Homework 6 Solution. Math 113 Summer 2016.

1. For each of the following ideals, say whether they are prime, maximal (hence also prime), or neither

   (a) $(x^4 + 2x^2 + 1) \subset \mathbb{C}[x]$

   (b) $(x^5 + 24x^3 - 54x^2 + 6x + 12) \subset \mathbb{Q}[x]$

   (c) $(x - a) \subset \mathbb{R}[x, y]$, where $a \in \mathbb{R}$.

   (d) $(4, 2x - 1) \subset \mathbb{Z}[x]$

   Solution:

   (a) Notice that $(x^2 + 1)(x^2 + 1) \in (x^4 + 2x^2 + 1)$, but $x^2 + 1 \notin (x^4 + 2x^2 + 1)$, because every nonzero polynomial in $(x^4 + 2x^2 + 1)$ has degree at least four. So $(x^4 + 2x^2 + 1)$ is not prime, hence not maximal.

   (b) This polynomial is irreducible by Eisenstein's Criterion (with $p = 3$). This implies that the ideal it generates is both prime and maximal, since $\mathbb{Q}[x]$ is a PID.

   (c) This ideal is prime since the quotient $\mathbb{R}[x, y]/(x - a) \cong \mathbb{R}[y]$ is an integral domain. But it is not maximal since the quotient is not a field (x has no multiplicative inverse, for example).

   (d) In the quotient ring $\mathbb{Z}[x]/(4, 2x - 1)$, we have the relations (I'll sloppily omit the "bar" in the notation here) $4 = 0$ and $2x - 1 = 0$, which together imply that $2 = 0$, and hence (since $0 = 2x - 1 = 0x - 1 = -1$) that $-1 = 0$, so $1 = 0$. Thus the quotient ring is the zero ring, which means the ideal is the unit ideal, which is neither prime nor maximal.

2. In this problem you will investigate a "dictionary" which relates notions of divisibility to principal ideals. Let R be a ring and a, b elements of R.

   (a) Prove that $a|b$ if and only if $b \in (a)$

   (b) Prove that a is a unit if and only if $(a) = R$ (we've used this in class many times)

   (c) Prove that if R is an integral domain, then $a = ub$ for some unit $u \in R$ if and only if $(a) = (b)$.

   (d) Prove that if R is an integral domain and (a) is a nonzero prime ideal, then a is an irreducible element.

   (e) Show, however, by finding an example in $\mathbb{Z}[\sqrt{-5}]$, then even if a is irreducible, the ideal (a) may not be prime[1].

   Solution:

   (a) $a|b$ if and only if there is an $r \in R$ such that $b = ra$ if and only if b is in the set $\{ra \,|\, r \in R\}$, which is precisely (a).

   (b) If $(a) = R$, then in particular, $1 \in (a)$, so $1 = ra$, which means a is a unit. Conversely, if a is a unit, say $ab = 1$, then since $ab \in (a)$, we have $1 \in (a)$, so for all $r \in R$, $r = 1 \cdot r \in (a)$ by closure under scaling.

[1] This can only happen when the ring is *not* a UFD.

(c) If $a = ub$ with u a unit, then $(a) \subseteq (b)$ because $a = ub$ and $(b) \subseteq (a)$ because $b = u^{-1}a$. Conversely, assume $(a) = (b)$, then since $a \in (b)$, we have $a = rb$ for some $r \in R$, and since $b \in (a)$ we have $b = sa$ for some $s \in R$. Putting these together gives $a = rb = rsa$, so $a(1 - rs) = 0$. Now if $a = 0$, then $(a) = (0) = (b)$, so $b = 0$, and we can write $a = 1b$; otherwise, since R is an integral domain, $1 - rs = 0$, so r and s are units. Thus $a = rb$, with r a unit.

(d) Suppose (a) is a nonzero prime ideal, and $a = bc$. Note that a is nonzero and a nonunit. We'll show that one of b, c must be a unit. Since $bc = a \in (a)$ and (a) is prime we must have either $b \in (a)$ or $c \in (a)$. Suppose without loss of generality that $b \in (a)$. Then $b = ra$ for some $r \in R$. Then $a = bc = rac$, so $a(1 - rc) = 0$, hence (since $a \neq 0$) $rc = 1$, so c is a unit, as desired.

