Galois theory for dummies

Ruben Spaans

May 21, 2009

1 Notes on notation

To help avoid vertical figures, I use the notation E/F if E is an extension to the field F. This is the same notation as Wikipedia uses. The author hopes that this will not give arise to confusion regarding a potential factor ring E/F. Hopefully it will be clear from the context what is meant. And to further prevent confusion, I often instead write E is [some kind of] extension to F.

2 Pronounciation guidelines

"Root" is pronounced /ɹʊt/.

3 Problem set 1

Let R be a commutative integral domain with unity in which for each pair $a, b \in R$, $\gcd(a, b)$ exists. Let $a, b, c \in R$.

Exercise 11.1.1 Show that $c(a, b)$ and (ca, cb) are associates.

Solution (with teaspoon) Let

$$d = \gcd(a, b) \text{ and } D = \gcd(ca, cb).$$

This implies

$$d|a, d|b, D|ca, D|cb \text{ (definition of greatest common divisor).}$$

Multiply with c to get

$$cd|ca \text{ and } cd|cb.$$

Then

$$cd|D,$$

because if cd divides ca and cb, it must also divide D which is the greatest common divisor of ca and cb. Rewrite this as

$$D = cdu$$

for some $u \in R$. We have from above

$$Dx = ca \text{ and } Dy = cb.$$

Substitute $D = cdu$ and get

$$cdux = ca \text{ and } cduy = cb.$$

In an integral domain, the cancellation law holds. [$ab = ac, a \neq 0 \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0 \Rightarrow a = 0$ or $b - c = 0 \Rightarrow b = c$ since we assumed $a \neq 0$.] Cancel c and get

$$a = dux \text{ and } b = duy \Rightarrow du|a \text{ and } du|b.$$

Since du divides both a and b, it must also divide the greatest common divisor of a and b, namely

$$d \Rightarrow du|d,$$

rewritten as

$$d = duv.$$

Cancel and get

$$1 = uv,$$

so u and v must be units. Then

$$(ca, cb) = D = cdu = c(a, b). \tag{1}$$

[We use the shorthand $=$ instead of $\sim$ for equalities where gcd is involved.]

Exercise 11.1.2 Show that if $(a, b) = 1$ and $a|c$ and $b|c$, then $ab|c$.

Solution Multiply by b and a, respectively: $ab|bc$ and $ab|ac$, so $ab|(ac, bc)$ by the definition of greatest common divisor.

$$\begin{aligned}(ac, bc) &= c(a, b) \text{ (by (1))} \\ &= c \text{ (by assumption } (a, b) = 1)\end{aligned}$$

so $ab|c$.

Exercise 11.1.3 Show that if $(a, b) = 1$ and $b|ac$, then $b|c$.

Solution $c(a,b) = (ca, cb) = c$. $b|ac$ combined with $b|cb$ (obvious) gives $b|(ca, cb) = c$.

Exercise 11.3.2 Show that each of the rings $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{-2}]$ is a (i) Euclidean domain and (ii) UFD. (iii) Explain why in the UFD $\mathbb{Z}[\sqrt{2}]$, $(5+\sqrt{2})(2-\sqrt{2}) = (11-7\sqrt{2})(2+\sqrt{2})$ even though each of the factors is irreducible.

Solution (i) Elements in $\mathbb{Z}[\sqrt{\pm 2}]$ can be written as

$$\{a + b\sqrt{\pm 2} | a, b \in \mathbb{Z}\}.$$

Define the norm as

$$N(a + b\sqrt{\pm 2}) = |a^2 \mp 2b^2|.$$

It's easy to show that

$$N((a + b\sqrt{\pm 2})(c + d\sqrt{\pm 2})) = N(a + b\sqrt{\pm 2})N(c + d\sqrt{\pm 2}),$$

which is even true for $a, b, c, d \in \mathbb{R}$.

For all $a, b \in R, a, b \neq 0$, there exists $\alpha, \beta \in \mathbb{Q}$ such that

$$ab^{-1} = \alpha + \beta\sqrt{2}$$

$$\Rightarrow a = b(\alpha + \beta\sqrt{2}). \tag{2}$$

We want q, r such that $a = bq + r, 0 \leq r < a$. We can find $\alpha_0, \beta_0 \in \mathbb{Z}$ such that

$$|\alpha - \alpha_0| \leq \frac{1}{2} \tag{3}$$

$$|\beta - \beta_0| \leq \frac{1}{2}. \tag{4}$$

From (2), (3) and (4) we get

$$a = b\underbrace{(\alpha_0 + \beta_0\sqrt{2})}_{q} + \underbrace{b(\alpha - \alpha_0) + b(\beta - \beta_0)\sqrt{2}}_{r}$$

Taking the norm:

$$N(r) = N(b)\underbrace{[(\alpha - \alpha_0)^2 - 2(\beta - \beta_0)^2]}_{H}.$$

We get

$$H = |\underbrace{(\alpha - \alpha_0)^2}_{\leq \frac{1}{4}} - \underbrace{2(\beta - \beta_0)^2}_{\leq \frac{1}{2}}]$$

$$H \leq \frac{1}{4} + \frac{1}{2} < 1.$$

From this we conclude that $r = 0$, since r is a non-negative integer and $r < 1$.

Same argumentation for $\mathbb{Z}[\sqrt{-2}]$.

(ii) We showed in (i) that the rings were Euclidean domains. Theorem 3.3 says that every Euclidean domain is a UFD. This again follows from theorem 2.1 (every PID is a UFD) and theorem 3.2 (every Euclidean domain is a PID).

(iii-1) First we find the units in $\mathbb{Z}[\sqrt{-2}]$. We have

$$u \in \mathbb{Z}[\sqrt{-2}] \text{ is a unit } \Leftrightarrow N(u) = 1$$

where $N : \mathbb{Z}[\sqrt{-2}] \to \mathbb{Z}$ is the norm.

If u is a unit, there exists a v such that $uv = 1$. Then,

$$N(1) = N(u)N(v) \Rightarrow N(u) = 1.$$

We want to find a, b such that

$$\left|u(a - b\sqrt{-2})\right| = N(u) = 1.$$

We recall that the norm of $\mathbb{Z}[\sqrt{-2}]$ is defined by

$$N(a + b\sqrt{-2}) = \left|a^2 - 2b^2\right| = \left|(a + b\sqrt{-2})(a - b\sqrt{-2})\right|. \tag{5}$$

We then get

$$u^{-1} = a - b\sqrt{-2} \text{ or}$$
$$u^{-1} = -(a - b\sqrt{-2}).$$

From this and (5) we get

$$u = a + b\sqrt{-2}$$

We see that the equation

$$N(u) = a^2 + 2b^2 = 1$$

only has the solutions $a \pm 1$.

(iii-2) Then, we wish to find the units in $\mathbb{Z}[\sqrt{2}]$. The unit u can be expressed as

$$u = a + b\sqrt{-2}$$

satisfying

$$N(u) = \left|a^2 - 2b^2\right| = 1.$$

We want to find a, b such that

$$a^2 - 2b^2 = 1,$$

this is Pell's equation and it has infinitely many solutions. Thus, $\mathbb{Z}[\sqrt{2}]$ has an infinite number of units.

(iii-3) The equality

$$(5 + \sqrt{2})(2 - \sqrt{2}) = (11 - 7\sqrt{2})(2 + \sqrt{2})$$

holds, despite that the factors are irreducible in $\mathbb{Z}[\sqrt{2}]$. The reason is that the factors on each side differ by multiplication by a unit.

$5 + \sqrt{2}$ is irreducible because $N(5 + \sqrt{2}) = 23$ and

$$\begin{aligned} 5 + \sqrt{2} &= (a + b\sqrt{2})(c + d\sqrt{2}) \\ 23 = N(5 + \sqrt{2}) &= \underbrace{N(a + b\sqrt{2})}_{=1}\underbrace{N(c + d\sqrt{2})}_{\text{or } =1}. \end{aligned}$$

Since the norm is a prime number, one on the factors must be a unit.

$-1 + \sqrt{2}$ is a unit in $[\sqrt{2}]$. Then, $(-1 + \sqrt{2})^2 = (3 - 2\sqrt{2})$ is also a unit.

We have

$$\begin{aligned} (5 + \sqrt{2}) &\sim (11 - 7\sqrt{2}) \\ \text{and } (2 - \sqrt{2}) &\sim (2 + \sqrt{2}). \end{aligned}$$

since for instance $(2 + \sqrt{2})(3 - 2\sqrt{2}) = 2 - \sqrt{2}$.

Exercise 11.3.8 Show that $\mathbb{Z}[\sqrt{-6}]$ is not a Euclidean domain.

Solution Take the norm of an arbitrary element in the ring.

$$N(a + b\sqrt{-6}) = a^2 + 6b^2$$

where $a, b \in \mathbb{Z}$. Units are ± 1. We recall theorem 11.3.3 which says that every Euclidean domain is a UFD. If we can show that $\mathbb{Z}[\sqrt{-6}]$ is not a UFD, we are done.

Consider 6, it can be written as $6 = 2 \cdot 3 = \sqrt{-6} \cdot (-\sqrt{-6})$. We want to show that all the factors are irreducible. We recall that an element is irreducible if it is not a product of two non-units.

Show that 2 is an irreducible: Rewrite 2 as the product of two elements in the ring.

$$2 = (a + b\sqrt{-6})x,$$

where $x = (c + d\sqrt{-6})$. Take the norm on both sides:

$$4 = N(2) = (a^2 + 6b^2)N(x)$$

The only possibilities for a, b such that $(a^2 + 6b^2)$ is a non-unit are $a = \pm 2$ and $b = 0$, which leads to $N(x) = 1$, a unit. Hence 2 is irreducible. The same kind of argumentation will lead to showing that 3 is an irreducible.

Show that $\sqrt{-6}$ is irreducible:

$$\sqrt{-6} = (a + b\sqrt{-6})(x)$$

Take the norm on both sides:

$$6 = (a^2 + 6b^2)N(x)$$

The only possibilities for a, b are $a = 0$ and $b = \pm 1$, leading to $N(x) = 1$. Hence $\sqrt{-6}$ is irreducible. Hence $\mathbb{Z}[\sqrt{-6}]$ is not an Euclidean domain, since we don't have unique factorization.

