6.4.8

If p is a prime, let $\mathbb{Z}_{(p)}$ denote the subset of $\mathbb{Q}$ consisting of fractions $\frac{m}{n}$, with $m, n \in \mathbb{Z}$, $\gcd(m,n) = 1$, such that p does not divide n. Show that $\mathbb{Z}_{(p)}$ is a subring of $\mathbb{Q}$. Then show that the non-zero ideals of $\mathbb{Z}_{(p)}$ have the form (p^n), $n = 1, 2, 3, \ldots$.

Solution:

For the first part, use the two-step subring test. We first show that $\mathbb{Z}_{(p)}$ is closed under subtraction. Let $\frac{a}{b}, \frac{c}{d} \in \mathbb{Z}_{(p)}$, we must check that $\frac{a}{b} - \frac{c}{d}$ is in $\mathbb{Z}_{(p)}$.

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bd}{bd}$$

This fraction is in $\mathbb{Z}_{(p)}$, if p does not divide bd. But this must be the case since p does not divide either b or d, and p is prime. We must no show that $\mathbb{Z}_{(p)}$ is closed under products. With notation as above we have:

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

which lies in $\mathbb{Z}_{(p)}$ by the same argument as above.

To prove the second statement, we first note that the fraction $\frac{m}{n} \in \mathbb{Z}_{(p)}$ with $\gcd(m,n) = 1$ has an inverse in $\mathbb{Z}_{(p)}$ if and only if p does not divide m. Therefore, any proper ideal (ideal not equal to the entire ring) is contained in (p), the ideal generated by p. It is straightforward to check that also (p^n) is an ideal for any $n = 1, 2, 3, \ldots$, and that $(p^n) = (p^m)$ if and only if $m = n$. If a does not divide p, the ideal $(ap^n) = (p^n)$, since $\frac{1}{a} \in \mathbb{Z}_{(p)}$, so $\frac{1}{a}ap^n = p^n \in (p^n)$.

To complete the solution of the problem, we must show that any ideal in $\mathbb{Z}_{(p)}$ is principal. Let $I \subset \mathbb{Z}_{(p)}$ be an ideal. It is straightforward to check that $I \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$, and that the ideal of $\mathbb{Z}_{(p)}$ generated by $I \cap \mathbb{Z} \subset \mathbb{Z}_{(p)}$ is equal to I. So any ideal in $\mathbb{Z}_{(p)}$ is generated by an ideal of $\mathbb{Z}$. Since all ideal of $\mathbb{Z}$ are principal, so are the ideals of $\mathbb{Z}_{(p)}$.

7.5.16

Show that for any finite extension E of a finite field there is an element $\theta \in E$ such that $E = F(\theta)$. We call such an extension simple.

Solution:

By theorem 7.5.4 we know there is a generator θ of the multiplicative group of units of E. For this θ, we must clearly have $E \subseteq F(\theta)$, and the opposite inclusion $F(\theta) \subset E$ is clear since $F \subset E$ and $\theta \in E$.

7.5.17

Show that no finite field is algebraically closed. In fact, show that for every finite field F and every positive integer n, there is an irreducible polynomial over F of degree n.

Solution:

The first statement has the following simple proof. Consider the polynomial

$$\prod_{\alpha \in F} (x - \alpha) + 1$$

This polynomial has no roots in F, so F cannot be algebraically closed.

To prove the stronger statement in the exercise, let p be the characteristic of F. Then $F \simeq \mathbb{F}_{p^m}$ for some m. Consider the degree n field extension $\mathbb{F}_{p^m} \subset \mathbb{F}_{(p^m)^n}$. By exercise 7.5.16, this is a simple extension, generated by say θ. Then the minimal polynomial of θ over F is an irreducible polynomial of degree n.

7.6.2

Consider the smallest field E containing $\mathbb{F}_5$ and roots of $x^2 - 2 = 0$ and $x^2 - 3 = 0$. What is the degree of E over $\mathbb{F}_5$ A primitive polynomial of degree 2 over $\mathbb{F}_5$ is $f(x) = x^2 + x + 2$. Let θ be a root of $f(x)$. What powers of θ represent $\sqrt{2}$ and $\sqrt{3}$ respectively.

