Math 562 **Spring 2012**
Homework 4 **Drew Armstrong**

Problems on Rings

1. We say that an ideal $I \subseteq R$ is prime if for all $a, b \in R$, $ab \in I$ implies that $a \in I$ or $b \in I$.

(a) Prove that $I \subseteq R$ is prime if and only if R/I is an integral domain.
(b) Prove that every maximal ideal is prime.

Proof. First note that the **zero element** of the ring R/I is $0 + I = I$ and that $a + I = I$ if and only if $a \in I$. Now suppose that $I \subseteq R$ is a prime ideal and consider **nonzero** cosets $a + I$ and $b + I$ in R/I (i.e. consider $a \notin I$ and $b \notin I$). Since I is prime this implies that $ab \notin I$, hence $ab + I \neq I$ and we conclude that R/I is an integral domain. Conversely, let R/I be an integral domain and consider $a, b \in R$ with $ab \in I$ (i.e. consider $ab + I = I$). Since $(a + I)(b + I) = ab + I = I$ and R/I is an integral domain we conclude that either $a + I = I$ (i.e. $a \in I$) or $b + I = I$ (i.e. $b \in I$). Hence $I \subseteq R$ is a prime ideal.

Now let $I \subseteq R$ be a **maximal** ideal. You showed on the previous homework that this implies that R/I is a field. Since every field is an integral domain, we conclude that I is a prime ideal. □

[Note that this result is quite general; it is true for any commutative ring with 1. The concepts of "prime" and "maximal" ideals are meant to generalize the concepts of "prime" and "irreducible" elements of a ring. (The intuition for this comes from PIDs.) However, even though maximal always implies prime for ideals, it is not always true that irreducible elements are prime. What's going on here?]

2. The following two proofs are **wrong**. Explain why, and **fix them**.

(a) Let R be an integral domain and consider a principal ideal $(a) \subseteq R$. If a is irreducible, then the ideal (a) is maximal, hence the ideal (a) is prime, hence the element a is prime. We conclude that every irreducible element is prime.
(b) Let $I \subseteq R$ be an ideal in an integral domain. If I is a prime ideal, then $I = (p)$ for some prime element $p \in R$. But every prime element of a domain is irreducible, hence p is irreducible and the ideal $I = (p)$ is maximal. We conclude that every prime ideal is maximal.

Proof. The problem is that these proofs fail when R is not a PID. **So let R be a PID.**

Claim 1: Every irreducible element of R is prime. **Proof:** Let $a \in R$ be irreducible and consider the ideal $(a) \subseteq R$. Let J be an ideal with $(a) < J \subseteq R$. **Since R is a PID** we can write $J = (b)$. Then note that $(b) = R$ since otherwise b would be a proper divisor of a. Hence $(a) \subseteq R$ is a maximal ideal and by Problem 1 it is also a prime ideal. That is, given $a|bc$ (i.e. $bc \in (a)$) it follows that $b \in (a)$ (i.e. $a|b$) or $c \in (a)$ (i.e. $a|c$). We conclude that the element $a \in R$ is prime.///

Claim 2: Every prime ideal of R is maximal. **Proof:** Let $I \subseteq R$ be a prime ideal. **Since R is a PID** we have $I = (a)$ for some element $a \in R$, and since (a) is a prime ideal it follows that $a \in R$ is a prime element (see the above proof). Then since R is an integral domain it follows that $a \in R$ is irreducible (if you don't remember the proof, do it now). Finally, consider an ideal J such that $(a) = I < J \subseteq R$. **Since R is a PID** we have $J = (b)$ for some $b \in R$ and then we must have $J = R$ since otherwise b is a proper divisor of a. We conclude that $I \subseteq R$ is a maximal ideal.///

□

3. Given a ring R, there exists a unique ring homomorphism $\varphi : \mathbb{Z} \to R$ defined by $\varphi(1_{\mathbb{Z}}) = 1_R$. If $\ker \varphi = (n) \subseteq \mathbb{Z}$, we say the ring R has "characteristic n".

(a) Prove that the characteristic of an integral domain is 0 or prime $p \in \mathbb{Z}$.

(b) Prove that a field F has characteristic 0 if and only if it contains a subfield isomorphic to $\mathbb{Q}$.