(e) For his one, we need some info on irreducibles in $\mathbb{Z}[\sqrt{-5}]$. We have a norm on $\mathbb{Z}[\sqrt{-5}]$ given by $n(a + b\sqrt{-5}) = a^2 + 5b^2$, but it doesn't satisfy the division algorithm. Nevertheless, we still have $n(ab) \geq n(a)$ for any $a, b \neq 0$. This implies that if an element factorizes, the norms of the factors are less than or equal to the norms of the original element. Also, we have $n(ab) = n(a)n(b)$, which implies that the norm of a unit must be 1. So the only units are ± 1. Moreover, looking at small values of a, b, we see that the possible norms of elements must be 1, 4, 5, 6, 9... This implies that the elements $2, 3$, and $1 \pm \sqrt{-5}$ are irreducible, because their norms are 4,5,6, so their only factors can have norm 1, hence must be units.

Now consider the ideal (2) generated by 2. Since $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 \in (2)$, but both of $1 \pm \sqrt{-5}$ are not in (2), this ideal is not prime, even though its generator is irreducible.

3. Use the division algorithm in $k[x]$ to prove the following lemma, which you might have wished you had for the last HW: If $a \in k$, and a nonconstant linear polynomial f is in the kernel of the evaluation map $\mathrm{Ev}_a \colon k[x] \to k$, then f generates the kernel, so $\ker \mathrm{Ev}_a = (f)$.

   Solution: We need to show that if $f = cx + d \in \ker Ev_a$, with $c \neq 0$, then $(f) = \ker \mathrm{Ev}_a$. Since f is in $\ker \mathrm{Ev}_a$, the ideal it generates is in $\ker \mathrm{Ev}_a$, since the kernel is an ideal. To show that $\ker \mathrm{Ev}_a \subseteq (f)$, pick $p \in \ker \mathrm{Ev}_a$; applying the division algorithm to p by f, there exists $q, r \in k[x]$ with $0 \leq \deg r < 1 = \deg f$, (ie $\deg r = 0$, so r is a constant) such that $p = qf + r$. Then, plugging in a, $0 = p(a) = f(a)q(a) + r(a) = 0 + r$, so $r = 0$, and $p = qf$; thus $\ker \mathrm{Ev}_a \subseteq (f)$.

4. Prove that any element r in a ring R which is not contained in any maximal ideal must be a unit in R. You may use the following fact: every *nonzero* ring contains a maximal ideal. [Hint: look for a maximal ideal in a suitable quotient, then look at its pre-image under the quotient map. Is it maximal? There is a very subtle difference between this and problem 10 from HW5]

   Solution: Let $r \in R$ and suppose that r is not contained in any maximal ideal. Consider the ideal $(r) \subset R$: we aim to show that $(r) = R$, so that $1 \in (r)$ and $1 = rs$, for some $s \in R$. Consider the quotient ring $S = R/(r)$, and let $\mathfrak{m} \subset S$ be a maximal ideal. Then, if $\pi : R \to S$ is the quotient homomorphism, we have that $\pi^{-1}(\mathfrak{m}) \supset (r)$, and $\pi^{-1}(\mathfrak{m})$ is an ideal.

   We claim that $\pi^{-1}(\mathfrak{m})$ is maximal: suppose that $I \supset \pi^{-1}(\mathfrak{m})$, and $I \neq \pi^{-1}(\mathfrak{m})$, we will show that $I = R$. Then, $\pi(I)$ is a subgroup of S (as $\pi(I)$ is the image of the homomorphism $I \to R \to S$), and if $s \in S$ then $s = \pi(r)$, for some r, so that $s\pi(x) = \pi(r)\pi(x) = \pi(rx) \in \pi(I)$, for any $x \in I$. Hence, $\pi(I) \subset S$ is an ideal containing $\mathfrak{m}$ (because $\pi(I) \supset \pi(\pi^{-1}(\mathfrak{m})) \supset \mathfrak{m}$). Moreover, if $\pi(I) = \mathfrak{m}$, then $I = \pi^{-1}(\pi(I)) = \pi^{-1}(\mathfrak{m})$, which is absurd. Hence, $\pi(I) = S$, by maximality of $\mathfrak{m}$ and $I = \pi^{-1}(\pi(I)) = \pi^{-1}(S) = R$. Hence, $\pi^{-1}(\mathfrak{m})$ is maximal. This contradicts that r is not contained in any maximal ideal. Thus, the only possibility is that $\mathfrak{m}$ does not exist, which implies that S is the zero ring (otherwise a maximal ideal must exist in S), and $R = (r)$. The result follows.