Exercise (Fermat) Prove that the diophantine equation $y^2 + 2 = x^3$ has only the integer solutions $y = \pm 5, x = 3$. [Hint: Use that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain with norm $N(a + b\sqrt{-2}) = a^2 + 2b^2$.]

Solution We have

$$y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}) = x^3 \overset{\text{UFD}}{=} (p_1 \cdots p_n) = 3. \tag{6}$$

Assume that $\gcd(y + \sqrt{2}, y - \sqrt{2}) = 1$, which is easy to show.

From (6) we get

$$x^3 = p_1^3 p_2^3 \cdots p_n^3$$

where p_i is irreducible (but not necessarily distinct).

We can rewrite:

$$\begin{aligned} y + \sqrt{-2} &= q_1 \cdots q_m = (p_{i_1})^3 \cdots (p_{i_j})^3 = z^3 \\ y - \sqrt{-2} &= s_1 \cdots s_t = (p_{k_1})^3 \cdots (p_{k_o})^3 = w^3 \end{aligned}$$

where $z, w \in \mathbb{Z}[\sqrt{-2}]$. $q_i \neq \pm s_l$ for $i \in \{1, 2, \ldots, m\}$, $l \in \{1, 2, \ldots, t\}$, the factors of x^3 occur in each one of the two above. Take norms:

$$N(p) | N(2y) = 4y^2 \ y \text{ is odd}$$

Furthermore,

$$\begin{aligned} y + \sqrt{-2} &= z^3 \\ &= (a + b\sqrt{-2})^3 \\ &= a^3 + 3a^2 b\sqrt{-2} + 3a(b\sqrt{-2})^2 + (b\sqrt{-2})^3 \\ &= \underbrace{a^3 - 6ab^2}_{=y} + \underbrace{(3a^2 b - 2b^3}_{=1}\sqrt{-2}. \end{aligned}$$

From $1 = b(3a^2 - 2b^2)$ we get $b = 1$ and $a = \pm 1$ and from this we get the solutions

$$y = \{-5, 5\} \Rightarrow x = 3.$$

Show that $\gcd(y + \sqrt{2}, y - \sqrt{2}) = 1$:

$$p|y + \sqrt{-2} \text{ and}$$
$$p|y - \sqrt{-2}$$

implies $p = \pm 1$ where $p \in \mathbb{Z}[\sqrt{-2}]$. This in turn implies

$$p|2y \text{ and}$$
$$p|2\sqrt{-2}$$

because $p|a$ and $p|b$ implies $p|a + b$ and $p|a - b$.

4 Problem set 2

Exercise 15.1.2 Show that $x^4 + 8 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$.

Solution First, a warning about a trap! We cannot use Eisenstein's criterion here. If we choose $p = 2$, we have $p^2|a_0$ and all conditions of Eisenstein's criterion are not fulfilled.

Let us assume that $x^4 + 8$ is reducible, and exhaust all possibilities.

We make use of theorem 15.1.7 which states that a root must divide a_0. The candidates are $\pm 1, \pm 2, \pm 4, \pm 8$. Also, Gauss' lemma states that a root of a polynomial over $\mathbb{Q}$ must reside in $\mathbb{Z}$, that's why all the candidates are integers. By insertion we find that none of these candidates are roots. Hence it must be a product of two polynomials of degree 2.

Lemma 15.1.6 says that if a polynomial is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$. Then

$$x^4 + 8 = (x^2 + ax + b)(x^2 + cx + d) \tag{7}$$

where $a, b, c, d \in \mathbb{Z}$. Multiply the factors to get

$$x^4 + 8 = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (bc + ad)x + bd$$

By relating the coefficients on each side to each other we get this set of equations:

$$\begin{aligned} a + c &= 0 \\ b + d + ac &= 0 \\ bc + ad &= 0 \\ bd &= 8 \end{aligned}$$

Assume that $a \neq 0$. Then $c = -a$. $bc + ad = 0$ leads to $b = d$. $bd = 8$ is then the same as $b^2 = 8$, which isn't possible. So $a = 0$, hence $c = 0$.

Let's examine the possibilities for b. Assume $b \neq 0$. Then $d = -b$ and $-b^2 = 8$, a contradiction. Hence $b = 0$ which also leads to $d = 0$. But then $bd = 0 \neq 8$, a contradiction. Every case leads to a contradiction to the assumption that $x^4 + 8$ is reducible to (7), hence $x^4 + 8$ is irreducible over $\mathbb{Q}$.

Exercise 15.1.4 Show that $f(x) = x^3 + ax^2 + bx + 1 \in \mathbb{Z}[x]$ is reducible over $\mathbb{Z}$ if and only if either $a = b$ or $a + b = -2$.

Solution If the polynomial is reducible, it can be written as

$$x^3 + ax^2 + bx + 1 = (x^2 + cx + d)(x + e) = x^3 + (e + c)x^2 + (ce + d)^x + ed$$

We immediately see that $ed = 1$. We then have two cases to examine.

$e = d = 1$ leads to $1 + c = a, 1 + c = b \Rightarrow a = b$.

$e = d = -1$ leads to $c - 1 = a, -c - 1 = b \Rightarrow a + b = -2$.

Easier solution: Evaluate the polynomial with $x = 1$ and $x = -1$, the only candidates for the linear factor, and relate a and b to each other.

We get:

$$\begin{aligned} f(1) = 1 + a + b + 1 &\Rightarrow ab = -2 \\ f(-1) = -1 + a - b - 1 &\Rightarrow a = b \end{aligned}$$

Exercise 15.1.6b Determine if $x^4 - 3x^2 + 9$ is irreducible over $\mathbb{Q}$.

Solution If there is any root, the root will reside in $\mathbb{Z}$, see theorem 15.1.7. We have candidates $\pm 1, \pm 3$ and ± 9 for roots. By evaluating the polynomial at x set to these candidates, we find that none of them are roots. Therefore, if the polynomial is reducible, it will have two factors of degree 2. We equate

$$\begin{aligned} x^4 - 3x^2 + 9 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd \end{aligned}$$

From the above we get

$$\begin{aligned} a + c &= 0 \\ b + ac + d &= -3 \\ ad + bc &= 0 \\ bd &= 9. \end{aligned}$$

Solving this we get

$$x^4 - 3x^2 + 9 = (1 - 3x + 3)(1 + 3x + 3)$$

Apparently I am missing something, because the solution from the lecture omitted the last details and concluded *reducible* at an earlier stage, not even writing out the right hand side coefficients of the terms x^2 and x.

Exercise 15.2.2 Show that $x^3 - 2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$. Find (if it exists) an extension K of $\mathbb{Q}$ having all roots of $x^3 - 2$ such that $[K : \mathbb{Q}] = 6$.

Solution $x^3 - 2 = 0$ has three complex roots:

$$\begin{aligned} x_1 &= \sqrt[3]{2} \\ x_2 &= \omega\sqrt[3]{2} \\ x_3 &= \omega^2\sqrt[3]{2}, \end{aligned}$$

where $\omega = e^{\frac{2\pi i}{3}}$ and $\omega^3 = 1$.

$K = \mathbb{Q}(x_1, x_2, x_3)$. ω is in K because $\frac{x_2}{x_1} = \omega$, so we can simplify: $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

So we have $K = \mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ and $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = 2$ and the basis is $\{1, \omega\}$. The minimal polynomial of ω over $\mathbb{Q}(\sqrt[3]{2})$ is $x^2+x+1 = \frac{x^3-1}{x-1}$.

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ because the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$. The basis is $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$.

So,

$$[\mathbb{Q}(\sqrt[3]{2}), \omega] : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 6.$$

Basis of K over $\mathbb{Q}$ is $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \omega, \omega\sqrt[3]{2}, \omega(\sqrt[3]{2})^2\}$.

Exercise 15.2.4 Find the smallest extension of $\mathbb{Q}$ having a root of $x^2 + 4 \in \mathbb{Q}[x]$.

Solution The roots of $x^2 + 4 = 0$ are $x_1 = 2i$ and $x_2 = -2i$.

$K = \mathbb{Q}(x_1, x_2) = \mathbb{Q}(i)$. The basis for K over $\mathbb{Q}$ is $\{1, i\}$.

Exercise 15.3.2 Prove that $\sqrt{2}$ and $\sqrt{3}$ are algebraic over $\mathbb{Q}$. Find the degree of

a) $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

b) $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$.

c) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

d) $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ over $\mathbb{Q}$.

Solution $\sqrt{2}$ and $\sqrt{3}$ are algebraic over $\mathbb{Q}$, since they are roots of polynomials x^2-2 and $x^2-3 \in \mathbb{Q}[x]$.

(a) The basis is $\{1, \sqrt{2}\}$, so the dimension is 2.

(b) The basis is $\{1, \sqrt{3}\}$, so the dimension is 2.

(c) We have $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. We know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and we need to find $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})]$. It's either 1 or 2, depending on whether $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$.

Does there exist $a+b\sqrt{2}$ such that $\sqrt{3} = a+b\sqrt{2}$?

$$\begin{aligned}\sqrt{3} &= a+b\sqrt{2}\\ 3 &= a^2+b^2+2ab\sqrt{2},\end{aligned}$$

and since $a^2, b^2 \in \mathbb{Q}$ we must from the above have $2ab\sqrt{2} \in \mathbb{Q} \Rightarrow \sqrt{2} \in \mathbb{Q}$, which is a contradiction.

If $a=0$ or $b=0$ we get $3 = b^2 \cdot 2$ and we get the same kind of argument as need to show that $\sqrt{2}$ is not rational, and it's not necessary to prove this. We are allowed to assume it's known.

Hence, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, so $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, hence the degree of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$ is 4.

(d) It is clear that $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$.

If we can express both $\sqrt{2}$ and $\sqrt{3}$ by $\sqrt{2}+\sqrt{3}$, we are done. Let

$$\alpha = \sqrt{2}+\sqrt{3}. \tag{8}$$

Square and get

$$\alpha^2 = 2+3+2\sqrt{6}.$$

We see that

$$\alpha^2 - 5 = 2\sqrt{6},$$

hence $\sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Multiply identity (8) with $\sqrt{6}$ and get

$$\begin{aligned}\alpha\sqrt{6} &= \sqrt{6}\sqrt{2}+\sqrt{6}\sqrt{3} &(9)\\ &= \sqrt{12}+\sqrt{18} &(10)\\ &= 2\sqrt{3}+3\sqrt{2} &(11)\end{aligned}$$

Combine (8) and (11) to get

$$\begin{aligned}\sqrt{6}\alpha - 2\alpha &= \sqrt{2}\\ 3\alpha - \sqrt{6}\alpha &= \sqrt{3}.\end{aligned}$$

We have now shown that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Hence $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ and $\mathbb{Q}(\sqrt{2},\sqrt{3})$ are subfields of each other. From (c) we have that the degree of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ over $\mathbb{Q}$ is 4.

