Solution to Sample Exam 2. Math 113 Summer 2014.

These problems are practice for the second exam, on rings and fields.

1. True or False

   (a) The canonical homomorphism $\pi\colon R \to R/I$ is surjective. **True:** Every coset $\overline{r}$ is the image of the element r.

   (b) Every homomorphism of rings is injective. **False:** See the previous problem.

   (c) The element $\overline{x}$ is a unit in $\mathbb{Q}[x]/(x^4+1)$. **True:** Since $\overline{x}^4 = -1$, we have $\overline{x}(-\overline{x}^3) = 1$, so $\overline{x}$ is a unit.

   (d) There exists a homomorphism $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$. **True:** The "diagonal map" $a \mapsto (a, a)$ is a homomorphism.

   (e) If R is a unique factorization domain and I a proper ideal of R, then R/I is a unique factorization domain. **False:** the quotient is often not even a domain, e.g., $R = \mathbb{Z}$, $I = (4)$, and $R/I = \mathbb{Z}/4\mathbb{Z}$.

   (f) If $\sigma \in \mathrm{Gal}(L : K)$, and $\alpha \in L$ is a root of $f \in K[x]$, then $\sigma(\alpha)$ is a root of f. **True:** This was a (very important) proposition from lecture, 10.1.5.

   (g) If R and S are domains, then $R \times S$ is a domain. **False:** The ring $R \times S$ will almost always have zero divisors, e.g., take $R = S = \mathbb{Z}$; in $\mathbb{Z} \times \mathbb{Z}$, $(1,0)(0,1) = (0,0)$, but neither $(1,0)$ nor $(0,1)$ are the zero element.

   (h) Every algebraic field extension is finite. **False:** It is possible to adjoin infinitely many algebraic elements, e.g., $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, ...)$

   (i) $\mathbb{Q}(i-\sqrt{7}) = \mathbb{Q}(i, \sqrt{-7}+1)$. **True:** Both of these fields can be written as $\mathbb{Q}(i, \sqrt{7})$.

   (j) The minimal polynomial of the extension $\mathbb{Q} \subset \mathbb{Q}(e^{2\pi i/3})$ is $x^3 - 1$. **False:** This polynomial is not irreducible. The correct minimal polynomial is $x^2 + x + 1$, the third "cyclotomic polynomial".

   (k) If F is any field, there exists a homomorphism $F \to \mathbb{C}$. **False:** Every homomorphism of fields must be injective, so for instance the "larger" field $\mathbb{C}(x)$ of rational functions cannot map to $\mathbb{C}$, simply because you cannot have an injective map from an infinite-dimensional space to a finite dimensional space.

   (l) If $K \subset L$ is a normal field extension of degree 4, then there exists exactly one intermediate subfield $F \neq K, L$. **False:** We have seen examples, such as $\mathbb{Q}(i, \sqrt{3})$, which have more than one intermediated subfield, in this case $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(i\sqrt{3})$. This can also be seen by observing that the extension is normal, and its Galois group is K_4, which has three proper nontrivial subgroups, so by the Galois correspondence, we get three proper nontrivial subextensions.

   (m) The polynomial $3x^4 - 30x^2 + 10x + 15$ is irreducible over $\mathbb{Z}$. **True:** Use Eisenstein with $p = 5$ to get that it's irreducible over $\mathbb{Q}$, and then note that the gcd of the coefficients is 1, so it's also irreducible over $\mathbb{Z}$.

   (n) If $f\colon R \to S$ is a surjective ring homomorphism, and $\mathfrak{m}$ a maximal ideal in S, then $f^{-1}(\mathfrak{m})$ is a maximal ideal in R. **True:** A surjective map induces a bijection of ideals, which preserves inclusions (by basically the same argument as proposition 7.4.1).

   (o) There exists a homomorphism $\mathbb{Q}[x]/(x^2 + 2x + 1) \to \mathbb{C}$. **True:** Map $\overline{x}$ to -1.

2. (a) If R is a ring, say what it means for an element $r \in R$ to be irreducible.

   Solution: $r \in R$ is **irreducible** it is nonzero, a nonunit, and if the only way to write $r = st$ is by taking either s or t to be a unit.

   (b) Give an example of an irreducible polynomial of degree larger than 2 in the ring $\mathbb{Q}[x]$.

   Solution: $x^4 + x + 1$, or any cyclotomic polynomial of big enough degree.

   (c) Let R be a domain and $I = (f)$ a nonzero ideal. Prove that if I is prime, then f is irreducible.