5. Let R be a ring, and $\mathfrak{n}$ the set of nilpotent elements in R.

   (a) Prove that $\mathfrak{n}$ is an ideal (remember that we allow 0 as a nilpotent).

   (b) Prove that $\mathfrak{n}$ is contained inside every prime ideal of R.

   (c) Prove that the ring $R/\mathfrak{n}$ has no nonzero nilpotent elements.

   Solution

   (a) 0 is nilpotent, so 0 is in $\mathfrak{n}$. If a, b are nilpotent, then we have $a^k = b^m = 0$ for some $k, m > 0$. Then if we expand $(a+b)^{k+m}$ we get

   $$(a+b)^{k+m} = a^{k+m} + (k+m)a^{k+m-1} + \binom{k+m}{2}a^{k+m-2}b^2 + \cdots$$

   and in each term, either a appears with exponent at least k, or b appears with exponent at least m, so all terms are zero. Thus $(a+b)^{k+m} = 0$, so $a+b$ is nilpotent. Also, if $a^k = 0$, then $(-a)^k = (-1)^k a^k = \pm 0 = 0$, so $-a$ is nilpotent. Thus $\mathfrak{n}$ forms an additive subgroup. Finally, to check closure under scaling, pick $a \in \mathfrak{n}$ and $r \in R$. Say $a^k = 0$, then $(ra)^k = r^k a^k = 0$, so $ra \in \mathfrak{n}$.

   (b) Let $\mathfrak{p}$ be any prime ideal, and a an element of $\mathfrak{n}$, so $a^k = 0$. Since $0 \in \mathfrak{p}$, $a^k \in \mathfrak{p}$. Thus $a(a^{k-1}) \in \mathfrak{p}$, so since $\mathfrak{p}$ is prime either $a \in \mathfrak{p}$ or $a^{k-1} \in \mathfrak{p}$. If $a \in \mathfrak{p}$ we're done; if not $a^{k-1} \in \mathfrak{p}$. Then $a(a^{k-2}) \in \mathfrak{p}$ so either $a \in \mathfrak{p}$ or $a^{k-2} \in \mathfrak{p}$. Continuing in this fashion, we must eventual arrive at the conclusion that $a \in \mathfrak{p}$. Since $a \in \mathfrak{n}$ was arbitrary, $\mathfrak{n} \subseteq \mathfrak{p}$.

   (c) Let $\bar{a} \in R/\mathfrak{n}$ be a nilpotent element, say $\bar{a}^k = 0$. We will show that $\bar{a}$ must be zero. Since $\bar{a}^k = 0$, $a^k \in \ker \pi_{\mathfrak{n}} = \mathfrak{n}$. Thus a^k is nilpotent, so $(a^k)^n = a^{kn} = 0$, showing that a itself is nilpotent. Thus $a \in \mathfrak{n}$, so $\bar{a} = 0$.

6. The ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain, with norm $n\colon \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$ given by $n(a+bi) = a^2+b^2$ (you don't need to prove that this makes $\mathbb{Z}[i]$ into a Euclidean domain).

   (a) Show that this norm satisfies the stronger condition $n(\alpha\beta) = n(\alpha)n(\beta)$

   (b) Deduce that if $\alpha|\beta$ in $\mathbb{Z}[i]$, then $n(\alpha)|n(\beta)$ in $\mathbb{N}$.

   (c) Show that $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $n(\alpha) = 1$. Use this to determine all the units in $\mathbb{Z}[i]$.

