MATH 4E03/6E03 Galois Theory, Fall 2014
Homework 2, Due Wednesday, October 15, 12:00 noon

Total: 18 marks.

(1) This exercise shows that

$$R \text{ is a PID if and only if } R \text{ is a UFD and every prime ideal is maximal.}$$

I have shown in class that (PID) ⇒ (prime ⇒ max). To show that (PID) ⇒ (UFD), we follow Garling (P.29). Remember that a UFD satisfies (ACCPI) and (irr ⇒ prime).

- To show that (PID) ⇒ (ACCPI), suppose we have a chain $(a_1) \subseteq (a_2) \subseteq \cdots$ of principal ideals. We define $J = \cup_{i=1}^{\infty}(a_i)$.

  (I) Show that J is an ideal. (1 mark)

  Answer: Given $a, b \in J$, say $a \in (a_i)$ and $b \in (a_j)$. We can assume $i \leq j$, then $a \in (a_j)$ and so $a + b \in (a_j) \subseteq J$. For any $r \in R$ and $a \in J$, again say $a \in (a_i)$, then $ra \in (a_i) \subseteq J$. □

  As in a PID, the ideal J is equal to (a) for some $a \in R$. Now that $a \in J = \cup_{i=1}^{\infty}(a_i)$ implies that $a \in (a_k)$ for some k, and so $(a) \subseteq (a_k)$. But we have

  $$(a_k) \subseteq (a_{k+1}) \subseteq \cdots \subseteq J = (a) \subseteq (a_k).$$

  By Sandwich, this shows that all (a_i) are equal for $i \geq k$.
- To show that (PID) ⇒ (irr ⇒ prime), given an irreducible $a \in R$. We want to show that (a) is a prime ideal. In fact, we can prove a stronger statement.

  (II) Given a PID R, show that (a) is a maximal ideal if a is irreducible. (1 mark)

  Answer: Let (a) is contained in a maximal ideal M, which is a principal ideal (m) as R is a PID. Therefore $a = mx$ for some $x \in R$. Since a is irreducible and m is not invertible, x is invertible, and so $(a) = (m)$ is maximal. □

  For then (a) is a prime ideal, since every maximal ideal is also a prime ideal.

We show that (UFD) + (prime ⇒ max) ⇒ (PID). Given an ideal I, we want to show that it is principal. Remember that in a UFD, every element has a decomposition into irreducibles (up to an invertible element which can be ignored) like $p_1 \ldots p_k$. Choose an element whose number of irreducible factors k is minimal among all choices in I. The proof will be done by induction on k.

(III) Prove that I is principal when $k = 1$, i.e., when there exists an irreducible element $p_1 \in I$. (1 mark)

Answer: We have $(p_1) \subseteq I$. But p_1 is irreducible, so is a prime (as in a UFD). Hence (p_1) is maximal by the given condition (prime ⇒ max), which forces $(p_1) = I$. □

Now assume that I is principal if $k = 1, \ldots, d-1$. Let I contain an element $p_1 \ldots p_d$, with d minimal. Define $J = \{x \in R,\ xp_d \in I\}$.

(IV) Prove that J is an ideal and $Jp_d = I$. (2 marks) (Hint: $Jp_d \subseteq I$ is clear. To show the reverse, you may have to use that (p_d) is a maximal ideal, since we are given (prime $\Rightarrow$ max).)

Answer: J is an ideal: For $a, b \in J$, we have $ap_d, bp_d \in I$, so that $(a+b)p_d \in I$ and $a + b \in J$. For $r \in R$ and $a \in J$, then $rap_d \in I$ and so $ra \in J$. (1 mark) Now we have $Jp_d \subseteq I$. To show the reverse, by the definition of J, it is enough to show that $I \subseteq (p_d)$. If not, then because (p_d) is maximal as hinted, we have $I + (p_d) = (1)$, or there exists $x \in I$ and $a \in R$ such that $x + ap_d = 1$. But now

$$p_1 \ldots p_{d-1} = p_1 \ldots p_{d-1} \cdot 1 = p_1 \ldots p_{d-1}(x + ap_d) = xp_1 \ldots p_{d-1} + ap_1 \ldots p_d \in I$$

since both x and $p_1 \ldots p_d$ lie in I. The above contradicts the minimality of d. (1 mark) □

Since $p_2 \ldots p_d \in J$, we apply induction assumption to conclude that J is principal, say $J = (a)$. Hence $I = (ap_d)$ is also principal.

