Math 562 **Spring 2014**
Exam 2 — Thurs Apr 3 **Drew Armstrong**

There are 4 problems with 12 parts. Each part is worth 2 points, for a total of 24 points.

1. Let R be a ring (i.e. commutative with 1). We say $u \in R$ is a **unit** if there exists $u^{-1} \in R$ such that $uu^{-1} = 1$. Let $R^\times \subseteq R$ be the set of units. We define an equivalence relation on R (called **association**) by setting

$$\text{“}\, a \sim b \,\text{”} \iff \text{“}\, \exists\, u \in R^\times \text{ such that } a = ub \,\text{”}.$$

(a) Given $a \in R$, we define the **principal ideal** $(a) := \{ar : r \in R\}$. Prove that for that for all $a, b \in R$ we have “ $a \sim b$ ” $\Rightarrow$ “ $(a) = (b)$ ”.

Proof. Assume that $a \sim b$ so that we have $a = ub$ for some unit $u \in R^\times$. Then for any $r \in R$ we have $ar = b(ur) \in (b)$ hence $(a) \leq (b)$. Conversely, since u is invertible we have $b = u^{-1}a$ and then for all $r \in R$ we have $br = a(u^{-1}r) \in (a)$, hence $(b) \leq (a)$. $\square$

We say that R is a **domain** if for all $a \neq 0$ and $b \neq 0$ we have $ab \neq 0$.

(d) Prove that if R is a domain then for all $a, b \in R$ we have “ $(a) = (b)$ ” $\Rightarrow$ “ $a \sim b$ ”.

Proof. Assume that R is a domain and that $(a) = (b)$. If $a = 0$ then we also have $b = 0$ and hence $a \sim b$. Otherwise, assume that a and b are nonzero. Since $a \in (b)$ we have $a = br$ and since $b \in (a)$ we have $b = as$ for some $r, s \in R$, hence

$$\begin{aligned} a &= (as)r \\ a &= a(sr) \\ a - a(sr) &= 0 \\ a(1 - sr) &= 0. \end{aligned}$$

Since R is a domain and since $a \neq 0$ this implies that $1 - sr = 0$, i.e., $sr = 1$. Since $a = br$ with $r \in R^\times$ we conclude that $a \sim b$. $\square$

2. Let R be a domain. Given $p, d \in R$ we say that d is a **proper divisor** of p if

- d divides p,
- d is not a unit, and
- d is not associate to p (i.e. there is no $u \in R^\times$ such that $p = ud$).

We say that $p \in R$ is **irreducible** if it has no proper divisors.

(a) Given $a \in R$, prove that $(a) = R$ if and only if $a \in R^\times$. [Hint: See Problem 1.]

Proof. If $(a) = R$ then we have $1 \in (a)$ and hence there exists $r \in R$ such that $1 = ab$. We conclude that $a \in R^\times$. Conversely, if $a \in R$ then for all $r \in R$ we have $r = (aa^{-1})r = a(a^{-1}r) \in (a)$. We conclude that $(a) = R$. $\square$

We say that an ideal $I < R$ is **maximal** if there is no ideal J such that $I < J < R$ (where “$<$” means strict inclusion of ideals.)

(b) If $(p) < R$ is a maximal ideal, prove that $p \in R$ is irreducible.

Proof. We will prove the contrapositive. Assume that p is **reducible**. By the definition given, there exists $d \in R$ such that d divides p (i.e. $(p) \leq (d)$), d is not a unit (i.e. $(d) \neq R$ by part (a)), and d is not associate to p (i.e. $(p) \neq (d)$ by Problem 1). Thus we have strict inclusions of ideals

$$(p) < (d) < R$$

which means that (p) is **not maximal**. □

We say that R is a **PID** if every ideal $I \leq R$ has the form $I = (a)$ for some $a \in R$.

(c) Now let R be a PID. If $p \in R$ is irreducible, prove that (p) is a maximal ideal.

Proof. Let $p \in R$ be irreducible and suppose for contradiction that there exists an ideal J with strict inclusions $(p) < J < R$. Since R is a PID we have $J = (d)$ for some $d \in R$. But then, as in part (b), this d is a proper divisor of p, contradicting the fact that p is irreducible. □

3. In this problem let R be a **PID**.

(a) Suppose we have $a, p \in R$ such that p does not divide a. Prove that we have a strict containment of ideals $(p) < (a) + (p)$.

