ASSIGNMENT 2: SOLUTIONS

Question 1.

Solution. $\gcd(9+49i, 31+39i) = 11-5i$ as
$$11-5i = 2i(31+39i) - (1+2i)(9+49i).$$
$\square$

Question 2.

Solution. By what we're given in the question, it follows that
$$(15+\sqrt{-118})(15-\sqrt{-118}) = 334 = 7^3$$
are two different factorizations of 343 in $\mathbb{Z}[\sqrt{-118}]$. We need to show that this is a factorization into irreducibles. We can do this via norm arguments.

For example, let's show $15 \pm \sqrt{-118}$ are irreducible. Suppose we can write
$$15+\sqrt{-118} = \alpha\beta = (a+b\sqrt{-118})(c+d\sqrt{-118})$$
for some $a,b,c,d \in \mathbb{Z}$, and hence
$$334 = |15+\sqrt{-118}| = (\alpha\beta)(\bar{\alpha}\bar{\beta}) = (\alpha\bar{\alpha})(\beta\bar{\beta}) = (a^2+b^2 118)(c^2+d^2 118).$$
Since $334 < 118^2$, then either $b=0$ or $d=0$. Wolog suppose $b=0$. Then $a^2 \mid 334 = 7^3$, so $a = \pm 1, \pm 7$. If $a = \pm 7$, then $|\beta| = 7$, but there is no choice of $c, d \in \mathbb{Z}$ that makes this possible (as $\sqrt{7} \notin \mathbb{Z}$). Therefore $a = \alpha = \pm 1$ is a unit so $15+\sqrt{-118}$ is irreducible. Since $15-\sqrt{-118} = \overline{15+\sqrt{-118}} = \bar{\alpha}\bar{\beta}$, our argument also shows that $15-\sqrt{-118}$ is irreducible.

A proof that 7 is irreducible can be done in a similar manner. $\square$

Question 3.

Solution. Let R denote the ring of integers of a number field and let I be an ideal with non-trivial factorization $I = I_1 I_2$ (*i.e.* $I_j \neq R$ for $j = 1,2$). Note that we can take $I_1, I_2 \neq 0$, otherwise the factorization is trivial. For $x \in I_j$, $rx \in I_j$ for any $r \in R$, so $I \subseteq I_1, I_2$. We need to show that $I \neq I_1$ and $I \neq I_2$. Wolog suppose that $I = I_1$. Then $I_1 I_2 = I_1 R$ which implies that $I_2 = R$ (divisibility property of ideals in R as $I_2 \neq 0$). This is a contradiction to the assumption that our factorization was non-trivial. Therefore $I \neq I_1$ and similarly $I \neq I_2$.

Now, if R/I is a field, then I is maximal, so by the property we established above, I is irreducible.

Sketch of the rest: Let $I = (15+\sqrt{-118}, 7)$, and one easily observes that $I^3 \supseteq (15+\sqrt{-118})$ since $15+\sqrt{-118}$ divides each of the generators of I^3. Next, you need to show that $15+\sqrt{-118} \in I^3$ (find some linear combination of the generators for I^3 that gives you $15+\sqrt{-118}$. Then conclude that $I^3 = (15+\sqrt{-118})$. A similar process shows that for $J = (15-\sqrt{-118}, 7)$, $J^3 = (15-\sqrt{-118})$.

It follows from the previous question that $(343) = I^3 J^3$. It remains to show that the ideals I, J are irreducible. Do this by showing that R/I and R/J are fields. For example, show that the map $\phi : R \to \mathbb{Z}/7\mathbb{Z}$ given by $\phi(a+b\sqrt{-118}) = a-b \pmod 7$ is as surjective homomorphism and then show that $\ker(\phi) = I$. Similarly for J. $\square$

Question 4.

Solution. To show $|\alpha| = a^2+b^2+c^2+d^2$, just write out the multiplication. Take $\alpha' = \frac{\bar{\alpha}}{|\alpha|}$. $\square$

Question 5.

Solution. Show closure of R under addition and multiplication by taking generic elements, adding or multiplying them together (as appropriate) and rearranging to get an element of R. The positivity of the norm of an element $\alpha \in R$ is trivial, and by simply computing the norm one shows that $|a| \in \mathbb{Z}$. $\square$

Question 6. Note: this question was not marked.

