Selected Solutions to Problems in Abstract Algebra

Edward Chernysh

This document is a compilation of curious/instructive problems relating to rings, modules, fields and Galois theory. Almost all problems come from the assignments of Math 456, a course given at McGill University in Winter 2018. A strong background in linear algebra and group theory is all that is required for these problems. The selected exercises are those I suspect will best prepare one for an examination relating to the aforementioned topics. For the most part, these solutions focus on ideas rather than blind computations.

1 Rings and Domains

Problem 1.1. *Let R be a commutative ring and let $\mathsf{P}(R)$ denote the ring of formal power series with coefficients in R. Prove that*

$$\mathsf{P}(R)^\times = \left\{ \sum_{n=0}^{\infty} a_n x^n : a_0 \in R^\times \right\}.$$

Deduce from this that all ideals in $\mathsf{P}(\mathbb{C})$ are principal.

Proof. First, suppose that $f(x) = \sum_0^\infty a_n x^n$ is a unit in $\mathsf{P}(R)$ with multiplicative inverse $g(x) = \sum_0^\infty b_n x^n$. Then, we have

$$1 = f(x)g(x) = \sum_{n=0}^{\infty} \sum_{k=0}^{n} a_k b_{n-k} x^n$$

whence $1 = a_0 b_0$ so that $a_0 \in R^\times$ by definition. Conversely, suppose that $f(x) = \sum_0^\infty a_n x^n$ with a_0 a unit. Let $b_0 := a_0^{-1}$ and define for $n > 1$:

$$b_n := -\frac{1}{a_0} \sum_{k=1}^{n} a_k b_{n-k}.$$

We claim that the formal power series $g(x) := \sum_0^\infty b_n x^n$ is the multiplicative inverse of $f(x)$. We will only prove that $f(x)g(x) = 1$ as a symmetric argument establishes $g(x)f(x) = 1$. First, notice that

$$\begin{aligned} f(x)g(x) = \sum_{n=0}^{\infty}\sum_{k=0}^{n} a_k b_{n-k} x^n &= a_0 b_0 + \sum_{n=1}^{\infty}\sum_{k=0}^{n} a_k b_{n-k} x^n \\ &= 1 + \sum_{n=1}^{\infty}\sum_{k=0}^{n} a_k b_{n-k} x^n. \end{aligned}$$

It therefore suffices to check that $\sum_{k=0}^{n} a_k b_{n-k} = 0$ for all $n > 1$. This is indeed the case since if $n > 1$ there holds

$$\sum_{k=0}^{n} a_k b_{n-k} = a_0 b_n + \sum_{k=1}^{n} a_k b_{n-k} = -\sum_{k=1}^{n} a_k b_{n-k} + \sum_{k=1}^{n} a_k b_{n-k} = 0.$$

This proves the first part. Now, we argue that $\mathsf{P}(\mathbb{C})$ has only principal ideals. Let $I \neq \{0\}$ be a two-sided ideal of $\mathsf{P}(\mathbb{C})$. Every element of $f \in I$ may be formally written as

$$f(x) = \sum_{n=0}^{\infty} a_n x^n$$

and since $I \neq \{0\}$ there exists at least one $f(x) \in I$ with some $a_n \neq 0$. Let now $N \in \mathbb{N}_0$ be the minimal N for which there exists $f(x) \in I$ with $a_N \neq 0$ and fix such a formal power series f. Now, we may factor this $f(x)$ as follows:

$$f(x) = x^N \tilde{f}(x),$$

where $\tilde{f}(x) \in \mathsf{P}(\mathbb{C})$ is a polynomial whose tail coefficient is non-zero. Since $\mathbb{C}$ is a field, we see from the first part that $\tilde{f}(x)$ will be a unit in $\mathsf{P}(\mathbb{C})$ and hence

$$f(x)\left[\tilde{f}(x)^{-1}\right] = x^N$$

will also live in I. Hence, $\left(x^N\right) \subseteq I$. Conversely, let $g(x) \in I$ be given and suppose without loss of generality that $g(x) \neq 0$. By the minimality of N, we see that

$$g(x) = \sum_{n \geq N} b_n x^n, \quad b_n \in \mathbb{C}$$

and hence $g(x)$ is a x^N-multiple of another power series in $\mathsf{P}(\mathbb{C})$. In any case, this means that $g(x) \in \left(x^N\right)$ which gives $I = \left(x^N\right)$, as was required. □

Problem 1.2. *Let R and S be two rings and denote by $R \oplus S$ the ring obtained via assigning coordinate-wise operations to the product $R \times S$. Prove that every left ideal in $R \oplus S$ is of the form $I \times J$ where $I \lhd R$ and $J \lhd S$. Describe a subring of $\mathbb{Z} \oplus \mathbb{Z}$ which is not of this form.*

Proof. Let $T \lhd R \oplus S$ be a left ideal and without loss of generality assume that $T \neq \{0\}$. We define two sets:

$$I := \{r \in R : \exists s \in S \text{ s.t. } (r, s) \in T\},$$
$$J := \{s \in S : \exists r \in R \text{ s.t. } (r, s) \in T\}.$$

First, it is easy to see that $0 \in I$. Similarly, if $r, r' \in I$ then one can find $s, s' \in S$ such that (r, s) and (r', s') belong to T. Then $r + r' \in I$ since

$$(r + r', s + s') = (r, s) + (r', s') \in T.$$

Also, if $a \in R$ then

$$(ar, 0) = (a, 0) \cdot (r, s) \in T$$

whence $ar \in I$. This implies that I is a (left) ideal of R. Likewise, one can easily show that J is a (left) ideal of the ring S. Clearly, $T \subseteq I \times J$. Conversely, suppose that $(r, s) \in I \times J$. There exists $s_1 \in S$ and $r_1 \in R$ such that

$$(r, s_1) \in T \quad \text{and} \quad (r_1, s) \in T.$$

This implies that

$$(r, s) = (1, 0) \cdot (r, s_1) + (0, 1) \cdot (r_1, s) \in T$$

which gives $T = I \times J$. For the last part of the problem, consider the subring of $\mathbb{Z} \oplus \mathbb{Z}$ given by the set

$$\{(x, x) : x \in \mathbb{Z}\}.$$

This set is not an ideal and hence is not of this form. □

Problem 1.3. *Let R be a commutative ring and let $a, b \in R \setminus \{0\}$ be co-prime[1]. Prove that if $a \mid bc$, then $a \mid c$.*

Proof. Assume $a \mid bc$. Let $x, y \in R$ be such that

$$1 = ax = by.$$

This gives $c = cax + bcy$ whence $a \mid c$. □

[1]If R is a commutative ring and $a, b \neq 0$, we say that a and b are *co-prime* provided $(a) + (b) = R$.

Problem 1.4. *Recall that $\mathbb{Z}[i]$ is a Euclidean domain when equipped with the norm-function $N(\cdot) = |\cdot|^2$, where $|\cdot|$ is the usual norm on $\mathbb{C}$. Suppose $\omega \in \mathbb{Z}[i]$ is irreducible. Prove that $\mathbb{Z}[i]/(\omega)$ is a finite field.*

Proof. Since ω is irreducible and $\mathbb{Z}[i]$ is also a PID, the ideal (ω) is maximal and hence $\mathbb{Z}[i]/(\omega)$ is a field.

We now prove that this field is also finite. For this, we need only show that every class in $\mathbb{Z}[i]/(2+3i)$ has a representative whose norm is no larger than $N(\omega)$. Fix an element of $\mathbb{Z}[i]/(\omega)$ and write it as

$$\alpha + (\omega).$$

We may as well assume that $\alpha \notin (\omega)$. Performing Euclidean division, we get

$$\alpha = \beta\omega + \gamma$$

where $\gamma = 0$ or $N(\gamma) < N(\omega)$. Now, $\alpha \equiv \gamma$ modulo (ω), and therefore we have found a desirable representative. This completes the proof. □

Problem 1.5. *Prove that $\mathbb{Z}[i]/(2+3i)$ is a field and show that $\mathbb{Z}[i]/(5)$ is not a field.*

Proof. The quotient ring $\mathbb{Z}[i]/(2+3i)$ is a field if and only if $(2+3i)$ is a maximal ideal in $\mathbb{Z}[i]$. As this is also a principal ideal domain, this is equivalent to $(2+3i)$ being a prime ideal. In turn, this is equivalent to $2+3i$ being a prime element. Hence, the claim is actually that $2+3i$ is irreducible in $\mathbb{Z}[i]$. Clearly, $2+3i$ is not a unit as $|2+3i|^2 \neq 1$. Suppose now that $2+3i = \alpha \cdot \beta$ for some $\alpha, \beta \in \mathbb{Z}[i] \setminus \{0\}$. From the norm, we see that

$$13 = |2+3i|^2 = |\alpha|^2 \cdot |\beta|^2.$$

But, 13 is prime whence either $|\alpha|^2 = 1$ or $|\beta|^2 = 1$. That is, one of α or β is a unit. This implies that $2+3i$ is irreducible, as was required.

