D-MATH
Prof. Brent Doran

Algebra II

FS 2014

Solutions

Rings & Fields

1. A review of the semester. Motivate your answers with either a proof or a counter-example.

   (a) Is the quotient of an integral domain necessarily an integral domain ?

   Solution : No. The ring of integers $\mathbb{Z}$ is an integral domain, but its quotient $\mathbb{Z}/6\mathbb{Z}$ is not.

   (b) Is the ring $R = \mathbb{Z}[x]/(x^3 + 1, 2)$ actually a field ?

   Solution : This ring is isomorphic to $\mathbb{F}_2[x]/(x^3 + 1)$ (cf. exercise sheet 1). Since $x^3 + 1$ factors over $\mathbb{F}_2$ into $(x + 1)(x^2 - x + 1)$, the ideal it generates is not maximal and the quotient ring is not a field.

   (c) Find all the ideals of R.

   Solution : By the previous subquestion, the problem reduces to finding all ideals of $\mathbb{F}_2[x]$ containing (x^3+1). Since $\mathbb{F}_2$ is a field, its polynomial ring must be a principal ideal domain and therefore a unique factorization domain. This means that the only proper non-trivial ideals are $(x + 1)$ and $(x^2 - x + 1)$.

   (d) Is $x^5 + 867x^4 + 153x + 351$ irreducible over $\mathbb{Z}$?

   Note : This exercise has been dropped from the exam. There was unfortunately a mix-up in the coefficients : The idea would have been to have a decomposition $x^5 + (3 \cdot 17^2)x^4 + (3^2 \cdot 17)x + 3 \cdot 107$ and to apply Eisenstein criterion for $p = 3$. However this doesn't work with $3 \cdot 117 = 351$ as 117 is a power of 3. You might also have lost some time by checking whether reduction modulo primes would work and noted that this doesn't for small primes. Sorry for that.

   (e) Can you find algebraic elements of any degree over $\mathbb{Q}$?

   Solution : Yes : Take your solution to exercise 2(c) of problem set 4 !

   (f) Give an example of a field extension of degree 10.

   Solution : Take the irreducible polynomial $x^{10} - 2$. Then $\mathbb{Q}(\sqrt[10]{2})$ has degree 10 over $\mathbb{Q}$.

   (g) Is the regular 7-gon constructible ? What about the regular 8-gon ?

   Solution : You know from the lecture that if a regular p-gon is constructible then $p - 1$ must be a power of 2 (Corollary 15.5.9 in Artin). Therefore, the regular 7-gon can not be constructed. On the other hand, it is easy to give an explicit ruler-and-compass construction of the angle $\pi/4$.

(h) What is the degree of the splitting field of $x^4 + 4$ over $\mathbb{Q}$?
Solution : Obviously

$$x^4 + 4 = (x^2 + 2i)(x^2 - 2i)$$

and the polynomial splits further when one notes that

$$(\pm 1 \pm i)^2 = 2i \qquad \text{and} \qquad (\pm 1 \mp i)^2 = -2i.$$

Hence the splitting field is $\mathbb{Q}(\sqrt{-1})$ and since the polynomial does not split over $\mathbb{Q}$, this extension has degree 2 over $\mathbb{Q}$.

(i) Consider the rings

$$\mathbb{Z}/(5) \times \mathbb{Z}/(5), \quad \mathbb{Z}/(25), \quad \mathbb{F}_{25}.$$

Say which one are fields and which ones are isomorphic to each other.
Solution : By definition, $\mathbb{F}_{25}$ is the finite field of 25 elements. The ring $\mathbb{Z}/(25)$ is not a field since e.g. 5 has no multiplicative inverse. Although $\mathbb{Z}/(5) \times \mathbb{Z}/(5)$ is a product of fields, it is itself not a field as (1,0) has no multiplicative inverse. The first two rings are not isomorphic to each other since e.g. the product ring contains no elements of order 25.