Exercise 15.3.4 Find a suitable number a such that

a) $\mathbb{Q}(\sqrt{2},\sqrt{5}) = \mathbb{Q}(a)$.

b) $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(a)$.

Solution (a) In general, see exercise 15.3.2 (d) for argumentation. The solution is $a = \sqrt{2}+\sqrt{5}$.

It's obvious that $\mathbb{Q}(\sqrt{2},\sqrt{5}) \supseteq \mathbb{Q}(\sqrt{2}+\sqrt{5})$. Square a and get

$$a^2 = 2 + 5 + \sqrt{10} = 2 + 5 + \sqrt{2}\sqrt{5}.$$

And that concludes the contents of my notes for this exercise.

(b) The solution is $a = \sqrt{3} + i$. It's obvious that $\mathbb{Q}(\sqrt{3}, i) \supseteq \mathbb{Q}(\sqrt{3}+i)$.

Square and get

$$a^2 = 3 - 1 - 2i\sqrt{3}.$$

Manipulate:

$$a(a^2 - 2) = 6i + 2\sqrt{3}$$
$$a^2 - 2 = 2i\sqrt{3}$$

We can then express $\sqrt{3}$ and i using a.

Exercise 15.3.6 If E is an extension field of F and $[E : F]$ is prime, prove that there are no fields properly between E and F.

Solution Let K be a field between E and F, $E/K/F$. We also have that

$$\underbrace{[E : F]}_{\text{prime}} = [E : K][K : F]$$

.

Hence either $[E : K] = 1$ and $K = E$, or $[K : F] = 1$ and $K = F$.

Exercise 15.3.10 Give an example of a field E containing a proper subfield K such that E is embeddable in K and $[E : K]$ is finite.

Solution The lecturer said that this exercise was unreasonable or something like that.

We have E/K and an embedding $\sigma : E \mapsto K$ such that

$$\begin{aligned} E = \mathbb{Q}(x) &= \frac{f(x)}{g(x)} \\ f(x), g(x) &\in \mathbb{Q}[x] \\ K = \mathbb{Q}(x^2 = y) &= \frac{h(y)}{k(y)} \\ h(y), k(y) &\in \mathbb{Q}[y] \end{aligned}$$

$[E : K] = 2$, since x is a root of $z^2 - y \in K[z]$.

$$\begin{aligned} x &\to y(= x^2) \\ \mathbb{Q} &\to \mathbb{Q} \text{ (id)} \\ &\Downarrow \\ E &\to K \\ \frac{f(x)}{g(x)} &\to \frac{f(y)}{g(y)} \ (y = x^2) \end{aligned}$$

5 Problem set 3

Exercise 16.1.2 Construct a splitting field E for $x^3 + x + 1 \in \mathbb{Z}/(2)[x]$ and list all its elements.

Solution By trying the candidate roots 0 and 1, we find that $f(x) = x^3 + x + 1 \in \mathbb{Z}/(2)[x]$ is irreducible. Let α be a root of $f(x)$. Then $x - \alpha$ is a divisor of $x^3 + x + 1$ in $E[x]$.

$\alpha + \alpha = 0$, so $\alpha = -\alpha$, because the splitting field E is a vector space over $\mathbb{Z}_2$.

Since α is a root, $(x-\alpha) = (x+\alpha)$ divides x^3+x+1. Perform the polynomial division and we get the other factor $x^2 + \alpha x + (\alpha^2 + 1)$.

We try to guess another root: α^2. Show that α^2 is a root of $(x^2+\alpha x+\alpha^2+1)$: Substitute x with α^2 and get $\alpha^4 + \alpha^3 + \alpha^2 + 1$. Knowing that $\alpha^3 + 1 = \alpha$ (which is true since α is a root of $x^3+x+1 \in \mathbb{Z}_2[x]$, and also that $\alpha^4+\alpha = \alpha^2$ (by multiplying the previous equation with α)), it evaluates to 0 and hence α^2 is a root.

To find the last root, divide $x^2 + \alpha x + (\alpha^2 + 1)$ by $(x + \alpha^2)$. This yields a root of $\alpha^2 + \alpha$.

$\mathbb{Z}_2(\alpha)$ has basis $\{1, \alpha, \alpha^2\}$, so elements are of the form $e(\in E) = a + b\alpha + c\alpha^2$, with $a, b, c \in \mathbb{Z}_2$. The elements are:

0	α^2
1	$\alpha^2 + 1$
α	$\alpha^2 + \alpha$
$\alpha + 1$	$\alpha^2 + \alpha + 1$.

$E = \mathbb{Z}_2(\alpha)$ is a field extension of $F = \mathbb{Z}_2$ with $[E : F] = 4$, and $|E| = [E : F]|F| = 4 \cdot 2 = 8$.

Exercise 16.1.5 Let E be the splitting field of a polynomial of degree n over a field F. Show that $[E : F] \leq n!$.

Solution Let $f(x) \in F[x]$, $f(x) = a_n x^n + \cdots + a_1 x + a_0$. The degree of $f(x)$ is n. Let α be a root of $f(x)$. We have

$$[F(\alpha) : F] \leq n$$

which is identical to the degree of the minimal polynomial $p(x)$ of α over F. $p(x)$ is a divisor of $f(x)$.

This implies that $\deg(p(x)) \leq \deg(f(x)) = n$. Rewrite $f(x)$ as

$$f(x) = (x - \alpha) f_1(x).$$

We have $\deg(f_1(x)) = n-1$. β is a root of $f_1(x)$ and $[F(\alpha, \beta) : F(\alpha)] \leq n-1$. Repeat the argument until we end up with a degree 1 polynomial. By then, $E = F(\alpha, \beta, \cdots)$ (F adjoined with all roots of $f(x)$) will therefore be the splitting field of $f(x)$. By multiplying the dimensions using the product rule, we get that $[E : F] \leq n!$.

Exercise 16.1.7 If an irreducible polynomial $p(x)$ over a field F has one root in a splitting field E of a polynomial $f(x) \in F[x]$, then $p(x)$ has all its roots in E.

Solution Follows immediately from theorem 16.2.1: Condition (ii) is fulfilled, since E is the splitting field of the family $(f(x))$ of polynomials in $F[x]$. This condition is equivalent to condition (i), which states that every irreducible polynomial in $F[x]$ that has a root in E splits into linear factors in E. The assumption in the problem is that we have an irreducible polynomial $p(x)$ over a field F which has one root in a splitting field E of a polynomial $f(x) \in F[x]$, Hence E is the splitting field of $p(x)$ over F.

There is also a solution in the back of the book, which pretty much uses the same method as in the proof of theorem 16.2.1. Regarding that proof, we recall from Algebra that if F is a finite field with p elements, $F[x]/(p(x))$ is a finite field with p^n elements where $p(x)$ is irreducible and $\deg(p(x)) = n$,

and $F[x]/(p(x)) \simeq F(\alpha)$ where α is a root of $p(x) = 0$ in some extension of F.

Exercise 16.1.8 Show that over any field $K \supset \mathbb{Q}$ the polynomial $x^3 - 3x + 1$ is either irreducible or splits into linear factors.

Solution The lecturer wasn't able to find the answer to this exercise. Here's the beginning of a potential solution.

$$\begin{aligned} x^3 - 3x + 1 &= (x - \alpha)(x - \beta)(x - \gamma) \\ &= x^3 + (-\alpha - \beta - \gamma)x^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)x - \alpha\beta\gamma \end{aligned}$$

Relate the coefficients of x of both sides:

$$\begin{aligned} -\alpha - \beta - \gamma &= 0 \\ \alpha\beta + \beta\gamma + \alpha\gamma &= -3 \\ -\alpha\beta\gamma &= 1 \end{aligned}$$

The question remains: can we express β and γ in terms of α?

Exercise 16.1.9 Let $f(x) = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$. Find the roots α, β of $f(x)$ such that

$$\mathbb{Q}(\alpha) \simeq \mathbb{Q}(\beta).$$

What is the splitting field of $f(x)$?

Solution $f(x)$ is irreducible, due to Eisenstein's criterion with $p = 2$. Let α and β be the two roots. Since $f(x)$ is irreducible, it is the minimal polynomial of both α and β over $\mathbb{Q}$, and we have

$$F(\alpha) \simeq F[x]/(f(x)) \simeq F(\beta).$$

Let $\sigma : F(\alpha) \mapsto F(\beta)$. Then, $\sigma(\alpha) = \beta$ and $\sigma(a) = a$ for any $a \in F$.

$x^2 = 1 \pm \sqrt{3}$

$x = \pm\sqrt{1 + \pm\sqrt{3}}$

$\beta = \sqrt{1 + \sqrt{3}} \in \mathbb{R}$, so $\mathbb{Q}(\beta) \subseteq \mathbb{R}$.

$\alpha = \sqrt{1 - \sqrt{3}} \notin \mathbb{R}$, so the splitting field E of $f(x) = x^4 - 2x^2 - 2$ is equal to $E = \mathbb{Q}(\alpha, \beta)$.

$[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. We seek $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)]$.

$\beta^2 = 1 + \sqrt{3}$, and $\sqrt{3} \in \mathbb{Q}(\beta)$.

The minimal polynomial of α over $\mathbb{Q}(\beta)$ is

$$x^2 - (1 - \sqrt{3}) \in \mathbb{Q}(\beta)[x].$$

Therefore, $[\mathbb{Q}(\alpha,\beta]) : \mathbb{Q}(\beta)] = 2$. So $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = 8$.

Exercise 16.2.2 Is $\mathbb{R}(\sqrt{-5})$ normal over $\mathbb{R}$?