Solution:

We consider $\mathbb{F}_5[x]/(x^2 + x + 2)$. This field has degree 2 over $\mathbb{F}_5$. Since E cannot be $\mathbb{F}_5$, this field is the smallest possibility. We must now check that it contains the necessary elements. Computing low powers of θ gives:

$$\begin{array}{c|c} \theta^0 & 1 \\ \theta^1 & \theta \\ \theta^2 & -\theta - 2 \\ \theta^3 & -\theta + 2 \\ \theta^4 & 3\theta + 2 \\ \theta^5 & -\theta - 1 \\ \theta^6 & 2 \end{array}$$

From which we can read off that θ^3 is a root of $x^2 - 2$. Furthermore, we know that in $\mathbb{F}_5$, $2^{-1} = 3$, so $(\theta^6)^{-1} = 3$. Since the polynomial is primitive $\theta^{24} = 1$, so $\theta^{18} = (\theta^6)^{-1}$. Therefore $\theta^{18} = 3$, which implies that θ^9 is a square root of 3. We can check that $\theta^{12} = -1$, so the other square roots of 2 and 3 are θ^{15} and θ^{21} respectively.

7.6.3

Show that $x^4 + x^2 + 2x + 2$ is a primitive irreducible polynomial over $\mathbb{F}_5$. What is the degree of the extension of $\mathbb{F}_5$ generated by any root of this polynomial.

Solution:

Let θ be a root of $f = x^4 + x^2 + 2x + 2$. The field $\mathbb{F}_5(\theta)$ is a subfield of $F(\theta)$. The polynomial is primitive if and only if the root generates the multiplicative group $\mathbb{F}_{5^4}^*$, so we must check that θ has order $5^4 - 1 = 624$. With a computer algebra system it is easy to check this. The degree of the extension is 4, since f is the minimal polynomial of θ, and f has degree 4.

7.6.4

Use the preceding exercise to find the intermediate fields between $\mathbb{F}_{5^4}$ and $\mathbb{F}_5$.

Solution:

The Galois group $G(\mathbb{F}_{5^4}, \mathbb{F}_5)$ is the cyclic group with four elements. Intermediate fields correspond to subgroups. There is a single non-trivial subgroup of the cyclic group $\mathbb{Z}_4$, namely the one generated by 2. Thus, there is a single intermediate field $\mathbb{F}_{5^2}$.

7.6.5

Suppose that F is a finite field and $f(x) \in F[x]$ with $n = \deg f$. Define the *reciprocal polynomial* $f^*(x) = x^n f(\frac{1}{x})$. Intuitively, f^* is the polynomial with reversed coefficients. Prove the following two facts, assuming $f(x)$ is non-constant and $a_0 a_n \neq 0$.

a) The polynomial f is irreducible over F if and only if f^* is.

b) If $F = F_q$, a finite field, the polynomial f is primitive if and only if f^* is primitive.

Solution:

a) First note that $(f^*)^* = f$, so it will suffice to show that if f is reducible, so is f^*. Then note that if $f(x) = g(x)h(x)$, we have $f(\frac{1}{x}) = g(\frac{1}{x})h(\frac{1}{x})$, so $f^* = g^* h^*$.

b) If θ is a root of f, then θ^{-1} is a root of f^*. So if θ generates $\mathbb{F}(\theta)^*$, so does θ^{-1}.

First note that $(f^*)^* = f$, so to

Exam 2017: Problem 1

Let F be a field and consider the set of matrices:

$$U(F) = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \right\}$$

a) Show that $U(F)$ is a group under matrix multiplication. Is is abelian?

b) The group $U(F)$ has a subgroup

$$H = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & a & 1 \end{bmatrix} \right\}$$

Show that H is abelian and normal. If $F \simeq \mathbb{Z}_2$ which group is H?

c) Set $U = U(\mathbb{Z}_2)$. Let $Z \subset Z_2 \times Z_2 \times Z_2$ be the set $X = \{(1, y, z) | u, z \in \mathbb{Z}_2\}$. Show that U acts on X and that the action induces an injective group homomorphism $U \to S_4$ where S_4 is the permutation group of sets with 4 elements. Which subgroup of S_4 is it?