Now, to prove that $\mathbb{Z}[i]/(5)$ is not a field it suffices to check that $\mathbb{Z}[i]/(5)$ is not an integral domain. To achieve this, consider the two elements

$$\zeta_1 := 1 + 2i + (5) \quad \text{and} \quad \zeta_2 := 1 - 2i + (5)$$

in $\mathbb{Z}[i]/(5)$. Since $|1 \pm 2i|^2 = 5$ and $|5|^2 = 25$, it is clear that $\zeta_{1,2} \not\equiv 0$. However,

$$\zeta_1\zeta_2 = 5 + (5) \equiv 0$$

which yields the desired result. □

Problem 1.6. *Let $\mathbb{F}$ be any one of the fields $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. Prove that the ideal (x, y) is not principal in $\mathbb{F}[x, y]$.*

Proof. First, notice that $(x, y) \lhd \mathbb{F}[x, y]$ is given by the family

$$\{a(x, y)x + b(x, y)x : a(x, y), b(x, y) \in \mathbb{F}[x, y]\}.$$

Suppose now that one can find $f = f(x, y) \in \mathbb{F}[x, y]$ such that $(f) = (x, y)$. Then, $x \in (f)$ implies that

$$x = f(x)\alpha(x, y), \quad \alpha(x, y) \in \mathbb{F}[x, y].$$

In any case, $0 = \deg_y(x) = \deg_y(f) + \deg_y(\alpha)$ whence $\deg_y(f) = 0$. Similarly, since $y \in (f)$, one can show that $\deg_x(f) = 0$ as well. Thus, we see that $f \in \mathbb{F}$. Since $(x, y) = (f)$ is non-zero, we cannot have $f = 0$ which implies that $f \in \mathbb{F} \setminus \{0\}$. But, $f \in (x, y)$ means that for some $a, b \in \mathbb{F}[x, y]$ we may write

$$f = a(x, y)x + b(x, y)y;$$

taking $x = y = 0$ implies that $f = 0$, which is a contradiction. □

Problem 1.7. *Using the Euclidean algorithm, find a generator for the ideal* $(1 + 3i, 2)$ *in* $\mathbb{Z}[i]$. *Show that* $\mathbb{Z}[i]/(1 + 2i)$ *is a field and determine the inverse of* $[2 + 3i]$ *in it.*[2]

Proof. First, we know that a generator for $(1 + 3i, 2)$ will be a gcd of the two elements. Since gcd are unique up to multiplication by units, any gcd will generate the ideal. Now, we write

$$\begin{aligned} 1 + 3i &= 2(1 + i) + (i - 1), \\ 2 &= (i - 1)(-1 - i). \end{aligned}$$

Thus, $(1 + 3i, 2) = (i - 1)$. Now, let us prove that $\mathbb{Z}[i]/(1 + 2i)$ is a field. This follows the same argument as in Problem 1.5 since $|1 + 2i|^2 = 5$ which is also prime, and so we will skip this part.

We now calculate $\gcd(1 + 2i, 2 + 3i)$ in $\mathbb{Z}[i]$. Clearly,

$$2 + 3i = 2(1 + 2i) + (-i)$$

implies that $(2 + 3i) - 2(1 + 2i) = -i$. Multiplying through by i, we find

$$(2 + 3i)i - 2i(1 + 2i) = 1.$$

Hence, $[i]$ is the inverse of $[2 + 3i]$ in $\mathbb{Z}[i]/(1 + 2i)$. □

[2]For a general $\xi \in \mathbb{Z}[i]$, we denote by $[\xi]$ it reduction in $\mathbb{Z}[i]/(1 + 2i)$.

Problem 1.8. *Let R be a PID and fix two $a, b \in R \setminus \{0\}$. Suppose that $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$. Prove that*

$$(d) = (a) + (b) \quad \textit{and} \quad (m) = (a) \cap (b).$$

Proof. Since greatest common divisors are unique up to multiplication by units, we need only show that a generator of $(a) + (b)$ is a gcd of a and b. To this end, let

$$(e) = (a) + (b)$$

and notice that $a, b \in (e)$ so that $e \mid a, b$. If $f \mid a$ and $f \mid b$, then $a, b \in (f)$ which gives

$$(e) = (a) + (b) \subseteq (f)$$

whence $f \mid e$. Since $e \sim d$, we have $(d) = (a) + (b)$. For the second part, we make use of a similar argument. Suppose that $\mu \neq 0$ is such that

$$(\mu) = (a) \cap (b).$$

Then, μ is clearly a multiple of both a and b. Furthermore, if $\eta = ax = by$ then $\eta \in (a) \cap (b) = (\mu)$ so that η is a multiple of μ. This makes μ a lcm of a and b. Again, these are unique up to multiplication by units and it follows that

$$(m) = (\mu) = (a) \cap (b).$$

□

Problem 1.9. *Write the following ideals in $\mathbb{Z}[i]$ as principal ideals:*

- $(1 + i, 1 - i)$;
- $(5, 7 + 4i)$.

Solution. Since $\mathbb{Z}[i]$ is an integral domain, we have

$$(1 + i) \subseteq (1 + i, 1 - i) = (1 + i) + (1 - i).$$

However, $1 - i = -i(1 + i)$ whence $(1 - i) \subseteq (1 + i)$. From the above, we obtain

$$(1 + i) \subseteq (1 + i, 1 - i) \subseteq (1 + i)$$

so that $(1 + i, 1 - i) = (1 + i)$. For the second part, we compute a gcd. WRite

$$\begin{aligned} 7 + 4i &= 5(1 + i) + (2 - i), \\ 5 &= (2 - i)(2 + i). \end{aligned}$$

Thus, $2 - i$ is a generator. □

2 Modules

Problem 2.1. *Let M be a finitely generated module over an integral domain R. Prove that if M is free, then M has finite rank.*

Proof. Let $\{x_1, \ldots, x_n\}$ be a finite set of generators for M and let I be an index set such that $M \cong R^{\oplus I}$. Thus, M has a maximally linearly independent subset having cardinality $|I|$. Now, let $\{b_i\}_{i\in I}$ be such a family. Every x_j can be written as a finite linear combination of the b_i. Hence, M is spanned by a finite subset of the family $\{b_i\}_{i\in I}$. Obviously, this finite subset will also be linearly independent. Let J be an index set for this finite subset of $\{b_i\}_{i\in I}$. Then $\{b_j\}_{j\in J}$ will be a *finite* basis for M over R in the sense that $M \cong R^{\oplus J}$. However, since $R^{\oplus I} \cong R^{\oplus J}$, we have that $|I| = |J| < \infty$. Therefore, I was finite to begin with! Finally, since $M \cong R^{\oplus I}$, every linearly independent subset of M has cardinality at most $|I| < \infty$. This means that $\mathrm{Rk}(M) \leq |I| < \infty$. □

Problem 2.2. *Let $\mathbb{F}$ be a field and $\mathbb{K}/\mathbb{F}$ a field extension. Let $A \in \mathsf{M}_n(\mathbb{F})$ and let R be its rational canonical form over $\mathbb{F}$. Prove that R is also the rational canonical form of A over $\mathbb{K}$.*

Proof. We know that R is the direct sum of companion matrices over $\mathbb{F}$, and hence over $\mathbb{K}$. Now, this means that R satisfies all the criteria of a rational canonical form for A over $\mathbb{K} \supseteq \mathbb{F}$. From the uniqueness, we see that R is the rational canonical form of A computed over $\mathbb{K}$. □

Problem 2.3. *Let $\mathbb{F}$ be a field and $\mathbb{K}/\mathbb{F}$ a field extension. Let $A, B \in \mathsf{M}_n(\mathbb{F})$. Show that if $A \sim B$ over $\mathbb{K}$, then $A \sim B$ over $\mathbb{F}$.*

Proof. Assume that $A \sim B$ over $\mathbb{K}$. Then, A and B share the same rational canonical form over $\mathbb{K}$. But, by the previous problem, this rational canonical form will be the rational canonical form of both A and B over $\mathbb{F}$. Thus, A and B share a rational canonical form over $\mathbb{F}$ whence $A \sim B$ over $\mathbb{F}$. □

Problem 2.4. *Let $n \leq 3$ and suppose $\mathbb{F}$ denotes a field. Let $A, B \in \mathsf{M}_n(\mathbb{F})$. Prove that $A \sim B$ if and only if both A and B share the same minimal and characteristic polynomials.*

Proof. Suppose first that $A \sim B$. Then, since A and B share the same rational canonical form, they share the same invariant factors. This means that A and B possess the same minimal and characteristic polynomials. For the converse, we consider two distinct cases. First, let us denote by $m(x)$ the minimal polynomial of A and B and by $\Delta(x)$ their characteristic polynomial.