   Solution: First note that since I is a nonzero ideal, $f \neq 0$; since I is prime, it's proper, so f is not a unit. Now suppose $f = gh$. Then $gh \in I$ so since I is prime, either g or h is in I. Suppose it's g, then we have $g = af$ for some $a \in R$. Thus $f = gh = afh$, so $f(1 - ah) = 0$ and since we're in a domain and $f \neq 0$, $1 - ah = 0$, so h is a unit.

3. (a) Let $\alpha = \sqrt[3]{\sqrt{2} + \sqrt{3}}$, and consider the field extensions

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(i, \alpha) = K$$

   Given that $[K : \mathbb{Q}] = 24$, determine $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2} + \sqrt{3})]$. Justify your answer.

   Solution: Let $k = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2}+\sqrt{3})]$, and note that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ by computations from class. So the degrees of the extensions in the tower are, in order from left to right, 2, 2, k, and 2. Since degree is muliplicative in towers, we get $8k = 24$, so $k = 3$.

   (b) Let $\omega = \dfrac{-1 + i\sqrt{3}}{2}$, a cube root of 1. Consider the extensions $\mathbb{Q} \subset \mathbb{Q}(\omega) \subset \mathbb{Q}(\sqrt[3]{7}, \omega)$. Let f and g be the automorphisms of $\mathbb{Q}(\sqrt[3]{7}, \omega)$ defined by

$$f\colon \begin{cases} \sqrt[3]{7} \mapsto \omega\sqrt[3]{7} \\ \omega \mapsto \omega \end{cases} \qquad g\colon \begin{cases} \sqrt[3]{7} \mapsto \sqrt[3]{7} \\ \omega \mapsto \omega^2 \end{cases}$$

   Show that $f \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{7}, \omega) : \mathbb{Q}(\omega))$.

   Solution: If $a + b\omega \in \mathbb{Q}(\omega)$, with $a, b \in \mathbb{Q}$ then $f(a + b\omega) = f(a) + f(b)f(\omega) = a + b\omega$.

   (c) Find an element $x \in \mathbb{Q}(\sqrt[3]{7}, \omega)$ such that $f(g(x)) \neq g(f(x))$.

   Solution: $\sqrt[3]{7}$ itself is such an element: $f(g(\sqrt[3]{7})) = f(\sqrt[3]{7}) = \omega\sqrt[3]{7}$; but $g(f(\sqrt[3]{7})) = g(\omega\sqrt[3]{7}) = g(\omega)g(\sqrt[3]{7}) = \omega^2\sqrt[3]{7}$.

   (d) Using (d), and given that $[\mathbb{Q}(\sqrt[3]{7}, \omega) : \mathbb{Q}] = 6$, prove that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{7}, \omega) : \mathbb{Q}) \cong S_3$.

   Solution: If we knew that the extension was normal, we would know that the Galois group has order 6; by (d), it's non-abelian, and hence must be isomorphic to S_3. So it remains to explain why the extension is normal. We can factorize it as $\mathbb{Q} \subset \mathbb{Q}(\omega) \subset \mathbb{Q}(\sqrt[3]{7}, \omega)$. The first extension is clearly normal, since the other root of the minimal polynomial $x^2 + x + 1$ is just ω^2. For the second extension, its minimal polynomial is $x^3 - 7$, and its roots are $\sqrt[3]{7}, \omega\sqrt[3]{7}$, and $\omega^2\sqrt[3]{7}$, all of which are in $\mathbb{Q}(\sqrt[3]{7}, \omega)$, so it's normal. A normal extension of a normal extension is normal, so we're done.

   (e) Prove that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{7}, \omega) : \mathbb{Q}(\omega)) \cong \mathbb{Z}/3\mathbb{Z}$.

   Solution: This is a degree 3 extension, and as explained in (d), it's normal, hence its Galois group is a group of order 3; up to isomorphism, it must be $\mathbb{Z}/3\mathbb{Z}$.

4. (a) For each of the following rings say, whether they are a field; domain; principal ideal domain; euclidean domain; unique factorization domain

   i. $\mathbb{Z}[x]$ **Solution:** UFD but not PID.

   ii. $\mathbb{Q}[x]/(x^2+x+1)$ **Solution:** Field.

   iii. $\mathbb{C}[x,y]$ **Solution:** UFD but not PID.

   (b) Define a principal ideal domain. **Solution:** A **principal ideal domain** is an integral domain in which every ideal is principal (can be generated by a single element).

   (c) Prove that if R is a principal ideal domain and I a prime ideal of R, then R/I is a principal ideal domain.