2. In this exercise, we compare

$$R_p = \mathbb{F}_p[x]/(x^2 - 2) \quad \text{and} \quad S_p = \mathbb{F}_p[x]/(x^2 - 3).$$

(a) Exhibit an explicit isomorphism between R_2 and S_2.
Solution : Consider the automorphism of $\mathbb{F}_2[x]$ sending 1 to 1 and x to $x+1$. By direct computation in $\mathbb{F}_2[x]$, one can check that

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

Hence φ descends to an isomorphism between R_2 and S_2.

(b) Prove that R_5 is a field, and that it has 25 elements.
Solution : Equivalently, we want to show that $x^2 - 2$ generates a maximal ideal. Since $\mathbb{F}_5$ is a field, it suffices to show that $x^2 - 2$ is irreducible over $\mathbb{F}_5$. This is clear as one can check directly that $x^2 - 2$ has no root in $\mathbb{F}_5$.
Any polynomial $f(x) \in R_5$ is a polynomial over $\mathbb{F}_5$ of degree $\leqslant 1$. It follows that there are exactly $5 \cdot 5 = 25$ possibilities.
(In fact, let $f(x) \in \mathbb{F}_5[x]$. By division with remainder, one can find polynomials $q(x)$ and $r(x)$ over $\mathbb{F}_5$ such that

$$f(x) = q(x)(x^2 - 2) + r(x),$$

where the degree of $r(x)$ is at most 1. Quotienting by the ideal $(x^2 - 2)$ in $\mathbb{F}_5[x]$ yields the claim.)

(c) Are R_5 and S_5 isomorphic ? What about R_{11} and S_{11} ?

Solution : One can quickly check that x^2-3 is also irreducible over $\mathbb{F}_5$, hence S_5 is also a field, and by the same line of argument as in (b), also contains 25 elements. Because all fields of same order are isomorphic, R_5 and S_5 are isomorphic.

On the other hand, one can check directly that x^2-2 is irreducible over $\mathbb{F}_{11}$, but

$$(5)^2 - 3 = 0,$$

and thus S_{11} is not a field.

3. We give here a direct proof that $\mathbb{Z}[\sqrt{5}]$ is not a unique factorization domain.

(a) Exhibit a factorization of x^2+x-1 into two linear polynomials over $\mathbb{Q}(\sqrt{5})$.

Solution :

$$x^2 + x - 1 = \left(x + \frac{1+\sqrt{5}}{2}\right)\left(1 + \frac{1-\sqrt{5}}{2}\right).$$

(b) Prove that x^2+x-1 is irreducible over $\mathbb{Z}[\sqrt{5}]$.

Solution : From the factorization above, we know that x^2+x-1 has two distinct roots in $\mathbb{Q}(\sqrt{5})$. Since a polynomial of degree 2 over a field can have no more than two roots and $\mathbb{Z}[\sqrt{5}] \subset \mathbb{Q}(\sqrt{5})$, there are no possible roots in $\mathbb{Z}[\sqrt{5}]$. Hence the polynomial must be irreducible.

(c) Conclude that $\mathbb{Z}[\sqrt{5}]$ is not a unique factorization domain.

Solution : Assume by contradiction that $\mathbb{Z}[\sqrt{5}]$ is a unique factorization domain. Then, by Gauss lemma, x^2+x-1 is reducible in $\mathbb{Z}[\sqrt{5}]$, which is false by (b).

4. Let p be a prime. We show that x^p-2 is irreducible over $\mathbb{Q}[\zeta_p]$, where ζ_p denotes the p-th root of unity.

(a) Why is $[\mathbb{Q}[\zeta_p, \sqrt[p]{2}] : \mathbb{Q}] \leqslant p(p-1)$ true ?