1. We first handle the case of $n = 2$. If $\deg m(x) = 1$ then there will be two invariant factors, both being $m(x)$, whose product is equal to $\Delta(x)$. This means that both A and B will have to share the same canonical form (and hence be conjugate). If $\deg m(x) = 2$, then in both cases we have $m(x) = \Delta(x)$. That is, both A and B have a single invariant factor given by $\Delta(x)$. Again, $A \sim B$ as they have the same rational canonical form over $\mathbb{F}$.

2. We once again argue based on the degree of $m(x)$. If $\deg m(x) = 1$ then in both cases we must have 3 invariant factors, each equal to $m(x)$ whence $A \sim B$ by the same arguments as above. One dispenses of the case $\deg m(x) = 3$ similarly. Suppose now that $\deg m(x) = 2$. Let $a(x) := \Delta(x)/m(x)$ so that $\deg a(x) = 1$. Then, in both cases, $a(x) \mid m(x)$ so that $a(x)$ is the first invariant factor. This leaves us with only one rational canonical form for both A and B whence $A \sim B$ over $\mathbb{F}$.

□

Problem 2.5. *Let $f : \mathbb{Z}^n \to \mathbb{Z}^n$ be a group homomorphism and represent f as a matrix $M \in \mathsf{M}_n(\mathbb{Z})$. Supposing that $\det(M) \neq 0$, prove that*

$$|\mathbb{Z}^n / f(\mathbb{Z}^n)| = |\det(M)|.$$

Proof. We first assume that M is diagonal. Let (m_{ij}) be the entries (in $\mathbb{Z}$) of the matrix M. Notice that the restriction $\det(M) \neq 0$ gives $m_{ii} \neq 0$ for all $i = 1, \ldots, n$. Now, it is easy to see that

$$f(\mathbb{Z}^n) = M\mathbb{Z}^n \cong \bigoplus_{i=1}^{n} m_{ii}\mathbb{Z}$$

whence, by the first isomorphism theorem,

$$\mathbb{Z}^n / f(\mathbb{Z}^n) \cong \bigoplus_{i=1}^{n} \mathbb{Z}/m_{ii}\mathbb{Z}.$$

In this case, we see that $|\mathbb{Z}^n / f(\mathbb{Z}^n)| = |\prod_1^n m_{ii}| = |\det(M)|$ as was required. Let us now relax the assumption that M is diagonal. Invoking the Smith Normal Form for a principal ideal domain, one may find digaonalizable matrices P and Q in $\mathsf{M}_n(\mathbb{Z})$ such that

$$M = PDQ$$

where $D \in \mathsf{M}_n(\mathbb{Z})$ is diagonal and $\det(M) = \det(D)$. Then, $M\mathbb{Z}^n \cong D\mathbb{Z}^n$ so that, by the first part,

$$|\mathbb{Z}^n / f(\mathbb{Z}^n)| = |\mathbb{Z}^n / D\mathbb{Z}^n| = |\det(D)| = |\det(M)|$$

which completes the proof. □

Problem 2.6. *Let $A \in \mathsf{M}_2(\mathbb{Q})$ satisfy the polynomial equation $A^3 = I$ where $A \neq I$. Determine the rational and Jordan canonical forms of A over $\mathbb{Q}$ and $\mathbb{C}$, respectively,*

Solution. Let $m(x) \in \mathbb{Q}[x]$ be the minimal polynomial of the matrix A. Clearly, we have that $m(x) \mid (x-1)(x^2+x+1)$. Now, $m(x)$ also divides the characteristic polynomial of A, which has degree 2. Hence $\deg m(x) \leq 2$. Also, $A \neq I$. Decomposing $m(x)$ into irreducible factors in $\mathbb{Q}[x]$, it becomes clear that minimal polynomial divides x^2+x+1. Since this is irreducible, we have $m(x) = x^2 + x + 1$. Hence, we have exactly one companion matrix so that the rational canonical form is equal to

$$\begin{pmatrix} 0 & -1 \\ 1, & -1 \end{pmatrix}$$

Now, $m(x)$ has degree 2 which gives $\Delta(x) = m(x) = x^2 + x + 1$, where $\Delta(x)$ is the characteristic polynomial of A. This is easily seen to be a separable polynomial and thus A is diagonalizable over $\mathbb{Q}$. Letting $\omega_{1,2}$ be the distinct complex roots of $\Delta(x)$, the Jordan normal form is equal to

$$\begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix}$$

□

Problem 2.7. *Let $\mathbb{F}$ be a field and suppose $A \in \mathsf{M}_n(\mathbb{F})$. Explain why A is conjugate to its transpose A^{T}.*

Solution. Carrying out Smith's algorithm on A, we arrive at a diagonal matrix whose nontrivial entries are the invariant factors of A in the "correct order". Now, interchanging row operations for column operations and vice-versa, we can arrive to the same matrix starting from A^{T}. But, these will also be the invariant factors of A^{T}. This means that A and A^{T} share the same rational canonical form over $\mathbb{F}$, and are hence conjugate. □

Problem 2.8. *Let M be a module over an integral domain R. Prove each of the following general facts.*

1. *M has rank 0 if and only if $M = \mathrm{Tor}(M)$.*[3]
2. *The rank of M is precisely that of $M/\mathrm{Tor}(M)$.*
3. *If N is a submodule of M, then $\mathrm{Rk}(N) \leq \mathrm{Rk}(M)$.*

[3]Let M be a module over a ring R. Then $\mathrm{Tor}(M)$ is defined to be the set of all $m \in M$ such that there exists $r \neq 0$ with $r \cdot m = 0$.

Proof. The last point is immediate: if $\mathcal{L}$ is a linearly independent family in N, then it is linearly independent in M over R. This means that $\mathrm{Rk}(N) \leq \mathrm{Rk}(M)$.

Let $\{m_1+\mathrm{Tor}(M), \ldots, m_N+\mathrm{Tor}(M)\}$ be a finite linearly independent family in $M/\mathrm{Tor}(M)$. Here, the $m_j \in M$ are arbitrary representatives. We will now show that $\{m_1, \ldots, m_N\}$ is a linearly independent in M. Suppose we have coefficients $r_j \in R$ for which

$$\sum_{j=1}^{N} r_j \cdot m_j = 0.$$

Then,

$$\sum_{j=1}^{N} r_j \cdot m_j + \mathrm{Tor}(M) = \sum_{j=1}^{N} \Big[r_j \cdot m_j + \mathrm{Tor}(M) \Big] = 0$$

in $M/\mathrm{Tor}(M)$. By the linear independence over R, we see then that $r_j = 0$ for all indices j. This means that $\{m_1, \ldots, m_N\}$ is linearly independent in M. Conversely, let $\{m_1, \ldots, m_N\} \subseteq M$ be linearly independent over R and suppose that

$$0 = \sum_{j=1}^{N} \Big[r_j \cdot m_j + \mathrm{Tor}(M) \Big] = \sum_{j=1}^{N} r_j \cdot m_j + \mathrm{Tor}(M).$$

This gives $\sum_{j=1}^{N} r_j \cdot m_j \in \mathrm{Tor}(M)$. Hence, there exists $\alpha \in R \setminus \{0\}$ such that

$$0 = \alpha \cdot \sum_{j=1}^{N} r_j \cdot m_j = \sum_{j=1}^{N} \alpha r_j \cdot m_j$$

whence $\alpha r_j = 0$ for all indices j. Since R is an integral domain, we see that r_j is equal to zero, for all indices. This proves that

$$\{m_1 + \mathrm{Tor}(M), \ldots, m_N + \mathrm{Tor}(M)\}$$

is linearly independent in $M/\mathrm{Tor}(M)$. We have therefore exhibited a correspondence between the finite linearly independent subsets of M and those of $M/\mathrm{Tor}(M)$. It follows that M and $M/\mathrm{Tor}(M)$ have the same rank.