Solution:

a) We use the one-step subgroup test. Let $A, B \in U(F)$, with:

$$A = \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 \\ d & 1 & 0 \\ e & f & 1 \end{bmatrix}.$$

Then

$$AB^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -d & 1 & 0 \\ -e+df & -f & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ a-d & 1 & 0 \\ -af+b+df-e & c-f & 1 \end{bmatrix}$$

which lies in $U(F)$, so $U(F)$ is a subgroup of the group of 3×3 matrices.

b) Let $A, B \in H$, with

$$A = \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & a & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 \\ d & 1 & 0 \\ e & d & 1 \end{bmatrix}.$$

Then the product is

$$AB = \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & a & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ d & 1 & 0 \\ e & d & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ a+d & 1 & 0 \\ ad+b+e & a+d & 1 \end{bmatrix} = BA$$

Where the final equality follows since addition and multiplication are commutative.

To see if H is normal, we check that it is preserved by conjugation.

$$\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ d & 1 & 0 \\ e & d & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -a & 1 & 0 \\ ac-b & -c & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ d & 1 & 0 \\ e & d & 1 \end{bmatrix}$$

Since each element of the subgroup is preserved, the subgroup itself is preserved. If $F = \mathbb{Z}_2$, there are 4 elements in H, so there are two possiblities for which group it is. We have

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

so H has an element of order larger than 2. So H cannot be $\mathbb{Z}_2 \times \mathbb{Z}_2$, so it must be $\mathbb{Z}_4$.

c) The action of U on X is defined by regular matrix multiplication.

$$\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \begin{bmatrix} 1 \\ x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ a+x \\ b+cx+y \end{bmatrix}$$

Since it is a group action on a set with four elements, it gives a group homomorphims to the permutation group S_4. To see that this map is injective, assume that

$$\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \begin{bmatrix} 1 \\ x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ x \\ y \end{bmatrix}$$

for all $x, y \in \mathbb{Z}_2$. By comparing the second coordinate, we see that a must be zero. Setting $x = 0$ and comparing the third coordinate gives that likewise b must be zero. Then finally, setting $x = 1$ and comparing third coordinates we find that c must be zero, hence the matrix was the identity matrix.

To find the image subgroup, one first checks that the eight elements of U are generated by the two matrices

$$R = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \quad F = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Subject to the relation $RF = FR^3, F^2 = I, R^4 = I$. This shows that U is isomorphic to D_4, and therefore the image subgroup must be $D_4 \subset S_4$.

Exam 2017: Problem 3

Let ω be the complex number $\omega = e^{\frac{2\pi i}{12}}$. Let $f(x) = x^6 + 1 \in \mathbb{Q}[x]$. Note that if α is a root for f then so is α^{2k+1} for any integer k and that $-\alpha = \alpha^7$.

a) Show that $f(x) = g(x)h(x)$ where $h(x)$ has degree 2 and $g(x)$ has degree 4. Hint: i is a root of f.

b) Show that $\mathbb{Q}(\omega)$ is the splitting field for $f(x)$

Solution:

a) Since f has only real coefficients, we know that $-i$ is another root of f. Therefore $h(x) = x^+1$ divides f, so we can write $f(x) = g(x)h(x)$ for some degree 4 polynomial g.

b) Following the hint we find that $\omega, \omega^3, \omega^5, \omega^7, \omega^9, , \omega^11$ are roots of f. From the definition of ω we see that they are all distinct. Thus, f has six roots in $\mathbb{Q}(\omega)$ and since the degree of f is six, $\mathbb{Q}(\omega)$ must be its splitting field.