[x]$

11.10 Using the same kind of arguments you made in exercises 11.7, 11.8, and 11.9, prove that $x^{14} - 27x^{11} + 15x^3 + 12$ does not factorize in $\mathbb{Z}[x]$ as a produc of lower degree polynomials, and therefore is irreducible in $\mathbb{Q}[x]$. Use 3 as the role played by 2 for exercises 7,8 and p in exercises 11.9

Suppose that $f(x) = g(x)h(x)$ for $g, h \in \mathbb{Z}[x]$

Then $g(x) = a_k x^k + ..a_0 x^0$,

And $h(x) = b_l x^l + ...b_0 x^0$, for $l, k \leq 14, l + k = 14$

deg 0 coefficient of f is 12

deg 0 coefficient of $g(x)h(x) = a_0 b_0 = 12$

So 3 divides one of a_0, b_0

without loss of generality, assume 3 divides a_0

Claim: 3 divides all coefficients of $g(x)$

By induction

base case: 3 divides deg 0 of product gxhx (shown above)

Inductive step

Inductive hypothesis

Assume that 3 divides first $m - 1$ terms of gx, and 3 does not divide b_0,show that it divides m term of gx.

The m term of of $f(x)$ is either -27, 15, or 0. All divisible by 3

The m'th term of $g(x)h(x)$ must be $a_m b_0 + a_{m-1} b_1 + ...a_0 b_m$

Since the m'th term of $f(x)$ divisible by 3, the m'th term of $g(x)h(x)$ must also be divisible by 3

Since the other terms $a_i b_j$ for $i + j = m, i < m$ are divisible by 3, the term $a_m b_0$ must also be divisible by 3.

So 3 divides a_m

So 3 divides all coefficients in $g(x)$

So the coefficient of x^{14} for product $g(x)h(x) = a_k b_l$ is also divisible by 3

Coefficient of x^{14} in $f(x)$ is 1

So $1 = a_k b_l$, but rhs divisible by 3, lhs not, contradiction

So $g(x), h(x)$ must not exist

So by corollary 11.5, $f(x)$ is irreducible in $\mathbb{Q}[x]$

11.13 Let us determine all irreducible polynomials of low degree in $\mathbb{F}_2[x], \mathbb{F}_3[x]$

1) Write down all degree two polynomials in $\mathbb{F}_2[x]$. Device which ones are irreducible and which ones have roots in $\mathbb{F}_2[x]$. For each degree two polynomial $f(x)$ that does have roots, describe the roots and the corresponding factorization of $f(x)$ in $\mathbb{F}_2[x]$ as a product of two degree one polynomials.

$x^2 + x + 1$, irreducible

$x^2 + x$, root 0, $f(x) = (x + 1)(x)$

$x^2 + 1$, root 1, $f(x) = (x - 1)(x + 1)$

x^2, root 0, $f(x) = (x)(x)$

2) Write down all degree 3 polynomials in $\mathbb{F}_2[x]$. Decide which ones have roots $\mathbb{F}_2$. For each degree 3 polynomial $f(x)$ that does have roots, describe the roots and the corresponding factorization of $f(x)$ in $\mathbb{F}_2[x]$, either as a product of 3 degree one polynomials, or as a product of a degree 1 and an ireducible degree 2 polynomial

$x^3 + x^2 + x + 1$, root 1 $(x - 1)(x + 1)(x + 1)$

$x^3 + x^2 + 1$, irreducible

$x^3 + x^2 + x + 1$, root 1, $(x - 1)(x + 1)(x - 1)$

$x^3 + x + 1$, irreducible

$x^3 + x^2$, root 0, $x(x^2 + x)$

$x^3 + x$, root 0 $x(x^2 + 1)$

$x^3 + 1$, root 1 $(x^2 + x + 1)(x - 1)$

x^3, root 0, $x * x * x$

3) Write down all degree 2 polynomials in $\mathbb{F}_3[x]$. Decide which ones are irreducible and which ones have roots in $\mathbb{F}_3$. For each degree 2 polynomial $f(x)$ that does have roots, describe the roots and the corresponding factorization of $f(x)$ as a product of two degree one polynomials.