Assume now that $\mathrm{Rk}(M) = 0$. If $\{m\} \subseteq M$ then $\{m\}$ cannot be linearly independent over R. Thus, $m \in \mathrm{Tor}(M)$ by definition. Conversely, if $M = \mathrm{Tor}(M)$ then for every $m \in M$ one can find $\alpha \neq 0$ with $\alpha \cdot m = 0$. This is the statement that $\mathrm{Rk}(M) = 0$. □

Problem 2.9. *Construct a torsion free module that is not free.*

Solution. As $\mathbb{Q}$ is a field containing the integral domain $\mathbb{Z}$, we are free to view $\mathbb{Q}$ as a $\mathbb{Z}$-module with respect to the obvious notions of multiplication and "vector" addition. Since $\mathbb{Q}$ is itself an integral domain containing $\mathbb{Z}$, it is immediate that $\mathrm{Tor}(M) = \{0\}$. We now show that $\mathbb{Q}$ is not free. Suppose, by way of contradiction, that $\mathbb{Q} \cong \mathbb{Z}^{\oplus I}$ for some index set I. If we fix any two non-zero elements of $\mathbb{Q}$

$$\frac{\alpha}{\beta} \quad \text{and} \quad \frac{\gamma}{\delta}$$

for $\alpha, \beta, \gamma, \delta \in \mathbb{Z} \setminus \{0\}$, then

$$(\gamma\beta)\frac{\alpha}{\beta} - (\alpha\delta)\frac{\gamma}{\delta} = 0.$$

This means that the largest linearly independent family in $\mathbb{Q}$ has cardinality 1. This means that $\mathbb{Q} \cong \mathbb{Z}$ as $\mathbb{Z}$-modules. This isomorphism of modules certainly includes an isomorphism of groups whence $(\mathbb{Q}, +) \cong (\mathbb{Z}, +)$. Since $\mathbb{Q}$ is not cyclic with respect to addition, we have attained a contradiction. This means that $\mathbb{Q}$ is not free as a $\mathbb{Z}$-module. □

Problem 2.10. *Construct a torsion module whose annihilator*[4] *is trivial.*

Solution. We consider $M := \bigoplus_{m\in\mathbb{N}} \mathbb{Z}/2^m\mathbb{Z}$ as a $\mathbb{Z}$-module with the obvious coordinate-wise operations. First, we claim that $\mathrm{Tor}(M) = M$. Let $m \in M$ be given and write it as

$$m = (a_1 + 2\mathbb{Z}, \ldots, a_l + 2^l\mathbb{Z}), \quad a_j \in \mathbb{Z}.$$

Then, clearly, $2^l \cdot m = \mathbf{0}$. This gives $\mathrm{Tor}(M) = M$. It remains to show that $\mathrm{Ann}(M) = \{0\}$. Let $r \in \mathrm{Ann}(M)$ be given and suppose without harm that $r \geq 0$. Choose $N \in \mathbb{N}$ such that $r < 2^N$. Then,

$$r \cdot (0, \ldots, 0, 1 + 2^N\mathbb{Z}, 0 \ldots, 0) = \mathbf{0}$$

whence $2^N \mid r$. Since $0 \leq r < 2^N$, we see that $r = 0$. This implies that $\mathrm{Ann}(M) = \{0\}$, as was required. □

3 Fields

Problem 3.1. *Let K/F be a field extension and suppose that $\alpha \in K$ is algebraic over F. Supposing that $[F(\alpha) : F]$ is odd, prove that $F(\alpha^2) = F(\alpha)$.*

[4] If M is a module over a ring R, we define the annihilator of M to be the set of all $r \in R$ such that $r \cdot m = 0$ for all $m \in M$.

Proof. It is immediate that $F(\alpha^2) \subseteq F(\alpha)$. By way of contradiction, suppose that $F(\alpha^2) \neq F(\alpha)$. In particular, we have[5] $[F(\alpha) : F(\alpha^2)] > 1$. We may always write

$$[K : F] = [F(\alpha) : F(\alpha^2)] \cdot [F(\alpha^2) : F].$$

Now, α is algebraic over $F(\alpha^2)$ since it satisfies the polynomial $x^2 - \alpha^2$ over $F(\alpha^2)$. By the assumption that $F(\alpha^2) \neq F(\alpha)$, we cannot[6] have $\alpha \in F(\alpha^2)$. This implies that $x^2 - \alpha^2$ is irreducible over $F(\alpha^2)$, and is therefore the minimal polynomial of α over $F(\alpha^2)$. From this, we see that

$$F(\alpha) = F(\alpha^2)(\alpha) \cong F(\alpha^2)[x]/(x^2 - \alpha^2)$$

whence $[F(\alpha) : F(\alpha^2)] = 2$. Combined with the expression for $[K : F]$ above, it follows that $[K : F]$ is even which is impossible. This contradiction gives $F(\alpha) = F(\alpha^2)$. □

Problem 3.2. *Let p be a prime and let $n \geq 1$ be an integer. Construct a field having p^n-elements. Prove that such a field is unique up to isomorphism. This field is then to be denoted by $\mathbb{F}_{p^n}$.*

Solution. Let $\mathbb{F}_p$ be the finite field $\mathbb{Z}/p\mathbb{Z}$. We first prove the uniqueness. Let F be a finite field having p^n and notice that it must have characteristic p.[7] Hence, F contains an isomorphic copy of $\mathbb{F}_p$. We can therefore consider the polynomial

$$f(x) = x^{p^n} - x$$

over $\mathbb{F}_p \subseteq F$. Now, this has at most p^n-roots in *any* field. Since the group of units $F^\times = F \setminus \{0\}$ would have order $p^n - 1$, one easily sees that

$$x^{p^n} = x$$

for all $x \in F$. Thus, F is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. The uniqueness of splitting fields then implies that F is unique up to isomorphism.

All of this hinges upon the existence of a field having p^n-elements, which we now establish. Consider the field of p-elements $\mathbb{F}_p$ and define

$$f(x) := x^{p^n} - x \in \mathbb{F}_p[x].$$

[5] If $[K : F] = 1$ then $\{1\} \subseteq F$ is a basis for K over F. This would imply that $K = F$.

[6] If $\alpha \in F(\alpha^2)$, then $F(\alpha^2) \supseteq F(\alpha)$ by the very definition of $F(\alpha)$. Of course, this contradicts the assumption that $F(\alpha) \neq F(\alpha^2)$.

[7] As a finite field, it will have non-zero characteristic, and we know that this will be a prime q. Therefore, F contains an isomorphic copy of some $\mathbb{Z}/q\mathbb{Z}$. But, F can be viewed as a vector space over $\mathbb{Z}/q\mathbb{Z}$ whence we see that $|F| = q^m$ for some $m \geq 1$. From the uniqueness of factorization, $m = n$ and $q = p$.

Let E denote the family of all roots to the polynomial $f(x)$ (considered in some algebraic closure). Computing the algebraic derivative of f and using the $\mathrm{Ch}(\mathbb{F}_p) = p$, we have

$$f'(x) = p^n x^{p^n - 1} - 1 = -1.$$

Thus, $\gcd(f, f') = 1$ so that f is a separable polynomial. This means that E consists of precisely p^n-elements. It is easy to see that $\{0, 1\} \subseteq E$. Moreover, if $x \in E$ and $x \neq 0$, then it is obvious that $x^{-1} \in E$. Also, for $x_{1,2} \in E$ we see that

$$(x_1 x_2)^{p^n} = x_1^{p^n} x_2^{p^n} = x_1 x_2$$

which means that E is closed under multiplication. To see closure under addition, recall that the "Freshman's dream" holds true in characteristic p. That is,

$$(x_1 + x_2)^{p^n} = x_1^{p^n} + x_2^{p^n} = x_1 + x_2.$$

From this, it is easy to see that E is a field which guarantees the existence. This completes the proof. □

Problem 3.3. *Let $n \in \mathbb{N}$ and $p \geq 2$ a prime. Prove that there exists an irreducible polynomial of degree n over $\mathbb{F}_p$.*

Proof. Let $\mathbb{F}_{p^n}$ be the field containing p^n-elements and recall that it contains $\mathbb{F}_p$ as a subfield (this is by construction). Now, the group of units $\mathbb{F}_{p^n}^{\times}$ is cyclic and thus has a generator θ. In this case, we must have $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$. Since $\mathbb{F}_{p^n}$ is finite, the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is also finite and therefore algebraic. Let then $m(x) \in \mathbb{F}_p[x]$ be the minimal polynomial of θ and observe that

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\theta) \cong \mathbb{F}_p[x]/(m(x)).$$

From this, one has $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = \deg m(x)$. Since $m(x)$ is irreducible, we have found our desired polynomial. □

Problem 3.4. *Let K/F be a finite extension of fields. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ having a root in K splits over K.*

Proof. We will first establish the " $\Longleftarrow$ " direction as it is shorter. Since K/F is finite, we may choose algebraic elements $\alpha_1, \ldots, \alpha_n$ such that $K = F(\alpha_1, \ldots, \alpha_n)$. For each j, let $m_j(x) \in F[x]$ be the minimal polynomial of α_j. Since these polynomials have a root in K (the α_j's), they must split over K by hypothesis. Thus, $\prod_1^n m_j(x)$ splits over K. If $L \supseteq F$ is a field over which $\prod_1^n m_j(x)$ splits, then L contains $\{\alpha_1, \ldots, \alpha_n\}$ whence $L \supseteq K$. Hence, K is the splitting field of $\prod_1^n m_j(x)$ over F.