Solution : Recall that ζ_p has irreducible polynomial $x^{p-1} + \cdots + x + 1$, so $[\mathbb{Q}[\zeta_p] : \mathbb{Q}] = p-1$. The polynomial $x^p - 2$ is well defined over $\mathbb{Q}[\zeta_p]$ and has root $\sqrt[p]{2}$, so $[\mathbb{Q}[\zeta_p, \sqrt[p]{2}] : \mathbb{Q}[\zeta_p]] \leqslant p$. Since both $\mathbb{Q}[\sqrt[p]{2}]$ and $\mathbb{Q}[\zeta_p]$ are subfields of $\mathbb{Q}[\zeta_p, \sqrt[p]{2}]$, we can conclude with the multiplicative property of the degree.

(b) Show that $[\mathbb{Q}[\zeta_p, \sqrt[p]{2}] : \mathbb{Q}] = p(p-1)$.

Solution : Furthermore, still by the multiplicative property of the degree, both p and $p-1$ must divide $[\mathbb{Q}[\zeta_p, \sqrt[p]{2}] : \mathbb{Q}]$. Together with (a), this yields the statement.

(c) Conclude that $x^p - 2$ is irreducible over $\mathbb{Q}[\zeta_p]$.

Solution : The statement now follows from

$$\begin{aligned} p(p-1) &= \left[\mathbb{Q}[\zeta_p, \sqrt[p]{2}] : \mathbb{Q}\right] \\ &= \left[\mathbb{Q}[\zeta_p, \sqrt[p]{2}] : \mathbb{Q}[\zeta_p]\right] [\mathbb{Q}[\zeta_p] : \mathbb{Q}] \\ &= \left[\mathbb{Q}[\zeta_p, \sqrt[p]{2}] : \mathbb{Q}[\zeta_p]\right] (p-1). \end{aligned}$$

5. On square roots in finite fields. Let F be a finite field of $q = p^r$ elements. We say that $a \in F$ has a square root if the congruence equation $x^2 \equiv a \bmod q$ has a solution.

(a) Show that $F^\times \to F^\times, x \mapsto x^2$ is a group homomorphism.

Solution : Since $F^\times$ is a cyclic group, it is abelian, and the map above is a homomorphism.

(b) Show that if $p = 2$ then every element has a square root in F.

Solution : If $p = 2$, $F^\times$ has odd order $2^r - 1$ and the kernel of the above homomorphism is trivial.

(c) Show that, if $p > 2$, the non-zero square roots of F are exactly the solutions to $x^{\frac{q-1}{2}} \equiv 1 \bmod q$. Deduce that -1 is a square root in F if and only if $q \equiv 1 \bmod 4$.

Solution : Since p is an odd prime, $q - 1$ must be even and

$$x^2 \equiv a \mod q \quad \iff \quad x^{q-1} \equiv a^{\frac{q-1}{2}} \mod q.$$

Now recall that every non-zero element of F is a root of the polynomial $x^{q-1} - 1$.

For the second statement, observe that $(-1)^{\frac{q-1}{2}} = 1$ if and only if 2 divides $(q-1)/2$, therefore if and only if $q \equiv 1 \bmod 4$.

(d) Consider the subfield K generated by $\{x^3 : x \in F\}$. Show that if K is not the whole of F, then F must be isomorphic to $\mathbb{F}_4$.

Solution : The map $F^\times \to K^\times$ has in (a) has range of order $\geqslant \frac{q-1}{3}$. Moreover, by assumption, $\#F = (\#K)^n$, for some $n \geqslant 2$. Combining these two facts, we have

$$\begin{aligned} \#K &\geqslant \frac{1}{3}(\#F - 1) + 1 \\ &\geqslant \frac{1}{3}\left((\#K)^2 - 1\right) + 1 \\ &= \frac{1}{3}(\#K - 1)(\#K + 1) + 1 \\ \implies \#K &\leqslant 2. \end{aligned}$$

Equality holds if and only if $n = 2$, and in this case $\#F = 4$.