Proof. By definition we have $(a) + (p) = \{ar + ps : r, s \in R\}$. Thus for all $ps \in (p)$ we have $ps = a0 + ps \in (a) + (p)$, hence $(p) \leq (a) + (p)$. But if $(p) = (a) + (p)$ then since $a \in (a) + (p)$ we have $a \in (p)$ which contradicts the fact that p does not divide a. We conclude that $(p) < (a) + (p)$. □

(b) Now suppose that $p \in R$ from part (a) is **irreducible**. In this case, prove that there exist $x, y \in R$ such that $1 = ax + py$. [Hint: R is a PID. Use Problem 2.]

Proof. Since R is a PID we have $(a) + (p) = (d)$ for some $d \in R$. Since $(p) < (d)$ and since p is irreducible we must have $(d) = R$ (otherwise d is a proper divisor of p). Then since $(a) + (p) = (d) = R$ we have $1 \in (a) + (p)$, so there exist $x, y \in R$ such that $1 = ax + py$. □

(c) Finally, suppose we have $a, b, p \in R$ such that: p is irreducible, p divides ab, and p does not divide a. Prove that p divides b. [Hint: Use part (b).]

Proof. Assume that p is irreducible, p divides ab (say $ab = pk$) and p does not divide a. By parts (a) and (b) there exist $x, y \in R$ such that $1 = ax + py$. Multiply both sides by b to get

$$\begin{aligned}
1 &= ax + py \\
b &= abx + pby \\
b &= pkx + pby \\
b &= p(kx + by).
\end{aligned}$$

We conclude that p divides b. □

4. Let R be a **PID** and suppose that we have

$$p_1 p_2 = q_1 q_2,$$

where $p_1, p_2, q_1, q_2 \in R$ are **irreducible**.

(a) Prove that p_1 divides q_1 or p_1 divides q_2. [Hint: See Problem 3.]

Proof. Since R is a PID and since p_1 divides q_1q_2, Problem 3(c) implies that p_1 divides q_1 or p_1 divides q_2. $\square$

(b) Without loss, you can assume that p_1 divides q_1. In this case prove that there exists a unit $u \in R^\times$ such that $q_1 = up_1$.

Proof. Without loss of generality, assume that p_1 divides q_1, say $q_1 = p_1u$ for some $u \in R$. If u is not a unit then p_1 is a proper factor of q_1. (Indeed, we know that p_1 divides q_1 and p_1 is not a unit (it's irreducible). If p_1 were associate to q_1 (say $q_1 = p_1v$ for some $v \in R^\times$) then $p_1u = q_1 = p_1v$ implies $p_1(u - v) = 0$ and hence $u = v \in R^\times$. Contradiction.) But we assumed that q_1 has no proper factor, hence u is a unit. $\square$

(c) Following (b), prove that we must also have $p_2 = uq_2$. [Hint: R is a domain.]

Proof. From part (b) we know that $p_1p_2 = q_1q_2 = up_1q_2$, and hence

$$\begin{aligned} p_1p_2 &= up_1q_2 \\ p_1p_2 - p_1uq_2 &= 0 \\ p_1(p_2 - uq_2) &= 0. \end{aligned}$$

Since R is a domain and since $p_1 \neq 0$ (it's irreducible) we conclude that $p_2 - uq_2 = 0$, hence $p_2 = uq_2$. $\square$

(d) Give a **specific example** of a ring R and irreducible elements $p_1, p_2, q_1, q_2 \in R$ where the above results fail. [Hint: Obviously, your R will not be a PID.]

Proof. Let $R = \mathbb{Z}[\sqrt{-3}]$ and note that

$$2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

On HW4 you showed that 2, $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ are irreducible in $\mathbb{Z}[\sqrt{-3}]$, but that 2 is not associate to either $1 + \sqrt{-3}$ or $1 - \sqrt{-3}$. By the results of (a),(b),(c) the ring $\mathbb{Z}[\sqrt{-3}]$ is not a PID. $\square$