13.2 Let K be a field with additive identity 0 and multiplicative identity 1. Write 2 for the sum $1+1$ and 4 for 2×2 Assume that $2 \neq 0$ in K., so that also $4 \neq 0$ In this exercise, we will mimicwhat was already done in exercise 10.1

1. Verify that for elements a, b of K, $(x+a)^2 = x^2 + 2ax + a^2$ and $x^2 + bx + \frac{b^2}{4}$

is the square of a first degree polynomial

$(x+a)^2 = x^2 + 2ax + a^2$. Done

$x^2 + bx + \frac{b^2}{4} = (x + \frac{b}{2})^2$

So they are both squares of degree one polynomials

2. Show that solving the equation $x^2 + bx + c = 0$, where b, c are in K, is equivalent to solving an equation of the form $(x + \frac{b}{2})^2 = (x + \frac{b}{2})^2 = \frac{d}{4}$ for a suitable element d of K. Write out the element explicitly in terms of the coefficients b, c

$(x^2 + bx + c = 0) \iff (x + \frac{b}{2})^2 - \frac{b^2}{4} + c = 0$

$(x + \frac{b}{2})^2 = \frac{b^2}{4} - c$

Then let $d = b^2 - 4c$, then $\frac{d}{4} = \frac{b^2}{4} - c$

Then $(x^2 + bx + c = 0) \iff (x + \frac{b}{2})^2 = \frac{d}{4}$

3. Deduce that if $d = 0$, then $x^2 + bx + c$ factors as $(x + \frac{b}{2})^2$, and the one and only solution to $x^2 + bx + c = 0$ is $x = \frac{-b}{2}$

If $d = 0$, then $(x + \frac{b}{2})^2 = 0$

Which means that $x = \frac{-b}{2}$ is a root

So the only solution to $x^2 + bx + c = 0$ is $x = -\frac{b}{2}$

Which means that it does have roots in K

Which means that it is reducible in K

4. Deduce that if d has no square root in K, then there is no solution to the equation $x^2 + bx + c = 0$, and therefore $x^2 + bx + c$ is irreducible in $K[x]$.

If d is not a square root in K, then $(x + \frac{b}{2})^2 = \frac{d}{4}$ has no solution in the field.

Then $x^2 + bx + c = 0$ has no solution

Then $x^2 + bx + c = 0$ has no degree 1 factors in the field. Then it must be irreducible.

5. If d is nonzero and does have a squareroot, then there are two solutions to $x^2 + bx + c = 0$ in K. Write out these solutions explicitly in terms of b and c.

d nonzero, and has squareroots in K.

So for $(x + \frac{b}{2})^2 = \frac{d}{4}$

We can write $x = \frac{\sqrt{d}}{2} - \frac{b}{2}$

And $x = -\frac{\sqrt{d}}{2} - \frac{b}{2}$

So it has 2 degree one factors in K, and is reducible.

6. Conclude that the quadratic formula works for quadratic equations with coefficients in any field K in which $2 \neq 0$

This is true, with the work shown above, using coefficients b, c

13.5 We have proved that $\sqrt{2}$ is not rational. More generally, one can use the same argument to show that every positive integer n that is not the square of an integer has a square root $\sqrt{n}$ that is irrational. Using this, state a criterion describing which polynomials $x^2 + bx + c$ in $\mathbb{Z}[x]$ have roots in $\mathbb{Q}[x]$, and which do not.

Since $2 \neq 0$ and $4 \neq 0$ in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$, we can apply the quadratic formula to check if a polynomial in $\mathbb{Z}[x]$ has roots in $\mathbb{Z}$

Applying the quadratic formula, we have $x = \pm\sqrt{d} - \frac{b}{2}$

This is $x = -\frac{b}{2} \pm \sqrt{b^2 - 4c}2$

So $x^2 + bx + c = 0$ has solutions in $\mathbb{Q}[x]$ only when $\sqrt{b^2 - 4c}$ is in $\mathbb{Q}$

So the polynomials in $\mathbb{Z}[x]$ in the form x^2+bx+c that have roots in $\mathbb{Q}[x]$ satisfy $b^2 \geq 4c$