$2x^2 + 2x + 2$ has root 1 $(2x + 1)(x + 2)$

$2x^2 + 2x + 1$ no root in $\mathbb{F}_3$

$2x^2 + 2x + 0$ has root 0 $(2x)(x + 1)$

$2x^2 + 1x + 2$ has root 2 $(2x + 2)(x + 1)$

$2x^2 + 1x + 1$ no root in $\mathbb{F}_3$

$2x^2 + 1x + 0$ has root 0 $(2x)(x + 1)$

$2x^2 + 0x + 2$ no root in $\mathbb{F}_3$

$2x^2 + 0x + 1$ has root 1 $(2x + 2)(x + 2)$

$2x^2 + 0x + 0$ has root 0 $(x)(2x)$

$1x^2 + 2x + 2$ no root in $\mathbb{F}_3$

$1x^2 + 2x + 1$ has root 2 $(2x + 2)(2x - 1)$

$1x^2 + 2x + 0$ has root 0 $(x)(x+2)$

$1x^2 + 1x + 2$ no root in $\mathbb{F}_3$

$1x^2 + 1x + 1$ has root 1 $(2x+1)(2x+1)$

$1x^2 + 1x + 0$ has root 0 $(x)(x+1)$

$1x^2 + 0x + 2$ has root 1 $(2x+1)(2x-1)$

$1x^2 + 0x + 1$ no root in $\mathbb{F}_3$

$1x^2 + 0x + 0$ has root 0 $(x)(x)$

11.16 Prove theorem 11.9, using theorem 11.8

Suppose $f(x)$ is a polynomial of positive degree in $\mathbb{Z}[x]$ and p is a prime number that does not divide the highest degree coefficient of $f(x)$.

If the reduction $[f](x)$ of $f(x)$ modulo p is irreducible in $\mathbb{F}_p[x]$, then $f(x)$ does not factor in $\mathbb{Z}[x]$ as a product of lower degree polynomials.

By contradiction

Assume that $f(x)$ factors in $\mathbb{Z}[x]$ as the product of lower degree polynomials, call them $g(x), h(x)$

Then theorem 11.8 tells us that the reductions of these polynomials modulo a prime number p satisfy

$[f](x) = [g](x)[h](x)$

But this contradicts that $[f](x)$ of $f(x)$ modulo p is irreducible in $\mathbb{F}_p[x]$

So $f(x)$ does not factor as the product of lower degree polynomials in $\mathbb{Z}[x]$

11.19 Prove Gauss's lemma, theorem 11.3, again. (Hint: first show that a polynomial $f(x)$ in $\mathbb{Z}[x]$ is primitive iff for every prime p, the reduction $[f](x)$ in $\mathbb{F}_p[x]$ is nonzero. Then, consider $g(x)h(x)$ and its reductions module primes p

Theorem 11.3: The product of primitive polynomials is primitive

If $g(x), h(x)$ are two primitive polynomials in $\mathbb{Z}[x]$, then their product is also primitive

Show that $f(x) \in \mathbb{Z}[x]$ primitive iff for every prime p, reduction $[f](x) \in \mathbb{F}_p[x]$ is nonzero

forwards: Assume $f(x)$ primitive

$f(x)$ is primitive, so the greatest common divisor of all coefficients of $f(x)$ is 1. Then there is no p that can divide all of the coefficients of $f(x)$

Then there will be some nonzero coefficients in the reduction modulo p

Then $[f](x) \in \mathbb{F}_p[x]$ is nonzero

backwards: Assume reduction $[f](x)$ is nonzero for all primes p

Then the greatest common divisor of $f(x)$ must not be divisible by a prime number

Then $f(x)$ must have coefficients with greatest common divisor 1

Then $f(x)$ must be primitive.

Consider $g(x)h(x)$ and its reductions modulo p.

$g(x), h(x)$ are primitive. Then their reductions modulo p are nonzero

$[g](x), [h](x)$ are nonzero, so we can take the nonzero coefficients of highest degree term of each, call them j, k

Then the product $[g](x)[h](x)$ will have the highest degree term with coefficient $j * k$

j, k are relatively prime to p, so their product is not divisible by p

So the coefficient of the highest degree term with coefficient jk is nonzero when reduced modulo p

So the product $[g](x)[h](x)$ has at least one nonzero term, so it is nonzero.

So $[f](x) = [g](x)[h](x)$ is nonzero

So $f(x)$ must be primitive.