(2) (c.f. Garling Ex.3.12) Let R be the integral domain $\mathbb{Z} + \sqrt{-5}\mathbb{Z}$. Show that $1 + \sqrt{-5}$ is not invertible in R. Moreover, show that $1 + \sqrt{-5}$ is irreducible but is not a prime element in R. (3 marks)

(Hint: Consider the *norm* map $\phi : R \to \mathbb{N}_{\geq 0}$, $\phi(a + \sqrt{-5}b) = a^2 + 5b^2$. The map ϕ is not a ring homomorphism: it does not satisfy $\phi(x + y) = \phi(x) + \phi(y)$. It satisfies $\phi(xy) = \phi(x)\phi(y)$ anyway.)

Answer: If $1 + \sqrt{-5}$ is invertible, then there exists $a + \sqrt{-5}b$ such that $(1 + \sqrt{-5})(a + \sqrt{-5}b) = 1$. Applying ϕ to the last equality we have

$$1 = \phi(1) = (1 + \sqrt{-5})(a + \sqrt{-5}b) = 6(a^2 + 5b^2),$$

which is clearly impossible. (1 mark)

To show that $1 + \sqrt{-5}$ is irreducible, suppose that $1 + \sqrt{-5} = (a + \sqrt{-5}b)(c + \sqrt{-5}d)$. We have to show that either $a + \sqrt{-5}b$ or $c + \sqrt{-5}d$ is invertible. Applying ϕ to the last equality we have

$$6 = \phi(1 + \sqrt{-5}) = \phi((a + \sqrt{-5}b)(c + \sqrt{-5}d)) = (a^2 + 5b^2)(c^2 + 5d^2).$$

Either $\{a^2 + 5b^2, c^2 + 5d^2\} = \{1, 6\}$ or $= \{2, 3\}$. But we can check that $a^2 + 5b^2 = 2$ has no integral solution, and same as $a^2 + 5b^2 = 3$. Therefore, we can assume that $a^2 + 5b^2 = 1$, which happens only when $a = 1$ and $b = 0$, and so $a + \sqrt{-5}b = 1$ which is clearly invertible. (1 mark)

Finally, $1 + \sqrt{-5}$ is not a prime, because $(1 + \sqrt{-5}) \supseteq ((1 + \sqrt{-5})(1 - \sqrt{-5})) = (6) = (2)(3)$, but both $(1 + \sqrt{-5}) \not\supseteq (2)$ and $(1 + \sqrt{-5}) \not\supseteq (3)$. (1 mark) □

Remark: Remember that every irreducible element in a UFD is also a prime element. This exercise shows that not all integral domain is a UFD. Neglecting this fact could lead to serious mistakes, e.g., wrong proofs of Fermat's Last Theorem.

(3) (Garling Ex.5.4) Suppose that K is a field and that f and g are relatively prime in $K[X]$, i.e., the ideal (f, g) generated by f and g is the whole polynomial ring $K[X]$. Show that $f - Yg$ is irreducible in $K(Y)[X]$. Here

$$K(Y) = \left\{ \frac{p(Y)}{q(Y)}, \text{ where } p(Y) \in K[Y] \text{ and } q(Y) \in K[Y] - \{0\} \right\}.$$

(3 marks) (Hint: $K(Y)[X]$ is a PID.)

Answer: Forget about the issue whether the polynomial $f - Yg$ is monic or not, just apply Gauss Lemma blindly, then

$$\begin{aligned} f - Yg \text{ is irreducible in } K(Y)[X] \quad &\Leftrightarrow \quad f - Yg \text{ is irreducible in } K[Y][X] \\ &\Leftrightarrow \quad f - Yg \text{ is irreducible in } K[X][Y] \\ &\Leftrightarrow \quad f - Yg \text{ is irreducible in } K(X)[Y]. \end{aligned}$$

Now the last statement is true because $f - Yg$ is a linear polynomial in Y (with coefficients in $K(X)$).

In class, I stated that you can apply Gauss Lemma only when the polynomial is monic. However, one can actually argue in certain ways that this condition can be dropped, see for example the proof in Dummit-Foote. This makes the solution of this question much easier than I thought, and I am sorry that the given hint may not help much.

(4) Show that $X^4 + 10X + 5$ is irreducible over the field $\mathbb{Q}[i]$, where $i = \sqrt{-1}$ and $\mathbb{Q}[i] = \{a + bi, \text{ where } a, b \in \mathbb{Q}\}$.

If you insist on using Eisenstein Criterion, then there are a number of steps you need to justify.

(a) First show that $\mathbb{Z}[i]$ is a PID. (3 marks)

(Hint: First define a norm map ϕ on $\mathbb{Z}[i]$ similar to Ex.(2) above, then formulate and prove an Euclidean algorithm on $\mathbb{Z}[i]$: for every $a, b \in \mathbb{Z}[i]$ and $b \neq 0$, there exists $q, r \in \mathbb{Z}[i]$ such that $a = bq + r$, with either $r = 0$ or $\phi(r) \leq \phi(b)$.)