13.8 Determine which elements in the set $\{[1],[2],...[p-1]\}$ of nonzero elements $\mathbb{F}_p$ are squares for each of the following values of $p: 3,5,7,11,13,19$

For $\mathbb{F}_3$: 1 has square roots 1 and 2
For $\mathbb{F}_5$: 1 has square roots 1 and 4
For $\mathbb{F}_5$: 4 has square roots 2 and 3
For $\mathbb{F}_7$: 1 has square roots 1 and 6
For $\mathbb{F}_7$: 2 has square roots 3 and 4
For $\mathbb{F}_7$: 4 has square roots 2 and 5
For $\mathbb{F}_{11}$: 1 has square roots 1 and 10
For $\mathbb{F}_{11}$: 3 has square roots 5 and 6
For $\mathbb{F}_{11}$: 4 has square roots 2 and 9
For $\mathbb{F}_{11}$: 5 has square roots 4 and 7
For $\mathbb{F}_{11}$: 9 has square roots 3 and 8
For $\mathbb{F}_{13}$: 1 has square roots 1 and 12
For $\mathbb{F}_{13}$: 3 has square roots 4 and 9
For $\mathbb{F}_{13}$: 4 has square roots 2 and 11
For $\mathbb{F}_{13}$: 9 has square roots 3 and 10
For $\mathbb{F}_{13}$: 10 has square roots 6 and 7
For $\mathbb{F}_{13}$: 12 has square roots 5 and 8
For $\mathbb{F}_{19}$: 1 has square roots 1 and 18
For $\mathbb{F}_{19}$: 4 has square roots 2 and 17
For $\mathbb{F}_{19}$: 5 has square roots 9 and 10
For $\mathbb{F}_{19}$: 6 has square roots 5 and 14
For $\mathbb{F}_{19}$: 7 has square roots 8 and 11
For $\mathbb{F}_{19}$: 9 has square roots 3 and 16
For $\mathbb{F}_{19}$: 11 has square roots 7 and 12
For $\mathbb{F}_{19}$: 16 has square roots 4 and 15
For $\mathbb{F}_{19}$: 17 has square roots 6 and 13

13.11 Theorem 13.7: Suppose p is a prime number satisfying $p \equiv 1 \pmod 4$. Then $[-1]$ is a square in $\mathbb{F}_p$

Prove Theorem 13.7, as follows.

1. Since p is odd, $p-1$ is even, so $\frac{p-1}{2}$ is an integer. Show that it satisfies the relation $p - \frac{p-1}{2} = \frac{p-1}{2} + 1$

p is odd, so it is in the form $2k+1, k \in \mathbb{Z}$

So LHS, $2k+1-\frac{2k+1-1}{2} = 2k+1-k = k+1$

And RHS, $\frac{2k+1-1}{2}+1 = k+1$

So they are equal

Then, observe that therefore, we can rewrite $1 \times 2 \times 3 \times ... \times (p-1)$ as the product of $1 \times 2 \times 3 \times .. \times \frac{p-1}{2}$

and $(p-1) \times (p-2) \times (p-3) \times ... \times (p - \frac{p-1}{2})$

Done. (This is just multiplying the first half of numbers, not including middle numbers, by the second half of numbers with middle.)

2. Notice that for each integer i, we have that $p - i \equiv -i$ (mod p). Deduce that $1 \times 2 \times 3 \times ... \times (p-1) \equiv (1 \times 2 \times 3 \times ... \times \frac{p-1}{2})((-1) \times -2 \times -3 \times ... \times \frac{-p-1}{2})$ modulo p

Yes, since we know that $1 * 2 * 3..(p-1) = (1 * 2 * 3...\frac{p-1}{2})((p-1)(p-2)...(p-\frac{p-1}{2})$

And we know the latter half is congruent to $(-1 * -2 * -3.... - \frac{p-1}{2})$

Then the entire thing is congruent to $(1 \times 2 \times 3 \times ... \times \frac{p-1}{2})((-1) \times -2 \times -3 \times ... \times \frac{-p-1}{2})$ modulo p

3. Combining this last congruence with the congruence of Wilson's theorem, deduce that

$(-1)^{\frac{p-1}{2}}(1 \times 2 \times 3 \times ... \times \frac{p-1}{2})^2 \equiv -1$ (mod p).