Solution Yes, since $\mathbb{R}(\sqrt{-5})$ is the splitting field of x^2+5, and hence (by definition) it is a normal extension, since it is the splitting of a family of polymomials, namely the family consisting of x^2+5.

Exercise 16.2.3 Let E be a normal extension of F and let K be a subfield of E containing F. Show that E is a normal extension over K. Give an example to show that K need not be a normal extension of F.

Solution E is the splitting field of some polynomial over F, and hence the splitting field of the same polynomial considered as a polynomial over K.

Example: Let $F = \mathbb{Q}, K = \mathbb{Q}(2^{1/3}), E = \mathbb{Q}(2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2)$, where $\omega = e^{i\frac{2\pi}{3}}$. The minimal polynomial of K over $\mathbb{Q}$ is x^3-2. K is not a splitting field of x^3-2 over $\mathbb{Q}$, since K doesn't contain all the roots.

Exercise 16.2.4 Let $F = \mathbb{Q}(\sqrt{2})$ and $E = \mathbb{Q}(\sqrt[4]{2})$. Show that E is a normal extension of F, F is a normal extension of $\mathbb{Q}$, but E is not a normal extension of $\mathbb{Q}$.

Solution $\sqrt{2}$ is a root of the polynomial x^2-2 over $\mathbb{Q}$, and F obviously contains all the roots of this polynomial. $2^{1/4}$ is a root of the polynomial $x^2-\sqrt{2}$ over F, and E obviously[1] contains all the roots of this polynomial.

But E is not a normal extension of $\mathbb{Q}$ since the minimal polynomial x^4-2 over $\mathbb{Q}$ has roots in $\mathbb{C}$.

Exercise 16.2.7 Show that the field generated by a root of x^3-x-1 over $\mathbb{Q}$ is not normal over $\mathbb{Q}$.

Solution According to theorem 42, x^3-x-1 has a real root. Furthermore, x^3-x-1 has only one real root (not shown, but see exercises 16.1.3-4). Let α be the real root. Hence $\mathbb{Q}(\alpha)$ is not a normal extension, since it doesn't contain all of the roots of x^3-x-1 over $\mathbb{Q}$.

Exercise 16.2.8 Find the smallest normal extension (up to isomorphism) of $\mathbb{Q}(2^{1/4})$ in $\bar{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$).

Solution The smallest normal extension of $\mathbb{Q}(2^{1/4})$ is $\mathbb{Q}$ adjoined all the roots of the minimal polynomial x^4-2 of $2^{1/4}$ over $\mathbb{Q}$. The missing roots are $\pm i2^{1/4}$, hence the smallest normal extension of $\mathbb{Q}(2^{1/4})$ is $\mathbb{Q}(2^{1/4}, i2^{1/4}) = \mathbb{Q}(2^{1/4}, i)$.

Exercise 16.2.11 Let $E \subset \bar{F}$ and $K \subset \bar{F}$ be normal extensions of a field F. Show that the subfield L generated by E and K is also normal over F.

[1] Exercise: Is this obviously obvious?

Solution Since E is normal over F, it is the splitting field of some polynomial $f_E(x)$ over F; similarly, K is the splitting field of $f_K(x)$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f_E(x)$ and $\beta_1, \ldots, \beta_m$ the roots of $f_K(x)$. Then $E = F(\alpha_1, \ldots, \alpha_n)$ and $K = F(\beta_1, \ldots, \beta_n)$, so $L = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$ and thus L is the splitting field of $f_E(x)f_K(x)$.

6 Problem set 4

Exercise 16.3.4 Let $f(x)$ be a polynomial of degree n over a field F of characteristic p. Suppose $f'(x) = 0$. Show that $p|n$ and that $f(x)$ has at most n/p distinct roots.

Solution We have

$$\begin{aligned} f(x) &= \underbrace{a_n}_{\neq 0} x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\ f'(x) &= \underbrace{na_n}_{=0} x^{n-1} + \cdots + 2a_2 x + a_1 = 0, \end{aligned}$$

because $f'(x) = 0$ and characteristic p of F forces $p|n$. If p didn't divide n, we would have $na_n \neq 0$ (which causes $f'(x) \neq 0$, which is absurd) or $a_n = p = 0$ (which causes $\deg(f(x)) < n$, which is absurd).

Hence $ia_i = 0$ for all $0 < i \leq n$ such that $p|i$, and $a_i = 0$ for all $0 < i < n$ such that p doesn't divide i. Hence

$$f(x) = a_n x^n + a_{n-p}x^{n-p} + a_{n-2p}x^{n-2p} + \cdots + a_{2p}x^{2p} + a_p x^p + a_0.$$

According to corollary 16.3.5 (whose proof I've pretty much repeated above), we have $f(x) = g(x^p)$ for some $g(y) \in F[y]$. The degree of $g(x)$ is $\frac{n}{p}$. Let $f(x) = g(x^p) = 0$. $g(y) = 0$ has at most $\frac{n}{p}$ distinct roots. Let α be one of these roots, i.e. $g(\alpha) = 0$ and $y = x^p = \alpha$. Let $a_1^p = \alpha$ and $a_2^p = \alpha$ be two roots of $x^p = \alpha$. Manipulate:

$$\begin{aligned} (a_1 - a_2)^p = \ & (*) \\ & a_1^p - a_2^p \\ \Rightarrow\ & a_1 = a_2. \end{aligned}$$

Therefore $x^p = a$ has only one distinct root. [In (*) we made use of the fact that in $\mathbb{Z}_p$, (where p is a prime number), $(a \pm p)^p = a^p \pm b^p$, since all other terms are divisible by p.] So $0 = f(\beta) = g(\beta^p)$, $\beta^p = \alpha$ for some root in $g(y) = 0$. Since β is uniquely determined by α, we get that $f(x)$ can have at most $\frac{n}{p}$ distinct roots.

Exercise 16.4.1 If F is a finite field of characteristic p, show that each element a of F has a unique pth root $\sqrt[p]{a}$ in F.

Solution Use the Frobenius automorphism, $\phi : F \to F$, $\phi(x) = x^p$. Since ϕ is a bijection, there exists a $\beta \in F$ such that $\phi(\beta) = \beta^p = \alpha$. Let β_1 and β_2 be two β's such that $\phi(\beta) = a$. We have

$$\beta_1^p = a, \beta_2^p = a$$
$$(\beta_1 - \beta_2)^p = \beta_1^p - \beta_2^p = 0 \Rightarrow \beta_1 = \beta_2.$$

Hence β is unique.

Exercise 16.4.2 Construct fields with 4, 8, 9, and 16 elements.

Solution In general, we can construct a field with p^n elements where p is a prime number and $n \geq 1 \in \mathbb{N}$, if we have an irrediculble polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree n. The field with p^n elements is then the factor field $\mathbb{Z}_p[x]/(f(x)) = GF(p^n)$. $f(x)$ can easily be found by brute force, if both p and n are small. If $n < 4$ we only need to make sure that $f(x)$ has no roots in $\mathbb{Z}_p$. For $n = 4$ and $n = 5$ we also need to make sure that no polynomial of degree 2 divides $f(x)$.

4 elements: $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x], GF(2^2) = \mathbb{Z}_2[x]/(x^2 + x + 1)$.

8 elements: $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x], GF(2^3) = \mathbb{Z}_2[x]/(x^3 + x + 1)$.

9 elements: $f(x) = x^2 + 1 \in \mathbb{Z}_3[x], GF(3^2) = \mathbb{Z}_3[x]/(x^2 + 1)$.

16 elements: $f(x) = x^4 + x + 1 \in \mathbb{Z}_2[x], GF(2^4) = \mathbb{Z}_2[x]/(x^4 + x + 1)$. TODO verify that $f(x)$ is irreducible. The one from my notes was wrong.

What do the elements look like? For instance, $GF(2^2) = \{a + b\alpha | a, b \in \mathbb{Z}_2\}$, where α is a root of $x^2 + x + 1$. In order to multiply two elements and get rid of α^2 and α's of higher degree, repeatedly apply the identity $\alpha^2 = \alpha + 1$ derived from the irreducible polynomial.

Exercise 16.4.3 Find generators for the multiplicative groups of fields with 8, 13 and 17 elements.

Solution $GF(2^3) - \{0\} = GF(2^3)^*, |GF(2^3)^*| = 7$. Since the order of the group is a prime, every element (except identity) is a generator.

$|GF(13)^*| = 12$: Find generator by trial and error. Find an element $a \in GF(13)^*$ such that all of $a, a^2, a^3, \cdots, a^{12}$ are distinct. $a = 2$ is a generator. It is actually enough to check that $a^4 \neq 1$ and $a^6 \neq 1$. In general, for each prime $p \leq \sqrt{|G|}$ that divides $|G|$ (where G is our multiplicative group), it is enough to check that $a^{|G|/p} \neq 1$. (TODO verify if this is correct.)

$|GF(17)^*| = 16$: Find a such that $a^8 \neq 1$. $a = 2$ is a generator.

Exercise 16.4.4 Find generators for the group of automorphisms of fields with 4, 8, 9, and 16 elements.

Solution These are Frobenius automorphisms. The generators ϕ for each group are given below.

4: $F = GF(2^2)$, $\phi : F \mapsto F$, $\phi(x) = x^2$.

8: $F = GF(2^3)$, $\phi : F \mapsto F$, $\phi(x) = x^2$.

16: $F = GF(2^4)$, $\phi : F \mapsto F$, $\phi(x) = x^2$.

9: $F = GF(3^2)$, $\phi : F \mapsto F$, $\phi(x) = x^3$.

It seems that for $F = GF(p^n)$ and $\phi : F \mapsto F$, the generator is $\phi(x) = x^p$.

Exercise 16.4.7 Prove that in any finite field any element can be written as the sum of two squares.

Solution Assume that $\text{char}(F) \neq 2$, that is, $|F| = p^n$, $p \neq 2$. Let $a \neq 0 \in F$, and

$$A = \{a - x^2 | x \in F\}, \text{ and}$$
$$B = \{y^2 | y \in F\}.$$

We have

$$|A| = \left\lfloor \frac{|F| + 1}{2} \right\rfloor, \text{ and}$$
$$|B| = \left\lfloor \frac{|F| + 1}{2} \right\rfloor.$$

This implies that $A \cap B \neq \emptyset$.