Answer: The proof that 'an integral domain admits an Euclidean algorithm (an Euclidean domain) is a PID' is shown in case when $R = \mathbb{Z}$ or $K[X]$, and the general situation is very similar to these two cases. Below I just show that the ring $\mathbb{Z}[i]$ admits an Euclidean algorithm. We define

$$\phi(a + bi) = a^2 + b^2. \qquad \text{(1 mark)}$$

and show that

> for every $\alpha, \beta \in \mathbb{Z}[i]$ and $\beta \neq 0$, there exists θ (quotient) and ρ (remainder) in $\mathbb{Z}[i]$ such that $\alpha = \beta\theta + \rho$ and $\phi(\rho) < \phi(\beta)$.

Let θ be the complex number in $\mathbb{Z}[i]$ which has closest distance to $\frac{\alpha}{\beta}$ in the complex plane, i.e., such that $|\frac{\alpha}{\beta} - \theta|$ is minimal, or $\phi(\frac{\alpha}{\beta} - \theta) = |\frac{\alpha}{\beta} - \theta|^2$ is minimal, and let $\rho = \beta(\frac{\alpha}{\beta} - \theta)$ (1 mark for defining θ and ρ). By simple geometry, $\frac{\alpha}{\beta}$ must lie in one of the four quadrants (area= $\frac{1}{2} \times \frac{1}{2}$) of a unit square with one of the corners being θ, so that we have

$$|\frac{\alpha}{\beta} - \theta| \leq \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \frac{1}{\sqrt{2}}$$

and so

$$\phi(\rho) = \phi(\beta)\phi(\frac{\alpha}{\beta} - \theta) \leq \phi(\beta)\left(\frac{1}{2}\right) \leq \phi(\beta). \qquad \text{(1 mark)}$$

(b) Show that $1 + 2i$ and $1 - 2i$ are prime elements in $\mathbb{Z}[i]$. (Again, make use of the norm defined above.) (1 mark)

Answer: The inverse of $1 + 2i$ is $\frac{1}{5} - \frac{2}{5}i \notin \mathbb{Z}[i]$, so that $1 + 2i$ is not invertible in $\mathbb{Z}[i]$. If $1 + 2i = (a + bi)(c + di)$, then applying the norm map defined by above, we have

$$(a^2 + b^2)(c^2 + d^2) = \phi(a + bi)\phi(c + di) = \phi(1 + 2i) = 1^2 + 2^2 = 5.$$

Since both $a^2 + b^2$ and $c^2 + d^2$ are integers, the above forces $a^2 + b^2 = 1$ and $c^2 + d^2 = 5$. The former statement holds only when $(a, b) = (1, 0)$ or $(0, 1)$, which means that $a + bi = 1$ or i, which is invertible in $\mathbb{Z}[i]$. We have just proved that $1 + 2i$ is irreducible, which is hence a prime (as in a PID). □

(c) Show that the given polynomial is irreducible over $\mathbb{Q}[i]$ by Eisenstein Criterion and Gauss Lemma. (1 mark)

Answer: We have proved that $1+2i$ is a prime number in $\mathbb{Z}[i]$. Since the prime factorization of 5 in $\mathbb{Z}[i]$ is $(1+2i)(1-2i)$, the prime number $1+2i$ divides $(a_3, a_2, a_1, a_0) = (0, 0, 10, 5)$ and $(1+2i)^2$ does not divide $a_0 = 5$. The polynomial $X^4 + 10X + 5$ is $(1+2i)$-Eisenstein, hence is irreducible in $\mathbb{Z}[i]$. This monic polynomial is irreducible in $\mathbb{Q}[i]$ by Gauss Lemma. □

Remark: The number 5 is a prime in $\mathbb{Z}$ but is not a prime in $\mathbb{Z}[i]$. You need to use the prime $1+2i$ for this question. Failing to notice this will receive no mark.

Remark: I am not sure if this is the only method. If you can provide other justified methods, you can also get 5 marks.

(5) (Garling Ex.4.5) Given field extensions L/K and $L(\alpha)/L$ such that the degrees $[L:K]$ and $[K(\alpha):K]$ are relatively prime. Show that the minimal polynomial of α over L has coefficients in K. (2 marks)

Answer: The idea is to show that m_α^L is equal to m_α^K. We know that m_α^L divides m_α^K (1 mark for stating this, which has been stated in class a couple times), and so it is enough to show that their degrees, which are respectively $[L(\alpha):L]$ and $[K(\alpha):K]$, are equal. We know that

$$[L(\alpha):L][L:K] = [L(\alpha):K(\alpha)][K(\alpha):K] = [L(\alpha):K].$$

But since $[L:K]$ and $[K(\alpha):K]$ are coprime, the above relation forces $[K(\alpha):K] = [L(\alpha):L]$ by simple arithmetic. (1 mark) □