Wilson's theorem tells us that if p is an odd prime number, then $1 \times 2 \times .. \times (p-1) \equiv -1$ (mod p).

And the second half of the factors $-1 \times -2 \times -3 ... \times \frac{-p-1}{2}$ can be rewritten as $(-1)^{\frac{p-1}{2}}(1 \times 2 \times .. \times \frac{p-1}{2})$

So $(1 * 2 * 3..(p-1) = [(1 * 2 * 3...\frac{p-1}{2})][(-1)^{\frac{p-1}{2}}(1 * 2 * 3 * ...\frac{p-1}{2})$

And by Wilsons theorem,

$(1 * 2 * 3..(p-1) = [(1 * 2 * 3...\frac{p-1}{2})][(-1)^{\frac{p-1}{2}}(1 * 2 * 3 * ...\frac{p-1}{2}) \equiv -1$ (mod p)

4. Conclude that if $\frac{p-1}{2}$ is even, then -1 is congruent to the square of an integer modulo p

So if $\frac{p-1}{2}$ is even, then the product $(1 * 2 * 3.. * \frac{p-1}{2})^2 \equiv -1$ (mod p).

So -1 is congruent to the square of an integer modulo p

5. Notice that $\frac{p-1}{2}$ is even precisely when 4 divides $p-1$, which means $p \equiv 1 \pmod 4$. Therefore, you have proved that if $p \equiv 1 \pmod 4$, then -1 is congruent to the square of an integer modulo p

If $\frac{p-1}{2}$ is even, it takes the form $\frac{p-1}{2} = 2k$

Then $p - 1 = 4k$, so it is divisible by 4

So $p \equiv 1 \pmod 4$.

6. Pass to $\mathbb{F}_p$ and conclude that if $p \equiv 1 (\text{mod } 4)$, then $[-1]$ is a square in $\mathbb{F}_p$

Yes, because we perform the same calculations in $\mathbb{F}_p$, using mod p for an odd prime p.

13.14 Start with the field $\mathbb{Q}$ of rational numbers. The number 2 does not have a square root in $\mathbb{Q}$. Therefore, we invent a square root of 2, that is, a symbol γ with the property that $\gamma = 2$. (We can think of γ as the real number $\sqrt{2}$, but let us work instead with γ as a new, abstract, entity, just as we have used i before when we wanted to work with a square root of -1). Now we need to create a field that contains all $\mathbb{Q}$, and γ as well. Since we need closure under addition, multiplication, and additive and multiplicative inverses, we will need at least the set K consisting of all expressions $a + b\gamma$, where a, b are rational numbers. Let us see whether the set K is sufficiently large. We define addition in K by the rule $(a + b\gamma) + (c + d\gamma) = (a + c) + (b + d)\gamma$

and multiplication by $(a+b\gamma)(c+d\gamma) = ac+ad\gamma+bc\gamma+bd\gamma^2 = (ac+2bd)+(ad+bc)\gamma$

Notice that we have used the fact that $\gamma^2 = 2$ to rewrite $bd\gamma^2$ as $2bd$, a rational number. It should be easy to see that K is a ring, that is, that it is closed under addition, multiplication, and additive inverses.

1. Check that K is a ring. Do not write out a proof of this. But we want a field, and the question now is whether we have to include additional elements to guarantee that every nonzero element in K has a multiplicativei nverse.

Yes, since it is closed under addition and multiplication, and additive inverses.