Conversely, let K be the splitting field of $f(x) \in F[x]$ over F. Let $p(x) \in F[x]$ be an irreducible polynomial having a root $\alpha \in K$. By passing to an algebraic closure of K, let β be any other root of $p(x)$. The claim amounts to showing that $\beta \in K$. Now, let us first extend the identity automorphism $\mathbf{1} : F \to F$ to an isomorphism $F(\alpha) \to F(\beta)$:

$$\begin{array}{lcc} \sigma: & F(\alpha) & \longrightarrow F(\beta) \\ & \big| & \big| \\ \mathbf{1}_F: & F & \longrightarrow F \end{array}$$

Now, $K(\alpha)$ is the splitting field of $f(x)$ over $F(\alpha)$. Certainly, $f(x)$ splits over $K(\alpha) \supseteq K$. Moreover, if $f(x)$ splits over a field $L \supseteq F(\alpha)$ then $L \supseteq K$ and $K \ni \alpha$ whence $L \supseteq K(\alpha)$. Similarly, $K(\beta)$ is the splitting field of $f(x)$ over $F(\beta)$. Since σ fixes F, we may extend it further to an isomorphism $K(\alpha) \to K(\beta)$ in the fashion of

$$\begin{array}{lcc} \varphi: & K(\alpha) & \longrightarrow K(\beta) \\ & \big| & \big| \\ \sigma: & F(\alpha) & \longrightarrow F(\beta) \\ & \big| & \big| \\ \mathbf{1}_F: & F & \longrightarrow F \end{array}$$

However, $K(\alpha) = K$ since $\alpha \in K$. The above then shows that $K = K(\alpha) \cong K(\beta)$ as F-vector spaces (since φ is an isomorphism fixing F). Now, we write

$$[K : F] = [K(\alpha) : F] = [K(\beta) : F] = [K(\beta) : K][K : F]$$

so that $[K(\beta) : K] = 1$. This yields $K = K(\beta)$, i.e. $\beta \in K$. We conclude that $p(x)$ splits over K as was asserted. □

Problem 3.5. *Let K/F be an extension of fields and let $K_{1,2}$ be fields with $F \subseteq K_{1,2} \subseteq K$. Suppose additionally that both K_1 and K_2 are splitting fields over F. Prove that K_1K_2 and $K_1 \cap K_2$ are both splitting fields over F.*

Proof. By hypothesis, K_1 is the splitting field of a polynomial $f_1(x) \in F[x]$ and likewise K_2 is that of some $f_2(x) \in F[x]$. Clearly, $f_1(x)f_2(x)$ splits over K_1K_2. If it splits over any field $L \supseteq F$, then both f_1 and f_2 will split over L. This implies that $L \supseteq K_1 \cup K_2$ whence $L \supseteq K_1K_2$. We conclude that K_1K_2 is a splitting field over F.

To show that $K_1 \cap K_2$ is a splitting field we will invoke the previous problem. Let $p(x) \in F[x]$ be irreducible and suppose that it has a root in $K_1 \cap K_2$. Then, $p(x)$ has a root

in both K_1 and K_2. As these are splitting fields over F, the previous problem implies that $p(x)$ splits over both K_1 and K_2, and therefore over K_1K_2. Using the previous problem once more, we infer that $K_1 \cap K_2$ is a splitting field over F. □

Problem 3.6. *Let F be a field and let $\overline{F}$ be the algebraic closure of F. Assume L is a field with $F \subseteq L \subseteq \overline{F}$. Prove that $\overline{F}$ is an algebraic closure of L.*

Proof. Recall that $\overline{F}$ is algebraically closed. Since L is a subfield of $\overline{F}$, we see that every polynomial with coefficients in L splits over $\overline{F}$. It remains only to check that $\overline{F}/L$ is algebraic. However, this is immediate from the fact that $\overline{F}/F$ is algebraic as every element of $\overline{F}$ solves a polynomial with coefficients in F, and hence L. □

Problem 3.7. *Let K/F be a finite and separable[8]. Prove that there exist finitely many subfields $F \subseteq E \subseteq K$.*

Proof. The claim is clear if $K = F$ and thus we assume $K \supset F$. We first show that there exists a field $L \supseteq K$ such that L/F is Galois. Since K/F is finite, we can choose *distinct* algebraic elements $\alpha_1, \ldots, \alpha_n$ in $K \setminus F$ such that $K = F(\alpha_1, \ldots, \alpha_n)$. For each j let $m_j(x)$ be the separable minimal polynomial of α_j over F. Denote by K_j the splitting field of m_j over F and note that K_j/F is Galois. Thus, the composite $\prod_1^n K_j$ is also Galois over F. As $\prod_1^n K_j$ contains every α_j and F, it also contains K.

We now know that there exists a field $L \supseteq K$ such that L/F is Galois. The Galois group $\mathrm{Gal}(L/F)$ is by definition finite and, moreover, if $F \subseteq E \subseteq K$ then

$$F \subseteq E \subseteq L.$$

By the fundamental theorem of Galois theory, such subfields are in correspondence with the subgroups of $\mathrm{Gal}(L/F)$. Since there are only finitely many such subgroups, only finitely many subfields $F \subseteq E \subseteq K$ can exist. □

Problem 3.8. *Let F be a field and K/F a field extension. Let $f(x), g(x)$ be non-constant polynomials and suppose that $r(x) = \gcd(f(x), g(x))$ in $F[x]$. Show that $r(x)$ is again the* gcd *of $f(x)$ and $g(x)$ in $K[x]$.*

Proof. First, notice that $r(x)$ certainly divides both $f(x)$ and $g(x)$ in $K[x]$. Let $w(x)$ be the gcd of $f(x)$ and $g(x)$ in the extension $K[x]$. Since $r(x)$ divides $f(x)$ and $g(x)$, we have $r(x) \mid w(x)$ in $K[x]$. However, in $F[x]$, we have

$$r(x) = a(x)f(x) + b(x)g(x)$$

[8]The extension K/F is called separable if K/F is algebraic and the minimal polynomial of each $\alpha \in K$ is a separable polynomial in $F[x]$.

for polynomials $a(x), b(x) \in F[x] \subseteq K[x]$. Therefore, $w(x) \mid r(x)$ in $K[x]$ whence it follows that $w(x) = r(x)$. □

Problem 3.9. *Prove two statements:*

1. *If $f(x) \in \mathbb{F}_p[x]$ is a non-zero polynomial with $\deg f = r$, then f is irreducible if and only if for all $1 \leq n \leq r/2$ one has*
$$\gcd\left(f(x), x^{p^n} - x\right) = 1.$$
2. *Let $f(x) \in \mathbb{F}_p[x]$. Then $f(x)$ has a root in $\mathbb{F}_p$ if and only if $\gcd(f(x), x^p - x) \neq 1$.*

Proof. We will begin by proving (1). First, assume that for some $1 \leq n \leq r/2$
$$\gcd\left(f(x), x^{p^n} - x\right) \neq 1.$$
But, we know that
$$x^{p^n} - x = \prod_{\substack{\mathbb{F}_p[x] \ni g \text{ monic} \\ \text{irred.} \\ \deg g \mid n}} g(x).$$
Thus, there exists a polynomial $p(x)$ of degree
$$1 \leq \deg p \leq n \leq \frac{r}{2} < r = \deg f$$
with $p(x) \mid f(x)$. Hence, $f(x)$ is reducible. Conversely, suppose that
$$\gcd\left(f(x), x^{p^n} - x\right) = 1, \quad \forall\ 1 \leq n \leq \frac{r}{2}.$$
Assume for a contradiction that f is reducible and choose a polynomial $p(x)$ dividing $f(x)$ with $\deg p(x) \geq 1$. Obviously, we may assume that $\deg p(x) \leq r/2$ and that $p(x)$ is monic. Decomposing $p(x)$ into irreducible factors, we are left with an irreducible monic divisor of the polynomial $f(x)$. Hence, we might as well assume that $p(x)$ is irreducible. But, for all n
$$x^{p^n} - x = \prod_{\substack{\mathbb{F}_p[x] \ni g \text{ monic} \\ \text{irred.} \\ \deg g \mid n}} g(x).$$
Clearly, $p(x)$ will appear in the product on the right for $n = \deg p(x) \leq r/2$, which would contradict the assumption about the gcd; namely that
$$\gcd\left(f(x), x^{p^n} - x\right) = 1, \quad \forall\ 1 \leq n \leq \frac{r}{2}.$$

This proves (1).

