Galois theory - Problem Set 1

To be solved on Monday 23.01

Problem 1. Let R be an integral domain.

(a) Let $a, x, y \in R$, $a \neq 0$. Show that if $ax = ay$, then $x = y$.

(b) Let $a, b \in R$. Show that if $a \mid b$ and $b \mid a$, then there exists a unit $u \in R$ such that $b = ua$.

(c) Let $a, u \in R$ where u is a unit. Show that a is a unit if and only if ua is a unit.

(d) Let $a, b, u \in R$ where u is a unit. Show that $a \mid b$ if and only if $ua \mid b$.

(e) Let $p \in R$. Show that if p is prime, then p is irreducible.

(f) Let $p, u \in R$ where u is a unit. Show that p is irreducible respectively prime if and only if pu is irreducible respectively prime.

(g) Let $a, p \in R$ with a not a unit and p prime. Show that if $a \mid p$, then there exists a unit $u \in R$ such that $a = up$.

(h) Let $a, b \in R$. Show that $a \mid b$ if and only if $(b) \subseteq (a)$.

Solution.

(a) Since $ax = ay$ we have $a(x - y) = ax - ay = 0$. Since R is an integral domain, we have $a = 0$ or $x - y = 0$. Since $a \neq 0$, we conclude that $x - y = 0$ or $x = y$.

(b) If $b = 0$, then since $b \mid a$ we have that $a = 0$ and so the claim holds for $u = 1$. Assume that $b \neq 0$. Since $a \mid b$, there exists $u \in R$ such that $b = ua$. It remains to show that u is a unit. Since $b \mid a$, there exists $v \in R$ such that $a = vb$. Then $b = ua = uvb$ and so $b1 = b(uv)$. By (a) we conclude that $1 = uv$ and so u is a unit.

(c) If a is a unit, then $(ua)a^{-1}u^{-1} = 1$ and so ua is a unit too. If ua is a unit, then $a(u(ua)^{-1}) = 1$ and so a is a unit.

(d) We have that $a \mid b$ if and only if there exists $c \in R$ with $b = ca$. Equivalently, we have $b = (cu^{-1})ua$, or $ua \mid b$.

(e) Let $p = ab$ for some $a, b \in R$. It is enough to show that a or b is a unit. Since p is prime, we have that $p \mid a$ or $p \mid b$. Without loss of generality, assume that $p \mid a$. Then $a = pc$ for some $c \in R$ and so

$$p1 = p = ab = (cp)b = p(cb)$$

gives $p1 = p(cb)$. By (a) we conclude that $1 = cb$ and so b is a unit, as required.

(f) Since u is a unit, we have by (c) that p is not a unit if and only if up is not a unit. Hence we only need to show that the second condition in the definition of irreducible and prime holds for p if and only if it holds for up. Then p being prime is equivalent to up being prime by (d) and it remains to consider the irreducible case.

Assume that p is irreducible and we show that up is irreducible. Let $up = ab$ for some $a, b \in R$ and assume that b is not a unit. It is enough to show that a is a unit. Then $p = u^{-1}ab$ and since b is not a unit and p is irreducible, we conclude that $u^{-1}a$ is a unit. Hence $a = uu^{-1}a$ is a unit.

Assume that up is irreducible and we show that p is irreducible. Let $p = ab$ for some $a, b \in R$ and assume that b is not a unit. It is enough to show that a is a unit. Then $up = u(ab) = (ua)b$. Since up is irreducible, we conclude that ua is a unit. Hence $a = u^{-1}ua$ is a unit.

(g) Since $a \mid p$, there exists $u \in R$ such that $p = ua$. By (e) we have that p is irreducible. Since a is not a unit, we conclude that u is a unit.

(h) We have that $a \mid b$ if and only if $b = ca$ for some $c \in R$. Equivalently, $b \in (a)$ or $(b) \subseteq (a)$.