Solution. Let $\alpha, \beta \in R$. Then $\alpha\beta^{-1} = a+bi+cj+dk \in \mathbf{H}$ and each of a,b,c,d is a distance of less than $1/2$ from an element of $\mathbb{Z} + \mathbb{Z}\cdot\frac{1}{2}$, so we can find a $q = a'+b'i+c'j+d'k \in R$ such that $a-a', b-b', c-c', d-d' < \frac{1}{2}$ and hence
$$|\alpha\beta^{-1} - q| < 4\left(\frac{1}{2}\right)^2 = 1.$$

By the multiplicativity of the norm, it follows that

$$|\alpha - q\beta| < |\beta|$$

and setting $r = \alpha - q\beta$ gives the desired result. Note that $\alpha\beta^{-1}$ is not necessarily equal to $\beta^{-1}\alpha$ so one should not write things such as $\frac{\alpha}{\beta}$ as it is ambiguous. Also, note that this does not prove that R is Euclidean domain (a domain is necessarily commutative). $\square$

Question 7. Note: this question was not marked.

Solution. Since we established that the norm is a map $|\cdot| : R \to \mathbb{Z}^+$, every left ideal $I \subset R$ has a minimal element with respect to the norm, call it α. Use the Eucliden property of R to show that $I = (\alpha)$. $\square$

Question 8. Note: this question was not marked. It was also not particularly well done from what I saw—in my brief skimming I did not see a single complete solution.

Solution. First of all, we need to treat the case where $p = 2$ separately. Take $\alpha = 1 + i$. Then $\alpha \in R$ and $N(\alpha) = 2$.

Next, consider the case where p is an odd prime. Then let

$$A = \left\{ a^2 \pmod p \;\middle|\; 0 \le a \le \frac{p-1}{2} \right\}.$$

(many of you took the set $A = \{a^2 \mid a \in \mathbb{Z}/p\mathbb{Z}\}$—this isn't good enough to give the necessary bound on the norm). Show that $|A| = \frac{p+1}{2}$. By translation, the sets

$$A_t = \left\{ t - a^2 \pmod p \;\middle|\; 0 \le a \le \frac{p-1}{2} \right\} \forall t \in \{1, \dots, p-1\}$$

also have cardinality $\frac{p+1}{2}$. In particular, fixing t gives $A \cap A_t \neq \emptyset$ and $A \cap A_{p-t} \neq \emptyset$. It follows that by choosing t to be a non-square mod p there exist $a, b, c, d \in \{0, 1, \dots, \frac{p-1}{2}\}$ not all 0 such that

$$t \equiv a^2 + b^2 \pmod p$$
$$p - t \equiv c^d + d^2 \pmod p$$

and hence

$$a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod p.$$

On the other hand, by construction we have that

$$a^2 + b^2 + c^2 + d^2 \le 4\left(\frac{p-1}{2}\right)^2 = (p-1)^2 < p^2.$$

Therefore, setting $\alpha = a + bi + cj + dk$ gives the desired element. $\square$

Question 9.

Solution. Let α be an element of R such that $p \mid |\alpha|$ but $p^2 \nmid |\alpha|$. Consider the ideal $I = Rp + R\alpha$. Observe that every element of I has norm divisible by p (since the norm is multiplicative) so $I \neq R$. We showed that every ideal in R is principal, so there exists $\beta \in I$ such that $I = R\beta$ and hence $|\beta| \mid |\alpha|$ and $|\beta| \mid p^2$. Thus $|\beta| \mid p$. But $\beta \in I$, so $p \mid |\beta|$ and it follows that $|\beta| = p$.

It remains to show that $|\beta|$ can be written as the sum of four squared integers. Write $\beta = a + bi + cj + d\frac{1+i+j+k}{2}$ where $a, b, c, d \in \mathbb{Z}$. If d is even we are done. If d is odd, we can multiply β by a suitable unit ω such that $\beta\omega$ has the desired form. Therefore $p = |\beta\omega| = |\beta|$ can be written as a sum of four squared integers. $\square$

Question 10.

Solution. Decompose every positive integer n into its prime factors and apply the previous question to obtain a product of elements of the form $\alpha = a + bi + cj + dk$ where $a, b, c, d \in \mathbb{Z}$ whose norm is equal to n using the multiplicitivity of the norm. Since elements of form $a + bi + cj + dk$ where $a, b, c, d, \in \mathbb{Z}$ retain their form under multiplication, conclude that every positive integer n can be written as the sum of four square integers.

To show the result is optimal, show that one cannot write 7 as a sum of three squares (or any other example you like). $\square$