UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
APPLIED ALGEBRA - MEM244 (FALL SEMESTER 2019-20)
LECTURER: G. KAPETANAKIS

1st exercise set - Answers

Exercise 1. Let a be an element of finite order k in the multiplicative group G. Show that for $m \in \mathbb{Z}$ we have $a^m = e$ if and only if $k \mid m$, where e stands for the identity element of G.

Answer. ($\Rightarrow$) Suppose $a^m = e$. Then, by Euclidean division, we have that there exists some $q, r \in \mathbb{Z}$, with $0 \leq r < k$ such that $m = qk + r$. It follows that

$$a^m = e \Rightarrow (a^k)^q a^r = e \Rightarrow a^r = e.$$

The minimality of e yields that $r = 0$ and the result follows.

($\Leftarrow$) $k \mid m$ implies that $m = k\ell$ for some ℓ. Hence

$$a^m = a^{k\ell} = (a^k)^\ell = e.$$

□

Exercise 2. For a commutative ring of prime characteristic p, show that

$$(a_1 + \cdots + a_s)^{p^n} = a_1^{p^n} + \cdots a_s^{p^n}$$

for all $a_1, \ldots, a_s \in R$ and $n \in \mathbb{N}$.

Answer. Let R commutative ring of characteristic p. We know that for every $a, b \in R$,

$$(a + b)^p = a^p + b^p.$$

It follows that

$$\begin{aligned}(a_1 + \cdots + a_s)^p &= (a_1 + \cdots + a_{s-1})^p + a_s^p \\ &= (a_1 + \cdots + a_{s-2})^p + a_{s-1}^p + a_s^p \\ &= \ldots \\ &= a_1^p + \cdots + a_s^p.\end{aligned}$$

The latter yields:

$$\begin{aligned}(a_1 + \cdots + a_s)^{p^n} &= (a_1^p + \cdots + a_s^p)^{p^{n-1}} \\ &= (a_1^{p^2} + \cdots + a_s^{p^2})^{p^{n-2}} \\ &= \ldots \\ &= a_1^{p^n} + \cdots + a_s^{p^n}\end{aligned}$$

□

Exercise 3. Let R be a commutative ring with a unit that does not have any zero-divisors. Show that $\operatorname{char} R = 0$ or p, where p is a prime number. Deduce that a finite field has prime characteristic.

Answer. Assume that $\operatorname{char} R = mn$, where $m, n \in \mathbb{Z}_{>1}$. It follows that

$$\mu := \underbrace{1 + \cdots + 1}_{m-\text{times}} \neq 0 \quad \text{and} \quad \nu := \underbrace{1 + \cdots + 1}_{n-\text{times}} \neq 0,$$

since $m, n < \operatorname{char} R$. However

$$\mu \cdot \nu = \underbrace{1 + \cdots + 1}_{mn-\text{times}} = 0,$$

that is, R has zero-divisors, a contradiction. The proof of the first statement is now complete.

The second statement follows immediately from the first. □

Exercise 4. Take $n > 1$ a square-free integer and the integral domain $\mathbb{Z}[\sqrt{-n}] := \{a + b\sqrt{-n} \mid a, b \in \mathbb{Z}\}$. Show that $\mathbb{Z}[\sqrt{-n}]^* = \{\pm 1\}$.

Answer. Define

$$\begin{aligned} \nu \ : \ \mathbb{Z}[\sqrt{-n}] &\to \mathbb{Z}_{\geq 0}, \\ a + b\sqrt{-n} &\mapsto a^2 + nb^2. \end{aligned}$$

It is not hard to check that for $x, y \in \mathbb{Z}[\sqrt{-n}]$, $\nu(xy) = \nu(x)\nu(y)$ and that $\nu(x) = 0 \iff x = 0$. It follows that $x \in \mathbb{Z}[\sqrt{-n}]^*$ implies $\nu(x) = 1$. We have that

$$\nu(a + b\sqrt{-n}) = 1 \iff a^2 + nb^2 = 1 \iff a = \pm 1 \text{ and } b = 0.$$

The result follows. □

Exercise 5. Take n as in Exercise 4. In addition, assume that n is not a prime and take p a prime divisor of n.

1. Show that p is not a prime in $\mathbb{Z}[\sqrt{-n}]$.
2. Show that p is irreducible in $\mathbb{Z}[\sqrt{-n}]$.

Answer.

1. Assume that p is prime. We have that $p \mid -n = (\sqrt{-n})^2$, hence $p \mid \sqrt{-n} \iff \nu(p) \mid \nu(\sqrt{-n}) \iff p^2 \mid n$, where ν as in the answer of Exercise 4. The latter is impossible because n is square-free.