Problem 2. Let R be an integral domain such that for every $x, y \in R$ we have that $\gcd(x, y)$ exists. Let $a, b, c \in R$.

(a) (Exercise 11.1.1 in the book.) Show that $\gcd(ca, cb) = c\gcd(a, b)$.

(b) (Exercise 11.1.2 in the book.) Show that if $\gcd(a, b) = 1$ and if $a \mid c$ and $b \mid c$, then $ab \mid c$.

(c) (Exercise 11.1.3 in the book.) Show that if $\gcd(a, b) = 1$ and $b \mid ac$, then $b \mid c$.

Solution.

(a) We have that $\gcd(a, b) = 0$ if and only if $a = b = 0$ since 0 divides only 0. Hence the claim is trivially true if $c = 0$ or $a = b = 0$ and so we may assume that $c \neq 0$ and $\gcd(a, b) \neq 0$.

Let $d = \gcd(a, b)$ and $e = \gcd(ca, cb)$. Since $d \mid a$ and $d \mid b$, there exist $r_1, r_2 \in R$ such that $a = r_1 d$ and $b = r_2 d$. Then $ca = r_1 cd$ and $cb = r_2 cd$ and so $cd \mid ca$ and $cd \mid cb$. Hence $cd \mid \gcd(ca, cb) = e$ and so there exists $s \in R$ such that $e = s(cd)$. Recall that the greatest common divisor is defined only up to a unit by Remark 1.10(1). Hence it is enough to show that s is a unit. Since $e \mid ca$ and $e \mid cb$, there exist $t_1, t_2 \in R$ such that $ca = t_1 e$ and $cb = t_2 e$. Using all this we have

$$(cd)r_1 = c(r_1 d) = ca = t_1 e = t_1(scd) = (cd)(t_1 s)$$

and so by Problem 1(a) we have that $r_1 = t_1 s$. Hence $a = t_1(sd)$. Similarly we have that $b = t_2(sd)$. Hence $sd \mid a$ and $sd \mid b$, which imply that $sd \mid \gcd(a, b) = d$. Then there exists $u \in R$ with $d = u(sd) = (us)d$. By Problem 1(a) we conclude that $us = 1$ and so s is a unit as required.

(b) Since $a \mid c$ and $b \mid c$, there exist $r_1, r_2 \in R$ such that $c = r_1 a$ and $c = r_2 b$. Then by (a) we have

$$c = c1 = c\gcd(a, b) = \gcd(ca, cb) = \gcd(r_2 ba, r_1 ab) = ab\gcd(r_2, r_1),$$

and so $ab \mid c$.

(c) Since $b \mid ac$, there exists $r \in R$ such that $ac = rb$. Then by (a) we have

$$c = c1 = c\gcd(a, b) = \gcd(ca, cb) = \gcd(rb, cb) = b\gcd(r, c),$$

and so $b \mid c$.

Problem 3. (Exercise 11.1.8 in the book.) Show that in the ring $\mathbb{Z}[\sqrt{-3}]$ the gcd of 4 and $2 + 2\sqrt{-3}$ does not exist.

Solution. Let us first compute the common divisors of 4 and $2+2\sqrt{-3}$. That is assume that $(a+b\sqrt{-3}) \mid 4$ and $(a + b\sqrt{-3}) \mid (2 + 2\sqrt{-3})$ for some $a, b \in \mathbb{Z}$. In particular, $(a, b) \neq (0, 0)$. Then there exist $x, y, z, w \in \mathbb{Z}$ such that

$$(a + b\sqrt{-3})(x + y\sqrt{-3}) = 4,$$
$$(a + b\sqrt{-3})(z + w\sqrt{-3}) = 2 + 2\sqrt{-3}.$$

We want to solve for x, y, z, w. Hence we divide both sides by $a + b\sqrt{-3}$ to obtain

$$x + y\sqrt{-3} = \frac{4}{a + b\sqrt{-3}},$$
$$z + w\sqrt{-3} = \frac{2 + 2\sqrt{-3}}{a + b\sqrt{-3}}.$$