Proof. To prove (a), let R be an integral domain and consider the unique homomorphism $\varphi : \mathbb{Z} \to R$, which is defined defined by $\varphi(1_\mathbb{Z}) = 1_R$. Since $\mathbb{Z}$ is a PID we know that $\ker\varphi = (n)$ for some n. Suppose that n has a **proper** factorization $n = ab$. In particular this means that $a, b \notin (n) = \ker\varphi$ so that $\varphi(a), \varphi(b) \neq 0_R$. But since φ is a homomorphism we also have $\varphi(a)\varphi(b) = \varphi(n) = 0_R$, which contradicts the fact that R is an integral domain. We conclude that n must be zero or prime.

To prove (b), let F be a field and consider the map $\varphi : \mathbb{Z} \to F$ defined by $\varphi(1_\mathbb{Z}) = 1_F$. If F has characteristic 0 then the map φ is injective and we can use this to define an injective homomorphism $\bar\varphi : \mathbb{Q} \hookrightarrow F$ by $\bar\varphi(a/b) := \varphi(a)/\varphi(b)$ whenever $b \neq 0_\mathbb{Z}$. This map is well-defined since if $a/b = c/d$ (i.e. $ad = bc$) then we obtain $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$, hence $\varphi(a)/\varphi(b) = \varphi(c)/\varphi(d)$. It's a homomorphism because $\bar\varphi(1_\mathbb{Z}/1_\mathbb{Z}) = \varphi(1_\mathbb{Z})/\varphi(1_\mathbb{Z}) = 1_F/1_F = 1_F$,

$$\bar\varphi\left(\frac{a}{b}\cdot\frac{c}{d}\right) = \bar\varphi\left(\frac{ac}{bd}\right) = \frac{\varphi(ac)}{\varphi(bd)} = \frac{\varphi(a)\varphi(c)}{\varphi(b)\varphi(d)} = \frac{\varphi(a)}{\varphi(b)}\cdot\frac{\varphi(c)}{\varphi(d)} = \bar\varphi\left(\frac{a}{b}\right)\bar\varphi\left(\frac{c}{d}\right),$$

and

$$\bar\varphi\left(\frac{a}{b}+\frac{c}{d}\right) = \bar\varphi\left(\frac{ad+bc}{bd}\right) = \frac{\varphi(ad+bc)}{\varphi(bd)} = \frac{\varphi(a)\varphi(d)+\varphi(b)\varphi(c)}{\varphi(b)\varphi(d)} = \frac{\varphi(a)}{\varphi(b)}+\frac{\varphi(c)}{\varphi(d)} = \bar\varphi\left(\frac{a}{c}\right)+\bar\varphi\left(\frac{c}{d}\right),$$

whenever the denominators are nonzero. Finally, the map $\bar\varphi$ is injective because $\bar\varphi(a/b) = \bar\varphi(c/d) \Rightarrow \varphi(a)/\varphi(b) = \varphi(c)/\varphi(d) \Rightarrow \varphi(a)\varphi(d) = \varphi(b)\varphi(c) \Rightarrow \varphi(ad) = \varphi(bc)$, and then the injectivity of φ implies $ad = bc \Rightarrow a/d = b/c$. Hence F contains a subfield isomorphic to $\mathbb{Q}$; namely, the homomorphic image $\bar\varphi(\mathbb{Q}) \subseteq F$.

Conversely, suppose that $K \subseteq F$ is a subfield isomorphic to $\mathbb{Q}$. Since φ maps $1_\mathbb{Z}$ to $1_F \in K \subseteq F$ it follows that φ maps $\mathbb{Z}$ into K. But K is a field of characteristic 0 (why?). Hence $\ker\varphi = (0)$ and we conclude that F has characteristic 0. □

[In general, given any field F we define its **prime subfield** $F' \subseteq F$ as the intersection of all subfields — equivalently, F' is the subfield generated by 1_F. It's a general fact that the prime subfield is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/(p)$, depending on the characteristic of F. You just proved the characteristic 0 case.]

Problems on Fields

4. Finite Implies Algebraic. Consider a field extension $F \subseteq K$. We say that $a \in K$ is algebraic over F if $f(a) = 0$ for some (monic) polynomial $f(x) \in F[x]$. We say that the extension $F \subseteq K$ is algebraic if every element of K is algebraic over F. Prove that if $[K : F] < \infty$ then $F \subseteq K$ is algebraic. [Hint: Consider the powers $1, a, a^2, \ldots$ of some $a \in K$. Are they independent over F?]