2. Compute $(a + b\gamma)(a - b\gamma)$. Show that you get $a^2 - 2b^2$, a rational number

Expanding, we get $a^2 + a\gamma b - a\gamma b - b^2\gamma^2$

And since $\gamma^2 = 2$, we have $a^2 - 2b^2$

3. Show that $a^2 - 2b^2$ cannot be 0 unless $a = b = 0$ (hint, suppose $a^2 - 2b^2 = 0$, but $b \neq 0$. Solve $a^2 - 2b^2 = 0$, for $\frac{a}{b}$)

Suppose that $a^2 - 2b^2 = 0$ and $b \neq 0$

Then $a^2 = 2b^2$

Then $a = \gamma b$

Then $\frac{a}{b} = \gamma$

But a, b are rational, they cannot be equal to γ, contradiction

4. Assume that a, b are not both 0. Since $a^2 - 2b^2 \neq 0$, you can divide the product $(a+b\gamma)(a-b\gamma)$ by a^2-2b^2. Deduce that $a+b\gamma$ has a multiplicative invere in K (What is it?) and that K is a field

Since $a^2 - 2b^2 = (a + b\gamma)(a - b\gamma) \neq 0$

Since non zero, we can divide

we get $\frac{(a+b\gamma)(a-b\gamma}{a^2-2b^2} = 1$

So $a + b\gamma$ has inverse $\frac{a-b\gamma}{a^2-2b^2}$

Since $a^2 - 2b^2$ is a rational number, this is $\frac{a}{a^2-2b^2} - \frac{b\gamma}{a^2-2b^2}$, which is an element in the ring

So K is a field.

So by constructing a ring K containing a square root γ of 2, we get multiplicative inverses "for free".

5. Conclude that $x^2 - 2$ has roots $\gamma, -\gamma$ in K and that $x^2 - 2$ factors in $K[x]$ as $(x-\gamma)(x+\gamma)$

Yes, this is true because $(x-\gamma), (x+\gamma) \in K[x]$, and has roots $\gamma, -\gamma$, and $(x-\gamma)(x+\gamma) = x^2 - x\gamma + x\gamma - \gamma^2 = x^2 - 2$

13.17 Start with the field $\mathbb{F}_5$. Form the set K consisting of all expressions $a + b\gamma$, where a, b are chosen from $\mathbb{F}_5$, and γ is some new formal symbol introduced to serve as a square root of 2. That is $\gamma^2 = 2$ Define addition multiplication in K by the following rules.

$(a + b\gamma) + (c + d\gamma) = (a + c) + (b + d)\gamma$

and multiplication by $(a+b\gamma)(c+d\gamma) = ac+ad\gamma+bc\gamma+bd\gamma^2 = (ac+2bd)+(ad+bc)\gamma$

1. Check that K is a ring.

Show that it is closed under addition

For $a + b\gamma$ and $c + d\gamma$, we have the sum $(a + c) + (b + d)\gamma$

We know $a + c \equiv e \pmod 5$ and $b + d \equiv f \pmod 5$

Then the sum is $e + f\gamma$, which is in K

Show that it is closed under multiplication

For $a + b\gamma, c + d\gamma$, product is $(ac + 2bd) + (ad + bc)\gamma$

We know $ac + 2bd \equiv e \pmod 5$ and $ad + bc \equiv f \pmod 5$

Then the product $e + f\gamma$ is an element in K.

2. Observe that there are twnety five elements in K

Yes, there are 5 choices are a, and 5 choices for b, for choices $0, 1, 2, 3, 4$

3. Compute $(a + b\gamma)(a - b\gamma)$ and show that you get $a^2 - 2b^2$, which is the same as $a^2 + 3b^2$, an element in $\mathbb{F}_5$

$(a + b\gamma)(a - b\gamma) = a^2 - ab\gamma + ab\gamma - b^2\gamma^2 = a^2 - 2b^2 = a^2 + 3b^2$ in $\mathbb{F}_5$

4. Show that $a^2 + 3b^2$ cannot be 0 unless $a = b = 0$

Assume that $a^2 + 3b^2 = 0$, and $b \neq 0$

Then $a^2 = -3b^2 = 2b^2$

Then $\frac{a^2}{b^2} = 2$

Then $\frac{a}{b} = \pm\gamma$

But a, b both rational, while γ is irrational, impossible. contradiction.