We now multiply the numerator and denominator of the right hand side by $a - b\sqrt{-3}$ to obtain

$$x + y\sqrt{-3} = \frac{4}{a^2 + 3b^2}(a - b\sqrt{-3}),$$
$$z + w\sqrt{-3} = \frac{2 + 2\sqrt{-3}}{a^2 + 3b^2}(a - b\sqrt{-3}).$$

Rearranging, we obtain

$$x + y\sqrt{-3} = \frac{4a}{a^2 + 3b^2} - \frac{4b}{a^2 + 3b^2}\sqrt{-3},$$
$$z + w\sqrt{-3} = \frac{2a + 6b}{a^2 + 3b^2} + \frac{2a - 2b}{a^2 + 3b^2}\sqrt{-3}.$$

It follows that

$$x = \frac{4a}{a^2 + 3b^2},$$
$$y = \frac{-4b}{a^2 + 3b^2},$$
$$z = \frac{2a + 6b}{a^2 + 3b^2},$$
$$w = \frac{2a - 2b}{a^2 + 3b^2}.$$

We investigate the cases for a and b so that all of x, y, z, w are integers:

- If $|a| > 4$, then x is not an integer.
- If $|b| > 2$, then y is not an integer.
- If $|a| = 4$ and $|b| = 1$, then x is not an integer.
- If $|a| = 4$ and $b = 0$, then z is not an integer.
- If $|a| = 3$ and $|b| = 1$, then y is not an integer.
- If $|a| = 3$ and $|b| = 0$, then x is not an integer.
- If $|a| = 2$ and $|b| = 1$, then x is not an integer.
- If $a = 0$ and $b = 0$, then this contradicts $(a, b) \neq (0, 0)$.
- If $a = 0$ and $|b| = 1$, then y is not an integer.

It follows then that

$$(a, b) \in \{(2, 0), (-2, 0), (1, 1), (1, 0), (1, -1), (-1, 1), (-1, 0), (-1, -1)\},$$

or that the common divisors of 4 and $2 + 2\sqrt{-3}$ are given by the set

$$C = \{2, -2, 1 + \sqrt{-3}, 1, 1 - \sqrt{-3}, -1 + \sqrt{-3}, -1, -1 - \sqrt{-3}\}.$$

Hence if $d := \gcd(4, 2+2\sqrt{-3})$ exists, then $d \in C$. Notice that $2 \nmid 1$ hence $d \neq 1$. Also 2 does not divide any of $1+\sqrt{-3}, 1-\sqrt{-3}, -1+\sqrt{-3}, -1-\sqrt{-3}$. Indeed, say that $2 \mid (1+\sqrt{-3})$. Then there exist $u, v \in \mathbb{Z}[\sqrt{-3}]$ such that

$$2(u+v\sqrt{-3}) = 1+\sqrt{-3}$$

or $2u = 1$ which is a contradiction, and similarly for the rest. Hence we are left with the only possibility that $d = 2$ (the case $d = -2$ is the same since gcd is defined only up to a unit). But we claim that $(1+\sqrt{-3}) \nmid 2$. Indeed, assuming otherwise there exist $k, l \in \mathbb{Z}[\sqrt{-3}]$ such that

$$(1+\sqrt{-3})(k+l\sqrt{-3}) = 2. \tag{1}$$

Taking complex norms gives

$$(1+3)(k^2+3l^2) = 4$$

or $k^2+3l^2 = 1$. Then only solutions are then $k = \pm 1, l = 0$. But these are not solutions of (1). Hence $d \neq 2$ and so $\gcd(4, 2+2\sqrt{-3})$ does not exist.

Problem 4. Let $k \in \mathbb{Z}$ and consider the map $\phi : \mathbb{Z}[\sqrt{k}] \to \mathbb{Z}$ defined by $\phi(a+b\sqrt{k}) = |a^2-kb^2|$.