Hence, for arbitrarily chosen $a \neq 0 \in F$, there exists $x, y \in F$ such that $a - x^2 = y^2$, or $x^2 + y^2 = a$.

For $\text{char}(F) = 2$, we have for all $x \in F, x = x^2 = x^2 + 0^2$.

Exercise 16.4.8 If F is a finite field, then $H \cup \{0\}$ is a subfield of F for each subgroup H of the multiplicative group F^* if and only if $|F^*|$ either 1 or prime of the form $2^n - 1$, where n is a positive integer.

Solution (not from lecture) $\Rightarrow$: Assume $\text{char}(F) = p > 2$ and p prime. We want to conclude that $\text{char}(F)$ can't be > 2. F is finite, so $|F| = p^n$ for some integer $n \geq 1$. Then $|F^*| = p^n - 1$. We know that $H \cup \{0\}$ is a subfield of F if $|H \cup \{0\}| = p^k$ for some k such that $k|n$, and we also have $p^k | p^n$. Assume that $k|n \Rightarrow p^k - 1 | p^n - 1$. TODO try to arrive at some kind of contradiction.

Hence $p^k - 1$ doesn't divide $p^n - 1$ for arbitrary $p > 2$ prime, n and k such that $k|n$, hence H can't be a subgroup of F^*. Hence we can't have $\text{char}(F) > 2$. $\text{char}(F) \neq 0$, since F is a finite field (Theorem 16.4.2). Hence $\text{char}(F) = 2$.

Claim: $H \subset F^*$ implies $H = \{0\}$ or $H = F^*$:

Assume $|H| = 2^k - 1$ and $k|n$. We get

$$\begin{aligned} 2^n - 1 &= (2^k - 1)(2^l - 1) \\ &= 2^{k+l} - 2^k - 2^l - 1 \end{aligned}$$

Add 1 to both sides and get

$$2^n = 2(2^{k+l-1} - 2^{l-1} - 2^{k-1} + 1)$$

which is absurd unless $k = 1$ or $l = 1$. Hence $|F^*| = 2^n - 1$ is a prime number or $|F^*| = 1$. Hence F^* has only the trivial subgroups $H = \{0\}$ and $H = F^*$ (since we must have that $|H|$ divides $|F^*|$).

$\Leftarrow$: Assume that for a finite field F, $|F^*|$ is either 1 or a prime of the form $2^n - 1$. We wish to show that for every subgroup H of F^*, $H \cup \{0\}$ is a subfield of F. F^* has only trivial subgroups, and the corresponding candidates for subfields are $H \cup \{0\} \simeq \mathbb{Z}_2$ and F itself, which are obviously subfields. Hence $H \cup \{0\}$ is a subfield for each subgroup H of F^* and hence the proof is finished.

TODO verify that this is correct, especially the first half.

Exercise 16.4.10 Without actually computing, find the number of irreducible polynomials of (i) degree 2 and (ii) degree 3 over each of the fields $\mathbb{Z}_3$ and $\mathbb{Z}_5$.

Solution (detailed) Our method is to calculate the number of reducible polynomials, and subtract that amount from the total number of polynomials. We make it easier on ourselves by calculating the number of *monic* polynomials, since we can afterwards multiply with 2 or 4 (to get the number of desired polynomials over $\mathbb{Z}_3$ and $\mathbb{Z}_5$, respectively).

(i) $x^2 + ax + b \in \mathbb{Z}_3[x]$. Altogether there are $3^2 = 9$ monic polynomials of degree 2 over $\mathbb{Z}_3$. The number of reducible monic polynomials of degree 2 are:

- 3, the number of polynomials such that all the roots are equal.
- $\binom{3}{2} = 3$, the number of polynomials with distinct roots.

Hence, there are $2 \cdot (9 - 3 - 3) = 6$ irreducible polynomials of degree 2 over $\mathbb{Z}_3$.

$x^3 + ax^2 + bx + c \in \mathbb{Z}_3[x]$: Altogether there are $3^3 = 27$ monic polynomials of degree 3 over $\mathbb{Z}_3$. The number of reducible monic polynomials of degree 3 are:

- $3 \cdot 3 = 9$ ways of factoring into irreducible polynomials of degree 1 and 2. There are 3 possible of each. We know from the previous part that there are 3 monic irreducible polynomials of degree 2.
- 3, the number of polynomials such that all the roots are equal.
- $2 \cdot \binom{3}{2} = 6$, the number of polynomials with two distinct roots, one of them appearing twice. Any two of these distinct roots can appear twice, so we multiply by 2.
- $\binom{3}{3} = 1$, the number of polynomials with three distinct roots.

Hence, there are $2 \cdot (27 - 9 - 3 - 6 - 1) = 16$ irreducible polynomials of degree 3 over $\mathbb{Z}_3$.

(ii) Same as (i), but over $\mathbb{Z}_5$. There are $5^2 = 25$ monic polynomials of degree 2 over $\mathbb{Z}_5$. The number of reducible monic polynomials of degree 2 are:

- 5, the number of polynomials such that all the roots are equal.
- $\binom{5}{2} = 10$, the number of polynomials with disticts roots.

Hence, there are $4 \cdot (25 - 5 - 10) = 40$ irreducible polynomials of degree 2 over $\mathbb{Z}_5$.

$x^3 + ax^2 + bx + c \in \mathbb{Z}_5[x]$: Altogether there are $5^3 = 125$ monic polynomials of degree 3 over $\mathbb{Z}_5$. The number of reducible monic polynomials of degree 3 are:

- $5 \cdot 10 = 50$ ways of factoring into irreducible polynomials of degree 1 and 2. There are 5 possible irreducible polynomials of degree 1, and from above we have that there are 10 monic (40 when we don't require monic) irreducible polynomials of degree 2 over $\mathbb{Z}_5$.
- 5, the number of polynomials such that all the roots are equal.
- $\binom{5}{2} \cdot 2 = 20$, the number of polynomials with two distinct roots, one of them appearing twice.
- $\binom{5}{3} = 10$, the number of polynomials with distinct roots.

Hence, there are $4 \cdot (125 - 50 - 5 - 20 - 10) = 160$ irreducible polynomials of degree 3 over $\mathbb{Z}_5$.

These answers are verified to be correct by a computer program that evaluates every possible relevant polynomial. Beware of bugs in the above code; I have only tested it, not proven it correct.

One can argue whether we have solved this exercise without *computing*, but the above method is approved by the lecturer. Hence, this method accompanied with a correct answer will yield full score on the exam.

Exercise 16.5.2 Find $\theta \neq \sqrt{3} + \sqrt{5}$ such that $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\theta)$.

Solution Not shown in the lecture, I think. θ can be found using the method in the proof of theorem 16.5.2. TODO do it. Just choose $\theta = \sqrt{3} - \sqrt{5}$?

Exercise 16.5.5 Prove that a finite extension of a finite field is separable.

Solution Let $\alpha \in E$, and let $p(x) \in F[x]$ be the minimal polynomial of α over F. $p(x) = 0$ has only distict roots (proved earlier, see the definition of separable), hence by definition $p(x)$ is separable. Hence E is a separable extension of F.

Textbook solution Let F be a field with p^m elements and E be an extension with F having p^n elements. Then $E = F(\alpha)$ where $\alpha \in E$ (corollary 16.4.7) and so $f(x) = x^{p^n} - x$, $f(\alpha) = 0$. This implies that α is a separable element (because of theorem 16.3.3, since $f'(x) = -1 \neq 0$), and hence $F(\alpha)$ is a separable extension of F.

Exercise 16.5.6 Prove that every extension of $\mathbb{Q}$ is separable.

Solution This follows immediately from one of the definitions of separable. If $p(x) \in \mathbb{Q}[x]$ is the minimal polynomial of an arbitrary element $\alpha \in E$ over $\mathbb{Q}$, $p(x) = 0$ has only distict roots, then, by definition E is separable.

Exercise 16.5.7 Let α be a root of $x^p - x - 1$ over a field F of characteristic p. Show that $F(\alpha)$ is a separable extension of F.

Solution $f'(x) = -1 \neq 0$ for all x. Hence $f(x)$ is a separable polynomial (theorem 16.3.3).

Theorem (unproven): Let $F(\alpha)$ be an extension to F. If α is separable element of F, then $F(\alpha)$ is a separable extension of F.

We recall that given a field F and an extension $F(\alpha)$, an element α is separable if the minimal polynomial of α over F is separable (has distinct roots).

If $p(x) \in F[x]$ is the minimal polynomial of α over F, then $p(x) | x^p - x - 1$ in $F[x]$. Hence $p(x)$ has distinct roots. Hence $F(\alpha)$ is a separable extension of F.

7 Problemset 5 (Exam 2004)

I was rather sleepy during this lecture, so some solutions can be incomplete or messy. Also, the solution to problem 3 b) uses Sylow theory, which not

every student has learned (only those who took MA2201).

Problem 1 a) Prove that if D is a domain that is not a field, then $D[x]$ is not a Euclidean domain.

Solution Theorem 11.3.2 and theorem 11.3.3 says that every Euclidean domain is a PID and UFD. so it suffices to show that $D[x]$ isn't PID or UFD. We recall that D is a PID (principal ideal domain) if every ideal in D is of the form $(a) = aD$ for some $a \in D$.

$D[x]$ is not a PID: Let $a \in D$ such that $a^{-1} \notin D$. The ideal $(a, x) = (a) + (x) = ar + xs$ for $r, s \in D$ is not principal, since it's generated by the two elements a and x.

Problem 1 b) Show that 3 is irreducible, but not prime, in the integral domain $\mathbb{Z}[\sqrt{-5}]$.

Solution Units in $\mathbb{Z}(\sqrt{-5})$ are ± 1. We have

$$3 = (a + b\sqrt{-5})(c + d\sqrt{-5}).$$

Take the norm on both sides and get

$$9 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Candidates for a, b, c, d are

$$b = d = 0 \Rightarrow a = \pm 1 \text{ or } c = \pm 1,$$

or

$$b = \pm 1, a = \pm 2 \Rightarrow d = 0, c = \pm 1.$$

Either way, one of the terms on the right side is forced to be a unit.

$9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, and $3|9$. If we can show that 3 doesn't divide $2 \pm \sqrt{5}$, then 3 is not a prime. We recall that a is a prime if a is not a unit and $a|bc \Rightarrow a|b$ or $a|c$.

