MATH 210B

Name: Quin Darcy
Instructor: Dr. Shannon

Due Date: 1/29/20
Assignment: Homework 1

2. Prove that 2 is irreducible in $\mathbb{Z}[\sqrt{10}]$.

Proof. Define $N\colon \mathbb{Z}[\sqrt{10}] \to \mathbb{Z}$ by $N(a+b\sqrt{10}) = (a+b\sqrt{10})(a-b\sqrt{10})$. Suppose $2 = (a+b\sqrt{10})(c+d\sqrt{10})$ for some $a, b, c, d \in \mathbb{Z}$. Evaluating this we get that

$$\begin{aligned} N(2) &= 4 \\ &= N\big((a+b\sqrt{10})(c+d\sqrt{10})\big) \\ &= N\big((a+b\sqrt{10})\big)N\big((c+d\sqrt{10})\big) \\ &= (a^2-10b^2)(c^2-10d^2). \end{aligned}$$

This yields two cases:

(i) $a^2-10b^2 = 4$ and $c^2-10d^2 = 1$. The solutions to these two equations are $a = \pm 2$, $b = 0$, $c = \pm 1$, and $d = 0$. Thus, $2 = a \cdot c = 2 \cdot 1$, or $2 = a \cdot c = (-2)\cdot(-1)$. Both of these solutions imply 2 is irreducible.

(ii) $a^2 - 10b^2 = 2$ and $c^2 - 10d^2 = 2$. Let $a = 10q + r$ where $0 < r < 10$, then $a^2 - 10b^2 = 100q^2 + 20qr + r^2 - 10b^2 = 10(10q^2 + 2qr - b^2) + r^2 = 2$. Letting $x = 10q^2 + 2qr - b^2$, we have that $2 - r^2 = 10x$ which has no solutions for all $r = 1, 2, \ldots, 9$. Similarly, we get the same result for $10x = -2 - r^2$. Thus, there are no solutions in this case.

Thus, 2 is irreducible in $\mathbb{Z}[\sqrt{10}]$. □

3. Assume that F and E are fields, and that $\varphi\colon F \to E$ is a ring homomorphism.

(a) If there exists $a \in F - \{0\}$ such that $\varphi(a) = 0$, then determine, with explanation, what can be concluded about φ.

Solution. Since $\varphi(a) = 0$ and $a \neq 0$ by assumption, then $\ker\varphi \neq \{0\}$ and so φ is not 1-1. Additionally, we have that for all $b \in F$, $\varphi(ab) = \varphi(a)\varphi(b) = 0\varphi(b) = 0$. Thus, $\varphi\big((a)_i\big) = 0$. Lastly, since F is a field and $a \neq 0$, then $(a)_i = F$ and so $\varphi(F) = 0$. Thus, $F = \ker\varphi$ and by the Fundamental Isomorphism Theorem, $\mathrm{im}(\varphi) \cong \{0\}$.

(b) If there does not exist $a \in F - \{0\}$ such that $\varphi(a) = 0$, then determine, with explanation, what can be concluded about φ, and prove that $\varphi(1_F) = 1_E$.

Solution. If there does not exist $a \in F - \{0_F\}$ such that $\varphi(a) = 0_E$, then $\ker\varphi = \{0\}$ and φ is 1-1. Additionally, we have that $\varphi(1_F) = \varphi(1_F \cdot 1_F) = \varphi(1_F)\cdot\varphi(1_F) = \big(\varphi(1_F)\big)^2$. Thus, $\big(\varphi(1_F)\big)^2 - \varphi(1_F) = 0_E$. Since E is a field (and so it is an integral domain), then by cancellation we have that $\varphi(1_F) = 0$ or $\varphi(1_F) = 1_E$. However, since $\ker\varphi = \{0_F\}$, then $\varphi(1_F) \neq 0_E$ and thus $\varphi(1_F) = 1_E$. Finally, by the Fundamental Isomorphism Theorem, we have that $\mathrm{im}(\varphi) \cong F/\{0\} \cong F$. Thus, there is an isomorphic copy of F in E.

8. Assume that V is a vector space over F, that $v \in V$ and $a \in F$. Prove the following

   (a) $0v = 0$.

   Proof. Since $0v = (0+0)v = 0v + 0v$, then subtracting $0v$ from both sides we obtain $0 = 0v$. □

   (b) $(-a)v = -(av)$.