Let us now establish (2). From Theorem 7.1.2 in the course notes, we see that

$$x^p - x = \prod_{\substack{\mathbb{F}_p[x] \exists g \text{ monic} \\ \text{irred.} \\ \deg g = 1}} g(x) = \prod_{j=1}^{p} (x - \alpha_j)$$

where $\{\alpha_1, \ldots, \alpha_p\}$, with $\alpha_1 = 0$, is an enumeration of $\mathbb{F}_p$. Of course, every $(x - \alpha_j)$ is irreducible in $\mathbb{F}_p[x]$. Now, suppose that $f(\beta) = 0$ for some $\beta \in \mathbb{F}_p$; then $(x - \beta) \mid f(x)$ in $\mathbb{F}_p[x]$ whence we see that

$$\gcd(f(x), x^p - x) \neq 1. \tag{$\star$}$$

Conversely, assume the equation ($\star$) holds. Then let $p(x)$ be a common divisor of both $f(x)$ and $x^p - x$ with $\deg p \geq 1$. Obviously f then has a root since any non-unit divisor of $x^p - x$ is a product of linear terms. □

Problem 3.10. *Suppose that a and b are constructible lengths. Prove that a/b is also a constructible length.*

Proof. We will work in the xy-plane. First, 1 is constructible and so we may draw a line from $(0, 0)$ to $(1, 0)$. About $(0, 0)$ we draw a circle of radius a and mark where it intersects the positive y-axis; this is the point $(0, a)$. Similarly since b is constructible, we may identify the point $(b, 0)$ on the positive x-axis. Draw a line, γ_1, connecting $(0, a)$ and $(b, 0)$. This line is parametrized by

$$\gamma_1(t) = -\frac{a}{b}t + a, \quad 0 \leq t \leq b.$$

Now, we draw a line passing through $(1, 0)$ that is parallel to γ_1; let us label this curve by γ_2. It is also easy to identify the parametrization of γ_2:

$$\gamma_2(t) = \frac{a}{b} - \frac{a}{b}t, \quad 0 \leq t \leq 1.$$

Then, γ_2 intersects the positive y-axis at the point $(0, a/b)$. Drawing a line from $(0, 0)$ to $(0, a/b)$, we see that a/b is constructible. □

4 Galois Theory

Problem 4.1. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 4 having a root $\alpha \in \mathbb{R}$ and let K denote the splitting field of $f(x)$ over $\mathbb{Q}$. Notice that $f(x)$ must be separable and*

assume that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_4$. *Show that there exists a subfield* E *with* $F \subseteq E \subseteq K$, *containing no quadratic* $\mathbb{Q}$*-subfields, such that* $[E : F] = 4$.

Proof. By hypothesis, $\alpha \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ with minimal polynomial $f(x)$. This implies that

$$E = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f(x))$$

and that $[E : \mathbb{Q}] = \deg f(x) = 4$. We now claim that E contains no quadratic subfields. Let H^E be the field associated to E in $\mathrm{Gal}(K/F)$ under the Fundamental Theorem of Galois theory and notice that

$$\frac{24}{|H^E|} = \left[\mathfrak{S}_{24} : H^E\right] = [E : \mathbb{Q}] = 4$$

which gives $|H^E| = 6$. As a subgroup of $\mathfrak{S}_4$, the only possibility is $H^E \cong \mathfrak{S}_3$. Assume for a contradiction that one can find a quadratic subfield $\mathbb{Q} \subseteq Q \subseteq E$, then $[Q : \mathbb{Q}] = 2$. If H^Q denotes the associated subfield, then the Fundamental Theorem again yields

$$\frac{24}{|H^Q|} = \left[\mathfrak{S}_4 : H^Q\right] = [Q : \mathbb{Q}] = 2$$

whence $|H^Q| = 12$. Since H^Q is a subgroup of $\mathfrak{S}_4$, inspection tells us that $H^Q \cong \mathfrak{A}_4$. However, $Q \subseteq E$ implies that $H^E \subseteq H^Q$ which yields $\mathfrak{S}_3 \subseteq \mathfrak{A}_4$ which we know to be impossible. □

Problem 4.2. *Let* p *be a prime and let* $f(x) \in \mathbb{Q}[x]$ *be an irreducible polynomial of degree* p. *Assume that* $f(x)$ *has exactly two roots in* $\mathbb{C} \setminus \mathbb{R}$. *If* K *is the splitting field of* $f(x)$ *over* $\mathbb{Q}$, *prove that* $K/\mathbb{Q}$ *is Galois with Galois group* $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_p$.

Proof. First, being irreducible over a field of characteristic 0, it is indeed true that $f(x)$ is separable. Thus, K/F is Galois. Now, we will always have an embedding

$$\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \mathfrak{S}_p.$$

Let $\zeta_{1,2} \in \mathbb{C}\setminus\mathbb{R}$ be roots of $f(x)$; the conjugate root theorem states that $\zeta_2 = \overline{\zeta_1}$. In any case, we can define an automorphism of K fixing F which takes $\zeta_1 \mapsto \zeta_2$ and $\zeta_2 \mapsto \zeta_1$. Hence, one can always find a permutation in $\mathrm{Gal}(K/\mathbb{Q})$ that can be viewed as a 2-cycle. Now, $f(x)$ is the minimal polynomial of all of its roots. It then follows from the multiplicativity of degrees that p divides $[K : F] = |\mathrm{Gal}(K/\mathbb{Q})|$. By Cauchy's theorem, we can choose an element of order p. Since $\mathrm{Gal}(K/\mathbb{Q})$ already "contains" a 2-cycle, this means that $\mathrm{Gal}(K/\mathbb{Q})$ is the whole of $\mathfrak{S}_p$. □

Problem 4.3. *Let K/F be a Galois extension and assume that $K = F(\alpha)$ for some $\alpha \in K$. Let H be a subgroup of* $\mathrm{Gal}(K/F)$ *and subsequently put*

$$f_H(x) := \prod_{\sigma \in H} (x - \sigma(\alpha)) \in K[x].$$

If K^H denotes the fixed field of H in K, prove that $f_H(x) \in K^H[x]$ and show that K is the splitting field of $f_H(x)$ over K^H. Finally, prove that K^H is generated over F by the coefficients of $f_H(x)$.

Proof. First, let $\tau \in H$ be given and extend it to a ring isomorphism

$$\tau : K[x] \to K[x]$$

obtained by fixing the free-variables x and acting upon the coefficients in K. Then, it is clear that

$$\tau f_H(x) = \prod_{\sigma \in H} (x - \tau(\sigma(\alpha))) = \prod_{\varsigma \in H} (x - \varsigma(\alpha))$$

whence it follows that τ fixes the coefficients of $f_H(x)$. Since $\tau \in H < \mathrm{Gal}(K/F)$ was arbitrary, we see that $f_H(x) \in K^H[x]$. Since σ is an automorphism of K, it is evident from the very definition that $f_H(x)$ splits over K. It it splits over any subfield containing K^H, then it must contain α as H contains the identity automorphism. Since $K = F(\alpha)$, we see that this field will contain K as well. We infer that K is the splitting field of $f_H(x)$ over the field K^H.