   Solution: Pick an ideal J of R/I. We must show that it's principal. By the correspondence between ideals in the quotient and ideals in R containing I, J corresponds to some ideal J' in R, which is principal since R is a PID; say $J' = (r)$. Now, for any $x \in J$, $x = \pi(y)$ for some $y \in J'$ (again by the correspondence just mentioned), and $y = ar$ for some r, since $J' = (r)$. Thus $x = \pi(y) = \pi(ar) = \pi(a)\pi(r)$, which shows that J is generated by $\pi(r)$, so it's principal.

   (d) Let $f\colon Z[x] \to \mathbb{Z}/2\mathbb{Z}$ be $f = g \circ h$, where $h\colon Z[x] \to \mathbb{Z}$ is the evaluation map at -1 and $g\colon \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is the quotient map. Prove that $\ker f = (x+1, x^2+1)$.

   Solution: First we check that $\ker f \supseteq (x+1, x^2+1)$, for which it is sufficient to check that $\ker f$ contains the two generators $x+1$ and x^2+1. But $f(x+1) = g(h(x+1)) = g(0) = 0$ and $f(x^2+1) = g(h(x^2+1)) = g(2) = 0$. The other inclusion is messy to check directly; instead observe that $\ker f$ is maximal because $\mathbb{Z}[x]/\ker f$ is a field, namely $\mathbb{Z}/2\mathbb{Z}$. since $\ker f$ is maximal, but also contained in $(x+1, x^2+1)$, they're either equal or else $(x+1, x^2+1)$ is the unit ideal. But $(1+x, x^2+1)$ is not the unit ideal, because in $\mathbb{Z}[x]/(x+1, x^2+1)$, $\overline{x} = -1$ and $\overline{x}^2 = -1$, so $(-1)^2 = -1$, hence $2 = 0$, and $\overline{x} = -1 = 1 = \overline{x}^2$. Thus $\mathbb{Z}[x]/(x+1, x^2+1) \cong \mathbb{Z}/2\mathbb{Z}$, so the ideal is not the whole ring[1]. Thus $\ker f$ must be equal to $(x+1, x^2+1)$.

5. (a) State the (first) isomorphism theorem for rings.

   Solution: If $f\colon R \to S$ is a ring homomorphism, then $R/\ker f \cong \operatorname{im} f$.

   (b) Consider the map $\phi\colon \mathbb{C}[x,y] \to \mathbb{C}[y]$ given by $\phi(p(x,y)) = p(y^2, y^3)$. Compute $\phi(x^2+xy+y^2)$.

   Solution: $\phi(x^2+xy+y^2) = (y^2)^2 + (y^2)(y^3) + (y^3)^2 = y^4 + y^5 + y^6$

   (c) Prove that $\operatorname{im} \phi = \mathbb{C}[y^2, y^3] \subset \mathbb{C}[y]$.

   Solution: $\operatorname{im} \phi = \{\phi(p(x,y) \mid p \in \mathbb{C}[x,y]\} = \{p(y^2, y^3) \mid p \in \mathbb{C}[x,y]\}$, and this is exactly the subring $\mathbb{C}[y^2, y^3]$.

   (d) Prove that $\ker \phi$ is a prime ideal in $\mathbb{C}[x,y]$.

   Solution: The image $\mathbb{C}[y^2, y^3]$ is a subring of a domain, hence a domain. Since $\mathbb{C}[x,y]/\ker \phi \cong \operatorname{im} \phi$, $\ker \phi$ is a prime ideal.

[1] This is not completely rigorous, because for all we know there is some other relation we did not notice, which forces $0 = 1$ as well. Here's a different proof for the sticklers. First of all, write $I = (x+1)$ and $J = (x^2+1)$, so that $(x+1, x^2+1) = I + J$. Suppose for contradiction that $I + J = \mathbb{Z}[x]$; then by the chinese remainder theorem (which was on a WS one day), $I \cap J = IJ$, and $\mathbb{Z}[x]/IJ \cong \mathbb{Z}[x]/I \times \mathbb{Z}[x]/J$. In our situation this reads, $\mathbb{Z}[x]/(x^3+x^2+x+1) \cong \mathbb{Z} \times \mathbb{Z}[i]$, where the map is determined by $\overline{x} \mapsto (-1, i)$. But this map cannot be surjective, for instance, $(0, i)$ is not in the image, so we have a contradiction, and $I + J \neq \mathbb{Z}[x]$.

(e) Is im ϕ a unique factorization domain?

Solution: No. In $\mathbb{C}[y^2, y^3]$, we have $y^6 = (y^2)^3 = (y^3)^2$; these factorizations are distinct because for example, they have different numbers of factors.