(a) Show that ϕ is multiplicative, that is for all $a, b, c, d \in \mathbb{Z}$ we have $\phi((a+b\sqrt{k})(c+d\sqrt{k})) = \phi(a+b\sqrt{k})\phi(c+d\sqrt{k})$.

(b) Show that for all $a, b, c, d \in \mathbb{Z}$ we have that if $(a+b\sqrt{k}) \mid (c+d\sqrt{k})$, then $\phi(a+b\sqrt{k}) \mid \phi(c+d\sqrt{k})$.

(c) Show that $a+b\sqrt{k} \in \mathbb{Z}[\sqrt{k}]$ is a unit if and only if $\phi(a+b\sqrt{k}) = 1$.

Solution.

(a) We compute

$$\begin{aligned}
\phi((a+b\sqrt{k})(c+d\sqrt{k})) &= \phi((ac+kbd)+(ad+bc)\sqrt{k}) \\
&= |(ac+kbd)^2 - k(ad+bc)^2| \\
&= |a^2c^2 + 2kabcd + k^2b^2d^2 - ka^2d^2 - 2kabcd - kb^2c^2| \\
&= |a^2c^2 - kb^2c^2 + k^2b^2d^2 - ka^2d^2| \\
&= |c^2(a^2-kb^2) - kd^2(a^2-kb^2)| \\
&= |(a^2-kb^2)(c^2-kd^2)| \\
&= |a^2-kb^2||c^2-kd^2| \\
&= \phi(a+b\sqrt{k})\phi(c+d\sqrt{k}).
\end{aligned}$$

(b) By assumption there exist $x, y \in \mathbb{Z}$ such that

$$(c+d\sqrt{k}) = (x+y\sqrt{k})(a+b\sqrt{k}).$$

By (a) we obtain

$$\phi(c+d\sqrt{k}) = \phi(x+y\sqrt{k})\phi(a+b\sqrt{k})$$

and so $\phi(a+b\sqrt{k}) \mid \phi(c+d\sqrt{k})$.

(c) Assume that $a+b\sqrt{k} \in \mathbb{Z}[\sqrt{k}]$ is a unit. Then $(a+b\sqrt{k}) \mid 1$ and so by (b) we obtain that $\phi(a+b\sqrt{k}) \mid \phi(1) = 1$. Hence $\phi(a+b\sqrt{k}) \in \{-1, 1\}$. But since $\phi(a+b\sqrt{k}) = |a^2-kb^2| \geq 0$, we conclude that $\phi(a+b\sqrt{k}) = 1$.

Assume now that $\phi(a+b\sqrt{k}) = 1$. Then $|a^2-kb^2| = 1$. We then have

$$(a+b\sqrt{k})(a-b\sqrt{k}) = a^2-kb^2 = \pm 1$$

and hence either $a-b\sqrt{k}$ or $-a+b\sqrt{k}$ is an inverse of $a+b\sqrt{k}$.

Problem 5. (Exercise 11.3.4 in the book.) Let $a = 3+2i$ and $b = 2-3i$ be two elements in $\mathbb{Z}[i]$. Find q and r in $\mathbb{Z}[i]$ such that $a = bq + r$ and $\phi(r) < \phi(b)$, where $\phi(x+yi) = x^2+y^2$.

Solution. We compute

$$\frac{a}{b} = \frac{3+2i}{2-3i} = \frac{(3+2i)(2+3i)}{(2-3i)(2+3i)} = \frac{13i}{4+9} = i.$$

Hence $a = bi + 0$ and $\phi(0) < \phi(b)$.

Problem 6. (Exercise 11.3.2 in the book) Show that the ring $\mathbb{Z}[\sqrt{2}]$ is a euclidean domain and a UFD. Explain why in the UFD $\mathbb{Z}[\sqrt{2}]$ we have

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

even though each of the factors is irreducible.