Let $a_1, \ldots, a_n$ denote the coefficients of $f_H(x)$ in K^H, we claim that $K^H = F(a_1, \ldots, a_n)$. Clearly, one already has that $F(a_1, \ldots, a_n) \subseteq K^H$. For the reverse inclusion, we will invoke the Fundamental Theorem of Galois theory. Let $\tau \in \mathrm{Gal}(K/F(a_1, \ldots, a_n))$ and observe that $\tau f_H(x) = f_H(x)$. Since τ is an automorphism of K, it permutes the family of points $\{\sigma(\alpha)\}$, i.e.

$$\{\sigma(\alpha) : \sigma \in H\} = \{\tau(\sigma(\alpha)) : \sigma \in H\}.$$

Since H contains $\mathbf{1}_K$, this means that $\tau(\alpha) = \sigma(\alpha)$ for some $\sigma \in H$. Notice that α generates K over F. As σ, τ are automorphisms $K \to K$ fixing F, we conclude that $\tau \equiv \sigma$ whence $\tau \in H$. This implies that

$$\mathrm{Gal}(K/F(a_1, \ldots, a_n)) \subseteq \mathrm{Gal}\left(K/K^H\right).$$

By the fundamental theorem, it follows that $K^H \subseteq F(a_1, \ldots, a_n)$. We conclude that $F(a_1, \ldots, a_n) = K^H$, as was required. □

Problem 4.4. *The purpose of this problem is to show that every finite group arises as the Galois group of some Galois extension of fields. We proceed in two parts.*

1. *Let $x_1, \ldots, x_n$ be n-free variables and let K be the field of fractions associated to $\mathbb{Q}[x_1, \ldots, x_n]$. Show that there exists an embedding $\mathfrak{S}_n \hookrightarrow \mathrm{Aut}(K/\mathbb{Q})$.*

2. *Let G be a finite group of order n. Using Cayley's theorem and the first part, show that G is the Galois group of a Galois field extension.*

Proof. Let $\sigma \in \mathfrak{S}_n$ be given, we may define an associated isomorphism of rings

$$\mathbb{Q}[x_1, \ldots, x_n] \to \mathbb{Q}[x_1, \ldots, x_n]$$

by fixing the coefficients in $\mathbb{Q}$ and sending x_i to $x_{\sigma(i)}$. This isomorphism may clearly be extended to an automorphism of K, denoted $\hat{\sigma}$, which fixes $\mathbb{Q}$. This allows us to consider the following function:

$$\Sigma : \mathfrak{S}_n \to \mathrm{Aut}(K/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(K), \quad \sigma \mapsto \hat{\sigma}.$$

It is clear that this is a group homomorphism. We now claim that Σ is injective. Assume that $\hat{\sigma} \equiv \hat{\varsigma}$. Then, for every $i \in \{1, \ldots, n\}$ one would have $x_{\sigma(i)} = x_{\varsigma(i)}$ whence $\sigma \equiv \varsigma$. This means that Σ is actually the desired embedding

$$\Sigma : \mathfrak{S}_n \hookrightarrow \mathrm{Aut}(K/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(K).$$

This establishes the first part. For the second part, Cayley's theorem gives an embedding $G \hookrightarrow \mathfrak{S}_n \hookrightarrow \mathrm{Aut}(K)$. Let now K^G denote the fixed field of G in K. Since G is finite, we know that K/K^G is Galois with Galois group G which concludes the proof. □

Problem 4.5. *Calculate the Galois groups of the polynomials $x^3 \pm 3x + 1$ over $\mathbb{Q}$. Verify first that they are separable polynomials!*

Proof. Since we are working in characteristic 0, the polynomials above are separable if they are irreducible. Let

$$f^{\pm}(x) := x^3 \pm 3x + 1 \in \mathbb{Q}[x],$$

we will prove that $f^{\pm}(x)$ is irreducible using the rational root theorem.[9] From this theorem, we see that the only roots to $f^{\pm}(x)$ are ± 1. Direct computation shows that ± 1 are not roots to $f^{\pm}(x)$ and thus we deem $f^{\pm}(x)$ to be irreducible over $\mathbb{Q}$.

[9] Let $r(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial in $\mathbb{Z}[x]$ and suppose that $p/q \in \mathbb{Q}$ is a root of $r(x)$, with $\gcd(p, q) = 1$. Then $p \mid a_0$ and $q \mid a_n$.

Let $K^{\pm}$ be the splitting field of $f^{\pm}(x)$ over $\mathbb{Q}$, then $K^{\pm}/F$ is Galois. Now, for a general cubic polynomial of the form

$$x^3 + ax^2 + bx^2 + c,$$

the *discriminant* looks like

$$\mathscr{D} = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

Let $D^{\pm}$ be the discriminant for $f^{\pm}(x)$. Then, in both cases $a = 0$ so that

$$D^{+} = -4(3)^3 - 27 = -5 \cdot 27,$$
$$D^{-} = -4(-3)^3 - 27 = 3^4.$$

Hence, D^{-} is a square but D^{+} is not. This implies that $\mathrm{Gal}(K^{-}/\mathbb{Q}) \cong \mathfrak{A}_3$ and $\mathrm{Gal}(K^{+}/\mathbb{Q}) \cong \mathfrak{S}_4$. On the other hand, D^{+} is clearly not a square, which makes $\mathrm{Gal}(K^{+}/\mathbb{Q})$ the whole of the permutation group $\mathfrak{S}_3$. □

Problem 4.6. *Calculate the Galois group of the polynomial $x^3 - 5x + 1$ over $\mathbb{Q}$.*

Proof. As before, this polynomial is easily seen to be irreducible, and hence separable over $\mathbb{Q}$. If K is its splitting field over $\mathbb{Q}$, then K/Q is Galois. The discriminant is equal to

$$D = -4(-5)^3 - 27 = 4 \cdot 125 - 27 = 500 - 27 = 473.$$

Since 473 is not a square, we have $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_3$. □

Problem 4.7. *Determine the Galois group of $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$.*

Proof. It is clear that the polynomial is separable over $\mathbb{Q}$. If K denotes its splitting field over $\mathbb{Q}$, then $K/\mathbb{Q}$ is Galois. Now, it is clear that $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$. Moreover,

$$\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2) \quad \text{and} \quad \mathbb{Q}(\sqrt{3}) \cong \mathbb{Q}[x]/(x^2 - 3).$$

Now, $x^2 - 2$ and $x^2 - 3$ are separable so that $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$. From the above,

$$|\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right)| = 2$$

whence $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right) \cong \mathbb{Z}/2\mathbb{Z}$. In a similar vein, one easily sees that $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is Galois with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Also, the splitting field of $(x^2 - 2)(x^2 - 3)$ is obviously $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3})$. This certainly means that

$$\mathrm{Gal}\,(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

□

5 Other Problems (from Dummit and Foote)

In this section we solve problems taken from Dummit and Foote that are straightforward in the sense that the exercises do not introduce new definitions. This is mostly because such problems cannot be asked during an exam.

5.1 Fields

Problem 5.1. *Prove that an algebraically closed field must be infinite.*

Proof. Let F be a finite field having elements $\alpha_1, \ldots, \alpha_n$. Consider the polynomial

$$f(x) := 1 + \prod_{j=1}^{n} (x - \alpha_j)$$

which certainly has coefficients in F. However, $f(\alpha) = 1$ for all $\alpha \in F$ which means that $f(x)$ has no roots in F. Hence, a finite field is never algebraically closed. □

Problem 5.2. *Let K/F be a field extension of degree p for some prime p. If $F \subseteq E \subseteq K$ where E is a field, prove that $E = F$ or $E = K$.*

Proof. We write $p = [K : F] = [K : E] \cdot [E : F]$; since p is prime one of these terms on the right will be equal to 1. Thus, either $K = E$ or $F = E$. □

Problem 5.3. *Let K/F be an algebraic extension of fields and suppose that R is a ring such that $F \subseteq R \subseteq K$. Prove that R is in fact a field.*

Proof. It suffices to check that every non-zero element of R has an inverse with respect to multiplication. Let $r \in R \setminus \{0\}$ and notice that $r \in K$, which is algebraic over F. Thus, r is a root of its minimal polynomial

$$a_n x^n + \cdots + a_1 x + a_0, \quad a_j \in F \subseteq R.$$

Now, since $r \neq 0$, we cannot have $a_0 = 0$. Thus, a_0 is invertible in F, and hence in R. We get then that

$$a_n r^n + \cdots + a_1 r = -a_0$$

whence

$$\underbrace{r\left(-a_0^{-1} \sum_{j=0}^{n-1} a_{j+1} r^j\right)}_{\in R} = 1.$$

This means that R is a field. □

Problem 5.4. *Let $f(x)$ be an irreducible polynomial of degree n over a field F and suppose $g(x) \in F[x]$. Prove that every irreducible factor of $f(g(x))$ has degree divisible by n.*