   Proof. We have that

$$\begin{aligned}(-a)v &= (-a)v + 0\\ &= (-a)v + \big(av - (av)\big)\\ &= \big((-a)v + av\big) - (av)\\ &= \big((-a) + a\big)v - (av)\\ &= 0v - (av)\\ &= 0 - (av)\\ &= -(av).\end{aligned}$$

   □

9. Assume that $\theta\colon \mathbb{Q} \to \mathbb{R}$ is a ring homomorphism, and that $\theta(\mathbb{Q}) \neq 0$. Find, with explanation, the range of θ, and what can be concluded about θ.

   Solution. Since both $\mathbb{Q}$ and $\mathbb{R}$ are fields, then by problem 3, part (b), we can conclude that θ is 1-1, $\theta(1) = 1$, and the range of θ is isomorphic to $\mathbb{Q}$. Since $\mathbb{Q} \subseteq \mathbb{R}$, then θ is the identity map.

10. Assume that V is a vector space over F, and that $\{v_1, \ldots, v_k\}$ is a linearly dependent subset of V, and $v_1 \neq 0$. Prove that there exists i, $1 < i \leq k$, such that $v_i \in \langle\{v_1, \ldots, v_{i-1}\}\rangle$.

    Proof. By the definition of linear independence, there exists $v_1, \ldots, v_i \in \{v_1, \ldots, v_k\}$ and there exists $a_1, \ldots, a_i \in F$, not all zero, such that $a_1v_1 + \cdots + a_iv_i = 0$. Thus, $v_i = -\frac{a_1}{a_i}v_1 - \cdots - \frac{a_{i-1}}{a_i}v_{i-1} \in \langle\{v_1, \ldots, v_{i-1}\}\rangle$. □

11. Prove that if $w \in \langle v_1, \ldots, v_k\rangle$, then $\langle v_1, \ldots, v_k\rangle = \langle w, v_1, \ldots, v_k\rangle$.

Proof. Let $x \in \langle v_1, \ldots, v_k \rangle$, then taking $b = 0$ we can write

$$x = bw + \sum_{i=1}^{k} c_i v_i,$$

for $c_1, \ldots, c_k \in F$. Thus, $x \in \langle w, v_1 \ldots, v_k \rangle$. Hence, $\langle v_1, \ldots, v_k \rangle \subseteq \langle w, v_1, \ldots, v_k \rangle$. Now let $x \in \langle w, v_1, \ldots, v_k \rangle$. Then for some $b, c_1, \ldots, c_k \in F$, we have that

$$x = bw + \sum_{i=1}^{k} c_i v_i.$$

However, since $w \in \langle v_1, \ldots, v_k \rangle$, then for some $a_1, \ldots, a_k \in F$, $w = \sum_{i=1}^{k} a_i v_i$, thus,

$$x = \sum_{i=1}^{k} a_i v_i + \sum_{i=1}^{k} c_i v_i = \sum_{i=1}^{k} (a_i + c_i) v_i.$$

Thus, $x \in \langle v_1, \ldots, v_k \rangle$. This means that, $\langle w, v_1, \ldots, v_k \rangle \subseteq \langle v_1, \ldots, v_k \rangle$. Therefore, $\langle v_1, \ldots, v_k \rangle = \langle w, v_1, \ldots, v_k \rangle$. □

12. Assume that $\{v_1, \ldots, v_n\}$ is a basis for V over F, that $v \in V$, and that there exists $a_1, \ldots, a_n \in F$, and $b_1, \ldots, b_n \in F$ such that

$$v = \sum_{i=1}^{n} a_i v_i = \sum_{i=1}^{n} b_i v_i.$$

Prove that for all i, $a_i = b_i$.

Proof. By assumption, we have that

$$\sum_{i=1}^{n} a_i v_i - \sum_{i=1}^{n} b_i v_i = \sum_{i=1}^{n} (a_i - b_i) v_i = 0.$$

Since $\{v_1, \ldots, v_n\}$ is a basis, then this set is linearly independent. Thus, $a_i - b_i = 0$ for all i. Therefore, $a_i = b_i$ for all i. □

13. Prove that if p is prime, then each element of $\mathbb{Z}_p$ is a root of $x^p - x$.

Proof. Letting $x^p - x = 0$, we can factor out an x to obtain $x(x^{p-1} - 1) = 0$. In MATH 210A, we proved that $\mathbb{Z}_p$ is a field for any prime p, thus we are allowed the cancellation property. Hence, $x = 0$ or $x^{p-1} - 1 = 0$. The latter is equivalent to $x^{p-1} \equiv 1 (\text{mod } p)$. Since p is prime, then for all $x = 1, 2, \ldots, p - 1$, the congruence is satisfied. Therefore, all elements of $\mathbb{Z}_p$ are roots of $x^p - x$. □