Solution. We define the function $\phi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ given by $\phi(a+b\sqrt{2}) = |a^2 - 2b^2|$ and we show that this gives $\mathbb{Z}[\sqrt{2}]$ the structure of a euclidean domain. By Problem 4(a) we have that ϕ is multiplicative and so condition (i) of Definition 2.1 follows. For condition (ii), let $\alpha = a_1 + a_2\sqrt{2}, \beta = b_1 + b_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ with $\beta \neq 0$. Then there exist $x, y \in \mathbb{Q}$ such that

$$\frac{\alpha}{\beta} = x + y\sqrt{2}.$$

Let $c_1 \in \mathbb{Z}$ be the closest integer to x so that $|x - c_1| \leq \frac{1}{2}$. Similarly let $c_2 \in \mathbb{Z}$ be such that $|y - c_2| \leq \frac{1}{2}$. Set $q := c_1 + c_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Then

$$\begin{aligned}
\alpha &= \beta(x + y\sqrt{2}) \\
&= \beta((x-c_1) + (y-c_2)\sqrt{2} + (c_1 + c_2\sqrt{2})) \\
&= q\beta + \beta((x-c_1) + (y-c_2)\sqrt{2}).
\end{aligned}$$

Set $r := \beta((x-c_1) + (y-c_2)\sqrt{2}) = \alpha - q\beta \in \mathbb{Z}[\sqrt{2}]$. It remains to show that $\phi(r) < \phi(\beta)$. Clearly we may extend ϕ to a function $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Z}$, so that again we have

$$\phi((a+b\sqrt{2})(c+d\sqrt{2})) = \phi(a+b\sqrt{2})\phi(c+d\sqrt{2})$$

for all $a, b, c, d \in \mathbb{Q}$. Then we have

$$\begin{aligned}
\phi(r) &= \phi(\beta)\phi((x-c_1) + (y-c_2)\sqrt{2}) \\
&= \phi(\beta)|(x-c_1)^2 - 2(y-c_2)^2| \\
&\leq \phi(\beta)((x-c_1)^2 + 2(y-c_2)^2) \\
&\leq \phi(\beta)(\frac{1}{4} + 2\frac{1}{4}) \\
&= \frac{3}{4}\phi(\beta) < \phi(\beta),
\end{aligned}$$

as required. Hence $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain and so it is a UFD. Now consider the factorizations

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

in $\mathbb{Z}[\sqrt{2}]$. Since $\mathbb{Z}[\sqrt{2}]$ is a UFD and these elements are irreducible, it follows that by factoring out some units we obtain the same factorization. By Problem 4(c) we have that $u \in \mathbb{Z}[\sqrt{2}]$ is a unit if and only if $\phi(u) = 1$. Notice that

$$\phi(2-\sqrt{2}) = |2^2 - 2\cdot 1^2| = 2 = \phi(2+\sqrt{2})$$

And hence we suspect that $2-\sqrt{2}$ and $2+\sqrt{2}$ differ by a unit. Indeed, we have

$$\frac{2-\sqrt{2}}{2+\sqrt{2}} = \frac{(2-\sqrt{2})^2}{2} = \frac{4-4\sqrt{2}+2}{2} = 3-2\sqrt{2}$$

and so $2-\sqrt{2} = (2+\sqrt{2})(3-2\sqrt{2})$. Since $\phi(3-2\sqrt{2}) = 9-8 = 1$, we have that $3-2\sqrt{2}$ is indeed a unit. Then, we have

$$(5+\sqrt{2})(2-\sqrt{2}) = (5+\sqrt{2})(2+\sqrt{2})(3-2\sqrt{2}) = (5+\sqrt{2})(3-2\sqrt{2})(2+\sqrt{2}) = (11-7\sqrt{2})(2+\sqrt{2}),$$

and hence no contradiction.