5. Assume that a, b are not both 0. Since $a^2 + 3b^2 \neq 0$, you can divide the product $(a + b\gamma)(a - b\gamma)$ by $a^2 + 3b^2$

Deduce that $a + b\gamma$ has a mutliplicative inverse and conclude that K is a field

$(a + b\gamma)(a - b\gamma) = a^2 + 3b^2$

Since $a^2 + 3b^2 \neq 0$, we can divide

$(a + b\gamma)\frac{a-b\gamma}{a^2+3b^2} = 1$

So $a + b\gamma$ has multiplicative inverse $\frac{a-b\gamma}{a^2+3b^2}$

So K is a field.

6. Calculate $(2\gamma)^2$ and observe that in building a field extension of $\mathbb{F}_5$ that contains a square root of 2, you have also constructed an extension that contains a square root

of 3. You have constructed a field extension of $\mathbb{F}_5$ with 25 elements that contains a squareroot for every element of $\mathbb{F}_5$. Call this new field $\mathbb{F}_{25}$

$(2\gamma)^2 = 4\gamma^2 = 8 = 3$

So 2γ is the square root of 3.

7. Recall that we found earlier that the quadratic equation $x^2 + 2x + 3 = 0$ has no solution in $\mathbb{F}_5$. Show that it has solutions in K. Use these solutions to factor x^3+2x+3 in $K[x]$ as a product of degree one polynomials

We know by quadratic formula that if $d = b^2 - 4c$ is nonzero and does have a squareroot, then there are two solutions to $x^2 + bx + c = 0$

Let $b = 2, c = 3$

Then $d = b^2 - 4c$

$d = 4 - 12 = -8 = 2 \in K$

Then $x = \frac{-2}{2} \pm \frac{\sqrt{2}}{2}$

And we know $\sqrt{2} \in K$ is $\pm\gamma$

So roots of $x^2 + 2x + 3$ are $x = -1 \pm \frac{\gamma}{2}$

In $K[x]$, so dividing by 2 is the same as multiplying by its multiplicativ inverse, 3

So $x = -1 \pm 3\gamma$

$(x - [-1 + 3\gamma])(x - [-1 - 3\gamma]) = x^2 + 2x - 17 = x^2 + 2x + 3$ in $K[x]$, and has roots $-1 \pm 3\gamma \in K$

8. Show that the field $\mathbb{F}_{25}$ has a primitive root by writing down the powers $(1 + 2\gamma)^i$ for $i = 1, 2, ...24$

$(1 + 2\gamma)^1 = 1 + 2\gamma$
$(1 + 2\gamma)^2 = 4 + 4\gamma$
$(1 + 2\gamma)^3 = 0 + 2\gamma$
$(1 + 2\gamma)^4 = 3 + 2\gamma$
$(1 + 2\gamma)^5 = 1 + 3\gamma$
$(1 + 2\gamma)^6 = 3 + 0\gamma$
$(1 + 2\gamma)^7 = 3 + 1\gamma$
$(1 + 2\gamma)^8 = 2 + 2\gamma$
$(1 + 2\gamma)^9 = 0 + 1\gamma$
$(1 + 2\gamma)^{10} = 4 + 1\gamma$
$(1 + 2\gamma)^{11} = 3 + 4\gamma$
$(1 + 2\gamma)^{12} = 4 + 0\gamma$
$(1 + 2\gamma)^{13} = 4 + 3\gamma$
$(1 + 2\gamma)^{14} = 1 + 1\gamma$
$(1 + 2\gamma)^{15} = 0 + 3\gamma$
$(1 + 2\gamma)^{16} = 2 + 3\gamma$
$(1 + 2\gamma)^{17} = 4 + 2\gamma$
$(1 + 2\gamma)^{18} = 2 + 0\gamma$
$(1 + 2\gamma)^{19} = 2 + 4\gamma$

$(1+2\gamma)^{20} = 3+3\gamma$
$(1+2\gamma)^{21} = 0+4\gamma$
$(1+2\gamma)^{22} = 1+4\gamma$
$(1+2\gamma)^{23} = 2+1\gamma$
$(1+2\gamma)^{24} = 1+0\gamma$

Since $(1+2\gamma)^1, (1+2\gamma)^2....(1+2\gamma)^{24}$ form a complete list of the nonzero elements in K, then $(1+2\gamma)$ is a primitive root of K

So $\mathbb{F}_{25}$ has primitive roots.