2. Let $a, b, c, d \in \mathbb{Z}$, such that $p = (a + b\sqrt{-n})(c + d\sqrt{-n})$. It follows that $\nu(a + b\sqrt{-n})\nu(c + d\sqrt{-n}) = \nu(p) = p^2$, i.e.,

$$\nu(a + b\sqrt{-n}) = 1, p \text{ or } p^2.$$

In the first case, $a+b\sqrt{-n} = \pm 1$, hence a unit. In the last case $c+d\sqrt{-n} = \pm 1$, hence a unit. So, the only case left to check is $\nu(a + b\sqrt{-n}) = p$. However, this implies

$$a^2 + nb^2 = p.$$

Since $p \mid n$ and p is prime, while n is non-prime, we get that $p < n$ and that above implies $b = 0$, which in turn implies $a^2 = p$, impossible. It follows that either $a + b\sqrt{-n}$ or $c + d\sqrt{-n}$ is a unit, that is, p is irreducible. □

Exercise 6. Take n as in Exercise 4. In addition, assume that $n + 1$ is not a prime and take p a prime divisor of $n + 1$.

1. Show that p is not a prime in $\mathbb{Z}[\sqrt{-n}]$.
2. Show that p is irreducible in $\mathbb{Z}[\sqrt{-n}]$.

Answer. 1. Assume that p is prime. We have that $p \mid n+1 = (1+\sqrt{-n})(1-\sqrt{-n})$, hence $p \mid 1 + \sqrt{-n}$ or $p \mid 1 - \sqrt{-n}$. Either case, implies that there exist some $a, b \in \mathbb{Z}$, such that $1 \pm \sqrt{-n} = pa + pb\sqrt{-n}$. The latter is clearly impossible.

2. Let $a, b, c, d \in \mathbb{Z}$, such that $p = (a + b\sqrt{-n})(c + d\sqrt{-n})$. It follows that $\nu(a + b\sqrt{-n})\nu(c + d\sqrt{-n}) = \nu(p) = p^2$, i.e.,

$$\nu(a + b\sqrt{-n}) = 1, p \text{ or } p^2.$$

In the first case, $a+b\sqrt{-n} = \pm 1$, hence a unit. In the last case $c+d\sqrt{-n} = \pm 1$, hence a unit. So, the only case left to check is $\nu(a + b\sqrt{-n}) = p$. However, this implies

$$a^2 + nb^2 = p.$$

Since $p \mid n + 1$ and p is prime, while $n + 1$ is non-prime, we get that $p \leq 2(n + 1)$, i.e., $p < n$. Now, the above implies $b = 0$, which in turn implies $a^2 = p$, impossible. It follows that either $a + b\sqrt{-n}$ or $c + d\sqrt{-n}$ is a unit, that is, p is irreducible. □

Exercise 7. Take $n > 2$ a square-free integer. Show that $\mathbb{Z}[\sqrt{-n}]$ is not a principal ideal domain.

Answer. In every PID, we know that all irreducible elements are prime. However, since $n > 2$, at least one of $n, n + 1$ is even and ≥ 4, hence non-prime divisible by $p = 2$. Now Exercises 5 and 6 imply that $p = 2$ is irreducible but not prime in $\mathbb{Z}[\sqrt{-n}]$. □

Exercise 8. Let R be a commutative ring with a unit. Show that

$$R[X]/\langle X^6 - X^5 + X - 1\rangle$$

is not a field.

Answer. $R[X]/\langle X^6 - X^5 + X - 1\rangle$ is a field iff $\langle X^6 - X^5 + X - 1\rangle$ is maximal, which holds iff $X^6 - X^5 + X - 1$ is irreducible. The latter however is not true, since

$$X^6 - X^5 + X - 1 = (X - 1)(X^5 + 1).$$

□

Exercise 9.

1. Find all the genuine ideals $I \trianglelefteq \mathbb{Z}$, such that $\langle 24\rangle \subseteq I$. Which of those are maximal?
2. Find all the genuine ideals $I \trianglelefteq \mathbb{Q}[x]$, such that $\langle x^3 - 4x^2 + 5x - 2\rangle \subseteq I$. Which of those are maximal?

Answer. If R is a PID's, we have that if $I, J \trianglelefteq R$, then $I \subseteq J$ iff $I = \langle i\rangle$ and $J = \langle j\rangle$ for some $j \mid i$. It follows that identifying the ideals J such that $I \subseteq J$ is equivalent to identifying the divisors of i.

1. According to the above, $\langle 24\rangle \subseteq I \iff I = \langle i\rangle$, for some $i \mid 24$. Since $24 = 2^3 3$, the divisors of 24 are

   $$1, 2, 4, 8, 3, 6, 12 \text{ and } 24.$$

   Since $\langle 1\rangle = \mathbb{Z}$, we exclude 1. The ideals in question are

   $$\langle 2\rangle, \langle 4\rangle, \langle 8\rangle, \langle 3\rangle, \langle 6\rangle, \langle 12\rangle \text{ and } \langle 24\rangle.$$

   Since maximal ideals are generated by irreducible elements, the maximal ideals of the above list are $\langle 2\rangle$ and $\langle 3\rangle$.

2. The answer of this item is similar the first one's, once we notice that

   $$x^3 - 4x^2 + 5x - 2 = (x - 1)^2(x - 2).$$

□