Problem 7. (Exercise 11.3.8 in the book.) Show that $\mathbb{Z}[\sqrt{-6}]$ is not a euclidean domain.

Solution. It is enough to show that $\mathbb{Z}[\sqrt{-6}]$ is not a PID. Notice that $2 \mid -6$ but $-6 = \sqrt{-6}\sqrt{-6}$ in $\mathbb{Z}[\sqrt{-6}]$ and $2 \nmid \sqrt{-6}$. Hence 2 is not prime. We claim that 2 is irreducible. Since $\phi(2) = 4 \neq 1$, we have that 2 is not a unit by Problem 4(c). Next assume that

$$2 = (a+b\sqrt{-6})(c+d\sqrt{-6})$$

for some $a,b,c,d \in \mathbb{Z}$ and that $c+d\sqrt{-6}$ is not a unit, and we show that $a+b\sqrt{-6}$ is a unit. By Problem 4(b) we have that $\phi(c+d\sqrt{-6}) \mid \phi(2) = 4$. Since $\phi(c+d\sqrt{-6}) \geq 0$, we have that $\phi(c+d\sqrt{-6}) \in \{1,2,4\}$. Since $c+d\sqrt{-6}$ is not a unit, we have that $\phi(c+d\sqrt{-6}) \in \{2,4\}$ by Problem 4(c). Assume to a contradiction that $\phi(c+d\sqrt{-6}) = 2$. Then

$$2 = \phi(c+d\sqrt{-6}) = |c^2+6d^2| = c^2+6d^2,$$

and $c^2+6d^2 = 2$ clearly has no solutions $c,d \in \mathbb{Z}$. Hence $\phi(c+d\sqrt{-6}) = 4$. But then by Problem 4(a) we have $\phi(a+b\sqrt{-6}) = 1$ and so $a+b\sqrt{-6}$ is a unit by Problem 4(c). Since every irreducible element in a PID is prime, and since 2 is irreducible but not prime, we conclude that $\mathbb{Z}[\sqrt{-6}]$ is not a PID and hence not a Euclidean domain.

Problem 8. (Exercise 15.1.1 in the book.) Show that $f(x) = x^3+3x+2 \in \mathbb{Z}_7[x]$ is irreducible over the field $\mathbb{Z}_7$.

Solution. We compute $f(0) = 2$, $f(1) = 6$, $f(2) = 2$, $f(3) = 3$, $f(4) = 1$, $f(5) = 2$, $f(6) = 5$ and so f has no root in $\mathbb{Z}_7$. It follows by Lemma 3.4(3) that f is irreducible in $\mathbb{Z}_7[x]$.

Problem 9. (Exercise 15.1.4 in the book.) 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. By Lemma 3.6(3) f is reducible over $\mathbb{Z}$ if and only if f has a root in $\mathbb{Z}$. Equivalently, there exists $r \in \mathbb{Z}$ such that

$$r^3+ar^2+br+1 = 0.$$

We may rewrite this as

$$r(r^2+ar+b) = -1$$

to obtain that either $r = 1$ or $r = -1$. If $r = 1$, then we have $1+a+b = -1$ and so $a+b = -2$. If $r = -1$, then we have $-(1-a+b) = -1$ and so $a = b$.

Problem 10. (Exercise 15.1.2 in the book.) Show that $f(x) = x^4+8 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$.