Proof. Let $p(x) \mid f(g(x))$ be irreducible and let $m := \deg p(x)$. Let α be a root of $p(x)$ in some algebraic closure. Since α is a root of the irreducible polynomial $p(x)$, we have

$$[F(\alpha) : F] = \deg p(x) = m.$$

Now, $p(x)$ divides $f(g(x))$ whence $f(g(\alpha)) = 0$. As $f(x)$ is also irreducible, we have that

$$[F(g(\alpha)) : F] = \deg f(x) = n.$$

Since $g(x)$ is a polynomial with coefficients in F, we have $g(\alpha) \in F(\alpha)$ so that the inclusion $F(g(\alpha)) \subseteq F(\alpha)$ holds. This allows us to write

$$m = [F(\alpha) : F] = [F(\alpha) : F(g(\alpha))] \cdot [F(g(\alpha)) : F]$$

whence $n \mid m$. □

Problem 5.5. *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be such that $\alpha_j^2 \in \mathbb{Q}$ for every index j. Let F denote the field $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Prove that $\sqrt[3]{2} \notin F$.*

Proof. There are two cases to distinguish. First, if $\alpha_j \in \mathbb{Q}$ for every index j, then $F = \mathbb{Q}$. In this case, it is known that $\sqrt[3]{2} \notin F$. Otherwise, assume there is some α_j which does not belong to $\mathbb{Q}$. Without harm, we assume that $\alpha_1 \notin \mathbb{Q}$. The minimal polynomial of α_1 over $\mathbb{Q}$ is then equal to $x^2 - \alpha_1^2$ whence

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha_1)] \cdot [\mathbb{Q}(\alpha_1) : \mathbb{Q}].$$

Since the minimal polynomial of α_1 has degree 2 over $\mathbb{Q}$, we see that $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 2$ so that $[F : \mathbb{Q}]$ is even. Actually,

$$[F : \mathbb{Q}] = 2 \cdot [F : \mathbb{Q}(\alpha_1)].$$

Now, the degree of each α_j over a field extension of $\mathbb{Q}$ will never be larger than 2. Thus, successive applications of the argument used above gives that

$$[F : \mathbb{Q}] = 2^m, \quad m \geq 1.$$

By way of contradiction, let us now suppose that $\sqrt[3]{2} \in F$. Then, $\mathbb{Q}(\sqrt[3]{2}) \subseteq F$. However,

$$\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2)$$

which means that

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

This means that $3 \mid [F : \mathbb{Q}] = 2^m$. This contradiction gives $\sqrt[3]{2} \notin F$. □

5.2 Galois Theory

Problem 5.6. *Let K/F be a Galois extension of degree p^n for a prime p and $n \geq 1$. Show that there exist Galois extensions of F, contained in K, having degrees p and p^{n-1}.*

Proof. First, the Galois group $\mathrm{Gal}(K/F)$ is a p-group. As a p-group, it center is non-trivial and is therefore a p-group in its own right. By Cauchy's theorem, we may chose an element $\sigma \in Z(\mathrm{Gal}(K/F))$ having order p. The subgroup $\langle\sigma\rangle$ is then a normal subgroup of $\mathrm{Gal}(K/F)$. If $E^{\langle\sigma\rangle}$ is the field corresponding to $\langle\sigma\rangle$, then E/F will be Galois. But then,

$$\left[E^{\langle\sigma\rangle} : F\right] = \frac{|\mathrm{Gal}(K/F)|}{|\langle\sigma\rangle|} = p^{n-1}.$$

Similarly, we know from group theory that $\mathrm{Gal}(K/F)$ will have a normal subgroup H of order p^{n-1}. Therefore, if E^H is the corresponding field, then E^H/F is Galois with degree

$$\left[E^H : F\right] = [\mathrm{Gal}(K/F) : H] = p.$$

This completes the proof. □

Problem 5.7. *Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ is Galois with Galois group isomorphic to $\mathbb{Z}/4\mathbb{Z}$.*

Proof. First, notice that

$$\left(\sqrt{2+\sqrt{2}}\right)^3 = \left(2+\sqrt{2}\right)^2 = 4 + 4\sqrt{2} + 2 = 6 + 4\sqrt{2}.$$

Also,

$$\left(\sqrt{2+\sqrt{2}}\right)^2 = 2 + \sqrt{2}.$$

This means that

$$\left(\sqrt{2+\sqrt{2}}\right)^4 - 4\left(\sqrt{2+\sqrt{2}}\right)^2 = 6 + 4\sqrt{2} - 8 - 4\sqrt{2} = -2.$$

We conclude that $\sqrt{2+\sqrt{2}}$ satisfies the polynomial

$$f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x].$$

By Eisenstein's criterion[10] with $p = 2$, we see that $f(x)$ is irreducible over $\mathbb{Q}[x]$. Since $\mathbb{Q}$ has characteristic 0, $f(x)$ is also a separable polynomial. Now, the roots of $f(x)$ are real and are given by

$$\pm\sqrt{2 \pm \sqrt{2}} \in \mathbb{R}.$$

Consider the field $\mathbb{Q}(\sqrt{2+\sqrt{2}})$. We claim that $f(x)$ splits over this extension of $\mathbb{Q}$. First of all, we point out that $\sqrt{2}$ lives in this extension since

$$\left(\sqrt{2+\sqrt{2}}\right)^2 = 2 + \sqrt{2} \in \mathbb{Q}(\sqrt{2+\sqrt{2}}).$$

Now,

$$\sqrt{2+\sqrt{2}} \cdot \sqrt{2-\sqrt{2}} = \sqrt{(2-\sqrt{2})(2+\sqrt{2})} = \sqrt{4-2} = \sqrt{2}$$

which then yields the identity

$$\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}.$$

In particular, all roots of $f(x)$ will live in the field extension $\mathbb{Q}(\sqrt{2+\sqrt{2}})$. This clearly implies that this extension is the splitting field of the separable polynomial $f(x)$ and is hence Galois. Actually, $f(x)$ is the minimal polynomial of $\sqrt{2+\sqrt{2}}$ over $\mathbb{Q}$ since it is irreducible, and thus

$$\left[\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right) : \mathbb{Q}\right] = \deg f(x) = 4.$$

Let now $\mathcal{G}$ denote the Galois group of this extension, we know that $\mathcal{G} = 4$. Consider the automorphism $\sigma \in \mathcal{G}$ obtained by fixing $\mathbb{Q}$ and mapping

$$\sqrt{2+\sqrt{2}} \mapsto \sqrt{2-\sqrt{2}}.$$

Then,

$$(\sigma \circ \sigma)\left(\sqrt{2+\sqrt{2}}\right) = \sigma\left(\sqrt{2-\sqrt{2}}\right) = \frac{\sigma\left(\sqrt{2}\right)}{\sigma\left(\sqrt{2+\sqrt{2}}\right)} = \frac{\sigma\left(\sqrt{2}\right)}{\sqrt{2-\sqrt{2}}}.$$

[10] Let $\mathfrak{a}(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. Assume there exists a prime p dividing all coefficients other than a_n (we need $p \nmid a_n$) such that $p^2 \nmid a_0$. Then $\mathfrak{a}(x)$ is irreducible over $\mathbb{Q}$.

Since σ fixes $\mathbb{Q}$, we calculate further

$$2 + \sigma\left(\sqrt{2}\right) = \sigma\left(\sqrt{2+\sqrt{2}}\right)^2 = 2 - \sqrt{2}.$$

Of course, this means that $\sigma\left(\sqrt{2}\right) = -\sqrt{2}$. Returning to the previous equation, we have

$$(\sigma \circ \sigma)\left(\sqrt{2+\sqrt{2}}\right) = -\sqrt{2+\sqrt{2}}.$$

Thus, $\sigma^2 \not\equiv \mathbf{1}$. That is, σ has order larger than 2 and so $\langle\sigma\rangle$ must be the whole of $\mathcal{G}$. This makes $\mathcal{G}$ a *cyclic* group of order 4, and the only such group is $\mathbb{Z}/4\mathbb{Z}$. □

This final fact was given as an exercise during the course, but the proof is long and tedious. As such, we shall simply state it; perhaps one day it will be of use to the reader.

Proposition. *Let p and ℓ be primes and consider the polynomial $f(x) = x^p - \ell$ over $\mathbb{Q}$. Clearly, this polynomial is irreducible*[11]*. Let K be the splitting field of $f(x)$ over $\mathbb{Q}$. Then $K/\mathbb{Q}$ is Galois with Galois group*

$$\mathrm{Gal}\,(K/\mathbb{Q}) \cong \mathbb{F}_p \rtimes \mathbb{F}_p^\times.$$

In particular, $|\mathrm{Gal}(K/\mathbb{Q})| = \varphi(p^2)$.

[11] This is a direct consequence of Eiseinstein's criterion.