   (d) Show that if $n(\alpha)$ is a prime in $\mathbb{N}$, then α is irreducible in $\mathbb{Z}[i]$.

   (e) Why don't the equalities $(4+i)(4-i) = 17 = (1+4i)(1-4i)$ contradict the fact that $\mathbb{Z}[i]$ is a UFD (which follows from the fact that it's a Euclidean domain)?

   Solution:

(a) The easiest way to see this is to observe that this norm is just $n(\alpha) = |\alpha|^2 = \alpha\overline{\alpha}$, the "norm square" from the complex numbers. Thus $n(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 = n(\alpha)n(\beta)$.

(b) Suppose $\alpha|\beta$, so that $\beta = \alpha\gamma$ for some $\gamma \in \mathbb{Z}[i]$. Then $n(\beta) = n(\alpha)n(\gamma)$, so $n(\alpha)|n(\beta)$.

(c) α is a unit iff there is a β with $\alpha\beta = 1$. If this is so, then $n(\alpha)n(\beta) = 1$, so $n(\alpha) = n(\beta) = 1$ (can't be -1 since the norm is a natural number). Conversely, if $n(\alpha) = 1$, then $a^2 + b^2 = 1$ implies $a = \pm 1$ and $b = 0$, or $a = 0$ and $b = \pm 1$. So the only elements with norm 1 are ± 1, $\pm i$. It's easy to check these are all units: 1 is, $(-1)(-1) = 1$, and $i(-i) = 1$. Thus the units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

(d) This follows more or less immediately from (b): suppose $n(\alpha)$ is a prime number. If $\alpha = \beta\gamma$, then $n(\alpha) = n(\beta)n(\gamma)$,

7. Let $R = k[[x]]$ be the ring of formal power series over a field k.

(a) Prove that the ideal (x) generated by x is maximal, by looking at the quotient $R/(x)$.

(b) In fact, this is the *only* maximal ideal of R. Use this and problem 4 to give a new proof of the worksheet problem from last week which said that the units in R are those power series with nonzero constant term, i.e., those $\sum a_i x^i$ for which $a_0 \neq 0$.

Solution:

(a) The map $k[[x]] \to k$ sending x to 0 has kernel (x) and is surjective, so the isomorphism theorem gives $k[[x]]/(x) \cong k$, a field, implying that (x) is maximal.

(b) If u is a unit in $k[[x]]$, then it cannot be contained in any maximal ideal. Since (x) is the only maximal ideal, $u \notin (x)$. But the elements of (x) are the power series which are multiples of x, i.e., those having no constant term. So since $u \notin (x)$, u must have nonzero constant term.

8. By definition, the **content** of a polynomial $f \in \mathbb{Z}[x]$, written $C(f)$, is the gcd of its coefficients. Prove **Gauss' Lemma**, which states that for $f, g \in \mathbb{Z}[x]$, $C(fg) = C(f)C(g)$. [Hint: First factor out the content from each polynomial, and reduce to the case where f and g both have content 1: in this case you have to prove that $C(fg) = 1$. Now argue by contradiction, supposing some prime p divides all coefficients of fg, and looking at their reduction mod p, as we did in the proof of Eisenstein's criterion.]

Solution:

We being with a simple observation: if you multiply a polynomial by some integer k, it has the effect of multiplying the content of that polynomial by k: $C(kf) = kC(f)$. Now, first suppose we have proved the result in the case that f and g have content 1, so that $C(fg) = 1$. Now we can deduce the result in general as follows: Write $f = aF$, $g = bG$, where $F, G \in \mathbb{Z}[x]$ have content 1, and $a = C(f)$, $b = C(g)$. Then $C(fg) = C(abFG) = abC(FG) = abC(F)C(G) = ab = C(f)C(g)$.