Proof. Let $F \subseteq K$ be an extension of fields and suppose that $[K : F] = n < \infty$. That is, K is a vector space of dimension n over F. Let $a \in K$ be any nonzero element and consider the set $\{1, a, \ldots, a^n\} \subseteq K$. If this set contains any repetition, say $a^j = a^k$, then a is a root of the polynomial $f(x) = x^j - x^k \in F[x]$. Otherwise the set $\{1, a, \ldots, a^n\}$ contains $n+1$ distinct elements. Since K has dimension n we know that any set of $> n$ elements must be linearly **dependent**. Hence there exist $c_0, \ldots, c_n \in F$ such that

$$c_0 + c_1 a + c_2 a^2 + \cdots + c_n a^n = 0.$$

We conclude that a is a root of the polynomial $f(x) = c_0 + c_1 x + \cdots c_n x^n \in F[x]$. □

5. Given a field extension $F \subseteq K$, let $F \subseteq \overline{F} \subseteq K$ denote the subset of elements that are algebraic over F. This is called the algebraic closure of F in K. Prove that $\overline{F}$ is a field. [Hint: Consider

$a, b \in \overline{F}$ and note that $F(a,b) \subseteq K$ contains $a+b, a-b, ab$ and a/b $(= ab^{-1})$. By Problem 4, it suffices to show that $[F(a,b) : F] < \infty$.]

Proof. For any $a, b \in \overline{F} \subseteq K$ with $b \neq 0$, we wish to show that $\{a+b, a-b, ab, a/b\} \subseteq \overline{F}$. We know by definition that $\{a+b, a-b, ab, a/b\} \subseteq F(a,b) \subseteq K$, thus by Problem 4 above it suffices to show that $[F(a,b) : F] < \infty$.

Note that $F(a,b) = F(a)(b)$. Since b is algebraic over F, it is certainly algebraic over $F(a)$, hence we know that $[F(a)(b) : F(a)] = [F(a,b) : F(a)]$ equals the degree of the minimal polynomial for b over $F(a)$, which is **finite**. Similarly since a is algebraic over F we know that $[F(a) : F] < \infty$. By the Tower Law we conclude that

$$[F(a,b) : F] = [F(a,b) : F(a)] \cdot [F(a) : F] < \infty.$$

$\square$

[This is quite a slick proof. We have shown that if $a, b \in K$ satisfy polynomial equations over F, say $f(a) = 0$ and $g(b) = 0$, then the elements $a+b, a-b, ab, a/b$ also satisfy polynomial equations. However, we didn't say how to **find** these polynomials. If you tried to construct the polynomials, you probably observed that it's not so easy. For example: We know that $\sqrt[3]{2}$ and $e^{2\pi i/3}$ are algebraic over $\mathbb{Q}$ and we know their minimal polynomials. Try to compute the minimal polynomial of $\sqrt[3]{2} + e^{2\pi i/3}$ over $\mathbb{Q}$.]

Problems on Galois Theory

6. Give a short proof that $\sqrt{2}$ is an element of the field $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{R}$. [Hint: By definition, the real inverse of $\sqrt{2} + \sqrt{3}$ is also in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. What is this inverse?]

Proof. Observe that $(\sqrt{3} + \sqrt{2})(\sqrt{3} - \sqrt{2}) = 3 - 2 = 1 \in \mathbb{R}$. Since $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ is a subfield of $\mathbb{R}$ we conclude that $(\sqrt{2} + \sqrt{3})^{-1} = (\sqrt{3} - \sqrt{2}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Finally, we get

$$\frac{1}{2}[(\sqrt{2} + \sqrt{3}) - (\sqrt{3} - \sqrt{2})] = \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

$\square$

7. Let $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ be the splitting field of $x^4 + 1 \in \mathbb{Q}[x]$.

(a) Prove that $K = \mathbb{Q}(\sqrt{2}, i)$.
(b) Prove that $[K : \mathbb{Q}] = 4$ and hence the Galois group $\mathsf{Gal}(K/\mathbb{Q})$ has order 4.
(c) Prove that $\mathsf{Gal}(K/F) \approx V := \mathbb{Z}/(2) \times \mathbb{Z}/(2)$, the "Klein Viergruppe".
(d) Draw and label the lattice of fields between $\mathbb{Q}$ and K.