13.20 Let p be an odd prime number and let a be a primitive root of $\mathbb{F}_p$. Recall that this means that the elements $a, a^2, ..a^{p-1}$ form a complete list of the nonzero elements of $\mathbb{F}_p$. Recall also that a^i is a square in $\mathbb{F}_p$, if i is even, and a^i is not a square if i is odd.

1. Perform the construction of Exercise 13.18 on $\mathbb{F}_p$ and a to obtain a new field $\mathbb{F}_p[\sqrt{a}]$ containing $\mathbb{F}_p$ in which a has a square root γ. Show that $\mathbb{F}_p[\sqrt{a}]$ has p^2 elements.

An element in $\mathbb{F}_p[\sqrt{a}]$ in the form $x + y\sqrt{a}, x, y \in \mathbb{F}_p$

For $x, y \in \{0, 1, 2, .., p-1\}$, then there are p choices for x, and p choices for y, for a total of p^2 choices possible.

Then there must be p^2 elements in $\mathbb{F}_p[\sqrt{a}]$

2. Show that ever element of $\mathbb{F}_p$ has a square root in $\mathbb{F}_p[\sqrt{a}]$. Thus in building a field with lots of square roots of a, we have succeededi n building a field with lots of square roots. Deduce that every polynomial $x^2 + bx + c$ in $\mathbb{F}_p[x]$ has a root in $\mathbb{F}_p[\sqrt{a}]$

Let z be an arbitrary element of $\mathbb{F}_p$

Show that z has a root in $\mathbb{F}_p$

Know that a is a primitive root in $\mathbb{F}_p$, then $a^m = z$ for some m

Know that $\sqrt{a}^2 = a$

Then $(\sqrt{a})^{2m} = x$

14.2 Let K be the collection of polynomial-like expressions in γ just intrdouced, with $\gamma^n = 2$

1. Show that for an arbitrary positive integer m one can write $\gamma^m = 2^q\gamma^r$ for unique nonnegative integers q, r with $r < n$ (Hint: use the division theorem for integers to write $m = nq + r$).

Let $\gamma^n = 2$

Then we know there exists nonnegative integers $q, r, r < n$ such that $m = nq + r$

Then $\gamma^m = \gamma^{nq+r}$

This is just $\gamma^{nq}\gamma^r$

Then $\gamma^m = 2^q\gamma^r$

2. Suppose $a_0 + a_1\gamma + a_2\gamma^2 + ...a_{n-1}\gamma^{n-1}$ and $b_0 + b_1\gamma + b_2\gamma^2 + .. + b_{n-1}\gamma^{n-1}$ are two elements of K. Using the result of part 1, show that you can define a multiplication rule for these two elements by treating them first as ordinary polynomials in γ and multiplying, then replacing the higher powers of γ by terms involving exponents less than n, so that the result is another element of K, a polynomial expression in γ of degree less than n.

Multiply the two elements, treating them as ordinary polynomials in γ

This is $a_0b_0 + a_0b_1\gamma + ... + (a_{n-1}b_{n-1})(\gamma^{2n-2})$

Then we can group the like terms

But we know by part 1 that for each power of each degree term of γ we can rewrite as $2^q\gamma^r, q, r \in \mathbb{N} \cup \{0\}, r < n$

Then the result is $a_0b_0 + ... + a_{n-1}b_{n-1}2\gamma^{n-2}$

Then the product of the elements is another element in K

3. Is K a field? Do not try to give a complete answer. Instead, think about the issue along the lines disccused in the previous exercise and show that the question can be reduced to the problem of solving a family of n linear equations in n unknowns

Similar to exercise 14.1, if we expand the left side, we get n equations for n unknowns. If we can solve the equations, then there exists an inverse.

Then K is a field.