Solution. By Lemma 3.6 it is enough to show that f is irreducible over $\mathbb{Z}$. If $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Z}[x]$, then g and h are monic polynomials since f is monic and $\deg(g), \deg(h) \in \{1,2,4\}$ since $\deg(g)\deg(h) = \deg(f) = 4$. Assume to a contradiction that $\deg(g) = 1$. Then $g(x) = x+a \in \mathbb{Z}[x]$ has a root in $\mathbb{Z}$, but f has no root in $\mathbb{Z}$. Hence $\deg(g) > 1$. If $\deg(g) = 4$, then $\deg(h) = 1$ and again we reach a contradiction. Hence $\deg(g) = \deg(h) = 2$. Then

$$\begin{aligned} g(x) &= x^2 + ax + b \\ h(x) &= x^2 + cx + d \end{aligned}$$

for some $a, b, c, d \in \mathbb{Z}$. Then

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

implies

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

From $a = -c$, we obtain

$$\begin{aligned} d + b - c^2 &= 0 \\ -c(d - b) &= 0 \\ bd &= 8 \end{aligned}$$

and so either $d - b = 0$ or $c = 0$ and so $d + b = 0$. In any case, $d = \pm b$. But then $bd = 8$ gives $\pm b^2 = 8$, which is impossible. Hence such a decomposition does not exist and f is irreducible.

Problem 11. Prove or disprove that $\sqrt[19]{17000}$ is a rational number.

Solution. Let $r = \sqrt[19]{17000}$. Then $r^{19} - 17000 = 0$ and so r is a root of the polynomial $f(x) = x^{19} - 17000 \in \mathbb{Z}[x]$. We have $17000 = 2^3 \cdot 5^3 \cdot 17$ and so by applying Eisenstein Criterion on $f(x)$ with $p = 17$ we have that $f(x)$ is irreducible over $\mathbb{Q}$. By Lemma 3.4(2) we conclude that f has no root in $\mathbb{Q}$. Since r is a root of f, it follows that $r \notin \mathbb{Q}$.

Problem 12. Find the unique factorization of $f(x) = x^4 + x^3 - 3x^2 + 3x + 3 \in \mathbb{Z}_5[x]$

Solution. We first find a root of $f(x)$. We have

$$f(x) = x^4 + x^3 - 3x^2 + 3x + 3 = x^4 + x^3 + 2x^2 + 3x + 3$$

and

$$f(0) = 3, \quad f(1) = 0.$$

and so 1 is a root of f. Dividing $f(x)$ by $x - 1$ we obtain

$$f(x) = (x - 1)(x^3 + 2x^2 + 4x + 2) = (x + 4)g(x),$$

where $g(x) = x^3 + 2x^2 + 4x + 2$ and $x + 4$ is irreducible by Lemma 3.4(1). Next we do the same process with $g(x)$. We know that 0 is not a root of g (since it is not a root of f) and so we start checking from 1.

$$g(1) = 4, \quad g(2) = 1, \quad g(3) = 4, g(4) = 4.$$

Hence g has no root in $\mathbb{Z}_5$. Since $\deg(g) = 3$, we have by Lemma 3.4(3) that g is irreducible. Hence

$$f(X) = (x + 4)(x^3 + 2x^2 + 4x + 2),$$

is the unique factorization of f in $\mathbb{Z}_5[x]$.

Problem 13. (Exercise 15.2.4 in the book.) Find the smallest extension of $\mathbb{Q}$ having a root of $f(x) = x^2 + 4 \in \mathbb{Q}[x]$.

Solution. The roots of f in $\mathbb{C}$ are $2i$ and $-2i$. Hence f has a root in $\mathbb{Q}(i)$. Since $x^2 + 1$ is irreducible, we have

$$[\mathbb{Q}(i) : \mathbb{Q}] = \deg(x^2 + 1) = 2.$$

Since this is the smallest possible degree of a non-trivial field extension, we conclude that $\mathbb{Q} \subseteq \mathbb{Q}(i)$ is the smallest extension of $\mathbb{Q}$ having a root of f.

Problem 14. (Exercise 15.2.1 in the book.) Show that $p(x) = x^2 - x - 1 \in \mathbb{Z}_3[x]$ is irreducible over $\mathbb{Z}_3$. Show that there exists an extension K of $\mathbb{Z}_3$ with nine elements having all roots of $p(x)$.