Proof. First suppose that $z^4 = -1$. Taking absolute value gives $|z|^4 = 1$, hence $z = e^{i\theta}$ for some angle $\theta \in \mathbb{R}$. Since $-1 = e^{i\pi}$ we obtain $e^{i4\theta} = e^{-i\pi}$, which implies that $4\theta = -\pi + 2\pi k$ for any integer $k \in \mathbb{Z}$. We conclude that the roots of $x^4 + 1$ are

$$(a_1, a_2, a_3, a_4) = (e^{i\pi/4}, e^{i3\pi/4}, e^{i5\pi/4}, e^{i7\pi/4}) = \left(\frac{1+i}{\sqrt{2}}, \frac{-1+i}{\sqrt{2}}, \frac{-1-i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}} \right)$$

hence the splitting field is $K = \mathbb{Q}(a_1, a_2, a_3, a_4) \subseteq \mathbb{C}$. To prove (a), first note that all of these roots are in $\mathbb{Q}(\sqrt{2}, i)$, hence $K \subseteq \mathbb{Q}(\sqrt{2}, i)$. Conversely, we have $\sqrt{2} = a_1 + a_4 \in K$ and $i = (a_1 + a_2)/(a_1 + a_4) \in K$, hence $\mathbb{Q}(\sqrt{2}, i) \subseteq K$. We conclude that $K = \mathbb{Q}(\sqrt{2}, i)$.

To prove (b), note that the inclusions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, i)$ are **strict** because $\sqrt{2}$ is not rational and i is not real. Hence the Tower Law implies that $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \geq 2 \cdot 2 = 4$. On the other hand, $\{1, \sqrt{2}, i, i\sqrt{2}\}$ is clearly a spanning set for $K = \mathbb{Q}(\sqrt{2}, i)$, hence $[K : \mathbb{Q}] \leq 4$

(because every spanning set contains a basis). We conclude that $[K:\mathbb{Q}]=4$, and it follows (for general reasons, not yet proved in class) that $|\mathsf{Gal}(K/\mathbb{Q})|=4$.

What could this group be? Recall that there are only two groups of size 4; they are isomorphic to $\mathbb{Z}/(4)$ and $V := \mathbb{Z}/(2)\times\mathbb{Z}/(2)$. To prove (c), we will show that $\mathsf{Gal}(K/\mathbb{Q}) \approx V$. Note that an element $\sigma \in \mathsf{Gal}(K:\mathbb{Q})$ is determined by the two values $\sigma(\sqrt{2}), \sigma(i)$, since $\sqrt{2}$ and i generate the splitting field. If we apply σ to the equations $z^2=2$ and $z^2=-1$ (for any $z\in K$) then we obtain $\sigma(z)^2=\sigma(2)=2$ and $\sigma(z)^2=\sigma(-1)=-1$, hence $\sigma(z)$ will be a root of x^2-2 (respectively, x^2+1) if and only if z is a root of x^2-2 (respectively, x^2+1). We conclude that σ is one of the four maps:

$$\mathsf{id}=\left\{\begin{array}{c}\sqrt{2}\mapsto\sqrt{2}\\ i\mapsto i\end{array}\right\},\ \sigma=\left\{\begin{array}{c}\sqrt{2}\mapsto-\sqrt{2}\\ i\mapsto i\end{array}\right\},\ \tau=\left\{\begin{array}{c}\sqrt{2}\mapsto\sqrt{2}\\ i\mapsto -i\end{array}\right\},\ \mu=\left\{\begin{array}{c}\sqrt{2}\mapsto-\sqrt{2}\\ i\mapsto -i\end{array}\right\}.$$

The group table is given by:

$\circ$	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	id	μ	τ
τ	τ	μ	id	σ
μ	μ	τ	σ	id

This can't be the group $\mathbb{Z}/(4)$ because there is no element of order 4 (in fact, every non-identity element has order 2), so it must be $\mathbb{Z}/(2)\times\mathbb{Z}/(2)$. More directly, each of σ,τ generates a group isomorphic to $\mathbb{Z}/(2)$, and then $\mathsf{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle\times\langle\tau\rangle \approx \mathbb{Z}/(2)\times\mathbb{Z}/(2)$.

Now to part (d). It is a bit, say, creative for me to ask you this since I haven't yet given you any theorems to this effect. It is easy to find a few intermediate fields:

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{Q}(\sqrt{2},i) \arrow[dl, "2"'] \arrow[d, "2"] \arrow[dr, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, "2"'] & \mathbb{Q}(i) \arrow[d, "2"] & \mathbb{Q}(i\sqrt{2}) \arrow[dl, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

But are there any more? I will return to this discussion in class.

$\square$