Assume that $3|2 \pm \sqrt{-5}$. We have

$$2 \pm \sqrt{-5} = 3(a + b\sqrt{-5})$$

for some $a, b \in \mathbb{Z}$. Take the norm:

$$9 = 9(a^2 + 5b^2),$$

the only possibilities are $b = 0$ and $a = \pm 1$. We get

$$2 \pm \sqrt{-5} = \pm 3,$$

an impossibility. Hence we have reached a contradiction to the assumption that $3|2 \pm \sqrt{-5}$. Hence 3 is irreducible, but not prime.

Problem 2 a) Determine the Galois group of $x^3 - 7 \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

Solution Let $E = \mathbb{Q}(\sqrt[3]{7}, \omega), \omega = e^{\frac{2\pi i}{7}}$. $\mathbb{Q}(\sqrt[3]{7})$ is an extension of $\mathbb{Q}$. We have $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3$ since the minimal polynomial of $\sqrt[3]{7}$ over $\mathbb{Q}$ is $x^3 - 7$. $\omega \notin \mathbb{Q}(\sqrt[3]{7})$, so $\mathbb{Q}(\sqrt[3]{7}, \omega) \neq \mathbb{Q}(\sqrt[3]{7})$. The minimal polynomial of ω over $\mathbb{Q}(\sqrt[3]{7})$ is $\frac{x^3-1}{x-1} = x^2 + x + 1 \in \mathbb{Q}(\sqrt[3]{7})$. Hence $[E : \mathbb{Q}] = 6$. The group $G(E|Q) \simeq S_3$ is the permutation of the roots.

Problem 2 b) Let E determine the splitting field of $x^3 - 7$ over $\mathbb{Q}$. How many intermediate fields $F(\mathbb{Q} \subset F \subset E)$, such that $[F : \mathbb{Q}] = 2$, are there? Give reasons.

Solution $|G(E|F)| = [E : F] = 3$. We wish to find $H \subset S_3$ such that $|H| = 3$. $H = \{\mathrm{id}, (123), (132)\}$. $H \triangleleft S_3$ (H is a normal subgroup of S_3.) This implies that F is unique.

Assume $[F : \mathbb{Q}] = 3$, $[E : F] = 2$. $F \Leftrightarrow H < S_3$, $|H| = 2$. $H = \{(12), (13), (23)\}$. The number of such F's are 3. Why on earth do we assume $[F : \mathbb{Q}] = 3$? This contradicts with what the problem asks for.

Problem 3 Let p be a prime. Let E be the splitting field of $x^p - 1 \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

a) Prove that $G(E/\mathbb{Q})$ is abelian of order $p - 1$.

Solution Let $\alpha \neq 1$ be a root. Consider α^q. $(\alpha^q)^p - 1 = (\alpha^p)^q - 1 = 1^q - 1 = 0$, so α^q is a root. $E = \mathbb{Q}(\alpha)$. $H = \{\alpha, \alpha^2, \ldots, \alpha^{p-2}\}$ is a basis for E over $\mathbb{Q}$. Hence $|G(E|\mathbb{Q})| = p - 1$.

$\phi \in G(E|\mathbb{Q})$. $\phi(\alpha) = \alpha^r, 1 \leq r \leq p - 1$.

Show that ϕ is commutative:

$\phi_1, \phi_2 \in G(E|\mathbb{Q})$. $\phi_1(\alpha) = \alpha^r, \phi_2(\alpha) = \alpha^s$.

$$\begin{aligned} \phi_1 \circ \phi_2(\alpha) &= \phi_1(\phi_2(\alpha)) \\ &= \phi_1(\alpha^s) \\ &= \underbrace{\phi_1(\alpha) \cdots \phi_1(\alpha)}_{s \text{ times}} \\ &= \alpha^{rs}. \end{aligned}$$

The other way round:

$$\begin{aligned}\phi_2 \circ \phi_1(\alpha) &= \phi_2(\phi_1(\alpha)) \\ &= \phi_2(\alpha^r) \\ &= \underbrace{\phi_2(\alpha) \cdots \phi_2(\alpha)}_{r \text{ times}} \\ &= \alpha^{sr}.\end{aligned}$$

Hence we have $\phi_1 \circ \phi_2 = \phi_2 \circ \phi_1$, and hence $G(E|\mathbb{Q})$ is commutative.

[ϕ is a homomorphism (isomorphism), so $\phi(a)\phi(b) = \phi(ab)$, allowing the step $\phi(\alpha^r) = \underbrace{\phi(\alpha) \cdots \phi(\alpha)}_{r \text{ times}}$.]

b) Let $\omega = e^{\frac{2\pi i}{31}}$. Prove that there exists a subfield F of $\mathbb{C}$ such that $[F(\omega) : F] = 5$.

Solution We have extensions $\mathbb{C}/F(\omega)/F/\mathbb{Q}$. We wish to find F such that $[F(\omega) : F] = 5$.

$F(\omega) = \mathbb{C}(\omega)$ is the splitting field of $x^{31} - 1 \in \mathbb{Q}[x]$. $G(E|\mathbb{Q})$ is abelian. $|G(E|\mathbb{Q})| = [E : \mathbb{Q}] = 30$. Sylow's main theorem says that for a prime number p, if $p^k||G|$, then G has a subgroup of order p^k for some $k \geq 1 \in \mathbb{Z}$. By applying this theorem with $p = 5, |G| = 30, k = 1$ we find that $G(E|\mathbb{Q})$ has a subgroup of order 5. By the main theorem of Galois theory, then there exists a field F such that $[F(\omega) : F] = 5$.

Problem 4 a) Let F be a field of characteristic p, where $0 < p \neq 3$. Let α be a root of $f(x) = x^p - x + 3 \in F[x]$ that lies in F. Show that $f(x)$ has p distinct roots in F. [HINT: Show that $\alpha + 1$ is a root.]

Solution Evaluate $f(x)$ at $\alpha + 1$:

$$\begin{aligned}f(\alpha + 1) &= (\alpha + 1)^p - (\alpha + 1) + 3 \\ &= \alpha^p + 1^p - (\alpha + 1) + 3 \\ &= \alpha^p - \alpha + 3 \\ &= 0,\end{aligned}$$

since we assumed that α is a root, so $\alpha + 1$ is a root. By induction, $\alpha + 2, \alpha + 3, \ldots$ are also roots.

Hence, the roots are $\alpha, \alpha + 1, \ldots, \alpha + (p - 1)$. Since the characteristic of F is p, they are distinct.

Problem 4 b) Without actually computing, find the number of monic irreducible polynomials of degree 2 over the field $\mathbb{Z}_7 = GF(7)$.

Solution The number of monic polynomials of degree 2 over $\mathbb{Z}_7$ is $7^2 = 49$.

The number of monic polynomials with two distinct roots are $\binom{7}{2} = 21$.

The number of monic polynomials with two equal roots are 7.

The number of monic irreducible polynomials are then $49 - 21 - 7 = 21$.

Problem 5 Prove that $\sqrt{2} + \sqrt[3]{3}$ is irrational. [HINT: Consider $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{3})$.]

Solution Assume $\sqrt{2} + \sqrt[3]{3} = a \in \mathbb{Q}$. Then $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt[3]{3})$ is an extension to $\mathbb{Q}$. This is already a contradiction, since

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$
$$[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3.$$

This problem can also be solved using the same technique as used when proving that $\sqrt{2}$ is irrational.

8 Problemset 6 (Exam 2006)

Problem 1 Let $f(x) \in F[x]$ be an irreducible polynomial over the field F, where F has characteristic 0. Let E be the splitting field over F, and assume that the Galois group $G = G(E|F)$ is abelian.

Show that every root α of $f(x)$ is a primitive element, ie. $E = F(\alpha)$.

Solution We have that

$$E = F(\alpha_1, \alpha_2, \cdots, \alpha_n).$$

since E is the splitting field of $f(x)$ over F. To show that

$$E = F(\alpha)$$

for an $\alpha \in E$, we must show that

$$\mathrm{id} = G(E|E) = G(E|F(\alpha)).$$

Equivalently, we must show that if $\sigma \in G(E|F(\alpha))$, then $\sigma = \mathrm{id}$. We have

$$\sigma \in G(E|F(\alpha)) \Leftrightarrow \sigma(\alpha) = \alpha.$$

A basis of $F(\alpha)$ is

$$\alpha, \alpha^2, \cdots.$$

If α is fixed, every element in $F(\alpha)$ is fixed. [If α is fixed, so is $\alpha^2, \alpha^3, \cdots$.] We have

$$\sigma = \mathrm{id} \Leftrightarrow \sigma(\alpha_i) = \alpha_i.$$

for $i = 1, 2, \cdots, n$. Another «basis» is $a_1^{k_1}, \cdots, a_n^{k_n}$. We have

$$H = G(E|F(\alpha)) = \{\sigma \in G(E|F) | \sigma(\alpha) = \alpha\}.$$

We want to show that

$$H = \{\mathrm{id}\} \Leftrightarrow \sigma(\alpha_i) = \alpha_i$$

for $i = 1, 2, \cdots, n$. There exists $\sigma_i \in G(E|F)$ such that $\sigma_i(\alpha) = \alpha_i$, since $f(x)$ is irreducible. Let

$$H_i = \{\sigma \in G(E|F) | \sigma(\alpha_i) = \alpha_i\}.$$

We claim that $H_i = \sigma_i H \sigma_i^{-1}$. (Which is also equal to H, since $G(E|F)$ is abelian.) If we can show this identity, then $\sigma \in H$ implies $\sigma(\alpha_i) = \alpha$, for $i = 1, 2, \cdots, n$ and hence $\sigma = \mathrm{id}$.

$$\begin{aligned} \tau &\in \sigma_i H \sigma_i^{-1} \\ \tau = \sigma_i \sigma \sigma^{-1} &\text{ for a } \sigma \in H. \end{aligned}$$

$$\begin{aligned} \tau(\alpha_i) &= \sigma_i \sigma \sigma_i^{-1}(\alpha_i) \\ &= \sigma_i \sigma(\alpha) \\ &= \sigma_i(\alpha) = \alpha_i. \end{aligned}$$

Hence $\tau \in H_i$. $H_i \supseteq \tau \sigma_i H \sigma_i^{-1}$. The other way: $\tau \in H_i$:

$$\begin{aligned} \sigma_i^{-1} \tau \sigma_i(\alpha) &= \sigma_i^{-1} \tau(\alpha_i) \\ &= \sigma_i^{-1}(\alpha_i) \\ &= \alpha. \end{aligned}$$

This implies

$$\sigma_i^{-1} \tau \sigma_i \in H,$$

which in turn implies

$$\sigma_i(\sigma_i^{-1} \tau \sigma_i) \sigma_i^{-1} = \sigma_i H \sigma_i^{-1} = \tau.$$

Simpler solution $E/F(\alpha)/F$. $F(\alpha)$ is a normal extension to F, since $G(E|F)$ is abelian. All subgroups of $G(E|F)$ are normal. $f(x)$ irreducible in $F[x] \Rightarrow$ all roots of $f(x)$ lie in $F(\alpha)$. Hence $F(\alpha) = E$.