So it remains to prove that $C(fg) = 1$ when $C(f) = C(g) = 1$. Suppose for a contradiction that $C(fg) > 1$, then some prime p must divide $C(fg)$. Thus p is a common divisor of all the coefficients of the polynomial fg. Thus when we reduce mod p, we get that $\overline{f}\overline{g} = \overline{fg} = 0$ mod p. But $\overline{f}, \overline{g} \in \mathbb{Z}/p\mathbb{Z}[x]$, which is a domain (since $\mathbb{Z}/p\mathbb{Z}$ is a field), so if $\overline{f}\overline{g} = 0$, then one of $\overline{f}$ or $\overline{g}$ must be zero in $\mathbb{Z}/p\mathbb{Z}[x]$. This means that all the coefficients of f (or of g) are divisible by p. But that contradicts our assumption that both polynomials have content 1. The contradiction implies that $C(fg) = 1$.

9. Use Gauss' Lemma to prove that if $f \in \mathbb{Z}[x]$ and $C(f) = 1$, then f is irreducible over $\mathbb{Z}$ if and only if f is irreducible over $\mathbb{Q}$.

   Solution: First we prove that irreducible over $\mathbb{Q}$ implies irreducible over $\mathbb{Z}$. Let $f \in \mathbb{Z}[x]$ have content 1, and suppose that we have a factorization $f = gh$ over $\mathbb{Z}$ (so $g, h \in \mathbb{Z}[x]$). Then this is also a factorization over $\mathbb{Q}$, because $\mathbb{Z}[x] \subset \mathbb{Q}[x]$. Since f is irreducible over $\mathbb{Q}$, then one of g or h is a unit in $\mathbb{Q}[x]$, i.e., a constant polynomial; say it's g. Then g is just a nonzero rational number. But since $g \in \mathbb{Z}[x]$ also, it must actually be an integer. Thus we have $f = gh$, with g an integer. But then $1 = C(f) = C(gh) = gC(h)$, by the remark at the beginning of the solution of problem 8. So g divides 1, hence must b ± 1. Thus g is a unit in $\mathbb{Z}[x]$, so f is irreducible.

   For the other direction, assume that f is irreducible over $\mathbb{Z}$, and suppose $f = gh$ with $g, h \in \mathbb{Q}[x]$. Then we can write $g = c\mathrm{wt}g$ and $h = d\mathrm{wt}h$ for some $c, d \in \mathbb{Q}$ and $\mathrm{wt}g, \mathrm{wt}h \in \mathbb{Z}[x]$ with $C(\mathrm{wt}g) = C(\mathrm{wt}h) = 1$ (proof: clear denominators in g to make it an integer polynomial. Then factor out the gcd of the coefficients to make it have content 1). Then we have $f = gh = cd\mathrm{wt}g\mathrm{wt}h$. This rational number cd must be an integer, of if not, say $cd = \frac{x}{y}$, with $\gcd(x, y) = 1$ and $y > 1$, then since $f \in \mathbb{Z}[x]$ and $\mathrm{wt}g\mathrm{wt}h \in \mathbb{Z}[x]$, it would have to be that y divides all the coefficients of $\mathrm{wt}g\mathrm{wt}h$. But this would mean that $q < C(\mathrm{wt}g\mathrm{wt}h = C(\mathrm{wt}g)C(\mathrm{wt}h) = 1$, a contradiction. Thus $cd \in \mathbb{Z}$, and so $1 = C(f) = C(cd\mathrm{wt}g\mathrm{wt}h) = cdC(\mathrm{wt}g)C(\mathrm{wt}h) = cd$, so $cd = 1$. Thus we have a factorization over $\mathbb{Z}$ $f = \mathrm{wt}g\mathrm{wt}h$, and since f is irreducible over $\mathbb{Z}$, either g or h is a unit in $\mathbb{Z}[x]$ and therefore also a unit in $\mathbb{Q}[x]$, so f is irreducible over $\mathbb{Q}$.

10. In this problem you will investigate the behavior of prime ideals under a ring homomorphism $f\colon R \to S$. First, a definition: if $I \subseteq R$ is an ideal, the **extension** of I across f is the ideal $I^e = (f(I))$ generated by $f(I)$. In other words, it consists of all elements of the form $\sum s_i f(r_i)$, for $r_i \in I$, $s_i \in S$.

