MATH 210A

Name: Quin Darcy **Due Date:** 11/27/19
Instructor: Dr. Shannon **Assignment:** Homework 10

5. Assume that D is an integral domain, and char(D) is finite. Prove that char(D) is prime.

   Proof. Let char$(D) = n$. Assume $n = kr$ for $1 < k < n$ and $1 < r < n$. In class we proved that char(D) is the least positive integer for which $n1 = 0$. Additionally, by part 4.(b), we have that $(kr)1 = (k1) \cdot (r1) = 0$. Since there are no zero divisors, then either $k1 = 0$ or $r1 = 0$. However, since $k, r < n$, then this contradicts char$(D) = n$. Therefore, n is not composite and must be prime. □

6. Prove that if F is a field, then the only ideals of F are $\{0\}$ and F.

   Proof. Suppose $a \neq 0$ and let $(a) \subseteq_i F$. Let $x \in F$. Then since $a^{-1} \in F$, then $a^{-1} \cdot x \in F$. Thus, $a \cdot (a^{-1} \cdot x) = x \in (a)$. Thus, $F \subseteq (a)$ and, by definition $(a) \subseteq F$. Hence, $F = (a)$. Now suppose $a = 0$. Then $(a) = \{0\}$. Therefore, the only ideals of F are $\{0\}$ and F. □

7. Assume that $(R, +, \cdot)$ is a field, $(S, \star, \#)$ is a ring, and that $\alpha\colon R \to S$ is a ring homomorphism of R onto S. Prove that either α is an isomorphism or $S = \{0\}$.

   Proof. Let $x, y \in R$ such that $x \neq y$. Assume that $f(x) = f(y)$. Then $f(x) - f(y) = f(x - y) = 0$. Since $x \neq y$, then $x - y \neq 0$ and thus there exists $(x - y)^{-1} \in R$. Hence, $f(x - y) \# f((x - y)^{-1}) = f((x - y) \cdot (x - y)^{-1}) = f(1_R) = 0$. Thus, $1_R \in \ker \alpha$. Since $\ker \alpha$ is an ideal of R, and $1_R \in R$, then $\ker \alpha = R$. Moreover, since α is onto, then $\ker \alpha = R$ implies $S = \{0\}$. Now suppose that $\ker \alpha \neq R$. Then since R is a field and $\ker \alpha$ is an ideal of R, then $\ker \alpha = \{0\}$. Thus, α is an isomorphism. □

8. Assume that $\theta\colon R \to S$ is an isomorphism onto S, and 1_R is an identity for R.

   (a) Prove that $\theta(1_R)$ is an identity for S.

   Proof. Consider $\theta(1_R) \in S$. Let $s \in S$. Since θ is an isomorphism, then there exists $r \in R$ such that $\theta(r) = s$. Then

   $$s \cdot \theta(1_R) = \theta(r) \cdot \theta(1_R) = \theta(r \cdot 1_R) = \theta(r) = s.$$

   Similarly, we get that $\theta(1_R) \cdot s = s$. Thus, for all $s \in S$, $\theta(1_R) \cdot s = s \cdot \theta(1_R) = s$. Finally, assume there exists $x \in S$ such that for all $s \in S$, $x \cdot s = s \cdot s = s$. Then $x = x \cdot \theta(1_R) = \theta(1_R)$. Hence, $\theta(1_R)$ is unique. Therefore, $\theta(1_R)$ is an identity for S. □

(b) Prove that if $x^2 = 1_R + 1_R$ has a solution in R, then $x^2 = 1_S + 1_S$ has a solution in S.

Proof. Let $a \in R$ denote a solution to $x^2 = 1_R + 1_R$. Then $a^2 = 1_R + 1_R$. Thus, $\theta(a^2) = \big(\theta(a)\big)^2 = \theta(1_R) + \theta(1_R) = 1_S + 1_S$. Therefore, $\theta(a)$ is a solution in S to $x^2 = 1_S + 1_S$. $\square$

(c) Prove that $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ are not isomorphic.

Proof. Assume that $\theta\colon \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$ is an isomorphism. In $\mathbb{Q}[\sqrt{2}]$ there is an element which satisfies $x^2 - 1 = 0$. Namely, $x = \sqrt{2}$. Then since θ is an isomorphism, then

$$\begin{aligned}\theta(x^2 - 2) &= \theta(x^2) - \theta(2)\\ &= \big(\theta(x)\big)^2 - \theta(1+1)\\ &= \big(\theta(x)\big)^2 - \big(\theta(1) + \theta(1)\big)\\ &= \big(\theta(x)\big)^2 - 2.\end{aligned}$$

Letting $x = \sqrt{2}$, we get that $\big(\theta(\sqrt{2})\big)^2 - 2 = 0$. This implies that there exists an element, namely, $\theta(\sqrt{2}) \in \mathbb{Q}[\sqrt{3}]$ whose square is 2. However, since no such element exists in $\mathbb{Q}[\sqrt{3}]$. Therefore, $\mathbb{Q}[\sqrt{2}] \ncong \mathbb{Q}[\sqrt{3}]$. $\square$

9. Assume that R is an integral domain. Prove that is a is prime, then a is irreducible. Prove that if R is a PID, then the converse hold.

Proof. Let $a \neq 0$ be prime. Assume that $a = bc$ for some $b, c \in R$. Then $a \mid bc$. Thus, $a \mid b$ or $a \mid c$. Without loss of generality, suppose $a \mid b$. Then there exists $k \in \mathbb{Z}$ such that $b = ak$. Thus, $a = bc = akc$. Thus, $a(1 - kc) = 0$. Since R is an integral domain, then either $a = 0$ or $1 - kc = 0$. Since we assumed $a \neq 0$, then it follows that $1 - kc = 0$ and so $1 = kc$. Therefore, $c \mid 1$ and a is irreducible.

Assume R is a PID and that a is irreducible. Then for a contradiction, assume there exists an ideal, I, of R such that $(a) \subsetneq I \subsetneq R$. Since R is a PID, then for some $u \in R$, $I = (u)$. Since $a \in I$, then $a = ur$ for some $r \in R$. Since a is irreducible, then either $u \mid 1$ or $r \mid 1$. If $u \mid 1$, then $u \cdot u^{-1} = 1 \in (u)$ which would imply $(u) = R$ and so this cannot occur. Hence, $r \mid 1$. Thus, $a \cdot r^{-1} = u$. Thus, $(u) = (a) = I$. Thus, (a) is maximal and by pg. 6, a is therefore prime. $\square$

10. Assume that R is a Euclidean domain, and that J is an ideal of R. Prove that there exists $b \in R$ such that $J = (b)$.

Proof. Let $J \subseteq R$ be a nonzero ideal of R. Let $a \in J$ such that $a \neq 0$ and $v(a)$ is a minimum of the set $\{v(x)\colon x \in J\}$. Since $a \in J$, then $aR \subseteq J$. Now suppose $b \in J$ such that $b \neq 0$. Then since R is a Euclidean domain, then there exists $q, r \in R$ such that $b = aq + r$ and $r = 0$ or $v(r) < v(a)$. Thus, $r = b - aq$. Since $b \in J$ and $-aq \in J$, then $r \in J$. Since $v(a)$ was assumed to be a minimum in J, then $v(a) \leq v(r)$. Thus, $v(r) \not< v(a)$. Hence, $r = 0$ and $b = aq$. Thus, $b \in aR$ which implies $J \subseteq aR$. Thus, $J = aR = (a)$. Therefore, J is a prime ideal. $\square$