Problem 2 Show that the diophantic equation $y^2 + 2 = z^4$ has no solutions in $\mathbb{Z}$.

[Hint: $\mathbb{Z}[\sqrt{-2}]$ is a unique factorization domain.]

Intended solution We have that

$$y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}) = z^4$$

must lead to the fact that y is odd. If y is even, then LS and HS can never be equal modulo 4. We need to show that

$$\gcd((y + \sqrt{-2})(y - \sqrt{-2})) = 1.$$

Units in $\mathbb{Z}[\sqrt{-2}]$ are ± 1. We have that $a + b\sqrt{-2} | y + \sqrt{-2}, y - \sqrt{-2}$ leads to

$$\begin{aligned} a + b\sqrt{-2} | 2y \text{ (sum)} \\ a + b\sqrt{-2} | 2\sqrt{-2} \text{ (difference).} \end{aligned}$$

Take the norm ($N(a + b\sqrt{-2}) = a^2 + 2b^2$) on both sides and get

$$\begin{aligned} a^2 + 2b^2 | 4y^2 \\ a^2 + 2b^2 | 8 \end{aligned}$$

which implies that $a^2 + 2b^2 | 4$. All possible a, b satisfying this:

$$\begin{aligned} a = \pm 1, b = 0 \\ a = 0, b = \pm 1 \\ a = \pm 2, b = 0. \end{aligned}$$

Try all those combinations, and plug them into $a + b\sqrt{-2} | y + \sqrt{-2}, y - \sqrt{-2}$, and we see that $a = \pm 1, b = 0$ is the only solution.

$$y + \sqrt{-2} = (c + d\sqrt{-2})^4 (d \neq 0).$$

We get

$$1 = 4c^3 d - 8cd^3 = 4cd(c^2 + 2d^2).$$

or real number=complex number if $d = 0$ or $c = 0$. So with $c \neq 0, d \neq 0$ we get a contradiction. Hence the equation has no solutions in $\mathbb{Z}$. It's easier to use square than power of 4.

Easier solution Let $h = z^2$ and rewrite to $y^2 + 2 = h^2$. Then

$$\begin{aligned} y < h \text{ or} \\ 1 + y \leq h. \end{aligned}$$

Square and get

$$1 + 2y + y^2 \leq h^2 \text{ or}$$
$$2y + y^2 < h^2$$

or $y^2 + 2 < h^2$ if $y \geq 1$ (since $y^2 + 2 \leq y^2 + 2y < h^2$). This is a contradiction to the assumption that there exists $h, y \in \mathbb{Z}$ such that $y^2 + 2 = h^2$.

Another easy solution $-2 = (y - h)(y + h)$, brute force on h, y and arrive at a contradiction:

One of $y - h$ and $y + h$ must be ± 1, the other must be ∓ 2 (both must have different signs). Then we get

$$y - h + y + h = 2y = \pm 1,$$

and $y = \pm\frac{1}{2}$, which is absurd, since we were seeking a solution in $\mathbb{Z}$.

Super-easy solution For any x, $x^2 \equiv 0$ or $1 \pmod 4$. For even $x = 2n$, $x^2 = 4n^2 \equiv 0 \pmod 4$. For odd $x = 2n + 1$, $x^2 = 4n^2 + 4n + 1 \equiv 1 \pmod 4$. We get

$$y^2 + 2 \equiv 2, 3 \pmod 4$$
$$h^2 \equiv 0, 1 \pmod 4,$$

so $y^2 + 2 = h^2$ can never be true.

Problem 3 Let F be a field of characteristic p, where p is a prime number. Let $f(x) \in F[x]$ be an irreducible polynomial with multiple roots. Show that there exist $s \in \{1, 2, 3, \ldots\}$ and an irreducible and *separable* polynomial such that $f(x) = g(x^{p^s})$.

Solution Use corollary 16.3.5. There exists $h_1(x) \in F[x]$ such that if $f(x) = h_1(x^p)$, $h_1(y)$ has to be irreducible. If $h_1(y)$ is not separable, use corollary 16.3.5 again. $h_1(y) = h_2(y^p)$. $h_2(z) \in F[z]$ is irreducible. $\deg(f(x)) > \deg(h_1(y)) > \deg(h_2(z))$. There must exist $h_s(x)$ which is separable.

$$f(x) = h_1(x^p) = h_2(x^{p^2}) = \cdots = h_s(x^{p^s}).$$

$g(x) = h_s(x)$ is the polyniomial we seek.

Problem 4 a) Let K be a Galois extension of F. Let $g(x) \in K[x]$ be irreducible over K, and let $\sigma \in G(K|F)$.

Show that $\sigma(g(x)) \in K[x]$ is irreducible over K.

Solution Assume that $\sigma(g(x)) = g_1(x)g_2(x)$. Then,

$$g(x) = \sigma^{-1}(g_1(x))\sigma^{-1}(g_2(x)).$$

Since $\deg(g_i(x)) = \deg(\sigma^{-1}(g_i(x)))$, then $\sigma(g(x))$ is reducible if and only if $g(x)$ is reducible. Since $g(x)$ is irreducible, it follows that $\sigma(g(x))$ is irreducible.

Problem 4 b) Let $f(x) \in F[x]$ be a (monic) irreducible polynomial over F of degree p, where p is a prime number. Show that if $f(x)$ is reducible in $K[x]$, then all the roots of $f(x)$ will lie in K. [F and K are as defined in a).]

Solution Let $f(x) = f_1(x)f_2(x)\cdots f_k(x)$ be the unique factorization of $f(x)$ into monic polynomials in $K[x]$. Let $G = G(K|F)$ and let $\sigma \in G$. Because of unique factorization, $\sigma(f_i(x))$ will be equal to some $f_j(x)$ for every $i \in \{1, 2, \cdots, k\}$. With suitable renumbering, we can assume that

$$\{\sigma(f_1(x))|\sigma \in G\} = \{f_1(x), f_2(x), \cdots, f_l(x)\}, l \leq k.$$

Let $i \in \{1, 2, \cdots, l\}$ and let $\sigma_i \in G$ such that $\sigma_i(f_1(x)) = f_i(x)$. Then,

$$\begin{aligned}\{\sigma(f_i(x))|\sigma \in G\} &= \{\sigma\sigma_i(f_1(x))|\sigma \in G\} \\ &= \{\sigma(f_i(x))|\sigma \in G\} \\ &= \{f_1(x), f_2(x), \cdots, f_l(x)\}.\end{aligned}$$

Hence G will act transitively on $\{f_1(x), f_2(x), \cdots, f_l(x)\}$, ie. permute them transitively. Also, $\sigma(g(x)) = g(x)$ for all $\sigma \in G$, where

$$g(x) = f_1(x)f_2(x)\cdots f_l(x).$$

But then $g(x) \in F[x]$, and since $f(x) \in F[x]$ is irreducible in $F[x]$, we must have that $g(x) = f(x)$, and therefore $l = k$. Hence $f_1(x), f_2(x), \cdots, f_k(x)$ must have the same degree r (since $f_i(x) = \sigma_i(f_1(x))$ for a $\sigma_i \in G$), and hence we must have that $k \cdot r = p$. But then we must have that $r = 1$ (since we know that $1 \leq r < p$, since it's assumed that $f(x)$ is reducible in $K[x]$. Hence, all $f_i(x)$ are linear and hence all the roots of $f(x)$ lie in K. $\square$

Problem 5 Let $f(x) = x^3 - 21x + 6 \in \mathbb{Q}[x]$, and let E be the splitting field of $f(x)$ over $\mathbb{Q}$. It can be shown that $E \subset \mathbb{R}$. Show that E is not a radical tower over $\mathbb{Q}$.

Solution

$$\begin{array}{ccll} E & & & \\ \vdots & & & \\ F_1(\alpha_2) & & & \\ | & & x^{n_2} - b \in F_1[x] & \alpha_2 = \sqrt[n_2]{b} \\ \mathbb{Q}(\alpha_1) = F_1 & & & \\ | & & x^{n_1} - a \in F_o[x] & \alpha_1 = \sqrt[n_1]{a} \\ \mathbb{Q} = F_0 & & & \end{array}$$

In general,

$$\begin{array}{l} E = F_k(\alpha_{k+1}) \\ \quad\quad | \quad\quad\quad \alpha_k \text{ is a root of } x^{n_k} - c \in F_k[x]. \\ F_k = F_{k-1}(\alpha_k) \end{array}$$

$x^{n_{k+1}} - c = 0$ has the roots $\alpha_{k+1}, \omega\alpha_{k+1}, \omega^2\alpha_{k+1}, \cdots, \omega^{n_{k+1}}\alpha_{k+1}$. where $\omega = e^{\frac{2\pi}{n_{k+1}}}$. Remember that E is normal over $F_k(\alpha_{k-1})$. Assume there exists such a radical tower from $\mathbb{Q}$ to E. [incomplete sentence in my notes] [If $x^{n_{k+1}} - c$ is] the minimal polynomial of α_{k+1} over F_k, then all the roots of that polynomial must lie in E, a contradiction.

In other words, we can't avoid complex values in the tower, therefore we can't have $E \subset \mathbb{R}$ when E is a radical tower over $\mathbb{Q}$.

Problem 42 State the definition of a radical tower.

9 Other problems

Midterm 2006 problem 4 Let $E/K/F$ be field extensions. Assume that K is algebraic over F, and E is algebraic over K. Show that E is algebraic over F.