12.2 For polynomials $a(x), b(x)$, prove that the last nonzero remainder by the Euclidean algorithm applied to $a(x)$ and $b(x)$ is a greatest common divisor of $a(x), b(x)$. (Hint: Do so by induction on the number of steps required until the euclidean algorithm terminates)

By induction (on number of steps for euclidean alg)

Base case: number of steps = 1

$b(x) = a(x)q(x) + 0$

Then $a(x)$ divides $b(x)$

Then by exercise 12.1, the greatest common divisor must be $a(x)$

Inductive step

Inductive Hypothesis:

Assume that if the number of steps to terminate the Euclidean algorithm is n steps, then the remainder, $r(x)$ is the greatest common divisor of $a(x), b(x)$

Show that if the number of steps to terminate the Euclidean algorithm is $n + 1$ steps, the remainder, $s(x)$ is the greatest common divisor of $a(x), b(x)$

If it takes $n + 1$ steps, then after the first iteration fo the euclidean algorithm, we have

$b(x) = a(x)q(x) + r(x)$

Then it takes n steps of the euclidean algorithm to find the last nonzero remainder for $a(x), r(x)$, call it $s(x)$

Then by the inductive hypothesis, $s(x)$ must be the greatest common divisor of $a(x), r(x)$

Then since $b(x) = a(x)q(x) + r(x)$,

Then $s(x)$ must be the greatest common divisor $b(x)$

12.5 For the pair of polynomials $a(x), b(x)$ below, use the Euclidean algorithm to find polynomials $r(x), s(x)$ such that $a(x)r(x) + b(x)s(x)$ equals the greatest common divisor of $a(x), b(x)$:

1. $a(x) = x^2 + 1$ and $b(x) = x^5 + 1$ in $\mathbb{Q}[x]$

i) $x^5 + 1 = (x^2 + 1)(x^3 - x) + (x + 1)$

ii) $x^2 + 1 = (x + 1)(x - 1) + 2$

2 is a gcd

$2 = x^2 + 1 - (x + 1)(x - 1)$, by ii

We know $x + 1 = x^5 + 1 - (x^2 + 1)(x^3 - x)$, by i

So $2 = (x^2 + 1) - [x^5 + 1 - (x^2 + 1)(x^3 - x)](x - 1)$

$2 = (x^2 + 1) + (x^2 + 1)(x^3 - x)(x - 1) - (x^5 + 1)(x - 1)$

$2 = (x^2 + 1)(1 + (x^3 - x)(x - 1)) + (x^5 + 1)(1 - x)$

2. $a(x) = x^2 + 2x + 1$ and $b(x) = x^3 + 2x^2 + 2$ in $\mathbb{F}_3[x]$

$x^3 + 2x^2 + 2 = (x^2 + 2x + 1)(x) + (2x + 2)$

$x^2 + 2x + 1 = (2x + 2)(2x + 2) + 0$

$(2x + 2)$ is a gcd

$2x + 2 = (x^3 + 2x^2 + 2) - (x^2 + 2x + 1)(x)$

12.8 Prove theorem 12.13, by mimicking hte proof of theorem 12.7, then prove corollary 12.14 by induction

Theoremm 12.13: Let K be a field. Let $p(x)$ be an irreducible polynomial in $K[x]$ and suppose $p(x)$ divides the product $b(x)c(x)$ of polynomials in $K[x]$. Then $p(x)$ divides $c(x)$, or $p(x)$ divides $b(x)$

If $p(x)$ divides $b(x)$, we are done. If not, since $p(x)$ is irreducible, and does not divide $b(x)$, so $p(x), b(x)$ are relatively prime polynomials in $K[x]$

Then by theorem 12.12, $p(x)$ must divide $c(x)$

Corollary 12.14: Let K be a field. Let $p(x)$ be an irreducible polynomial in $K[x]$ that divides a product $a_1(x)a_2(x)...a_n(x)$ of polynomials in $K[x]$. Then $p(x)$ divides one of the factors $a_i(x)$

By induction (on n)

Base case: True, by theorem 12.13

Inductive Step

Inductive Hypothesis:

Assume that if irreducible $p(x)$ divides $a_1(x)...a_n(x)$, then it divides one of the factors $a_i(x)$

Show that if irreducible $p(x)$ divides $a_1(x)...a_{n+1}(x)$, then it divides one of the factors $a_i(x)$

Split up the product into two terms, $a_1(x)...a_n(x)$ and $a_{n+1}(x)$

Then by theorem 12.13, it must divide one of the two terms.

Case 1: $p(x)$ divides $a_{n+1}(x)$

If $p(x)$ divides $a_{n+1}(x)$, we are done

Case 2: $p(x)$ divides $a_1(x)...a_n(x)$

Then by inductive hypothesis, $p(x)$ divides one of the $a_i(x)$ for $1 \leq i \leq n$

So in either case, $p(x)$ divides one of the $a_i(x)$