Solution. Since $p(0) = 2$, $p(1) = 2$, $p(2) = 1$, we conclude that p is irreducible over $\mathbb{Z}_3[x]$ by Lemma 3.4(3). Let $K = \mathbb{Z}_3[x]/(p(x))$ and $\alpha = \overline{x} = x + (p(x)) \in K$. Then in K we have

$$p(\alpha) = \overline{x}^2 - \overline{x} - 1 = \overline{x^2} - \overline{x} - \overline{1} = \overline{x^2 - x - 1} = \overline{p(x)} = 0$$

and so α is a root of p. Since p is irreducible, we have that $K = \mathbb{Z}_3(\alpha)$ and

$$[\mathbb{Z}_3(\alpha) : \mathbb{Z}_3] = \deg(p) = 2$$

and $1, \alpha$ is a $\mathbb{Z}_3$-basis of $\mathbb{Z}_3(\alpha)$. In other words,

$$\mathbb{Z}_3(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Z}_3\} = \{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\}$$

and $\mathbb{Z}_3(\alpha)$ has 9 elements. Multiplication in $\mathbb{Z}_3(\alpha)$ is done via $\alpha^2 - \alpha - 1 = 0$. To find the other root of p we have

$$x^2 - x - 1 = p(x) = (x - \alpha)(x - \beta) = x^2 + (\beta - \alpha)x + \alpha\beta$$

for some $\beta \in \mathbb{Z}_3(\alpha)$. We obtain that $\alpha\beta = -1$ and so $\beta = -\alpha^{-1}$. From $\alpha^2 - \alpha - 1 = 0$ we have $\alpha(\alpha - 1) = 1$ and so $\beta = -\alpha^{-1} = -(\alpha - 1) = 1 + 2\alpha$ is the other root of p.

Problem 15. (Exercise 15.2.2 in the book.) Show that $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ 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. The polynomial f is irreducible over $\mathbb{Q}$ by Eisenstein criterion for $p = 2$. The roots of f in $\mathbb{C}$ are

$$r_1 = 2^{1/3}e^{2\pi i/3}, \quad r_2 = 2^{1/3}e^{4\pi i/3}, \quad r_3 = 2^{1/3}e^{6\pi i/3} = 2^{1/3}.$$

Let $\omega_k = e^{2\pi ik/3}$ for $k = 1, 2, 3$. Then $r_k = 2^{1/3}\omega_k$. Then f has all its roots in $K = \mathbb{Q}(2^{1/3}, \omega_1)$. It remains to show that $[\mathbb{Q}(2^{1/3}, \omega_1) : \mathbb{Q}] = 6$. Since $2^{1/3}$ is a root of f, and since f is irreducible, we have that

$$[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = \deg(f) = 3.$$

On the other hand, we have that $\omega_1 \notin \mathbb{Q}(2^{1/3})$ since $\omega_1 \notin \mathbb{R}$. Notice that ω_1 is a root of $x^3 - 1$ and

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

Since ω_1 is not a root of $x - 1$, we have that ω_1 is a root of $x^2 + x + 1$. Moreover, since ω_1 is not real, the other root of $x^2 + x + 1$ is also not real and so $x^2 + x + 1$ is irreducible over $\mathbb{Q}(2^{1/3})$. Therefore

$$[\mathbb{Q}(2^{1/3}, \omega_1) : \mathbb{Q}(2^{1/3})] = \deg(x^2 + x + 1) = 2.$$

Since $\mathbb{Q} \subseteq \mathbb{Q}(2^{1/3}) \subseteq \mathbb{Q}(2^{1/3}, \omega_1) = K$, we conclude that

$$[K : \mathbb{Q}] = [\mathbb{Q}(2^{1/3}, \omega_1) : \mathbb{Q}] = [\mathbb{Q}(2^{1/3}, \omega_1) : \mathbb{Q}(2^{1/3})] \cdot [\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 2 \cdot 3 = 6,$$

as required.