Solution [Fraleigh] Let $\alpha \in K$. We must show that α is algebraic over F. Because K is algebraic over E, α is a root of some polynomial $a_0 + a_1x + \cdots + a_nx^n \in E[x]$. Because E is algebraic over F, the a_i's are algebraic over F. Hence $F(a_0, a_1, \cdots, a_n)$ is an extension of F of some finite degree m (theorem F31.11). Since α is algebraic over E of degree $r \leq n$, the multiplication rule shows that $F(a_0, a_1, \cdots, a_n, \alpha)$ is a finite extension of F of degree $\leq mr$. Theorem F31.3 says that all finite field extensions are algebraic, hence α is algebraic over F, hence E is algebraic over F.

10 Alphabetic encyclopædia of definitions

Algebraic (element), let E be an extension of F. An element $\alpha \in E$ is algebraic over F is there exists a non-constant polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.

Algebraic (extension), an extension field E over F is called algebraic if each element of E is algebraic over F. That is, for each element $\alpha \in E$ there exists a non-constant polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.

Cyclotomic polynomial, the nth *cyclotomic polynomial* is the monic polynomial $\phi_n(x) = \prod_\omega x - \omega$, the product over all primitive nth roots of unity

($\omega = e^{2\pi i/n}$. For p prime, $\phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p-1}{x-1}$. This can be intuitively explained like this: We seek a polynomial where the roots are all the primitive nth roots of unity, except 1. The equation $x^p = 1 \Rightarrow x^p - 1 = 0$ almost satisfies this, then we divide by $x - 1$ to get rid of the factor representing a root of 1. For p prime, $\phi_p(x)$ is also the minimum polynomial of $\omega = e^{2\pi i/p}$ over $\mathbb{Q}$.

Euclidean domain, a commutative integral domain E with unity is called a *Euclidean domain* if there exists a function $\phi : E \to \mathbb{Z}$ satisfying the following axioms:

1. If $a, b \in E^* = E - \{0\}$ and $b|a$, then $\phi(b) \leq \phi(a)$.
2. For each pair of elements $a, b \in E, b \neq 0$, there exist elements q and r in E such that $a = bq + r$, with $\phi(r) < \phi(b)$.

Frobenius automorphism (endomorphism), let F be a field with p^n elements. The automorphism $\phi : F \mapsto F$, given by $\phi(x) = x^p$ is called the Frobenius automorphism. Generated by ϕ, the automorphisms form a cyclic group of order n.

Galois extension, an extension E of F that is finite, normal and separable.

Galois field, $GF(p^n)$ is the finite field with p^n elements, and it's also called a *Galois field*.

Irreducible (element), a non-zero element a of an integral domain R with unity is called an *irreducible element* if it is not a unit and every divisor of a is improper, that is, if $a = bc, b, c \in R$, then either b or c is a unit.

Norm, the norm on a ring $\mathbb{Z}[\sqrt{D}]$ is defined by:

$$N(a + b\sqrt{D}) \stackrel{\text{def}}{=} \left|(a + b\sqrt{D})(a - b\sqrt{D})\right| = \left|a^2 - Db^2\right|$$

It satisfies the following:

1. $N(x) \in \mathbb{N} = \{1, 2, 3, \cdots\}$ if $x \neq 0, N(0) = 0$.
2. $N(xy) = N(x)N(y)$.
3. $N(x) = 1 \Leftrightarrow x$ is a unit in $\mathbb{Z}[\sqrt{D}]$.

Normal, normal extension, an extension E of a field F is called normal if every irreducible polynomial in $F[x]$ that has a root in E splits into linear factors in E. See theorem 16.2.1 for two more equivalent conditions. An extension E of a field F is called a normal extension if E is the splitting field of a family of polynomials (could be just one polynomial) in $F[x]$.

Perfect field is a field where all finite (or equivalently, all algebraic) extensions are separable.

Prime (element), if p is a non-zero non-unit, p is a *prime element* if, whenever p divides a product ab, then p divides a or p divides b.

Prime (field), a field is called *prime* if it has no proper subfield.

Primitive (element), let E be an extention of a field F. an element $\alpha \in E$ is a primitive element if it generates the extension, that is, $E = F(\alpha)$.

Separable (element), let E be an extension of a field F. An element $\alpha \in E$ that is algebraic over F is called separable over F if its minimal polynomial over F is separable.

Separable (extension), an algebraic extension E of a field F is called a *separable extension* if each element of E is separable over F.

Separable (polynomial), an irreducible polynomial $f(x) \in F[x]$ is called a *separable polynomial* if all its roots are simple (ie. all roots are distinct).

Simple (extension), let E be an extension of a field F. E is a simple extension if it is generated by the adjunction of a single element α, that is, $E = F(\alpha)$.

Simple (root), a root of a polynomial is simple if the multiplicity of that root is 1.

Splitting field, a splitting field of a polynomial $f(x) \in F[x]$ is a field extension E over F over which $f(x)$ factorizes into linear factors.

Example 1 The splitting field of $f(x) = x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$.

Example 2 The splitting field of $f(x) = x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega, \sqrt[3]{2})$, where $\omega = e^{\frac{2\pi i}{3}}$.

Example 3 The splitting field of $f(x) = x^2 + 1$ over $\mathbb{R}$ is $\mathbb{R}(\sqrt{-1}) = \mathbb{C}$.

Transitive action (on $\{1, 2, \cdots, n\}$), let $G = G(E|F)$ be a Galois group. Given $i, j \in \{1, 2, \cdots, n\}$, G acts transitively on $\{\alpha_1, \cdots \alpha_n\}$, if there exists σ such that $\sigma(\alpha_i) = \alpha_j$.

11 Theorems

Theorem 11.2.1 Every PID is a UFD, but a UFD is not necessarily a PID.

Theorem 11.3.2 Every Euclidean domain is a PID.

Theorem 11.3.3 Every Euclidean domain is a UFD.

Proof Follows from applying theorem 11.3.2, then 11.2.1. □

Lemma 15.1.5 (Gauss' lemma) Let $f(x) \in \mathbb{Z}[x]$ be primitive. Then $f(x)$ is reducible over $\mathbb{Q}$ is and only if $f(x)$ is reducible over $\mathbb{Z}$.

Lemma 15.1.6 If $f(x) \in \mathbb{Z}$[x] is reducible over $\mathbb{Q}$, then it is also reducible over $\mathbb{Z}$.

Theorem 15.1.7 Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ be a monic polynomial. If $f(x)$ has a root $a \in \mathbb{Q}$, then $a \in \mathbb{Z}$ and $a|a_0$.

Theorem 15.1.8 (Eistenstein's criterion) Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x], n \geq 1$. If there is a prime p such that $p^2 \not| a_0, p|a_0, p|a_1, \cdots, p|a_{n-1}, p \not| a_n$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Example 1 $f(x) = x^n - p \in \mathbb{Q}[x]$ is irredicuble using prime p.

Theorem 16.2.1 Let E be an algebraic extension of a field F contained in an algebraic closure $\bar{F}$ of F. Then the following conditions are equivalent.

(i) Every irreducible polynomial in $F[x]$ that has a root in E splits into linear factors in E.

(ii) E is the splitting field of a family of polynomials in $F[x]$.

(iii) Every embedding α of E in $\bar{F}$ that keeps each element of F fixed maps E onto E. (In other words, σ may be regarded as an automorphism of E.)

Theorem 16.3.3 Let $f(x) \in F[x]$ (F field) be a polynomial of degree ≥ 1 with α as a root. Then α is a multiple root if and only if $f'(\alpha) = 0$.

Proof By the division algorithm and by the assumption that α is a root of $f(x)$, we can write $f(x) = (x - \alpha)g(x)$. Then $f'(x) = (x - \alpha)g'(x) + g(x)$. Clearly, α is a multiple root of $f(x)$ if and only if $g(\alpha) = 0$. Because $f'(\alpha) = g(\alpha)$, the theorem follows.

Corollary 16.3.5 Any irreducible polynomial $f(x)$ over a field of characteristic 0 has simple roots. Also any irreducible polynomial $f(x)$ over a field F of characteristic $p \neq 0$ has multiple roots if and only if there exists $g(x) \in F[x]$ such that

$$f(x) = g(x^p).$$

Theorem 16.4.1 The prime field (field which has no proper subfields) of a field F is either isomorphic to $\mathbb{Q}$ or to $\mathbb{Z}_p$, p prime.

Theorem 16.4.2 Let F be a finite field. Then:

(i) The characteristic of F is a prime number p and F contains a subfield $F_p = \mathbb{Z}_p$.

(ii) The number of elements of F is p^n for some positive integer n.

Theorem 16.4.3 Any finite field F with p^n elements is the splitting field of $x^{p^n} - x \in F_p[x]$. Consequently, any two finite fields with p^n elements are isomorphic.

Theorem 16.4.6 The multiplicative group of nonzero elements of a finite group is cyclic.

Corollary 16.4.7 Let E be a finite extension of a finite field F. Then $E = F(\alpha)$ for some $\alpha \in E$.

Theorem 16.4.8 Let F be a finite field. Then there exists an irreducible polynomial of any given degree n over F.

Theorem 16.5.2 If E is a finite separable extension of a field F, then E is a simple extension of F. We recall that a E is a simple extension of F if $E = F(\alpha)$ for some $\alpha \in E$. We also recall that E is a separable extension of F if the minimal polynomial of each element of E over F has distinct roots.

Theorem (Sylow theorem 1) Let G be a finite group, and let p be a prime number. If p^m divides $|G|$, then G has a subgroup of order p^m.

Remark This theorem is included here, since it is used in one of the exam solutions (until someone finds an alternate solution).

Theorem 42 If a polynomial $f(x) \in \mathbb{R}[x]$ has odd degree, then $f(x) = 0$ has a root in $\mathbb{R}$.

Proof Let $\deg(f(x)) = n$. If $a_n > 0$, we have

$$\lim_{x \to -\infty} f(x) = -\infty$$

and

$$\lim_{x \to \infty} f(x) = \infty.$$

If $a_n < 0$, it's the other way around. $f(x) = 0$ then has a root in $\mathbb{R}$ because of the intermediate value theorem. It is left as a boring exercise to the reader to prove that $f(x)$ is continuous on the interval $(-\infty, \infty)$.