    (a) Prove that if $J \subseteq S$ is an ideal, then the pre-image $f^{-1}(J)$ is an ideal in R. Prove further that if J is prime, so is $f^{-1}(J)$. This says that "primes pull back".

    (b) Show by giving an example that if $I \subseteq R$ is an ideal, then $f(I)$ is not necessarily an ideal (this is the reason why we define the extension of an ideal - it's the smallest ideal containing the image of I)

    (c) Now let $f\colon \mathbb{Z} \to \mathbb{Z}[i]$ be the inclusion of the usual integers into the Gaussian integers. Let p be a prime, and (p) the ideal it generates in $\mathbb{Z}$. In this case the extension $(p)^e$ is just the ideal generated by the (usual) integer p in the ring $\mathbb{Z}[i]$ (note this will be much larger than the ideal (p) in $\mathbb{Z}$). Prove the following facts:

       i. If $p = 2$, then $(p)^e$ is the same as the ideal generated by $(1 + i)^2$, which is not prime.

       ii. If $p \equiv 1 \mod 4$, then $(p)^e$ is not a prime ideal in $\mathbb{Z}[i]$.

       iii. If $p \equiv 3 \mod 4$, then $(p)^e$ is a prime ideal in $\mathbb{Z}[i]$

       These examples show that extensions of primes need not be prime, or "primes do not push forward". In proving ii and iii, you may use the following famous theorem of Fermat: a prime $p > 2$ can be written as $a^2 + b^2$ for some $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \mod 4$

Solution:

(a) We have shown in the group theory part of the course that the preimage of a subgroup under a homomorphism is a subgroup. So it remains to check closure under scaling. So let $x \in f^{-1}(J)$, and $r \in R$. Then $f(rx) = f(r)f(x)$, and this is in J because $f(x)$ is in J. This shows that $rx \in f^{-1}(J)$. Now assume further that J s a prime ideal. To show that $f^{-1}(J)$ is prime, suppose $xy \in f^{-1}(J)$, and $x \notin f^{-1}(J)$. Then $f(xy) = f(x)f(y) \in J$, and since J is prime, $f(x)$ or $f(y)$ must be in J. But $f(x) \notin J$ because $x \notin f^{-1}(J)$. So $f(y) \in J$ and hence $y \in f^{-1}(J)$, so $f^{-1}(J)$ is prime.

(b) For example, let $f : \mathbb{Z} \to \mathbb{Q}$ be the inclusion of the integers into the rationals, and (n) some ideal in $\mathbb{Z}$. Then its image is just the set of multiples of n, regarded as a subset of $\mathbb{Q}$, but this isn't an ideal in $\mathbb{Q}$ since the only ideals there are 0 and $\mathbb{Q}$.

(c) i. The extension of (2) is just (2), regarded as an ideal in $\mathbb{Z}[i]$, so here 2 can be scaled by any gaussian integer. But since $(1+i)^2 = 2i$, and i is a unit, we have $(2) = (2i) = ((1+i)^2)$. Then we can see that $1 + i \notin (2)$ but it's square is, which violates the definition of prime ideal.

ii. First write, by Fermat's theorem, $p = x^2 + y^2$ with $x, y \in \mathbb{Z}$ and note that this can be further rewritten as $p = (x + iy)(x - iy)$ when we're working in $\mathbb{Z}[i]$. Moreover, since $p \geq 3$, $x, y, \geq 1$. Then the ideal generated by p in $\mathbb{Z}[i]$ can be written as the ideal generated by $(x+iy)(x-iy)$ in $\mathbb{Z}[i]$. This is not prime because the product $(x + iy)(x - it)$ is in there but $x + iy$ is not (if it were, $x - iy$ would have to be a unit, but it's not since its norm is greater than one, since $a, b \geq 1$).

iii. The extension of (p) is prime, because, p is irreducible in $\mathbb{Z}[i]$ when $p \equiv 3 \mod p$. To see this suppose we have a factorization $p = ab$. Clearly a, b cannot both be integers > 1 (or < -1) since p is prime. But if a, b have imaginary parts, then in order for their product to be an integer, they must be conjugates of one another, so ab would have the form $x^2 + y^2$, which is impossible, again by Fermat's theorem.